SOSİAL TƏDQİQATLAR MƏRKƏZİ

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

AZƏRBAYCANDA KİBERCİNAYƏT VƏ KİBERTƏHLÜKƏSİZLİK BAROMETRİ

ANALİTİK HESABAT

ÖLKƏ ÜZRƏ KİBERCİNAYƏTLƏRƏ VƏ KİBERTƏHLÜKƏSİZLİYƏ İCTİMAİ RƏYDƏ MÜNASİBƏTİN KƏMİYYƏT VƏ KEYFİYYƏT ƏSASLI TƏHLİLİ

SOSİAL TƏDQİQATLAR MƏRKƏZİ

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

AVROPA İTTİFAQININ, AVROPA ŞURASININ VƏ SOSİAL TƏDQİQATLAR MƏRKƏZİNİN BİRGƏ LAYİHƏSİ

AZƏRBAYCANDA KİBERCİNAYƏT VƏ KİBERTƏHLÜKƏSİZLİK BAROMETRİ

Ölkə üzrə kibercinayətlərə və kibertəhlükəsizliyə ictimai rəydə münasibətin kəmiyyət və keyfiyyət əsaslı təhlili

(Oktyabr 2021 – Yanvar 2022)

İctimai rəy sorğusu əsasında təqdim edilən

ANALİTİK HESABAT

Avropa İttifaqı və Avropa Şurası tərəfindən maliyyələşdirilən "Kiber Şərq" (CyberEast), həmçinin Avropa İttifaqı tərəfindən həyata keçirilən "Kibertəhlükəsizlik-Şərq" (Cybersecurity East) layihələri çərçivəsində hazırlanmışdır.

Bakı - 2022

Layihə koordinatoru:

Georgi COXADZE
Layihə meneceri
Giorgi.Jokhadze@coe.int
Avropa Şurasının Kibercinayət Proqramı İdarəsi (C-PROC)
Buxarest, Rumıniya

Besnik LİMAY
Qrup rəhbəri
Tel.: +383 44 506 403
besnik.limaj@gfa-group.de
“GFA” Konsaltinq Qrupu

Məsuliyyətlə bağlı bildiriş:

Bu hesabat Avropa İttifaqı və Avropa Şurası tərəfindən birgə maliyyələşdirilən layihənin tərkib hissəsi olaraq ərsəyə gətirilib. Hesabat Avropa İttifaqı tərəfindən ekspertlər qrupu Donika Emini (Kosovo), Dan Petre və Vlad Turanu (“D&D Tədqiqat”, Rumıniya), eləcə də Ruland van Zeyst (Niderland) ilə birgə hazırlanıb. Burada ifadə edilən fikirlər heç bir halda tərəflərdən hər hansı birinin rəsmi mövqeyinin əks etdirilməsi kimi istifadə edilə bilməz.

Layihənin tədqiqatçı-ekspertlər qrupu:

- **Avropa İttifaqı** tərəfindən ekspertlər qrupu:
  Ruland van Zeyst (Niderland), Dan Petre və Vlad Turanu (“D&D Tədqiqat”, Rumıniya) və Donika Emini (Kosovo)

- **Azərbaycan (Sosial Tədqiqatlar Mərkəzi)** tərəfindən tədqiqat qrupu:
  Zahid Oruc (layihə rəhbəri), Tahirə Allahyarova, A.Balayeva, İ.Şahbazov, Z.Əfəndiyev və B.Əliyev.

Təşkilat haqqında məlumat

Sosial Tədqiqatlar Mərkəzi 2019-cu ildə təsis edilib. Mərkəzin məqsədi sosial münasibətlərin dinamikasını təhlil etmək, bu sahədə mövcud tendensiyaları müəyyənləşdirmək və müxtəlif sosioloji, siyasi, iqtisadi və mədəni problemlərə dair araşdırmalar aparmaqdır. Mərkəz mütəmadi olaraq həyata keçirdiyi sorğuların nəticələrini dərc edir və müəyyən konfidensial tədqiqatları aidiyyəti dövlət orqanlarına təqdim edir. Bu günədək Mərkəz 60.000-dən çox respondenti əhatə edən 70-dən çox sorğu və tədqiqat layihəsi həyata keçirib.

MÜNDƏRİCAT

1. Akronimlər.....5
2. İcmal.....6
3. Problemin təsviri.....9
4. Giriş.....10
5. Kəmiyyət tədqiqatı.....19
5.1. Xülasə.....19
5.2. Texniki məlumat.....20
5.3. Tədqiqatın metodologiyası.....20
5.4. Ümumi Əhali Qrupu (ÜƏQ).....21
5.4.1. İnternetdən istifadə.....21
5.4.1.1. Onlayn fəaliyyətlər.....21
5.4.2. Kİbercinayətkarlıq üzrə bilik səviyyəsi.....25
5.4.2.1. Məlumatlılıq.....25
5.4.2.2. Fişinq (phishing).....26
5.4.2.3. Rənsamveə (ransomware).....29
5.4.2.4. Hədə-qorxu, zorakılıq-təhqir və sui-istifadə.....31
5.4.2.5. Kibermüdaxilə (DDoS).....33
5.4.2.6. Şəxsiyyət/kimlik (fərdi məlumatların) oğurluğu.....34
5.4.2.7. Kibercinayətkarlıq: narahatlıq və gözləntilər.....36
5.4.3. Nəticə.....38

5.5. Müəssisələr/Şirkətlər.....38
5.5.1. Təşkilati məlumat.....38
5.5.2. İnternetdən istifadə.....39
5.5.3. Kibertəhlükəsizlik üzrə bilik səviyyəsi.....40
5.5.3.1. Kibertəhlükəsizliyin rolu.....40
5.5.3.2. Ümumi prioritet və etibarlılıq.....43
5.5.3.3. Məlumatlılığın artırılması.....44
5.5.3.4. Autentifikasiya və şifrələmə.....45
5.5.3.5. Tədarük/təchizat zənciri.....46
5.5.3.6. Dövlətin/hökumətin rolu.....46
5.5.3.7. Kibercinayətkarlıqla bağlı vəziyyət.....47
5.5.4. Nəticə.....48

6. Keyfiyyət tədqiqatı.....50
6.1. Xülasə.....50
6.2. Texniki məlumat.....51
6.3. Tədqiqatın metodologiyası.....51
6.4. Ümumi Əhali Qrupu (ÜƏQ).....52
6.4.1. Onlayn fəaliyyətlər (ümumi istifadə).....53
6.4.2. Kibercinayətkarlıq və kibertəhlükəsizlik üzrə bilik səviyyəsi.....55
6.4.3. Fişinq (phishing).....56
6.4.4. Rənsamveə (ransomware).....57
6.4.5. Hədə-qorxu, zorakılıq-təhqir və sui-istifadə.....57
6.4.6. Şəxsiyyət/kimlik (fərdi məlumatların) oğurluğu.....58
6.4.7. Kibermüdaxilə (DDoS).....58
6.4.8. Kibercinayətkarlıq: narahatlıq və gözləntilər.....59

6.5. Kibercinayət qurbanları.....60
6.5.1. Onlayn fəaliyyətlər (ümumi istifadə).....60
6.5.2. Kibercinayətkarlıq və kibertəhlükəsizlik üzrə bilik səviyyəsi.....60

6.5.3. Fişinq (phishing).....61
6.5.4. Rənsamveə (ransomware).....62
6.5.5. Hədə-qorxu, zorakılıq-təhqir və sui-istifadə.....62
6.5.6. Şəxsiyyət /kimlik (fərdi məlumatların) oğurluğu.....62
6.5.7. Kibermüdaxilə (DDoS).....62
6.5.8. Kibercinayətkarlıq: narahatlıq və gözləntilər.....62

6.6. İT mütəxəssisləri.....63
6.6.1. Onlayn fəaliyyətlər (ümumi istifadə).....63
6.6.2. Kibercinayətkarlıq və kibertəhlükəsizlik üzrə bilik səviyyəsi.....63
6.6.3. Fişinq (phishing).....65
6.6.4. Rənsamveə (ransomware).....66
6.6.5. Hədə-qorxu, zorakılıq-təhqir və sui-istifadə.....66
6.6.6. Şəxsiyyət/kimlik (fərdi məlumatların) oğurluğu.....66
6.6.7. Kibermüdaxilə (DDoS).....66
6.6.8. Məlumatların pozulması.....66
6.6.9. Rəhbər şəxslərin (CEO) adından istifadə edilməklə dələduzluq/ Biznes e-poçtu riskləri (BEC).....66
6.6.10. Kibercinayətkarlıq: narahatlıq və gözləntilər.....66

6.7. İXP (internet xidməti provayderləri) mütəxəssisləri.....67
6.7.1. Onlayn fəaliyyətlər (ümumi istifadə).....67
6.7.2. Kibercinayətkarlıq və kibertəhlükəsizlik üzrə bilik səviyyəsi.....67
6.7.3. Kibercinayətkarlıq və kibertəhlükəsizliyə dair İXP ilə əlaqədar xüsusiyyətlər.....69
6.7.4. Fişinq (phishing).....70
6.7.5. Rənsamveə (ransomware).....70
6.7.6. Hədə-qorxu, zorakılıq-təhqir və sui-istifadə.....70
6.7.7. Şəxsiyyət/kimlik (fərdi məlumatların) oğurluğu.....70
6.7.8. Kibermüdaxilə (DDoS).....70
6.7.9. Kibercinayətkarlıq: narahatlıq və gözləntilər.....71

6.8. Hüquq-mühafizə orqanları (HMO).....71
6.8.1. Onlayn fəaliyyətlər (ümumi istifadə).....72
6.8.2. Kibercinayətkarlıq və kibertəhlükəsizlik üzrə bilik səviyyəsi.....72
6.8.2.1 Əlaqələndirmə.....74
6.8.2.2 Kibercinayətlərin qarşısının alınması.....77
6.8.2.3 Zərərçəkənlərə qayğı göstərilməsi.....78
6.8.2.4 Kibercinayətlərin qarşısının alınmasında preventiv yanaşma.....78
6.8.2.5 Kiberpotensial, kiberqabiliyyətlər.....78
6.8.3. Kibercinayətkarlıq: narahatlıq və gözləntilər.....79
6.9. Nəticə.....79

7. Ümumi nəticələr.....82
8. Əlavələr.....88
8.1. Demoqrafik göstəricilər.....88
8.2. Anket.....91

1. Akronimlər

Aİ - Avropa İttifaqı
AŞ - Avropa Şurası
ATƏT - Avropada Təhlükəsizlik və Əməkdaşlıq Təşkilatı
BMT - Birləşmiş Millətlər Təşkilatı
BTİ - Beynəlxalq Telekommunikasiya İttifaqı
CM - Cinayət Məcəlləsi
DİN - Daxili İşlər Nazirliyi
DÖT - Dövlət-özəl tərəfdaşlığı
DTX - Dövlət Təhlükəsizliyi Xidməti
Əİ - Əşyaların İnterneti
HMO - Hüquq-mühafizə orqanları
XDMX - Xüsusi Dövlət Mühafizə Xidməti
XRİTDX - Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti
İKT - İnformasiya-kommunikasiya texnologiyaları
İT - İnformasiya texnologiyaları
İXP - İnternet xidməti provayderləri
KƏM - Kibertəhlükəsizlik Əməliyyatları Mərkəzi
Kİ - Kritik infrastruktur
KİMM - Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi
KOS - Kiçik və orta sahibkarlıq
KPG - Kibertəhlükəsizlik üzrə potensialın gücləndirilməsi
QKİ - Qlobal Kiberhəssaslıq İndeksi
QKİ - Qlobal Kiber İndeks
MDB - Müstəqil Dövlətlər Birliyi
RİNN - Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi
ÜDM - Ümumi daxili məhsul
ÜƏQ - Ümumi əhali qrupu
ÜMMQ - Ümumi Məlumatların Mühafizəsi Qaydası

Layihənin məqsədi:

1. Azərbaycanda kibercinayətlər və onlayn təhlükəsizlik üzrə real vəziyyətin dəyərləndirilməsi üçün ictimai rəyin bu sahəyə münasibətinin kəmiyyət və keyfiyyət əsaslı təhlili;

2. Azərbaycanda mövcud vəziyyətin Avropa Şurasına üzv dövlətlər tərəfindən təsdiq edilən "Kibercinayətkarlıq haqqında" Budapeşt Konvensiyasına uyğunluğunun qiymətləndirilməsi;[1]

3. Azərbaycanın ümumi təhlükəsizliyini gücləndirmək məqsədilə kiberhücumlara qarşı dayanıqlılığın yüksəldilməsi, kibertəhlükəsizliyin təmin edilməsi istiqamətində aidiyyəti qurumların işinin və hüquq-mühafizə orqanlarının potensialının gücləndirilməsi;

4. Kibertəhlükəsizliyə və kiberhücumlara qarşı mübarizəni daha da gücləndirən və təkmilləşdirən təklif və tövsiyələri təqdim etməklə Avropa qurumları ilə qarşılıqlı texniki və əməkdaşlıq mexanizmlərinin inkişafı yönündə, həmçinin kibercinayətlərlə mübarizə üzrə səmərəli milli konsepsiya və strategiyanın, dövlət proqramının hazırlanması və həyata keçirilməsinə töhfə verilməsi.

2. İcmal

Paytaxt və şəhər-kənd əraziləri arasında rəqəmsal fərqə malik ölkə olmaqla Azərbaycan kibertəhlükəsizliklə bağlı maraq doğuran bir nümunədir. Tarixi və geosiyasi səbəblərlə əlaqədar olaraq, müstəqilliyini bərpa etdikdən sonra istər fiziki, istərsə də kibertəhlükəsizliklə bağlı məsələlər Azərbaycanın xarici və daxili siyasətinin daimi prioritetləri kimi qalmışdır. Pandemiya şəraitinin meydana gəlməsi ilə onlayn fəaliyyət səviyyəsi artdıqca kibertəhlükəsizlik məsələsi daha çox əhəmiyyət daşımağa başladı. Bu da kiberhücumlar üçün yeni imkanlar yaratdı. Bu baxımdan, botnetlərin[2] fəaliyyəti və fişinq[3] (phishing) 2021-ci il ərzində ən çox yayılmış kibercinayət əməlləri kimi qeydə alınıb. Digər tərəfdən məlum olub ki, əks tədbirlərin həyata keçirilməsi istiqamətində Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi (KİMM) 2021-ci ilin əvvəlindən etibarən kiberdələduzluq halları, bu cür cinayətlərdən müdafiə üsulları barədə ictimaiyyətin məlumatlılığını 40% həddində artırmağa nail olub.

Keçirilən sorğunun nəticələrinə əsasən smartfonlar (ağıllı mobil telefon) şəxsi ehtiyaclar üzrə ən çox istifadə edilən cihaz kimi qeydə alınıb. Təhlil göstərir ki, respondentlərin 73,3%-i rəqəmsal cihazlardan istifadə edərkən bəzi ehtiyat tədbirləri görürlər. Bununla yanaşı, respondentlərin nisbətən geniş hissəsinin (62,8%) "kibercinayət" sözü ilə tanış olmadığı məlum olub. Müvafiq şəkildə, rəyi soruşulanların 93,6%-nin fişinq barədə məlumatsız olduğu təsbit edilib. Respondentlərin əksəriyyəti (86.7%) hesab edib ki, onlayn cinayət fəaliyyəti hesab edilən hər hansı bir cəhdin hədəfinə çevrilməyib. Həmin şəxslərə mövzu üzrə anlayışlar izah edildikdən sonra bu halda respondentlərin 74,3%-i belə növ cinayətin baş verməsi haqqında eşitdiklərini ifadə edib. Fişinq qurbanlarından sorğu suallarını cavablandıranların xeyli hissəsi (69.6%) sözügedən hadisələrdən ciddi şəkildə təsirlənmədiklərini və ya belə halları narahatlıq hesab etmədiklərini qeyd ediblər. Bununla yanaşı, respondentlərin yarıdan çoxu (56.9%) fikirləşir ki, qonşuluqda kimsə fişinq mesajı alarsa və daha sonra bunun qeyri-qanuni əməl olduğunu bilərsə, aidiyyəti qurumlara (polisə) bildirər. Sorğu iştirakçılarının 52,7%-i özünü və ailəsini qorumaq üçün fişinq haqqında yetərli məlumata malik olduğunu qeyd edib.

Tədqiqatın nəticələri sübut edir ki, sorğu iştirakçılarının 97,7%-i "rənsamveə" (ransomware)[4] sözü ilə tanış deyil. Respondentlərin 60,7%-nin rəyinə əsasən qonşuluqda kiməsə qarşı rənsamveə hücumu baş verərsə və beləliklə, onların kompüter və mobil telefonlarına, yaxud oradakı fotoşəkil və digər

[1] Azərbaycan kibercinayətkarlıqla mübarizədə tarixi nailiyyət hesab edilən Budapeşt Konvensiyasını 2008-ci ildə imzalayıb, 2010-cu ildə ratifikasiya edib.

[2] **Botnet** - istifadəçinin xəbəri olmadan kompüteri məsafədən idarə etməyə imkan verən zərərli proqramlarla – botlarla yoluxmuş kompüter və ya internet bağlantısı olan cihazlardan ibarət şəbəkədir.

[3] **Fişinq** (phishing) - kiberdələduzluğun xüsusi növü olub, istifadəçiləri aldatma yolu ilə, adətən, maliyyə xarakterli fərdi məlumatları - bank hesablarını, kredit kartlarını və internetə çıxış üçün lazım olan digər informasiyanı əldə etməyə yönələn əməldir.

[4] **Rənsamveə** (ransomware) - istifadəçi və ya təşkilatın sənədlər, şəkillər, videolar, verilənlər bazası və s. daxil olmaqla mühüm məlumatları şifrələyən və istifadəçinin ehtiyat nüsxələrini silən, şəxslərdən, yaxud təşkilatlardan məlumatı qaytarmaq üçün "haqq" (ödəniş) tələb edən zərərli proqram növüdür. Bu cinayət qlobal miqyas alıb və son illərdə cinayətkarların milyonlarla dəyərində "fidyə" (haqq) ödənilməsi tələblərini irəli sürdüyü məlumdur.

məlumatlarına giriş imkanı itirilərsə, zərərçəkmiş şəxslər səlahiyyətli orqanlara və ya polisə bu barədə məlumat verərlər.

Respondentlərin demək olar ki, üçdə ikisi kibertəhdid və zorakılıq-təhqir (sui-istifadə, istismar və s.) ilə bağlı fikir bildirməkdən imtina edib. Bu istiqamətdə sualları cavablandırmağa razılaşanların isə 91%-i onlayn zorakılıqla üzləşməyib. Əksəriyyət şəxsi hesablarına giriş məlumatlarının son 12 ayda onlayn şəkildə ələ keçirilməsinə (yayılmasına) dair xəbərsiz olub. Digər tərəfdən, respondentlərin 61,6%-i özünü və ailəsini onlayn şəxsiyyət (kimlik) oğurluğu hadisəsindən mühafizə etmək üçün lazımi qədər məlumata malik olduğunu qeyd edib. Sorğu iştirakçılarının az hissəsi bu növ cinayətdən əziyyət çəksə belə, respondentlərin 40,6%-nə görə, məlumatlara daxil olunması və onlayn şəxsi məlumatlar/kimlik oğurluğu ən çox narahatlıq yaradan kiberpozuntudur.

Tədqiqatda İT mütəxəssisləri ilə fokus qruplarda təmsil olunan qurum/müəssisə və ya təşkilatların əhəmiyyətli hissəsində kibertəhlükəsizlik məsələlərinə cavabdeh xüsusi təşkilati rol/vəzifə və ya şöbənin olmadığı aşkara çıxıb. İT büdcəsi daxilində kibertəhlükəsizliyə çəkilən xərclərin həcmi isə, ümumiyyətlə, aşağı olmaqla yanaşı, əksər müəssisələrin sığortası yoxdur. Müşahidələr göstərdi ki, ISO 27001 standartları fokus qrup iştirakçısı olan müəssisələrdə ən çox riayət edilən geniş yayılmış təhlükəsizlik standartıdır. Alınan qənaətə əsasən müəssisələrin/şirkətlərin çoxunda kibertəhlükəsizliyə yanaşma çox aşağıdır, yaxud ümumiyyətlə mövcud deyil. Hazırda mövcud olan kibertəhlükəsizlik texnologiyaları arasında viruslardan, casus proqramlarından və s. qorunmaq üçün proqram təminatından istifadə üstünlük təşkil edir, spam/fişinq filtrasiyası, məlumatların mühafizəsi və nəzarət isə yalnız bundan sonra gəlir. Kibercinayətkarlığın qurbanı olma ilə bağlı suallara dair rəylər fokus qrupunda iştirak edən müəssisələr arasında zərərçəkmişlərlə (qurbanlarla) bağlı halların çox aşağı olduğunu üzə çıxarır. Bununla yanaşı, sorğuda iştirak edənlərin müvafiq olaraq 45,3%-i və 46,9%-i qabaqcıl təhlükəsizlik texnologiyaları və bu istiqamətdə ayrılan daha miqyaslı büdcələrin işlədikləri qurumların təhlükəsizliyini yaxşılaşdırmağa kömək edəcəyini düşünür. Müəssisələrin 65,6%-i noutbuklarda fayl şifrələməsi qaydasından istifadə edir. COVID-19 pandemiyasının müəssisələrə qarşı kibercinayətkarlığı kəskinləşdirməsinin aşkar edilməsi yönündə cavablar isə demək olar ki, bərabər şəkildə bölünüb.

Tədqiqat çərçivəsində fokus qruplar kibercinayətlərlə bağlı insanların fikirlərinə dair olduqca faydalı məlumatlar təqdim ediblər. Ümumi prosesdə 57 iştirakçı (tədqiqatlar üzrə qartopu texnikasından istifadə edilməklə) başlıca olaraq iki istiqamətdə cəlb edilib: a) tədqiqat qrupu üzvlərinin tədris həyata keçirdiyi universitetlərin tələbələri və b) digər agentliklərlə əməkdaşlıq çərçivəsində formalaşmış əlaqələr vasitəsilə. Beləliklə, ilkin araşdırmada mövzu üzrə zərərçəkmiş şəxslər əvvəlcədən müəyyən edilib, sorğu çərçivəsində onların mobil telefon nömrələrinin qeydiyyatı aparılıb, sonra Sosial Tədqiqatlar Mərkəzinin (STM) İctimai rəyin öyrənilməsi departamentinin əməkdaşları tərəfindən həmin insanlarla əlaqə saxlanılıb. Digər tərəfdən, bir sıra hüquq-mühafizə orqanlarına rəsmi dəvət məktubu göndərilib. QHT nümayəndələri və İT sektorunun mütəxəssisləri isə həm rəsmi dəvət məktubu, həm də STM-in İT/Media departamenti tərəfindən əlaqə saxlanılmaqla prosesə cəlb olunub.

Ümumi Əhali Qrupunun (ÜƏQ) rəylərində müxtəlif tezliklərdə yalnız üç kibercinayət hadisəsinə rast gəlinib: onlayn zorakılıq, şəxsi məlumatlar (kimlik) oğurluğu və fişinq. Bütün digər kibercinayətlər (rənsamveə, şəxsi məlumatların yayılması) barədə məlumatlılıq isə olduqca məhdud səviyyədə qeydə alınmaqla, sözügedən anlayışlar əsasən heç vaxt eşidilməyən növlərdir. Kibercinayətkarlığın qurbanı olma baxımından şəxsiyyət (kimlik) oğurluğu halları meydanagəlmə tezliyi və təsir miqyası nöqteyi-nəzərindən fərqlənir. ÜƏQ-lər arasında onlayn zorakılıq hadisələri şəxsiyyət oğurluğuna (4 bank kartı və 3 sosial media hesabı oğurluğu) nisbətdə çox yayılsa da (9 hal), birincinin zərərçəkmiş respondentlərə təsirə malik olmadığı məlumdur. Aparılan araşdırmaya görə, bütün iştirakçıların fişinq zəngləri və e-poçtları qəbul etməsi, lakin yalnız iki nəfər zərərçəkmiş şəxsin müəyyən edilməsi faktı özlüyündə bu kibercinayət növü və ondan müdafiə üzrə yüksək məlumatlılığın olmasını əks etdirir.

Sorğunun nəticələri göstərir ki, əksər respondentlər onlayn rejimdə çalışarkən və smartfonlardan istifadə edərkən özlərini təhlükədə hiss edirlər. “Heç nə və heç bir yer

təhlükəsiz deyil" ifadəsi bu baxımdan üstünlük təşkil edən cavablardandır. Təhlükəsizliklə bağlı fokus qruplardan əldə edilən ən mühüm yanaşmalardan biri isə internet xidməti provayderlərinin (İXP) nümayəndələri tərəfindən irəli sürülüb. Belə ki, görülən bütün ciddi tədbirlərə baxmayaraq, hətta onlar da özlərini tam təhlükəsiz şəraitdə hiss etmədiklərini bildiriblər. Səbəb kimi istifadə edilən avadanlıq və proqram təminatlarının bütünlüklə xaricdən idxal olunması göstərilib.

Kibercinayətin qavranılma səviyyəsinə gəldikdə, "internet cinayətləri" və "informasiya cinayətləri" ifadələri ÜƏQ-lər arasında mövzu ilə bağlı bütün məqamları əhatə edən fikirlər kimi tez-tez qeyd edilsə də, İT mütəxəssislərinin bu nöqteyi-nəzərdən cavabları kəskin fərqlənir.

Bu qisim respondentlərə görə, digər cinayətlərlə müqayisədə kibercinayətlər potensial olaraq daha təhlükəlidir. Belə qənaət mövcuddur ki, zorakılıq və mülkiyyət əleyhinə cinayətlər, adətən, fərdlər, yaxud ictimai səviyyədə baş verdiyi halda, kibercinayətlərin geniş cəmiyyət miqyasında təsiri mümkün ola bilər. Bundan əlavə, İT mütəxəssisləri, İXP və hüquq-mühafizə orqanlarını təmsil edən bəzi respondentlər ziyan verilməsi məqsədilə başqasının avtomobilinin və ya ağıllı ev sisteminin asanlıqla zədələnməsinin mümkünlüyü fikrini səsləndiriblər.

Əksər ÜƏQ-lər və zərərçəkənlər arasında fişinq ən narahatedici kibercinayət növü kimi qeyd edilməklə, digər qruplarda müxtəlif cavablara (kibermüdaxilə/DDoS, kritik infrastruktur sahələrinə hücum) da rast gəlinib.

Hüquq-mühafizə orqanlarını təmsil edən respondentlərin baxışlarına əsasən, kibercinayətkarlığın əhəmiyyətli dərəcədə narahatedici tərəfi kritik infrastruktura ziyan yetirmək və beləliklə, qarışıqlıq, xaos yaratmaq xüsusiyyətidir. Bundan başqa, bir sıra qrupların rəylərində kibertəhdid kimi müəyyən hallarda vəziyyətin intiharla nəticələnə biləcəyinə dair qənaət də mövcuddur.

Keçirilmiş sorğunun nəticələrinin təhlilinə əsasən, bütün respondentlərin "kibercinayət" sözü, həmçinin qeyd olunmuş cinayət növlərinin əksəriyyətinə dair məlumatlı olması, lakin fişinq və rənsamveə haqqında demək olar ki, eşitmədikləri aydın olur. Bununla yanaşı, müvafiq izah təqdim edildikdən sonra sorğu iştirakçılarının adıçəkilən anlayışları da tanımaları nəticələr sırasındadır.

Müəyyən qrup respondentlər (18-21yaş) gələcəkdə kibercinayətkarlığın qurbanı olma ehtimallarına əsasən polisə müraciət ediləcək əsas struktur kimi yanaşsalar da, ümumilikdə ÜƏQ-lər, eləcə də QHT nümayəndələri bu təsisatı hadisə barədə məlumat bildiriləcək qurum kimi istisna etməyərək, əslində İT ekspertinə müraciətə müsbət baxdıqlarını bəyan ediblər. Belə ki, respondentlər baş vermiş kiberhadisə nəticələrinin həlli üzrə polisin səriştəliliyinə yüksək dərəcədə inanmasalar da, polisə şikayət etməyi əsas vasitələrdən biri kimi nəzərdə saxlayıblar. Bununla da sorğu nəticələrindən də göründüyü kimi, kibercinayətlərin aşkarlanması və qeydiyyata alınmasında İT sektoru ilə polis arasında möhkəm əməkdaşlığa ehtiyac duyulur.

Məktəblilərin üzləşdikləri risklərin vurğulanması özlüyündə problemin olduqca vacib tərəfini əhatə edir. Sorğu çərçivəsində fokus qrupların birindən gələn təklifə əsasən ümummilli və məktəb səviyyəsində bu istiqamətdə maarifləndirmə işlərinin aparılması xüsusi əhəmiyyət kəsb edir. Bütün bu kimi təkliflərin valideyn, yaxud təhsil sektorunda çalışan üç nəfər qadın və bir nəfər kişi respondent tərəfindən irəli sürülməsi isə tədqiqatın digər maraqlı məqamlarındandır. Belə vəziyyət məktəblərdə problemin ciddiliyini nümayiş etdirən haldır. Beləliklə, gələcəkdə analoji istiqamətdə yalnız valideynlərdən ibarət fokus qrupların təşkilinin vacibliyi respondentlərin rəyində də öz təsdiqini tapır. Qadın respondentlərdən birinin qeyd etdiyi kimi, bəzən müəllimlər istəmədən fişinq məktublarının yayılmasında əsas rol oynayırlar. Şagirdlər arasında smartfon və planşetlərdən yüksək istifadə səviyyəsi nəzərə alındıqda, belə alt qrupda kibercinayətkarlığın yüksək miqyasda "qaranlıq (bilinməyən) rəqəmlər"inin mövcudluğu ehtimalı nəzərə çarpır.

İstisnasız, sorğunun aparıldığı bütün qruplar elektron xidmətlərdən (e-gov və e-ticarət) istifadənin artması, eyni zamanda, əvvəllər kağız üzərində toplanan məlumatların rəqəmsallaşdırılması nəticəsində kibercinayətkarlıq hallarının gələcəkdə intensivləşəcəyinə dair ortaq qənaətə malikdir. Buna baxmayaraq, ÜƏQ-lər ilə keçirilmiş sorğunun cavab göstəriciləri ilə fokus qruplarla müsahibələrin nəticələri arasında ən diqqətçəkən fərq kibercinayətkarlıqla bağlı gözləntilərə aiddir. Demək

olar ki, hər bir fokus qrup iştirakçısı kibercinayətkarlığın gələcəkdə kəskin səviyyəyə çatacağını gözləsə də, ÜƏQ-lərin təxminən yarısı əksinə, bu istiqamətdə geriləmə olacağını düşünür. Ümumi rəylərdə belə təəccüblü məqamların meydana gəlməsi seçmə meyarlarına uyğun izah edilə bilər. Fokus qruplar üçün iştirakçılar müəyyən edilərkən hansısa kriteriyalar (məsələn, internetdən fəal istifadə, İT və ya İXP sektorunu təmsil etmə və s.) üzrə seçmə aparılır və beləliklə, nəticələrin müqayisəsi zamanı müxtəlif göstəricilər yaranır. Ümumi əhali sorğusunda isə seçmə təsadüfi qaydada həyata keçirilib.

Ümumilikdə, bu nəticəyə gəlmək olar ki, Azərbaycanda kibercinayətlərin bütün formaları geniş yayılmayıb. Bir çox kibercinayət növləri üzrə zərərçəkmə nisbəti istər fərdi, istərsə də təşkilati miqyasda olduqca aşağıdır. Respondentlərin əsas mövzuya dair məlumatsızlığı müşahidə edilən faktlardandır. Nisbətən yayılmış hal olmasına baxmayaraq, əksəriyyət "fişinq" termini haqqında xəbərsizdir. Bankların fişinq və ya bank kartı oğurluğu məsələlərilə məşğul olmağa meyilli olmadığı, o cümlədən polisin cinayətkarları təqib etmək qabiliyyəti və bu istiqamətdə peşəkarlıq və təcrübə çatışmazlığına dair ciddi şikayətlərin mövcudluğu da üzə çıxan amillərdir.

KİMM, DTX və DİN maarifləndirmə yönündə əhəmiyyətli tədbirlər həyata keçirsələr də, xüsusilə kadrların hazırlanması və ya təkmilləşdirilməsi, həmçinin daha uğurlu tədqiqatların aparılması baxımından bu istiqamətdə çox iş görülməlidir. Ümumiyyətlə, kibercinayətlər demək olar ki, fokus qruplar arasında birmənalı şəkildə digər cinayət növlərindən potensial yüksək təhlükəli hesab edilib. Sorğu iştirakçılarının əksəriyyəti öz növbəsində kibercinayətləri digər cinayətlərlə müqayisədə daha ciddi hadisə kimi qiymətləndirib.

3. Problemin təsviri

Kibercinayət və kibertəhlükəsizlik nədir?

Kibercinayət kompüter cihazları və internetdən istifadəni əhatə edən cinayətdir. Fərdlərə, bir qrup insana, hökumət və özəl təşkilatlara qarşı törədilə bilər. Adətən, insanların nüfuzuna xələl gətirmək, fiziki və ya mental zərər yetirmək, yaxud hansısa fayda qazanmaq, pul əldə etmək, nifrət məzmunlu mətnləri və terrorizmi yaymaq və s. məqsədilə həyata keçirilir.

Kibertəhlükəsizlik mahiyyət etibarilə internetlə əlaqəli olduğundan, Azərbaycanda istifadəçilərin səviyyəsi ilə bağlı statistikaya diqqət yetirmək lazım gəlir.

2022-ci ilin yanvarında Azərbaycan əhalisi 10,26 milyon nəfər olub.[5] 2021-ci ilin yanvarında ölkədə 8,26 milyon internet istifadəçisi qeydə alınıb və 2020-2021-ci illər dövründə ümumi internet istifadəçilərinin sayı 202 min (+2,5%) nəfər artıb. Beləliklə, 2021-ci ilin yanvarında ölkədə internet penetrasiya göstəricisi *(internet istifadəçisi olan ümumi əhali faizi* - **red**.) 81,1% olub. Bununla yanaşı, həmin ilin yanvarında sosial media istifadəçilərinin sayı 4,3 milyon nəfər olub ki, bu da ümumi əhali sayının 42,2%-nə bərabərdir. Müvafiq şəkildə, 2020-2021-ci illər ərzində sosial media istifadəçilərinin sayının 600 min (+16%) nəfər artması statistik faktdır. Həmin dövrdə ölkə üzrə 11,3 milyon mobil telefon istifadəçisi mövcud olub. Mobil qoşulma miqyası 2020-ci ilin yanvarından növbəti ilin eyni dövrünədək müddətdə 92 min (+0,8%) say həddində artıb. Ümumilikdə, 2021-ci ilin yanvar ayı üzrə Azərbaycanda mobil qoşulma miqyası əhalinin 111,0%-nə ekvivalent olub. (**Qeyd:** Xeyli sayda insan birdən çox mobil qoşulma əlaqəsinə malikdir və bu səbəbdən mobil qoşulmalar üzrə göstəricilər ümumi əhalinin 100%-dən çoxunu əhatə edə bilər).[6] Son olaraq, mütləq qeyd edilməlidir ki, ölkə əhalisinin 57,2%-i şəhər mərkəzlərində, 42,8%-i isə kənd yerlərində yaşayır.

[5] Azerbaijan Population (LIVE). - https://datareportal.com/reports/digital-2022-azerbaijan
[6] Digital 2021 Azerbaijan. - datareportal.com/reports

4. Giriş

4.1. Azərbaycanda kiberhücumlar və təhdidlərə cavab: problemin dinamikasına nəzər

Ölkədə kiberhücumlar tarixinin tədqiqi göstərir ki, 2000-ci ilin yanvarında erməni hakerlər tərəfindən Azərbaycanın 20-yə yaxın dövlət saytı ilə yanaşı, ABŞ-nin Bakıdakı səfirliyi və bir sıra beynəlxalq təşkilatların internet saytlarının hədəf alınması, rəsmi Bakı və aparıcı dövlət nümayəndələrinə, xüsusilə keçmiş Prezident Heydər Əliyevə qarşı düzgün olmayan və təbliğat xarakterli materialların yerləşdirilməsi ilə Qafqaz regionunda rəqəmsal münaqişələr genişlənməyə başlamışdı. Bundan əlavə, 2012-ci ilin yanvarında müəyyən dövlət və xəbər agentliklərinin internet saytları da dövlət əleyhinə fikirlərin yayılması məqsədini güdən hücuma məruz qalmışdı.[7]

Digər bir araşdırmaya əsasən, *"Staksnet" (Stuxnet) adlı "kompüter qurdu"nun hücumu dünyanın bir çox dövlətlərini təsirə məruz qoyduğu kimi Azərbaycan ictimaiyyətinin diqqətini kibertəhlükəsizliklə bağlı məlumatlılıq mövzusuna cəlb etdi".* "Staksnet" əsasən İrandakı kompüter şəbəkələrinə qarşı yönəlmişdi, lakin Azərbaycan daxil olmaqla bir sıra digər dövlətlərdə də aşkarlandı. Şübhəsiz ki, effektiv əks-tədbirlərlə operativ reaksiya nəticəsində bu "kiber-raket"in ("cyber-missile") yaratdığı ziyan məhdudlaşdırılsa da, "Staksnet" hadisəsi Azərbaycanda kiberməkanın mövcud müdafiə vasitələri üçün xəbərdarlıq mahiyyəti daşıyırdı.

Ölkənin səlahiyyətli qurumları tərəfindən 2012-ci ildə 25 kiberhücumun mənşəyi ilə bağlı araşdırma aparıldı. Bu hücumların 24-nün İran, digər birinin isə Niderlanddan icra olunduğu müəyyən edildi.[8]

Beləliklə, kibertəhlükəsizlik məsələsi Azərbaycanın milli təhlükəsizliyi üçün ən ciddi narahatlıq və çağırışlardan birinə çevrildi.[9]

İddialara görə, Azərbaycan kiberməkanına İran əsaslı hücumlar onsuz da gərginləşən Bakı-Tehran ikitərəfli münasibətlərini daha da pisləşdirib. Ancaq bunlara paralel olaraq, ölkənin aidiyyəti strukturları Ermənistan, İran və hətta Rusiyadan qaynaqlanan potensial kiberhücumlara qarşı kibertəhlükəsizliyin gücləndirilməsi istiqamətində işlər də aparırlar.

Kiberhücumlar barədə ilk olaraq iqtidarda olan Yeni Azərbaycan Partiyası (YAP) tərəfindən məlumat verilib və həyata keçirilmiş araşdırma zamanı hakerlərin İP (İnternet Protokol) ünvanlarının İran mənşəli olması sübuta yetirilib. Bir ay sonra isə Azərbaycanın AZAL aviaşirkətinin, o cümlədən bir telekanalın internet saytlarının iranlı hakerlər tərəfindən hücuma məruz qalmasına dair xəbərlər yayılıb.[10]

2018-ci il iyulun 18-də Mingəçevir Su Elektrik Stansiyasının yarımstansiyalarında ölkə miqyasında elektrik enerjisinin kəsilməsi hadisəsi ilə bağlı kritik infrastruktura təhdidlərin qiymətləndirilməsi bu sahədə ciddi strateji problemləri üzə çıxardı və Azərbaycanın milli təhlükəsizliyini diqqət mərkəzinə gətirdi.[11]

4.2 Kibertəhdidlərin artması

Hazırda Azərbaycanda cəmiyyət səviyyəsində vətəndaşlara vacib xidmətlərin demək olar ki, əksəriyyəti rəqəmsallaşdırılıb və sözügedən istiqamətdə işlər sürətləndirilmiş rejimdə davam etdirilir. Ümumiyyətlə, bu prosesə qlobal müstəvidə təkan verilməklə, bütün dövlətlərin gələcəyi rəqəmsal transformasiya və onun statusundan asılıdır. Əslində, son 10 ildə Azərbaycanda kibertəhlükəsizliyin təmin edilməsi istiqamətində müxtəlif addımlar atılıb. Ötən üç il müddətində isə bununla bağlı fəaliyyətlər intensivləşdirilib.

COVID-19 pandemiyası dövlət və özəl sektor, səhiyyə, təhsil, ticarət və digər bir çox sahələrdə rəqəmsallaşmaya keçidə zəmin hazırladı. Bu gedişatla mövcud vəziyyət hökuməti və vətəndaşları texnologiyaların köməyi ilə dəyişikliklərə uyğunlaşmağa sövq etdi. Belə demək mümkünsə, pandemiya cəmiyyətin rəqəmsallaşdırılması işində Azərbaycanda sıçrayışa şərait yaratdı.

---

[7] Marcus Franda, Launching into Cyberspace: Internet Development and Politics in Five World Regions (London: Lynne Rienner Publishers, 2002), p.121

[8] Government probe traces cyber-attacks to Iran, Netherlands.- https://www.azernews.az/nation/40524.html

[9] Azerbaijan Cybersecurity Governance Assessment. Ms. Natalia Spînu. DCAF. Switzerland. November 2020, p.4

[10] https://www.azernews.az/nation/40524.html

[11] "Critical Infrastructure" and its protection: the world experience and the need for implementation in Azerbaijan. - newtimes.az/en/politics

Kibertəhlükəsizlik mövzusu 2021-ci ildə Azərbaycanda sözün həqiqi mənasında medianın daimi başlığına çevrildi. "Kiberdələduzluğun yüksəlişi: kimdir günahkar?" və s. kimi müzakirə mövzuları dünyada və ölkəmizdə kibercinayətlərin indiyədək görünməyən səviyyəsini üzə çıxardı. Ekspertlər Azərbaycanda kiberhücumların artması barədə fikirlər səsləndirirlər. Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti (XRİTDX) tərəfindən təqdim edilən statistik məlumatlara əsasən, 2021-ci ildə kiberhücumların artım tempi 38% təşkil edib ki, əvvəlki il müvafiq göstərici 28% olub. XRİTDX-nin rəsmi nümayəndəsi Tural Məmmədov "Pandemiya dövründə Azərbaycanda kiberdələduzluq" mövzusuna həsr olumuş konfransda bu fikirləri qeyd edib: *"Məlumdur ki, ölkənin üç ən böyük şəhərinin çox sayda sakini kibercinayətkarların hədəfi olub. Azərbaycan dilindən istifadə etməklə həyata keçirilən kibertəhlükələrin sayı artıb. Eyni zamanda, əhalinin belə təhlükələr barədə məlumatlandırılması istiqamətində görülən tədbirlərin də həcmi 40 faiz yüksəlib".*[12]

Tədqiqatın nəticələrinə görə, insanlar şəxsi məlumatlarını üçüncü tərəflərlə paylaşmaqdan narahatlıq keçirdiklərini ifadə ediblər. Ən çox ünvanlanan suallardan biri sözügedən vəziyyətlərdə başlıca günahkarın kim olması ilə əlaqəlidir: məsələn, bank, yoxsa müştərilər? Bu baxımdan, kiberdələduzluqdan ən çox şikayət edənlər sırasında "Kapital Bank"ın müştəriləri çoxluq təşkil edib. Qeydə alınan məlumatlara əsasən, ekspertlər, KİV-lər, aidiyyəti qurumlar ictimaiyyətin diqqətini bu cür hallarda riayət olunmalı bir sıra davranışlara yönəltməklə bağlı maarifləndirmə işləri aparıblar.

4.3. Yeni "Ağıllı kənd/şəhər" konsepsiyası: həyata keçirilməsi və kibertəhlükəsizliyin əhəmiyyəti

Azərbaycan iqtisadi inkişafı maksimum səviyyəyə çatdırmaq üçün rəqəmsal rabitə, avtomatlaşdırma və bərpa olunan enerji kimi ən son texnologiyalardan istifadə etməklə Qarabağın işğaldan azad edilmiş ərazilərində "ağıllı şəhərlər və kəndlər" konsepsiyasını həyata keçirməyə başlayıb. "Ağıllı şəhər" layihəsi çərçivəsində artıq sözügedən yerlərdə smart şəhərlərin salınması prosesinin reallaşdırılması istiqamətində ilkin addımlar da atılıb. Tədqiqatlarda qeyd edilir ki, "Ağıllı şəhərlər" tamamilə texnoloji vasitələrə tabe olduqlarına görə kibertəhlükə hədəfinə çevrilə bilərlər. Belə yaşayış məkanlarının kibertəhlükəsizlik tələbləri əsasən əməliyyatların təhlükəsizliyindən asılıdır. "Ağıllı şəhər" modelinin tətbiqi, ona qarşı təhdidlər, layihənin zəif tərəfləri tədqiqatçılar tərəfindən geniş şəkildə müzakirə olunur. Mütəxəssislərdən birinin iddiası belədir: *"Azərbaycanda paytaxt - digər şəhər/kənd ərazilərinin müqayisəsində rəqəmsal uçurum mövcuddur. Sabit internetə giriş imkanı baxımından kənd və şəhər ev təsərrüfatları arasında 20 faizlik fərq var. Bu rəqəmsal fakt əsasən sabit infrastruktur çatışmazlığı və kəndlərdə rəqəmsal savadlılığın aşağı olması ilə əlaqədardır. Ölkədə həmçinin genişzolaqlı internet daha sürətli, ucuz və əlçatan edilməlidir. Hazırda internetin ümumi mobil genişzolaqlı əhatə dairəsi və qəbulu yüksək olsa da, şəhər və kənd yerləri arasında internetin keyfiyyəti/sürəti, istifadəsi və sərfəliliyi baxımından əhəmiyyətli rəqəmsal fərqlilik mövcuddur"* (Dünya Bankı, 2019).[13]

4.4. Ölkəyə xaricdən kibertəhdidlər və kiberhücumların mənbələri

Kiberhücumların mənbəyi ilə bağlı qeyd etmək lazımdır ki, son illər erməni hakerlərin fəallığı nəzərə çarpır. 2020-ci ilin payızında baş vermiş İkinci Qarabağ müharibəsi dövründə erməni hakerlər Azərbaycan Mərkəzi Bankı da daxil olmaqla ölkənin bank sisteminə hücumlara cəhd göstəriblər. Məlumatlara əsasən, erməni hakerlər tərəfindən həyata keçirilmiş kibertəhdidlər zərərsizləşdirilib, Mərkəzi Bankın və digər bankların iş prosesində ciddi problemlər yaranmayıb. Həmin dövrdə baş vermiş xarici kiberhücumlarla bağlı Azərbaycan tərəfi kifayət qədər sübutlar toplayaraq yuxarıdakı cinayət xarakterli hadisələrin qiymətləndirilməsi üçün beynəlxalq kibercinayətkarlıqla mübarizə təşkilatlarına müraciət edib.[14]

---

[12] Растет число киберугроз на азербайджанском... - az.sputniknews.ru
[13] Building Smart Cities and Villages in Azerbaijan: Challenges and Opportunities. - bakuresearchinstitute.org
[14] Во время Отечественной войны армянские хакеры пытались атаковать ЦБА. - az.sputniknews.ru

Potensial erməni kibercinayətkarları həmin dövrdə fişinq hücumları da həyata keçirirdi. Paralel olaraq, istifadəçilərə qarşı DDoS (distributed denial-of-service – bir neçə sistemdən müdaxilə hücumu/paylanmış mənbələrdən sistemdə "xidmətdən imtina" vəziyyətinə səbəb olan kiberhücum) əməliyyatları baş tutsa da, belə cəhdlər bu tip fəaliyyətlərin qarşısını almaq üçün nəzərdə tutulmuş müdafiə mexanizmi tərəfindən bloklanırdı.

Etiraf edilə bilər ki, istər fərdlər, istərsə də təşkilatların üzləşdikləri təhlükələrə baxdıqda, qeyd edilən statistika aysberqin yalnız görünən hissəsini əhatə edir. İstənilən halda, göstəricilər kibertəhdidlərin təkamül və artan miqyası haqqında ümumi məlumat təqdim edir.

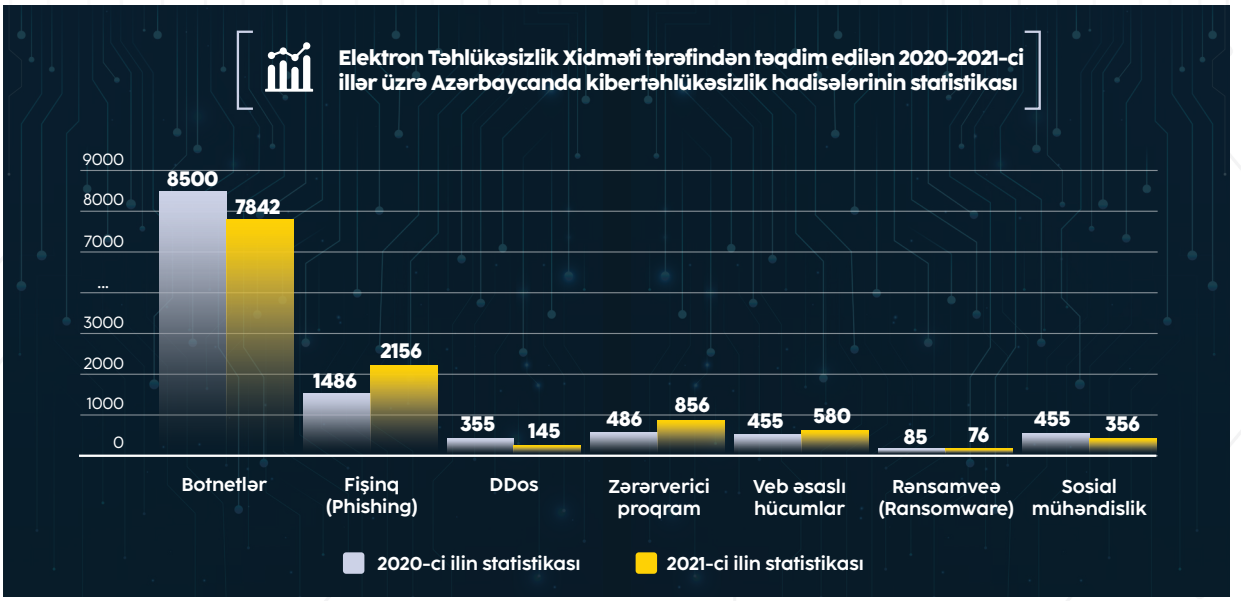
4.5. Artan daxili kibercinayətkarlıq, daxili təhlükələr

2021-ci il noyabrın 20-də təqribən on min vətəndaşa qarşı dələduzluq törədən kiberdəstə üzvləri ifşa edilib. Təhqiqat zamanı məlum olub ki, bir qrup şəxs ölkə daxilində "Sığorta" adında şirkət yaradıb. Bu şəxslər Azərbaycanda "OCOS" beynəlxalq dələduzluq piramidası ("Ponzi sxemi") tətbiq ediblər. Onlar internetdə xüsusi yerli proqramlar vasitəsilə əslində mövcud olmayan kriptovalyuta yaradaraq guya onun beynəlxalq valyuta bazarında satışını təşkil etməklə, şişirdilmiş yüksək mənfəət vəd edərək vətəndaşların vəsaitlərini fırıldaqçılıq yolu ilə mənimsəyiblər. Beləliklə, həmin fırıldaqçılar qurduqları şəbəkə biznesinə çoxlu sayda vətəndaşı piramida formasında cəlb edərək onlara saxta kriptovalyuta satıblar. Araşdırmaya görə, kiberdəstə üzvləri ümumilikdə 10 minə yaxın vətəndaşı bu üsulla aldadaraq külli miqdarda pul ələ keçiriblər.[15] Qeyd etmək lazımdır ki, itki barədə dəqiq məlumat verilməsə də, cinayətkarlar müxtəlif qurbanlardan üç min dollardan on min dollaradək pul məbləğləri aldıqlarını etiraf ediblər.

İlk irimiqyaslı kiberdələduzluq hadisəsində zərərçəkənlərin say çoxluğu (on min nəfərə yaxın) daxili kibertəhlükələrin artdığını sübut edir. Digər tərəfdən, bu, əhalinin yeni cinayətlərlə bağlı maarifləndirilməsinə yüksək səviyyədə ehtiyac olduğunu təsdiqləyir.

4.6. Azərbaycanda 2020-2021-ci illər üzrə kibertəhlükəsizlik hadisələrinin statistikası

Qeyd: İnsidentlərə əsaslanan statistikaya vətəndaşlar, özəl təşkilatlar, müstəqil kibertəhlükəsizlik şirkətlərindən bildirilən və Elektron Təhlükəsizlik Xidməti tərəfindən toplanılan datalar daxildir:



Mənbə: 2020-2021-ci illər üzrə Azərbaycanda kibertəhlükəsizlik hadisələrinin statistikası. / Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Xidməti tərəfindən təqdim edilib.

[15] Members of the gang who committed fraud against about 10,000 citizens were exposed. - www.txtreport.com/news

- Botnetlərdən sonra ən geniş yayılmış kibercinayətkarlıq növü fişinqdir. Bu kiber növ üzrə 2020-ci ildəki göstərici 30% artıb;
- "Emotet" adlı troyan (belə viruslar sistemə daxil edildikdən sonra tədricən onu ələ keçirir) ən çox istifadə edilən növ kimi qeydə alınıb;
- Ən geniş yayılmış fişinq ssenariləri ödəniş kartı nömrələrinin, internet bankçılığında login (sistemə giriş) detalları, sosial media və elektron poçt ünvanı məlumatlarının ələ keçirilməsinə aid hallardır. Kibercinayətkarlar bu məqsədlərin reallaşdırılması üçün saxta sms və votsap (WhatsApp) mesajları, həmçinin, fişinq (saxta nüfuzlu qurumdan daxil olan zəng-lə/mesajlarla şəxsi məlumatların öyrənilməsi) vasitələrindən istifadə ediblər. Fişinq hücumları ilə bağlı ümumiyyətlə kəskin artım diqqəti cəlb edib;
- 2021-ci ildə Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Xidməti zombi fəaliyyəti aparan 7842 sayda İP ünvanı haqqında məlumatlar toplayıb. Bu, 2020-ci ildə müşahidə edilən müvafiq göstəriciyə olduqca yaxın rəqəmdir. Belə fəaliyyətlərin daha çox "Andromeda", "Emotet" və "Avalanç" botnetləri vasitəsilə həyata keçirildiyi məlumdur. Son aylarda "Flubot" zərərverici proqramı ilə də sistemlərə nüfuz edilməsində artım nəzərə çarpıb.

Bilinən məqam odur ki, 2021-ci ilin əvvəlindən etibarən KİMM kiberdələduzluq halları və onlardan müdafiə üsulları üzrə əks tədbirlər olaraq ictimai məlumatlılıq səviyyəsini 40% gücləndirib. Sözügedən istiqamətdə əhalinin maarifləndirilməsi ilə əlaqədar genişmiqyaslı işlərin aparılması ölkədə nağdsız ödənişlərə ehtiyac və bu ödənişləri müvafiq qaydada həyata keçirən şəxslərə qarşı kiberhücumların sayının artması ilə sıx şəkildə bağlıdır. Bu məsələlərə dair insanlara dəstək göstərilməsi üçün müxtəlif təşkilatlar, şirkətlər və Azərbaycanın dövlət departamentlərinin internet resurslarını təqlid edən zərərli saytlar haqqında məlumatları ehtiva edən onlayn platforma – *blacklist.gov.az* təsis edilib.

4.7. Azərbaycanda kibertəhlükəsizlik sahəsində hüquqi-tənzimləyici çərçivələr

Bir çox ölkələrdə olduğu kimi, Azərbaycanda da milli kibertəhlükəsizlik siyasətinin inkişaf etdirilməsi zəruri məsələdir. Hökumətin informasiya və kommunikasiya sistemləri, o cümlədən hərbi və kommersiya layihələri kiberhücumlar və kibercasusluğa qarşı getdikcə daha həssas qrupu təşkil edir. Bu baxımdan, kibermənzilin idarə edilməsi dövlət səviyyəsində əhəmiyyətli mövzudur. Azərbaycanda rəhbər orqanlar həyata keçirdikləri siyasət çərçivəsində kibertəhlükəsizliyin prioritetləşdirilməsi üzrə fəallığa malikdirlər.

Qeyd edilənlərlə əlaqəli hüquqi-tənzimləyici məzmunlar (qanunlar, doktrinalar və qanunvericiliyin təkmilləşdirilməsi) dövlətin kibertəhlükəsizliyinin, bu sahədə dövlət siyasətinin prinsip və istiqamətlərinin yaradılması üzrə hüquqi və təşkilati çərçivə formalaşdırır. Buraya həmçinin dövlət orqanları, müəssisələr, institutlar, təşkilatlar, fərdlər və vətəndaşların sözügedən sferada səlahiyyətləri, eyni zamanda onların fəaliyyətlərinin koordinasiyası üzrə başlıca prinsiplər də daxildir. Azərbaycanın kibertəhlükəsizlik siyasəti ilə bağlı hüquqi-tənzimləyici bazanın inkişafına əsas etibarilə 1999-2000-ci illərdə başlanılıb.[16]

Mövzu üzrə hüquqi sənədlərdən başqa, müəyyən siyasət istiqamətləri bilavasitə kibertəhlükəsizliyə aiddir. Qeyd edilməlidir ki, kibertəhlükəsizlik və ya onunla bağlı özəl sektorla əməkdaşlığa dair ayrıca strategiya mövcud deyil, lakin müxtəlif siyasətlərin həyata keçirilməsində kibertəhlükəsizlik imkanlarının inkişafı üçün bəzi müddəalar təsbit edilib. Bu kimi strategiyalara **"Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya" və "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair Milli Strategiyanın həyata keçirilməsi üzrə 2016-2020-ci illər üçün Dövlət Proqramı"-nı, həmçinin "Azərbaycan 2020: gələcəyə baxış" İnkişaf Konsepsiyasını və "Azərbaycan Respublikasında telekommunikasiya və informasiya texnologiyalarının inkişafına dair Strateji Yol Xəritəsi"**ni aid etmək olar.

"Azərbaycan Respublikasında infor-

[16] UNIDIR-The United Nations Institute for Disarmament Research. Cyber Policy Portal. - unidir.org/cpp/en/states/azerbaijan

masiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya" Beynəlxalq Telekommunikasiya İttifaqı (BTİ) və Aİ tərəfindən hazırlanmış bütün təcrübə və tövsiyələri nəzərə alan sənəddir. Strategiyanın əsas məqsədi informasiya cəmiyyətinin qurulması və İKT-nin inkişafı daxil olmaqla ölkənin davamlı sosial-iqtisadi və mədəni səviyyədə yüksəlişi üçün vətəndaşlar, icmalar və dövlət tərəfindən onun imkanlarından səmərəli istifadə etməkdir. Müvafiq strategiyanın həyata keçirilməsi üçün Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi əlaqələndirici qurum təyin edilib. *"CyberCrime@EAP"* regional layihənin jurnalında dərc edilmiş məqalədə ifadə edildiyi kimi, həmin strategiya kibertəhlükəsizliyin çoxsaylı aspektlərini əhatə edir. Bu baxımdan, informasiya təhlükəsizliyinə nail olunması əsas prioritetlərdəndir. Məqsəd rəqəmsal məkanda təhlükəsizliyi inkişaf etdirmək, İKT-dən istifadəyə inamı artırmaq, qanunvericilik bazasını təkmilləşdirmək və məlumatlılığı yüksəltməkdir. Bu məqsədlərə çatmaq üçün vəzifələr sırasına isə informasiya təhlükəsizliyi üzrə dövlət siyasətinin hazırlanması, bu istiqamətdə xarici ölkələrdən asılılığın azaldılması, "elektron hökumət" şəbəkələrinin mühafizəsi, kibertəhlükələrin əhəmiyyətinin ölkə miqyasında elan edilməsi, kibertəhlükəsizlik sahəsində texniki peşəkarlığın inkişaf etdirilməsi, uşaqların istifadəsi üçün "təhlükəsiz internet" platformasının gücləndirilməsi, cəmiyyətdə və şirkətlər arasında məlumatlılığın artırılması və eləcə də informasiya təhlükəsizliyi mədəniyyətinin təşviqi daxildir.

Yuxarıda qeyd edilən strategiya hər biri dövlət proqramları ilə müşayiət olunan iki mərhələdə həyata keçirilir. 2016-2020-ci illər üçün Dövlət Proqramı Milli Strategiyanın tətbiqi istiqamətində yeddi prioritet üzrə konkret addımlardan ibarətdir. İnformasiya təhlükəsizliyinə dair tədbirlər planına əsasən, Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi (RİNN), Dövlət Təhlükəsizliyi Xidməti (DTX) və Müdafiə Nazirliyi (MN) kibertəhlükəsizliyə dair normativ hüquqi aktların yenilənməsinə məsul olan qurumlardır.

"Telekommunikasiya və informasiya texnologiyalarının inkişafına dair Strateji Yol Xəritəsi"nə və İKT sektorunun "SWOT" təhlilinə əsasən şəbəkə və informasiya təhlükəsizliyinə qarşı artan çağırışlar əsas təhlükələr sırasındadır. Bu baxımdan, strateji məqsədlərdən biri milli kibertəhlükəsizliyə hazırlığın və məlumatlılığın artırılmasıdır.

Qanunvericilik bazasına aid sənədlərin bəziləri aşağıdakılardır:

- "Dövlət sirri haqqında" Azərbaycan Respublikasının Qanunu, 2004
- Milli Təhlükəsizlik Konsepsiyası, 2007
- "Kibercinayətkarlıq haqqında" Konvensiyanın təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu, 2009
- Azərbaycan Respublikasının Hərbi doktrinası, 2010
- "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu, 2010
- "İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı, 2012
- "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qanununda dəyişiklik edilməsi barədə Azərbaycan Respublikasının Qanunu, 2012
- Azərbaycan Respublikasının Cinayət Məcəlləsi / Kibercinayətlər
- Azərbaycan Respublikasının Xüsusi Dövlət Mühafizə Xidmətinin Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyi haqqında Əsasnamənin və Agentliyin strukturunun təsdiq edilməsi barədə Azərbaycan Respublikası Prezidentinin Fərmanı, 2012
- "Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Xidmətinin fəaliyyətinin təmin edilməsi haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı, 2012
- "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanununda dəyişikliklər edilməsi barədə Azərbaycan Respublikasının Qanunu, 2017
- "Rəqəmsal transformasiya sahəsində idarəetmənin təkmilləşdirilməsi haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı, 2021
- Banklarda informasiya təhlükəsizliyinin idarə edilməsi Qaydası, 2021
- Azərbaycan Respublikasının Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti haqqında Əsasnamənin təsdiq edilməsi barədə Azərbaycan Respublikası Prezidentinin Fərmanı, 2021
- "Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi tədbirlər haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı, 2021.

4.8. "Milli Kibertəhlükəsizlik Strategiyası"nın statusu

Qeyd edildiyi kimi, 2014-2020-ci illər üzrə kibertəhlükəsizliyə dair strategiya vətəndaşların, özəl sektor və dövlət qurumlarının İKT-dən geniş şəkildə istifadəsi amilinə köklənərək Azərbaycanda informasiya cəmiyyətinin əsaslarını yaratmaqla, eyni zamanda, növbəti mərhələdə fəaliyyətin planlaşdırılması şərtlərini müəyyən edir.

İnformasiya Cəmiyyətinin İnnovativ İnkişafı və Elektron İdarəetmə Departamentinin təqdim etdiyi məlumata əsasən, ötən 3-4 il ərzində gələcək üçün yeni strategiyanın hazırlanması prosesi davam etdirilib. Son vaxtlar mətbuatda da "Azərbaycan kibertəhlükəsizlik strategiyası hazırlayır" kimi başlıqlar altında məqalələr dərc edilməkdədir. Yuxarıda adı çəkilən departamentin rəhbəri hələ 2019-cu ildə Azərbaycanda 2019-2022-ci illər dövrünü əhatə edəcək kibertəhlükəsizlik strategiyasının işlənib hazırlanması barədə qeyd etmişdir.[17]

Həmçinin, Rəqəmsal İnkişaf və Nəqliyyat Nazirliyinin (RİNN) məlumatına əsasən, ölkədə 2021-2025-ci illər üçün İnformasiya və Kibertəhlükəsizlik üzrə Milli strategiya artıq hazırlanıb və təsdiq edilməsi gözlənilir. Nazirlikdən bildirildiyi kimi, strategiyanın həyata keçirilməsi üzrə əhatə edilmiş tədbirlər planı bu sahədə qanunvericiliyin təkmilləşdirilməsinə dair şərtləri və müddəaları özündə birləşdirir. Qeyd edilir ki, təsdiqləndikdən sonra sənəd ictimaiyyətə təqdim ediləcəkdir. Strateji sənəd kibertəhlükəsizlik sahəsində fəaliyyətin növbəti qaydada təşkili və təkmilləşdirilməsi işinə xidməti nəzərdə tutur. Beləliklə, kibertəhlükəsizlik strategiyası hazırda işlənməkdədir. Bununla yanaşı, RİNN kibertəhlükələrin real vaxt rejimində monitorinqi istiqamətində də kiberəməliyyat mərkəzinin yaradılması planını həyata keçirmək niyyətindədir.[18]

Prosesin gecikmə amilini bəzi əlavələrin edilməsi ilə izah edən Nazirlik rəsmisi mövzu üzrə yeni məqamların ortaya çıxdığını qeyd etməklə, eyni zamanda, aydınlaşdırıb ki, informasiya təhlükəsizliyi məsələləri Strategiyada hələ öz əksini tapmayıb. Ona görə də hazırda bu iki məsələ informasiya təhlükəsizliyi və kibertəhlükəsizlik strategiyasında birləşdirilməlidir. Bu baxımdan mühüm sənədin ərsəyə gətirilməsi yönündə işlər davam etdirilir.

"Azərbaycan İnternet Forumu" adlı QHT-nin rəhbərinin sözlərinə görə, *"Rəqəmsallaşma sahəsində idarəetmənin təkmilləşmə dərəcəsinə əsasən Nazirliyin keçmiş formatı dövründə bəzi struktur dəyişiklikləri aparıldı və bir neçə yeni dövlət qurumu yaradıldı. Dəyişməyən yalnız Elektron Təhlükəsizlik Xidməti idi. Müşahidələr onu deməyə əsas verir ki, bu təşkilat qarşısına qoyduğu bir çox vəzifələri yerinə yetirə bilməyib. Hətta son vaxtlar vəziyyət o həddə çatıb ki, digər dövlət qurumları sözügedən təsisatın səlahiyyətlərini icra etməyə başlayıb. Uzun müddətdir ki, hazırlanma prosesində olan "İnformasiya təhlükəsizliyi və kibertəhlükəsizlik strategiyası" isə hələ müzakirə edilməyib. Əhalinin rəqəmsal savadlılığının artırılması işində də ciddi problemlər mövcuddur. Bundan əlavə, özəl sektorda kibertəhlükəsizlik sahəsi üzrə metodiki və informasiya təminatının təşkili səmərəli qurulmayıb və kifayət qədər əlçatan deyil".*

4.9. Azərbaycanda kibertəhlükəsizliyin əsas aktorları

Azərbaycanda kibersərhədlərin mühafizəsi ilə aparıcı dövlət qurumları məşğul olur: Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi (RİNN), Dövlət Təhlükəsizliyi Xidməti (DTX), özünün nəzdində olan İnformasiya Texnologiyaları İnstitutu (İTİ) vasitəsilə Azərbaycan Milli Elmlər Akademiyası (AMEA) və Azərbaycan Respublikasının Mərkəzi Bankı (AMB).

Ölkənin dövlət idarələri arasında kompüter şəbəkələrinin qorunması üzrə Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi (KİMM) / cert.gov.az yaradılıb. RİNN-in nəzdində sertifikatlaşdırma orqanı kimi fəaliyyət göstərən Elektron Təhlükəsizlik Xidməti də mövcuddur. Nazirlik həmçinin Azərbaycan vətəndaşlarına ictimai xidmətlər üzrə dövlət agentliyi olan "ASAN xidmət" vasitəsilə əhalinin hökumət xidmətlərinə çıxışında rahatlığının təmin olunması yönündə də irəliləyişə nail olub. Hazırda bu elektron hökumət platforması vasitəsilə 450 elektron xidmət həyata keçirilir.

[17] Azerbaijan develops strategy for cyber security | eufordigital.eu
[18] Azərbaycanda kibertəhlükəsizlik üzrə beşillik strategiya hazırlanıb | Xəbərlər.az

2021-ci ildə RİNN-in Məlumat Hesablama Mərkəzinin nəzdində Kiberhücumların Simulyasiya Laboratoriyası təsis edilib. Laboratoriya kibertəhlükəsizlik proseslərini öyrənir, bu sahədə mütəxəssislər hazırlayır və mümkün kiberhücumlara qarşı cavab tədbirləri həyata keçirir.[19]

2020-ci ildə çirkli pulların yuyulmasına və kiberterrorizmin maliyyələşdirilməsinə qarşı mübarizə sisteminin milli risk qiymətləndirilməsi məqsədilə Koordinasiya Şurası yaradılmaqla, "Açıq hökumətin təşviqinə dair 2020-2022-ci illər üçün Milli Fəaliyyət Planı" təsdiq edilib. Lakin məhz kibertəhlükələrin və risklərin qiymətləndirilməsinin aparılması üzrə analoji institut/qurum mövcud deyil.

Son dövrlərdə bir sıra özəl aktorlar da qeyd olunan istiqamətlər üzrə fəaliyyət göstərirlər. Məsələn, Azərbaycan şirkəti olan "DEFSCOPE" 2018-ci ildən qlobal arenada kibertəhlükəsizlik fəaliyyətləri icra edir. Qısa müddət ərzində şirkət dünya üzrə çoxsaylı layihələr həyata keçirməklə, aparıcı beynəlxalq qurumlarla əməkdaşlıq edib. Şirkət hal-hazırda Kanada, ABŞ və Avropadakı müştərilərinə ən son məhsul və xidmətlər təqdim edir.

2022-ci il fevralın 22-də Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyası təsis edilib.

4.10. Kibertəhlükəsizlik sahəsində regional və beynəlxalq əməkdaşlıq

Aydındır ki, başqa dövlətləri ikitərəfli və çoxtərəfli əməkdaşlığa cəlb etmədən sağlam və təhlükəsiz kiberməkana nail olmaq mümkün deyil. Birtərəfli təşəbbüslərə paralel olaraq, Azərbaycan dövlət orqanları qlobal kibertəhlükəsizlik mexanizmlərinin təkmilləşdirilməsi üzrə də dövlətlərlə əlaqələrin qurulmasında fəallıq nümayiş etdirir.

Başqa sözlə, Azərbaycan kibertəhlükəsizlik sahəsində qabaqcıl təcrübənin öyrənilməsində və tətbiqində maraqlı olmaqla, eyni zamanda beynəlxalq əməkdaşlıq sahəsində də daimi səylər həyata keçirir. Bu istiqamətdə 2009-cu ildən Avropa ölkələri arasında rəqəmsal həllər üzrə üçüncü yeri tutan Estoniya ilə sıx əməkdaşlıq əlaqələri qurulub. Ən yaxşı nümunələrdən biri kimi Estoniya ilə tərəfdaşlıq çərçivəsində formalaşdırılan Azərbaycanda "Asan imza"nın tətbiqi qeyd oluna bilər. Mobil şəxsiyyət xidməti və "Asan imza"nın rəqəmsal funksiyası ictimai və özəl elektron xidmətlərə istənilən yerdə və təhlükəsiz çıxışı təmin edir. Rəqəmsal mobil imza qanunvericilik səviyyəsində milli kimliyə bərabər qəbul edilir.

Kiberməkanın mühafizəsi həmçinin Azərbaycan-Rumıniya ikitərəfli münasibətlərinin əsas istiqamətlərindən biridir.[20] Bundan başqa, Gürcüstan və Çexiya da daxil olmaqla, Azərbaycan iyirmidən çox ölkənin kompüterlərlə bağlı fövqəladə hallara cavab qrupları ilə beynəlxalq əməkdaşlığa da başlayıb.

Qeyd etmək lazımdır ki, 1995-ci ildən etibarən NATO-nun "Sülh və təhlükəsizlik naminə elm" proqramında (STEP) Azərbaycan da fəal iştirak edir. Bu proqram meydana gələn təhlükəsizlik çağırışlarına cavab üçün beynəlxalq səyləri asanlaşdırmaqla, NATO və tərəfdaş dövlətlərin təhlükəsizliyinin gücləndirilməsi üzrə ümumi maraqlara aid məsələlərdə sıx əməkdaşlığa şərait yaradır. Eyni zamanda, NATO tərəfindən rəhbərlik edilən əməliyyatları, missiyaları dəstəkləyir, fəlakətlərin və böhranların qarşısının alınmasında erkən xəbərdarlıq və proqnozlaşdırma işini inkişaf etdirir. Bunlarla yanaşı, qeyd edilən proqram həmçinin NATO-ya üzvlüyə maraqlı olan dövlətlərin hazırlığı prosesinə dəstək göstərir. Əməkdaşlığın son dövrlərdəki aparıcı istiqamətləri sırasına kibermüdafiə, terrorizmlə mübarizə, fəlakətlərin proqnozlaşdırılması və qarşısının alınması (*Disaster Forecasting and Prevention)* məsələləri daxildir. Belə fəaliyyətlər Qabaqcıl Tədqiqatlar üzrə Seminarın (NATO ARW) Türkiyə və Polşadan olan mütəxəssisləri tərəfindən idarə edilir.

NATO-Azərbaycan əməkdaşlığının əsasları dünyada yaranan təhdidlərə qarşı mühüm əhəmiyyət kəsb edir. Təşkilat çərçivəsində Niderland da kiberməkanın qorunmasına dair öz təcrübələrini Azərbaycanla bölüşüb.[21] Ümumiyyətlə, kibertəhlükəsizlik məsələsi nüvə silahının yayılmaması, enerji təhlükəsizliyi və terrorizmlə mübarizə ilə eyni dərəcədə vacib amildir.

Beynəlxalq konvensiyalara qoşulma. Azərbaycan beynəlxalq kiberhüquqların güclü tərəfdarı olan aparıcı dövlətlərdən biridir və "Kibercinayətkarlıq haqqında" Konvensiyanı imza-

[19] Deloitte – Kiber və Texnologiya Xəbərləri İcmalı
[20] Azerbaijan Interested in Political Dialogue with NATO – Romanian Envoy, April 04, 2013 www.news.az
[21] Dutch Envoy Comments on Hacker Attacks on Azerbaijan Websites, www.news.az
[22] Chart of signatures and ratifications of Treaty www.coe.int

layaraq ratifikasiya edib (imzalanıb: 30/06/2008, ratifikasiya edilib:15/03/2010; qüvvəyə minmə tarixi: 01/07/2010).[22]

2008-ci il iyunun 30-da Azərbaycanın kiberqanunların təşviqi kampaniyası Avropa Şurası tərəfindən "Kibercinayətkarlıq haqqında" Konvensiyaya qoşularkən yüksək qiymətləndirilib. Azərbaycan kibercinayətlərlə mübarizə üzrə Avropanın çoxtərəfli alyansına daxil olduqdan sonra kiberməkanda cinayətlər və digər qeyri-qanuni fəaliyyətlərin qarşısının alınmasında kompüter mütəxəssislərini işə cəlb edib. Bununla da ölkə internetdən, kiberməkandan qeyri-qanuni istifadənin qadağan edilməsinə dair beynəlxalq müstəvidə mövcud olan ilk müqavilənin ən fəal üzvlərindən birinə çevrilib. "Kibercinayətkarlıq haqqında" Budapeşt Konvensiyası ilə bağlı, Avropa Şurasının həmin vaxt Bakıdakı nümayəndəsi (K.Yerokostopulos) Azərbaycanın kibercinayətkarlıqla mübarizədə qeyd-şərtsiz dəstəyini uğurlu hesab edib. Budapeşt müqaviləsinin fundamental məqsədi kompüter şəbəkələrindən yanlış istifadə, müəllif hüquqlarının pozulması, onlayn fırıldaqçılıq, uşaq pornoqrafiyası, şəbəkə təhlükəsizliyinin pozulması və s. daxil olmaqla internet cinayətlərini əhatə etməkdir.[23]

Yuxarıda qeyd olunan çoxtərəfli fəaliyyətlərlə yanaşı, Azərbaycan daxildə də məişət kibercinayətlərinin qarşısının alınması üzrə rəqəmsal qanunları layihələndirir. Bu yaxınlarda ölkədə kibertəhlükəsizlik sahəsində vəziyyətin yaxşılaşdırılması istiqamətində addımların atılması ilə bağlı fərman imzalanıb. Fərmanda ilk növbədə əsas məsələ kimi Azərbaycanda elektronlaşdırılmış resursların təhlükəsizliyinə diqqət yetirilir.

Kompüterdən sui-istifadənin qadağan edilməsi və kibertəhlükəsizliyin gücləndirilməsi üçün kiberqanunvericilik iki hissəyə bölünür. Bunlardan biri "Milli təhlükəsizlik haqqında" Qanun (iyun 2004), digəri "İcazəsiz məlumat toplanılmasının mühafizəsi haqqında" Qanundur (sentyabr 2004).

Bundan başqa, **Azərbaycan Respublikası Cinayət Məcəlləsinin 30-cu fəsli ("Kibercinayətlər") kompüter sistemlərinə icazəsiz giriş və onların təhlükəsizliyinin pozulması, kompüter viruslarının inkişafı və istifadəsi kimi bir çox istiqamətləri əhatə edən qayda və normaları müəyyən edir.**

Azərbaycan, Gürcüstan, Moldova və Ukraynanın Demokratiya və İqtisadi İnkişaf naminə - GUAM təşkilatı çərçivəsində tərəfdaşlığı regional əməkdaşlığa nümunədir. Hal-hazırda reallaşdırılan "Cybersecurity EAST24" (EU4Digital) isə Avropa İttifaqı və Avropa Şurasının birgə layihəsidir. Avropa Şurası vasitəsilə reallaşdırılan kibercinayətkarlıqla mübarizənin aspektləri əsasən Azərbaycanda müvafiq dövlət qurumlarının sözügedən sahədə potensialının təkmilləşdirilməsi ilə bağlı layihələrə yönəlib.

2015-ci ildə RİNN-in nəzdində fəaliyyət göstərən Elektron Təhlükəsizlik Mərkəzi kibertəhlükəsizlik sahəsində qlobal birliyin tamhüquqlu üzvü seçilib.

Ümumiyyətlə, "Şərq Tərəfdaşlığı" proqramı çərçivəsində kibertəhlükəsizlik standartlarının gücləndirilməsi üzrə indiyədək mühüm səylər göstərilib. Qeyd edildiyi kimi, 2008-ci ildə Azərbaycan Avropa Şurasının "Kibercinayətkarlıq haqqında" Konvensiyasını imzalayıb və Avropa İttifaqının mexanizmi olan Şərq Tərəfdaşlığı (ŞT) çərçivəsində həyata keçirilən kibercinayətkarlıqla mübarizə sahəsində əməkdaşlıq layihəsində də fəal iştirak edir. ŞT-nin əsası qoyulduqdan sonra (2009) keçən 13 il ərzində Avropa Şurasının başlıca kibertəhlükəsizlik standartlarını dəstəkləyən çoxsaylı müqavilələr həmin standartların tətbiqində faktiki olaraq dövlətləri kibertəhlükəsizliyə daha da yaxınlaşdıran strateji çərçivə təqdim edib.

Sözügedən kontekstdə, Avropa İttifaqı və Avropa Şurası tərəfindən maliyyələşdirilən "Kiber Şərq" (CyberEast) və Avropa İttifaqı tərəfindən həyata keçirilən "Kibertəhlükəsizlik-Şərq" (CyberSecurity EAST) layihələri "Şərq Tərəfdaşlığı" ölkələrinin cinayət ədaləti və təhlükəsiz cəmiyyətin kibertəhlükəsizlik və kibercinayətkarlıqla mübarizə ilə bağlı imkanlarını inkişaf etdirməkdə dəstək məqsədi daşıyır.

4.11. Azərbaycanda kibertəhdidlərin tədqiqinin vəziyyəti

Azərbaycanda kibertəhlükəsizlik və kibercinayətkarlığın təfərrüatlı təhlili üzrə çoxsaylı araşdırmalar aparılmadığı üçün sözügedən sahədə böyük boşluq mövcuddur. Bu səbəbdən Avropa İttifaqının təşəbbüsü ilə həyata keçirilən layihələri (EU4Digital, Cybersecurity, CyberEast və s.) qeyd etmək lazımdır. Mövcud tədqiqatlar kibertəhlükəsizlik siyasəti ilə bağlı

[23] Convention on Cybercrime, Budapest, 23.XI.2001. rm.coe.int

müxtəlif məsələlərin təsvirini təqdim edir.[24] Kibertəhlükəsizliklə bağlı akademik tədqiqatlar isə Azərbaycan Milli Elmlər Akademiyasının (AMEA) tabeliyində olan İnformasiya Texnologiyaları İnstitutunda aparılır. Azərbaycanın kibertəhlükəsizlik siyasəti və strategiyasının qiymətləndirilməsi üzrə rəsmi qurumlar səviyyəsində ətraflı tədqiqatlar hələ həyata keçirilməyib.

Müvafiq istiqamət üzrə özəl təşkilatların son dövrlərdəki fəaliyyətinə nəzər yetirdikdə, iki şirkət – Deloit Azərbaycan və Kasperski ölkədə kibertəhlükələrin təhlili ilə bağlı daha fəal görünür.

Deloit Araşdırma Mərkəzinin Bakı kiberkomandası 8 yanvar 2021-ci il tarixində ilk kibertəhlükəsizlik icmalını təqdim edib.[25] İcmal hədəf obyekti kimi Azərbaycanda fəaliyyət göstərən 26 bankı seçib. Araşdırma çərçivəsində onların internetdə açıq olan resursları öyrənilib. Burada lazımi meyarlar toplusu kibertəhlükəsizliyin qiymətləndirilməsində istifadə edilib: əlçatanlıq, domen reputasiyası, HTTP başlıqlarının təhlükəsizlik parametrləri, TLS və SSL təhlükəsizliyi, e-poçt sızması, açıq portlar, kibersquattinq və GDPR tələblərinə əsaslanan şəxsi məlumat təhlükəsizliyinə uyğunluq.

Tədqiqat nəticəsində müəyyən edilib ki, Azərbaycanda bəzi banklar bütün kibertəhlükəsizlik standartlarını və təcrübələrini tətbiq etmirlər. Təhlildə zəif təhlükəsizlik parametrlərindən və ya istifadəçi məlumatlılığının olmaması səbəbindən veb-serverlərdə həssas şifrələmə protokollarının istifadəsindən başlayaraq, nəticələrə dair müxtəlif faktlar qeyd edilib. Hesabatda araşdırma zamanı müəyyən edilmiş bütün problemlər işıqlandırılıb və onların mümkün həll yollarına aid tövsiyələr də təqdim edilib. "Biz icmalda tədqiqat nəticələrinin kritiklik səviyyəsini qiymətləndirmədik. Buna baxmayaraq, qlobal təcrübəmiz göstərir ki, kibersahədə heç bir risk kiçik deyildir. İnfrastrukturun qorunması üzrə ən yaxşı idarəetmə kursunun icrasına gəldikdə, bütün bank liderləri kibertəhlükəsizlik üzrə sükan arxasına keçmirlər. Bir çox banklar veb-serverlərini qurarkən standart təhlükəsizlik üzrə ən yaxşı təcrübələrə əməl etmirlər. Nəticədə, hətta xüsusi proqram təminatından istifadə etmədən də biz bir sıra banklarda mühüm nöqsanların mövcudluğunu aşkar etmişik. Üstəlik, bunların çoxu yeni problemlər və ya təzəcə yaranmış strukturun ilk sınaq günü pozuntuları deyil, kifayət qədər ənənəvi və bilinən kibertəhlükəsizlik məsələləri idi. Həmin çatışmazlıqlar əhəmiyyətsiz kimi görünsə də, onlar məxfi maliyyə məlumatlarının sızmasına və ya müştəri hesablarından vəsaitlərin birbaşa oğurlanmasına gətirib çıxara bilər. Eyni zamanda, bank işçilərinin kibertəhlükəsizlik məsələlərində qeyri-məlumatlılığının da şahidi olduğumuz hallar qeydə alınıb. Bu, banklarda tətbiq edilən mövcud kibertəhlükəsizlik siyasətlərinin və kibertəhsil proqramlarının zəifliyinin göstəricisidir. Əslində, düzgün maarifləndirmə səviyyəsinə yiyələnməyən bank işçisi tərəfindən uğursuz bir kliklәmə bütün bank məlumatlarını təhdid edə bilər".

Azərbaycandakı Kasperski şirkəti də son vaxtlar bir sıra sorğular keçirir. 2021-ci ilin yekununda apardığı sorğunun nəticələrini açıqlayan şirkət qeyd edib ki, son bir ildə Bakı, Sumqayıt və Gəncə şəhərlərində istifadəçilərin 87%-i kibertəhlükələrlə üzləşib. Bu, onu göstərir ki, adıçəkilən şəhərlərdə hər 10 istifadəçidən 9-u kibertəhlükələrə məruz qalıb: *"Təhlükələrin əksəriyyəti (80%) anlıq messencerlər (WhatsApp, SMS, Viber), 32%-i sosial şəbəkələr, 28%-i isə telefon zəngləri vasitəsilə meydana gəlib. Bundan başqa, dələduzların 27%-nin bank strukturlarını, 27%-nin şirkətləri, 17%-nin ticarət obyektlərini, 15%-nin isə onlayn platformaların satıcılarını saxta formada təmsil etdikləri məlumdur. Həmçinin, bu da aydındır ki, 34% hallarda dələduzlar guya lotereyadan uduşları köçürməyi, 25% hallarda investisiyalardan qazanc əldə etməyi, 14% hallarda isə sadə və mənfəət gətirən əməliyyatda iştirak etməyi təklif ediblər. Kiberdələduzlar kart məlumatları (36% hallarda), pul vəsaitlərinin kartdan karta köçürülməsi, vətəndaşların şəxsi və ödəniş məlumatları (21%) haqqında öyrənməyi hədəfləyərək, 16% hallarda qurbanlardan saxta keçidə (linkə) daxil olmağı xahiş ediblər".*[26]

2020-ci ildən bəri Ermənistanın mühari-

[24] Marcus Franda, Launching into Cyberspace: Internet Development and Politics in Five World Regions (London: Lynne Rienner Publishers,2002); Azerbaijan Cybersecurity Governance Assessment Author Ms. Natalia Spînu (2020). DCAF.Switzerland; K. Makili-Aliyev & Rehman. (2013). A.Cyber-Security Objective: Azerbaijan in the Digitalized World. SAM Review. - ict.az/en

[25] Azerbaijani banks cybersecurity review. Cyber Risk Advisory. 2020. Deloitte Research Centre.

[26] Azerbaijan talks cyberthreats faced by local users in several large cities. - en.trend.az/business

bədəki məğlubiyyəti və bəzi qisas cəhdləri səbəbindən kibertəhdidlər və kibermüharibə məsələləri davamlı narahatlıq doğuran hal kimi qalmaqdadır. Əvvəlki tədqiqat hesabatlarında da qeyd olunduğu kimi, "Şərq Tərəfdaşlığı"na üzv əksər ölkələr üçün kibertəhlükələrin əsas mənbələri xaricdəndir, çünki bu dövlətlərin demək olar ki, hər biri yaxın qonşuları ilə kifayət qədər mürəkkəb və çətin münasibətlərdə iştirak edirlər. Azərbaycan hakimiyyəti kibertəhlükəsizlik tədbirlərinin istər dövlət, istərsə də ümumi əhali səviyyəsində gücləndirilməsinin vacibliyini qəbul edir.

Ölkələrin kibertəhlükələrin qarşısının alınması və kiberinsidentlərin idarə edilməsindəki hazırlığını ölçən Milli Kibertəhlükəsizlik İndeksinə görə, Azərbaycan bu sırada 82-ci yerdədir. Digər indekslər üzrə Azərbaycanın mövqeyi belədir: Qlobal Kibertəhlükəsizlik İndeksində 40-cı, İKT İnkişaf İndeksində 65-ci, Şəbəkələşmiş Hazırlıq İndeksində 76-cı yer.[27]

"Qlobal Kibertəhlükəsizlik İndeksi 2020" (GCI) hesabatında Azərbaycan reytinqini 15 pillə yaxşılaşdıraraq 40-cı yerə yüksəlib. Ümumilikdə, müvafiq istiqamətdə Azərbaycan 89,31 balla MDB məkanında Rusiya və Qazaxıstandan sonra üçüncüdür.

5. Kəmiyyət tədqiqatı

5.1. Xülasə

Tədqiqat zamanı məlum olub ki, respondentlər arasında smartfon şəxsi ehtiyaclar üzrə ən çox istifadə edilən cihaz növüdür. Onların 73,3%-i cihazlardan istifadə edərkən bəzi ehtiyat tədbirləri gördüklərini bildiriblər. Sorğuda iştirak edənlərin 62,8%-i "kibercinayət" sözü ilə tanış deyil, qalan 37,1%-nin isə bu termin haqqında məlumatlı olması aydındır. Həmçinin, respondentlərin əksəriyyəti (86,7%) hesab edir ki, onlar onlayn cinayət fəaliyyəti hesab etdikləri hər hansı cəhdlərin hədəfinə çevrilməyiblər. Bu şəxslərə müvafiq anlayışın tərifi izah edildikdən sonra isə 74,3% belə cinayətlərin baş verdiyi barədə eşitdiyini ifadə edib. Sorğuda iştirak edənlərin 93,6%-nin "fişinq" sözü ilə tanış olmadığı məlum olub. Eyni zamanda, qurbanlar arasında əksəriyyətin (69,6%) bu hallardan ciddi təsirlənməyərək, yaranmış vəziyyəti narahatlıq kimi görmədiyi müəyyən edilib. Suallara cavab verənlərin yarıdan çoxu (52,7%) düşünür ki, özünü və ailəsini qorumaq üçün həmin kiberhadisə haqqında kifayət qədər məlumatlıdır. Digər istiqamət üzrə nəticələrə gəldikdə, respondentlərin 97,7%-nin "rənsamveə" sözü ilə tanış olmadığı müəyyən edilib. Bu terminin müvafiq izahından sonra respondentlərin 60,7%-i hesab edib ki, qonşuluqda kiməsə qarşı rənsamveə hücumu baş verərsə və onlar öz kompüterlərinə, mobil telefon və ya buradakı məlumatlarına, fotoşəkillərə giriş imkanını itirdikləri halda, bu barədə səlahiyyətli orqanlara/polisə məlumat verərlər. Respondentlərin demək olar ki, üçdə ikisi onlayn hədə-qorxu, zorakılıq-təhqir və sui-istifadə ilə bağlı sualları cavablandırmaqdan imtina edib. Bununla belə, respondentlərin 91%-i (bu kimi həssas mövzulara dair fikir bildirməyə razılıq ifadə edənlər) onlayn sui-istifadə/zorakılıq-təhqirə məruz qalmadığını bildirib. Əksəriyyət öz şəxsi hesablarına giriş məlumatlarının son 12 ayda onlayn şəkildə ifşa olunması (yayılması) ilə bağlı məlumatlı deyil. Sorğuda iştirak edənlərin 61,6%-i isə özünü və ailəsini onlayn şəxsiyyət (kimlik) oğurluğu hadisəsindən qorumaq üçün yetərli səviyyədə məlumatlı olduğu qənaətindədir. Respondentlərin olduqca az bir hissəsi buna məruz qaldığını qeyd etsə də, məlumatların məxfiliyinin pozulması və onlayn şəxsiyyət (kimlik) oğurluğu 40,6% respondent üçün ən çox narahatlıq doğuran kibercinayət növüdür.

Tədqiqatın nəticələrinə əsasən, müəssisə və qurumların əhəmiyyətli hissəsinin kibertəhlükəsizliyə cavabdeh olan xüsusi təşkilati rolu /vəzifəsi və ya departamenti mövcud deyil. İT büdcəsi daxilində kibertəhlükəsizliyə çəkilən xərclərin həcmi isə ümumiyyətlə aşağıdır və əksər müəssisələrin sığortası yoxdur.Tədqiqat nümunəsində rast gəlinən ISO 27001 standartları ən geniş yayılmış təhlükəsizlik təlimatı/çərçivəsidir. Şirkətlərin çoxu daxili strategiyaya uyğun olaraq kibertəhlükəsizliyə aşağı, yaxud ümumiyyətlə mövcud olmayan səviyyədə yanaşma nümayiş etdirirlər. Hal-hazırda istifadə edilən kibertəhlükəsizlik texnologiyalarının əksəriyyəti sırasında viruslardan, casus və digər zərərli proqramlardan müdafiə üzrə həllərə/proqram təminatlarına üstünlük verilməsi məlumdur. Bu mənada spam/fişinq

[27] National Cybersecurity Index – Azerbaijan. 17 Mart 2020

filtrasiyası, məlumatların qorunması və onlara nəzarət tədbirləri müvafiq sırada növbəti cavabları təşkil edir.

Kibercinayətkarlığın qurbanı olma ilə bağlı suallara verilən cavablar müəssisə və təşkilatlar arasında zərərçəkmə səviyyəsinin çox aşağı olduğunu üzə çıxarır. Bu baxımdan, respondentlərin müvafiq olaraq 45,3%-i və 46,9%-i qabaqcıl təhlükəsizlik texnologiyaları və sərf edilən irimiqyaslı büdcələrin lazımi istiqamətdə tətbiqinin təşkilatların müdafiəsini yaxşılaşdırmağa kömək edəcəyini düşünür. Tədqiqatın nəticələri sübut edir ki, rəyi soruşulan qurumların 65,6%-i noutbuklarda fayl şifrələməsindən istifadə edir. COVID-19 pandemiyasının müəssisələrə qarşı kibercinayətkarlıq hallarını kəskinləşdirməsi ilə əlaqədar cavablar isə demək olar ki, bərabər şəkildə bölünüb.

5.2. Texniki məlumat – respondentlərin strukturuna ümumi baxışı təmin etmək üçün diaqramlar təqdim edilir

5.3. Tədqiqatın metodologiyası - tədqiqatla bağlı şərtlərdə təsbit edilib və bütün ölkə üzrə xüsusiyyətlər təqdim edilir

Tədqiqat dizaynı: Çarpaz tədqiqat dizaynı tətbiq edilib.

Seçmə nümunəsi və əhatə dairəsi

Sosioloji tədqiqat zamanı sorğu aparılmasının üz-üzə (face to face) müsahibə metodunun təşkili üçün bütün inzibati rayonları əhatə edən əhali üzrə milli reprezentativ anketdə ümummilli miqyasda klaster seçmə nümunəsi tətbiq edilib. Ölkədə həyata keçirilmiş ən son siyahıya alınmaya (2020-ci il) əsasən, əhalinin sayı 10.067.100 nəfər olaraq qeydə alınıb. Sorğuda hədəf əminlik intervalı və xəta əmsalı müvafiq şəkildə 95% və 3%-dir (və ya daha az). İnzibati rayonlar üzrə üç yaşayış məntəqəsi tipi - şəhər, rayon və kəndlər əhatə olunub ki, onların bölgüsü müvafiq cədvəldə təqdim edilir.[28]

Avropa Şurası tərəfindən müəyyən edilmiş meyarlara uyğun olaraq xüsusi bir nümunə istifadə edilib. Sorğunun aparılmasında seçki dairəsi, ev təsərrüfatları, o cümlədən fərdlər səviyyəsində üç mərhələdə təbəqəli model tətbiq edilib. İntervüyerlər respondentlərin evlərində üz-üzə qaydada anket sorğusu aparıblar. Sorğuda iştirak etmək üçün hər ailədən yalnız bir respondent seçilməklə, gender-yaş və gender-təhsil kvotaları nəzərə alınıb. Ümumilikdə, 1600 respondentdən ibarət yekun seçmə üzrə əlaqə saxlanılanların cavab nisbəti 48%-dən ibarət olub.

Məlumatların toplanılması

Tədqiqat məlumatlarının toplanılması üzrə üçbucaqlılıq ilə nəticələn iki üsul müəyyən edilib. Data yığılmasının birinci mərhələsində ölkə üzrə 1600 respondent arasında üzbəüz sorğu keçirilib. Sorğunun orta davametmə müddəti təqribən 13 dəqiqə (median = 12.50 dəqiqə, standart deviasiya = 3.36 dəqiqə) təşkil edib.

Müəssisə və təşkilatlarla sorğunun aparılmasına gəldikdə, 64 respondent arasında üzbəüz sorğu keçirilib. Bu rəqəmin 100-dən aşağı olmasının əsas səbəbləri aşağıdakılardır: a) əlaqə saxlanılan bir çox şirkətlərdə/qurumlarda İT-dən istifadə çatışmazlığı; b) həvəsləndirici amillərin çatışmazlığı; c) sorğuda iştirak üçün rəsmi məktubla müraciət edilən şirkətlərdən cavab alınmasının gecikməsi.

Sorğunun sahə işinin aparılmasına 20 intervüyer cəlb olunub. İntervüyerlər seçmə üzrə müəyyən edilmiş ev ünvanlarına üz tutmaqla sorğu anketindəki sualları iştirakçılara (respondentlərə) birbaşa təqdim ediblər. Sorğuda iştirak barədə respondent razılığı əldə olunduqdan sonra ev təsərrüfatları və ya ailədə 18 yaşdan yuxarı bir nəfər tərəfindən suallar cavablandırılıb. Mümkün qədər əhalinin bütün təbəqələrinin sorğuda iştirakının əhatə olunması üçün sorğu həftənin müxtəlif günlərində və günün müxtəlif vaxtlarında aparılıb.

Təhlil

Sorğu nəticəsində toplanılan məlumatlar SPSS (Statistical Package for the Social Sciences/Sosial Elmlər üzrə Statistik Paket) proqramı vasitəsilə təhlil edilib.

[28] Yaşayış məntəqələrinin rəsmi təsnifatında şəhər əhalisinin sayı 15.000 nəfərdən çox olan və işçi qüvvəsinin böyük hissəsi sənaye və büdcədən maliyyələşən təşkilatlarda çalışan coğrafi vahiddir (Dövlət Statistika Komitəsi, 2019-cu il)). Bir rayon və ya daha kiçik ərazi-inzibati vahid isə əhali sayının maksimum 15.000 nəfər təşkil etdiyi bir yaşayış məntəqəsini nəzərdə tutur. Kəndlərin əhalisinin səviyyəsi müxtəlifdir.

Etik məsələlər

Sorğu zamanı respondent cavablarının anonimliyi (konfidensiallığı) qorunub. Fokus qruplarda iştirak edən bütün iştirakçılar ad və soyadlarını qeyd etməklə, öz imzalarını təqdim ediblər. Zum (zoom) onlayn proqramı vasitəsilə sorğuya qoşulanlar hansısa qaydada imza etməyib.

Sorğu suallarının müzakirəsinə başlamamışdan öncə respondentlər məlumatlandırılıb, onlardan sorğuda iştirak haqqında razılıq alınıb.

Təlimlərin təşkili

İntervüyerlər (sorğunu aparan təlimatlandırılmış şəxslər) sahə işi üzrə çoxillik təcrübəyə malik olmaqla, əksəriyyətinin sosiologiya, psixologiya və sosial iş istiqamətində təhsil dərəcələri vardır. Sahə işi başlamamışdan əvvəl bütün intervüyerlərə sorğu layihəsinin koordinatoru və meneceri tərəfindən təlim keçirilib. Daha sonra onlardan öz aralarında test sorğusu keçirmələri tələb edilib, ardınca pilot tədqiqat aparılıb.

Sahə işi

Sahə işinin aparılması əsasən maneəsiz davam etsə də, qarşıya çıxan ən ciddi problem bir sıra kəndlərdə (xüsusən, dağlıq ərazilərdə) internetin demək olar ki, tamamilə olmaması ilə bağlı olub. Bu, məlumatların toplanılmasına başlandıqdan sonra intervüyerləri müxtəlif seçmə nöqtələrinə keçməyə sövq edən amildir. Tez-tez rast gəlinən digər məqam isə bəzi insanların (xüsusən, ucqar kəndlərdə) internetdən ilk növbədə yalnız müəyyən məqsəd və fasilələrlə, məsələn, lazım olduqda Votsap (WhatsApp) mesajlaşmaları və ya Yutub (YouTube) platformasına baxılması üçün istifadə etmələridir. Belə fərdlər əsasən passiv istifadəçilər hesab olunurlar. Onlar sorğuda uyğunluq təşkil etməsələr də, bu kimi iştirakçılarla əlaqəli qeyd edilən hal sahə işinin müddətinin müəyyən dərəcədə uzanmasına səbəb olan faktordur.

Müəssisə və şirkətlərlə işin aparılması baxımından ən böyük maneə isə şəhərlərdən kənarda yerləşən qurumlar (şirkətlər) tərəfindən İT təhlükəsizlik tədbirlərinin olduqca məhdud səviyyədə tətbiqi ilə bağlıdır. Beləliklə, kənd ərazi vahidlərində yerləşən müəssisələrlə aparılan müsahibələr zamanı və sahə işinin əvvəlində ilkin məlumatlar təhlil edilərkən data toplanılmasının əhəmiyyətli dərəcədə gecikdirilməsinə gətirib çıxaran məqam aydın olub. Bundan başqa, bizneslərin əksəriyyətinin oflayn qaydada həyata keçirilməsi nəticəsində sorğuda iştirak edən müəssisələrin nadir hallarda İT təhlükəsizlik tədbirlərindən istifadəyə meyilli olması məlum olub. Məhz bununla əlaqədar olaraq belə tipli müəssisələri təmsil edən nümayəndələr sorğu zamanı bir çox suallara cavablar təqdim etməyiblər. Sorğu prosesində data toplanılmasının daha səmərəli şəkildə baş tutması üçün seçmənin ikinci mərhələsi təşkil edilib.

5.4. ÜMUMİ ƏHALİ QRUPU

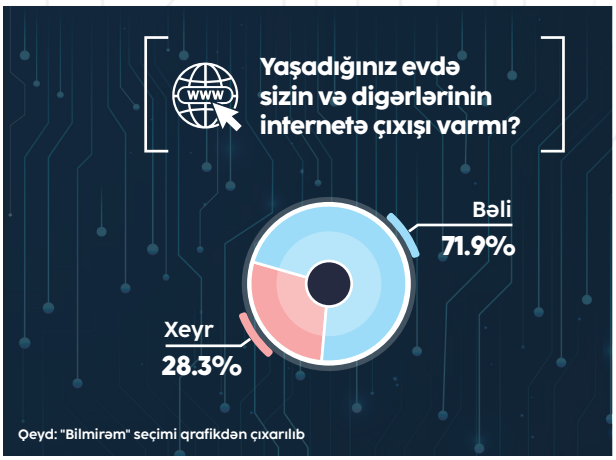
5.4.1. İnternetdən istifadə

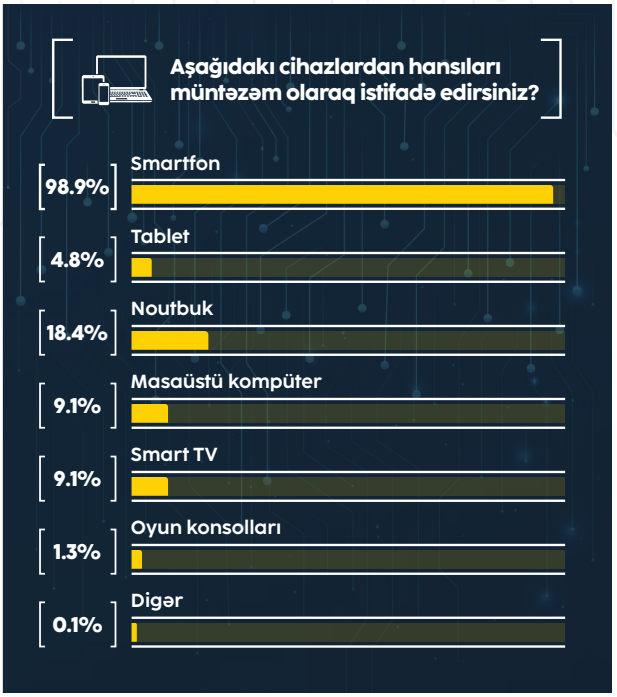
5.4.1.1. Onlayn fəaliyyətlər

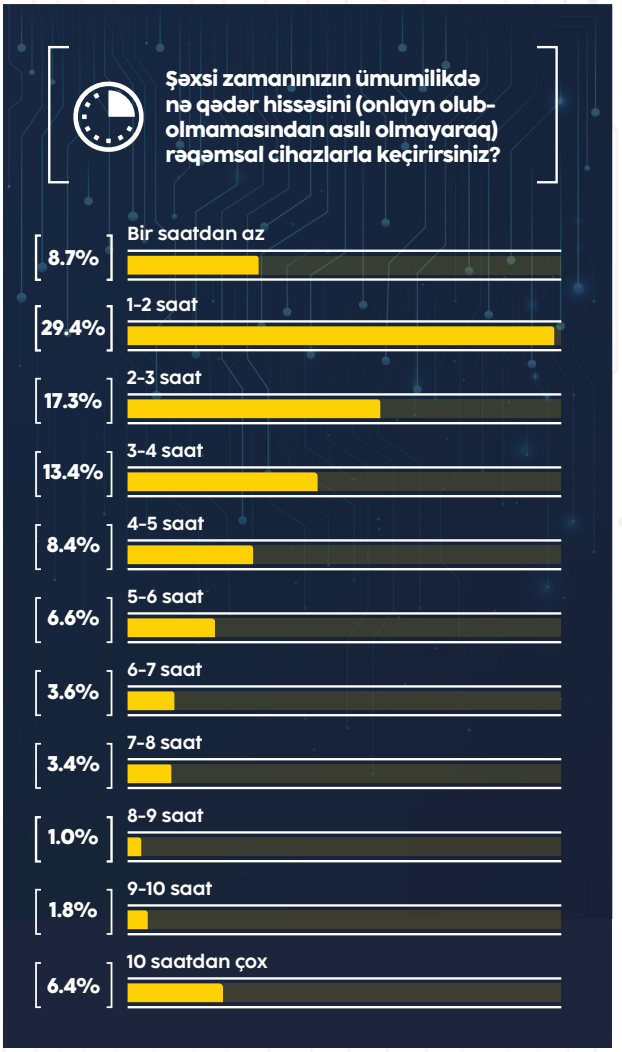
Əlaqə saxlanılmış əhali sayı (2283) üzrə sorğuda ev təsərrüfatlarının 71,9%-nin (1643 nəfərin) internetə çıxışının olduğu məlum olub. Respondentlərin 28.3%-nin isə internetə heç bir çıxışı olmayıb.

Şəhər əhalisinin internetə çıxış imkanlarının geniş olması sorğunun nəticələrində də öz əksini tapıb.

Nəticələrə əsasən, smartfonlar şəxsi ehtiyaclar üzrə ən çox istifadə edilən cihaz növüdür (98,9%). Bakı şəhəri və Aran rayonları (əhalinin ən çox yaşadığı iqtisadi rayonlar) daxil olmaqla, coğrafi yerləşmə amili və şəxsi istifadə cihazlarının növləri arasında korrelyasiya mövcuddur. Ümumilikdə, smartfon və kompüter istifadəçilərinin 81%-ni şəhərlərdə yaşayanlar təşkil edir.

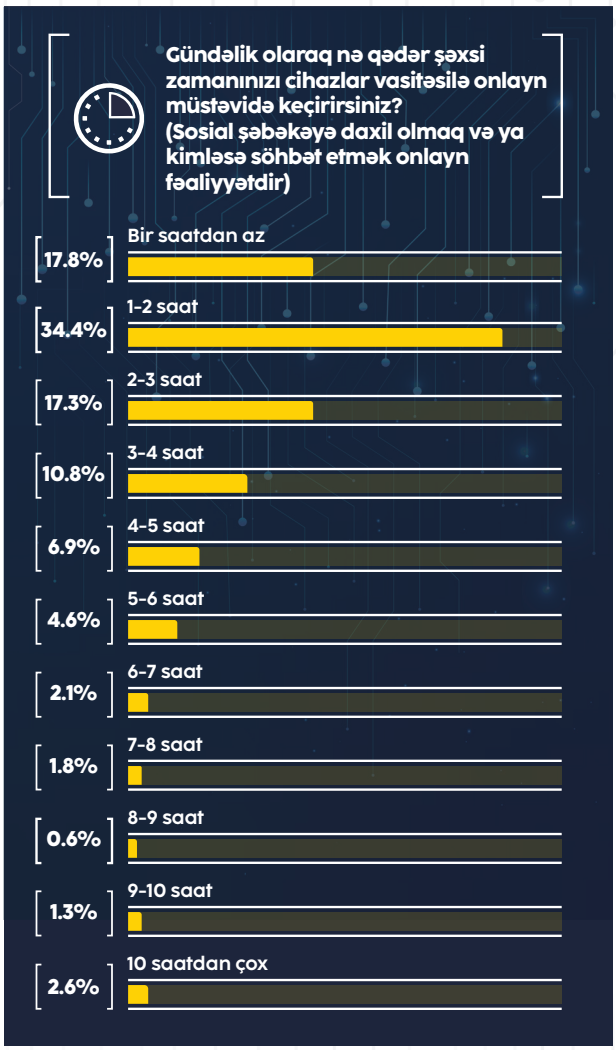






Seçmənin 29,4%-i onlayn olub-olmamasından asılı olmayaraq şəxsi zamanının 1-2 saatını rəqəmsal cihazlardan (smartfon, tablet, kompüter və s.) istifadəyə həsr edir. Bu versiya cins, yaş tərkibi, təhsil, coğrafi amil kateqoriyaları üzrə ən çox üstünlük verilən cavabdır. Respondentlərin 17,3%-i 2-3 saat, 13,4%-i 3-4 saat vaxtını rəqəmsal cihazlarla keçirir. Bir saatdan az vaxt keçirənlərin faiz göstəricisi isə 8,7%-dir.

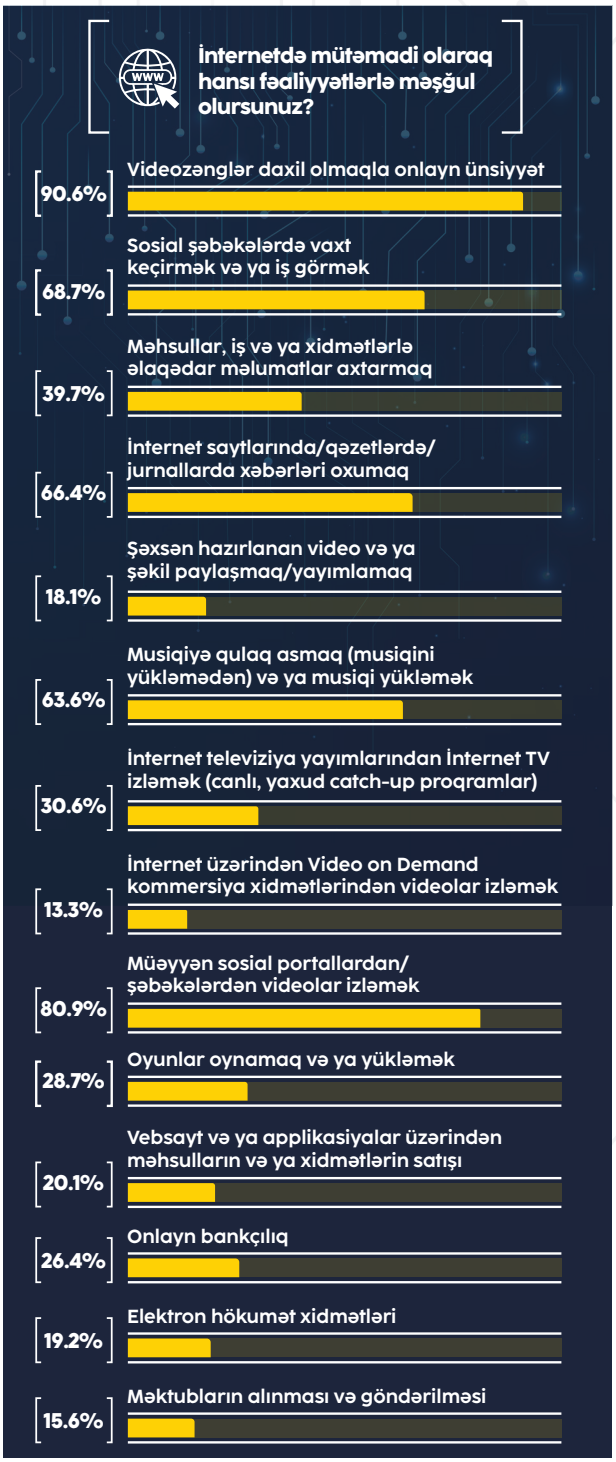
Bu nəticə onlayn rejimdə keçirilən ümumi vaxt müddətilə müəyyən qədər yaxın göstəricidir. Belə ki, cavablara əsasən respondentlərin 34,4%-i gündəlik cəmi 1-2 saat vaxtını onlayn rejimdə keçirir. Sorğu iştirakçılarının 17,3%-i 2-3 saat, 10,8%-i 3-4 saat onlayn rejimdə olur. Seçmənin cəmi 17,8%-nin onlayn rejimdə keçirdiyi vaxt müddəti 1 saatdan az olur.



İnternet vasitəsilə onlayn ünsiyyət (videozənglər daxil olmaqla) ən geniş yayılmış (90,6%) onlayn fəaliyyət növüdür. Kənd sakinlərinə nisbətən şəhər sakinləri rəqəmsal cihazlarda 4 saatdan çox onlayn olur. Buna əsasən şəhər sakinlərinin kibertəhlükələrlə bağlı daha çox risk qrupunda olduğunu demək mümkündür. Digər tərəfdən, ən geniş yayılmış cavablardan biri Video on Demand - VOD (istənilən anda istənilən videoya baxmaq imkanı) kommersiya xidmətlərindən videolar izləmək (məsələn, Netflix, HBO, GO, Amazon Prime, YouTube və s.) üzrə göstəricidir (80,9%) ki, bu statistika kibercinayətə məruzqalma riski nisbətən aşağı hesab edilən onlayn fəaliyyətdir.

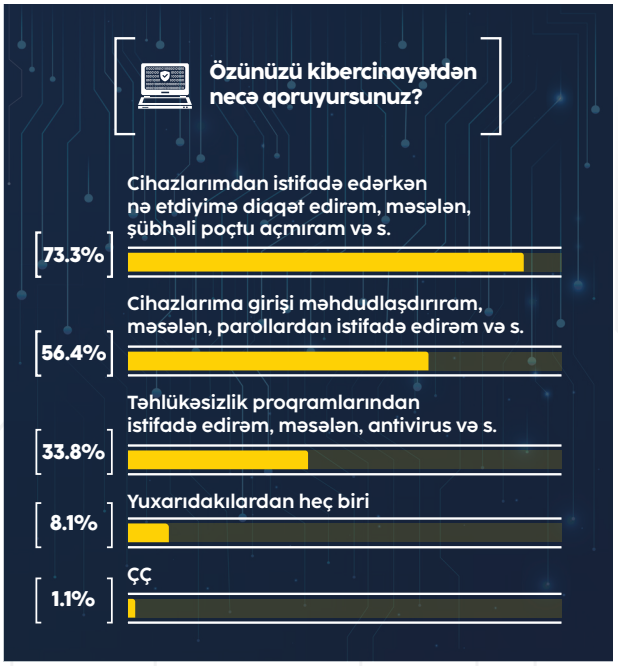
Bundan başqa, respondentlərin 68,7%-i internetdən sosial şəbəkələrdə vaxt keçirmək, 66,4%-i onlayn qəzet və jurnallarda xəbərləri oxumaq, 39,7%-i məhsullar, iş və ya xidmətlərlə bağlı məlumatlar axtarmaq, 28,7%-i oyunlar oynamaq və ya yükləmək, 26,4%-i onlayn bankçılıq məqsədilə istifadə edir.

Sorğu nəticələrinin bir neçə kateqoriya üzrə təhlili göstərir ki, vebsayt və ya applikasiyalar üzərindən məhsulların və ya xidmətlərin satışı, elektron hökumət xidmətlərindən istifadə və onlayn bankçılıq cavab variantları daha çox kişi respondentlər tərəfindən seçilib. E-mail göndərmək və ya qəbul etmək tələbələr arasında, internet vasitəsilə zənglər etmək, sosial şəbəkələrdə vaxt keçirmək və ya iş görmək, oyunlar oynamaq və ya yükləmək tam orta təhsili olan respondentlər arasında geniş yayılıb.



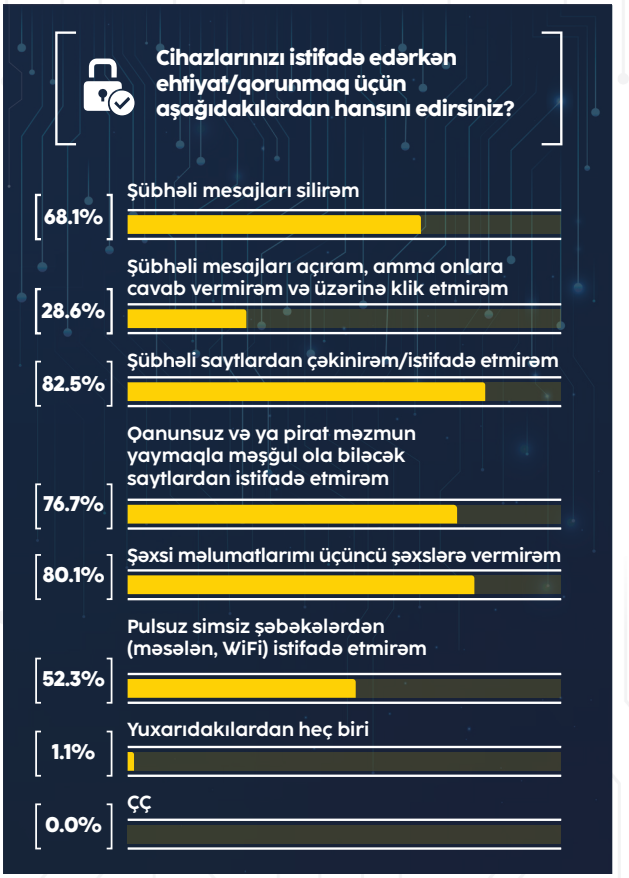
Zərərçəkmə amilinə dair risklərdən danışarkən, respondentlərin 73,3%-i cihazlardan istifadə etdikdə bəzi ehtiyat tədbirləri gördüklərini ifadə edib. Bu baxımdan, cihazlara giriş məhdudiyyətinin tətbiqi ən geniş yayılmış (56,4%) tədbirlərdən biri olmaqla, seçmədə 18-24 yaşlılar və tam orta təhsili olan respondentlər arasında daha aktual cavabdır. Demoqrafik göstəricilərlə korrelyasiya üzrə gender aspektindən baxdıqda, əsasən kişi respondentlər tərəfindən sorğu anketində sadalanan bütün müdafiə tədbirlərinin görülməsi ehtimalı daha yüksək nəzərə çarpır. Ümumilikdə isə internetdə 4 saatdan çox vaxt sərf edən şəxslərin sorğu anketində qeyd olunan hər bir qoruyucu tədbiri həyata keçirməsi ehtimalı daha yüksək səviyyədə müşahidə edilib. Belə hal peşə təhsili və bakalavr dərəcəsi olan respondentləri də əhatə edir.

Qeyd edildiyi kimi, kibercinayətdən qoruma üsulları kimi respondentlərin 56.4%-i şəxsi cihazlarına girişi məhdudlaşdırdığını (məsələn, paroldan istifadə etməklə), 33.8%-i təhlükəsizlik proqramlarından (məsələn, antivirus və s.) istifadə etdiyini qeyd edib.

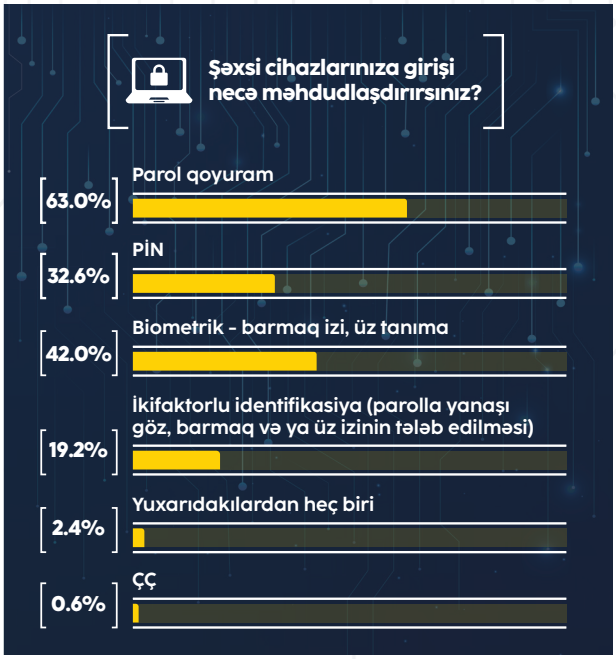


Cihazlardan istifadə edərkən müntəzəm olaraq tətbiq edilən ən geniş yayılmış davranış şübhəli saytlardan yayınmaqdır (82,5%). Sorğuda respondentlərin yalnız üçdə birinin zərərli proqramlara qarşı tətbiqlərdən (məsələn, antivirus) istifadə etməsi faktı isə narahatlıq doğurmaqla yanaşı, bu istiqamətdə məlumatlılığın artırılmasının zəruriliyini də sübut edir. Yuxarıdakı suallarla bağlı fokus qrup və əhali ilə keçirilən sorğu arasında hər hansı mühüm fərq müşahidə edilməyib.

Bundan başqa, respondentlərin 80,1%-i cihazlardan istifadə edərkən ehtiyat (qorumaq) məqsədilə şəxsi məlumatlarını üçüncü şəxslə (digər insanlarla) bölüşmür, 68,1%-i şübhəli mesajları silir, 76,7%-i qanunsuz və ya pirat məzmun yaymaqla məşğul ola biləcək saytlardan istifadə etmir, 52,3%-i pulsuz simsiz şəbəkələrdən (məsələn, vayfay (Wi-Fi)) istifadə etmir. Qeyd edək ki, bu sualda respondentlərə bir neçə cavab variantını seçmək imkanı verilib.

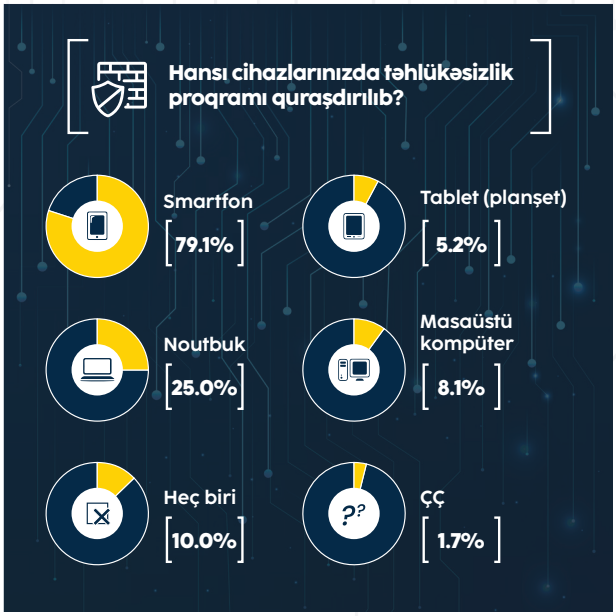


Şifrədən (paroldan) istifadə şəxsi cihazlara daxil olarkən ümumilikdə ən çox tətbiq edilən giriş məhdudiyyəti/mühafizə üsuludur. Respondentlər tərəfindən qeyd edilən digər üsullar biometrik (barmaq izi, üz tanıma) (42.0%), PİN kod (32.6%), ikifaktorlu identifikasiyadır (yəni parolla yanaşı göz, barmaq və ya üz izinin tələb edilməsi) (19.2%). İkifaktorlu identifikasiyadan istifadə daha çox tam orta təhsili olanlar və kişi respondentlər tərəfindən qeyd olunub.



Fokus qruplar üzrə də bu cavab geniş yayılıb. Sorğu iştirakçılarının üçdə biri PİN kodu qeyd edib, lakin digər əhali qrupları arasında bu cavab variantına demək olar ki, rast gəlinməyib.

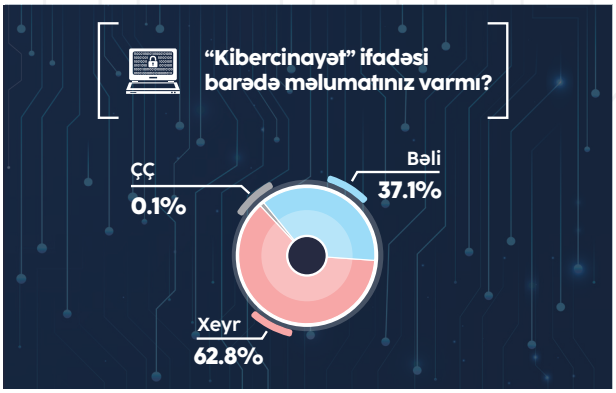
Nəticələrə əsasən, smartfon istifadəçilərinin əksəriyyəti (79,1%) cihazlarında müvafiq məqsədlə təhlükəsizlik proqramı quraşdırıb. Respondentlərin 25,0%-i noutbuklarında, 8,1%-i masaüstü kompüterlərində, 5,2%-i isə planşetlərində təhlükəsizlik məqsədilə proqramlar yazdırıblar.



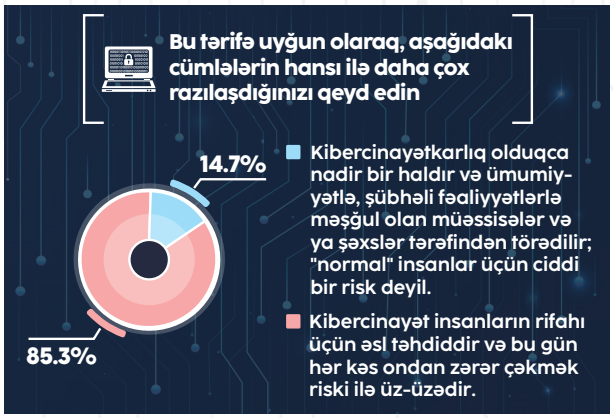
5.4.2. Kibercinayətkarlıq üzrə bilik səviyyəsi

5.4.2.1. Məlumatlılıq

Sorğunun nəticələrinə əsasən nisbətən geniş kütlənin (62,8%) "kibercinayət" sözünə bələd olmadığı məlum olur. Respondentlər arasında bu anlayışla bağlı məlumatlılıq səviyyəsi 37,1% təşkil edir.



Müvafiq anlayışa dair izahla tanış edildikdən sonra isə 85,3% respondent "Kibercinayət insanların rifahı üçün əsl təhdiddir və bu gün hər kəs ona hədəf olmaq riski ilə üz-üzədir" cavabını seçib. Nəticələrin təhlilinə əsasən, kişi qrupuna aid respondentlər, şəhər sakinləri, həmçinin bakalavr, yaxud magistr dərəcəsinə malik olanlar və eyni zamanda, ağıllı telefon və kompüter isifadəçiləri "kibercinayət" sözü ilə nisbətən daha yaxşı tanışdır.



Fokus qruplara nəzər yetirdikdə, seçmədə bütün respondentlərin "kibercinayət" sözünü bilməsi (məktəb, bank təlimi, jurnalistika, 2020-ci ildə Ermənistanla müharibə və s. kontekstində), o cümlədən təqdim edilmiş əlaqəli cinayət növlərinin bir çoxu haqqında təsəvvürləri müşahidə edilsə də, zərərçəkmə baxımından geniş yayılmış fişinq – elektron dələduzluq, eləcə də rənsamveə - məlumatların girov saxlanılması hal-

larına dair məlumatlılıq səviyyəsi mövcud deyil. Digər tərəfdən, respondentlərin belə hadisələri onlara müvafiq izah təqdim edildikdən sonra tanımaları da diqqətçəkən amillər sırasındadır.

"Kibercinayət" sözünün qavranılması ilə bağlı "internet cinayətləri" və "informasiya cinayətləri" ifadələrini ümumi əhali qrupları və QHT nümayəndələri mövzu üzrə məsələləri hərtərəfli əhatə edən anlayışlar kimi tez-tez ifadə ediblər. Lakin İT mütəxəssislərinin və hüquq-mühafizə orqanlarının nümayəndələrinin kibercinayət barədə biliklərinin ÜƏQ-lərin baxışlarından tamamilə fərqlənməsi də qeydə alınan vacib məqamdır. Belə ki, birincilər üçün kibercinayət sadəcə cəhd deyil, məqsədə nail olunan hər hansı cinayət əməlidir. Həmçinin, iştirakçıların bir qrupu müvafiq terminin olduqca mürəkkəb və detallı növləri haqqında da söhbət açıblar. Onlar müzakirə olunan bütün cinayət kateqoriyaları üzrə dərin məlumatlılığa malik olduqlarını nümayiş etdiriblər. Digər fokus qrupuna daxil olan hüquq-mühafizə orqanları əməkdaşlarının yanaşmasına əsasən, kibercinayət başqa cihazlardakı informasiyanın və mənbələrə giriş imkanının korlanmasını, yaxud məlumat sistemlərinin bütövlüyünün zədələnməsini əhatə edir.

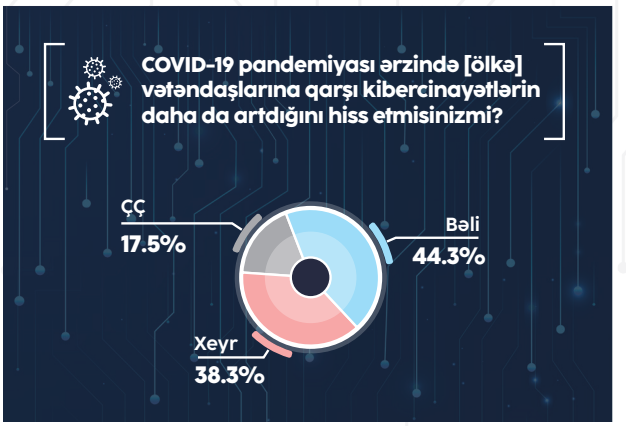
"Fikrimcə, əsl kibercinayət bütün sistemlərə - virus əleyhinə proqramlar və qurduğumuz təhlükəsizlik divarına nüfuz edən hallardan ibarətdir. Hesab edirəm ki, həqiqi cinayət bizi müdafiəsiz edir. Lakin hər gün qarşılaşdığımız və sistemlərin məruz qaldığı sadə hücum və ya problemlər bizim üçün bu mənada yüksək əhəmiyyət kəsb etmir" – deyə İT mütəxəssisləri və QHT qrupunun respondentləri bildirib.

"Kibercinayət fəaliyyətləri və buna dair potensial hər yerdə mövcuddur. İnternet, bankomatlar, kart ödəniş terminalları və s. burada vacib yer tutur. Əgər sistemlərin idarə edilməsində insan faktoru, yəni idarəedici məsul şəxs varsa, bu halda, təhlükəsiz şərait yoxdur və sistemin işində boşluğun yaranmasına meyillilik istisna deyil" – deyə onlar əlavə ediblər.

İnternet xidməti provayderi (təminatçısı): *"Bizim üçün belə vəziyyətlər mənfəət və nüfuz itkisi deməkdir. Hücumlar səbəbindən sistem çökdükdə telefonlarımız susmur. Bu baxımdan, şirkətlərin əməliyyatlarını saatlarla dayandırma məcburiyyəti ilə üzləşdiyi halların şahidi olmuşam".*

ÜƏQ-lərin fikrincə, kibercinayət dedikdə, əksər hallarda insanların pullarının və şəxsi məlumatlarının oğurlanması nəzərdə tutulur.

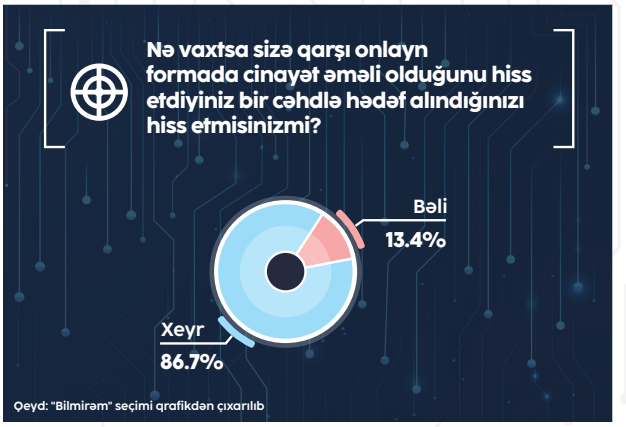
İnsanların çoxu (44.3%) hesab edir ki, COVID-19 pandemiyası ilə əlaqədar vətəndaşlara qarşı kibercinayətkarlıq halları daha da artıb. Bu fikir əsasən 18-24 yaş qrupunu təmsil edən respondentlər tərəfindən səsləndirilib. Respondentlərin 38,3%-i bu fikrin əksini düşünsə də, 17,5%-i bu suala cavab verməkdə çətinlik çəkib.



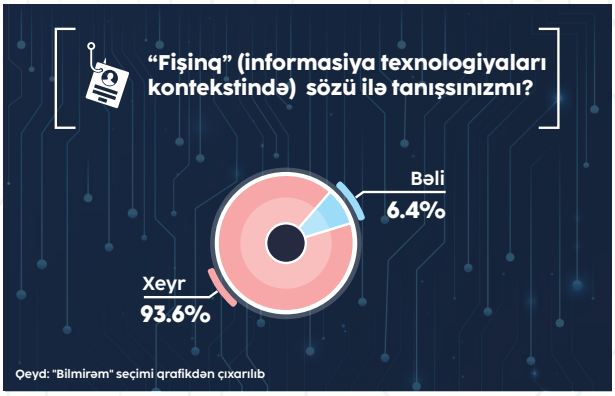
5.4.2.2. Fişinq (phishing)

Respondentlərin əksəriyyətinin (86,7%) fikrinə əsasən, onlar kompüter və ya onlayn cinayət cəhdlərinin hədəfi olmayıblar. Bu göstərici onu deməyə əsas verə bilər ki, elektron dələduzluq halları ümummilli miqyasda ciddi narahatlıq yaradan problem deyil. Həmçinin, kibercəhdlər və demoqrafik göstəricilər arasında əhəmiyyətli korrelyasiyanın qeydə alınmaması da sözügedən hadisələrə məruzqalma ehtimalı daha yüksək hər hansı qrupun olmadığını üzə çıxarır.

Respondentlərin cəmi 13,4%-i nə vaxtsa kompüter və ya onlayn cinayət cəhdlərinin hədəfi olduğunu düşünür.



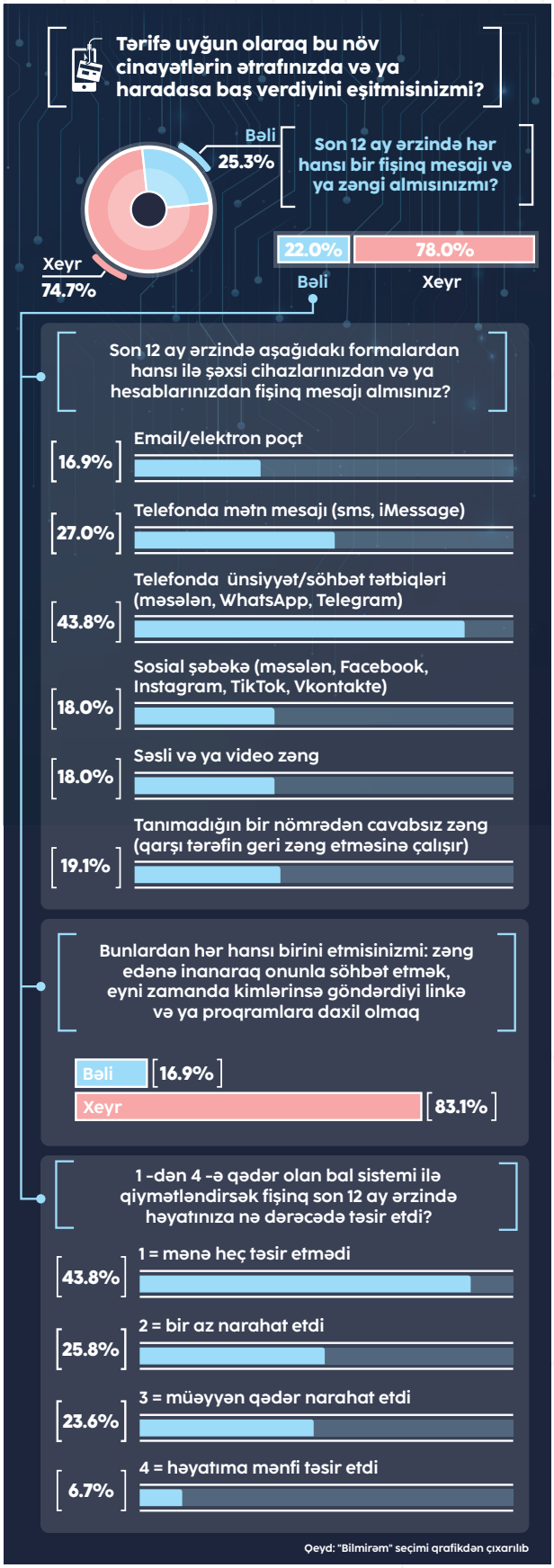
Sorğunun nəticələrindən aydın olur ki, respondentlərin az bir hissəsi (6,4%) "fişinq" (phishing) sözü ilə tanışdır. Bu anlayışla bağlı heç bir məlumatı olmayanlar isə kifayət qədər çoxluq təşkil edir (cəmi 93,6%)



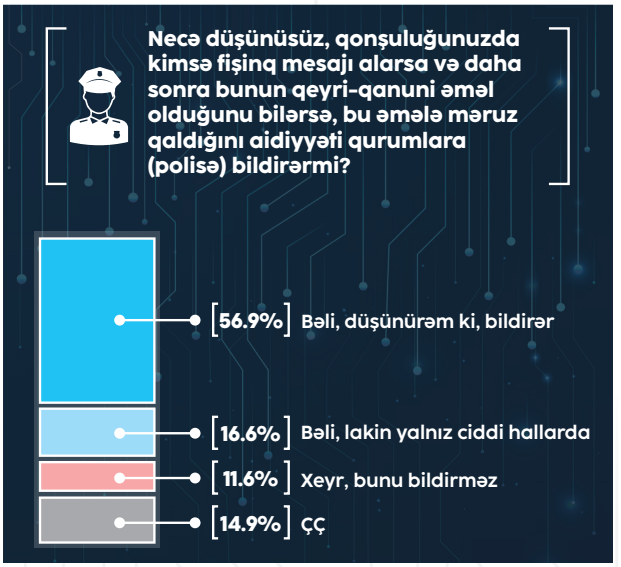
Korrelyasiya baxımından magistr təhsil dərəcəsinə malik olanlar və ağıllı telefon, həmçinin, kompüter istifadəçiləri bu barədə daha məlumatlıdır. Bakalavr və magistr dərəcəsi olanların müvafiq surətdə təxminən üçdə biri və yarısı bu cür cinayətlərin baş verməsi haqqında heç vaxt eşitmədiyini bəyan edib. Beləliklə, bu kimi hallarla (elektron dələduzluq məqsədli mesaj və ya zənglərin qəbulu) bağlı yüksək korrelyasiya müşahidə edilməyib.

Müvafiq suala verilən cavablardan məlum olur ki, canlı xidmət təklifi üzrə özünü texnologiya şirkətinin nümayəndəsi kimi təqdim edən hər hansı şəxs tərəfindən respondentlərin böyük əksəriyyəti ilə (94,1%) əlaqə saxlanılmayıb.

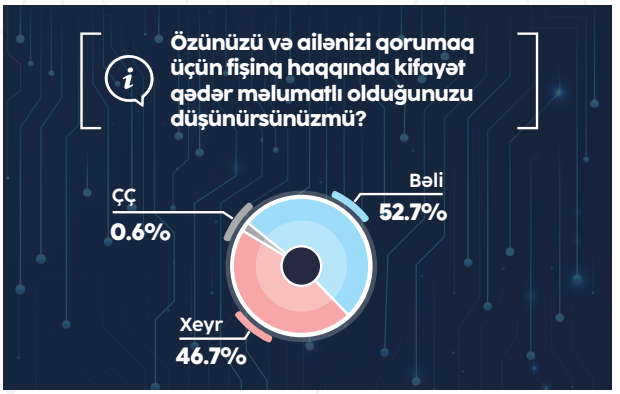
Müvafiq anlayışa dair izah təqdim edildikdən sonra da respondentlərin 74,7%-i bu tipli cinayət hallarının baş verməsi haqqında eşitmədiklərini bildirib. Lakin cavab verənlərin müəyyən hissəsi ötən 12 ay ərzində sözügedən məzmunlu mesajlar aldığını (xüsusilə elektron poçt və sosial şəbəkələr vasitəsilə) qeyd edib. Zərərçəkənlərə gəldikdə isə nəticələrdən aydın olur ki, əksəriyyətinin həyatı belə hadisələrdən ciddi şəkildə təsirlənməyib və ya onlar bunu narahatlıq kimi qəbul etməyiblər.



Respondentlərin yarıdan çoxu (56,9%) hesab edir ki, qonşularından kimsə fişinq mesajı alarsa, zərərçəkənlər bu barədə səlahiyyətli orqanlara, yaxud polisə məlumat verərlər. Bununla bağlı sosial-demoqrafik xüsusiyyətlər üzrə hər hansı əhəmiyyətli korrelyasiya aşkar edilməyib. Respondentlərin 22,1%-i ölkədəki fişinq cinayətlərinə dair sadəcə təşviş hiss etsə də, onların yarısı mövzu ilə bağlı olduqca narahatlıq keçirdiklərini bildiriblər. Gənc respondentlərin fişinq fəaliyyətləri ilə əlaqədar həyəcanlı olmaları ehtimalı isə özlüyündə daha yüksəkdir. Eyni zamanda, nəticələr sübut edir ki, belə hadisələrlə əlaqədar narahatlıq dərəcəsi artdıqca respondentin sorğu anketində sadalanan bütün qabaqlayıcı tədbirlərdən istifadə ehtimalı da müvafiq olaraq yüksəlir.



Respondentlərin 52,7%-i özünü və ailəsini qorumaq üçün fişinq haqqında kifayət qədər məlumatlı olduğunu düşünür. Rəyi soruşulanların 46,7%-i isə bunun əksini qeyd edib.



Fokus qrup iştirakçılarının demək olar ki, hamısı fişinq cəhdləri ilə üzləşdiyini qeyd edib. ÜƏQ-lərdə yalnız beş zərərçəkmə halının məlum olması müəyyən mənada məsələ ilə əlaqədar insanların özləri və iş yerlərini necə qoruması ilə bağlı məlumatlılıq səviyyəsini göstərir. Digər tərəfdən, zərərçəkmişlərin öz təcrübələrini paylaşması da belə hallara hansı formada məruz qalmaları və bununla bağlı müvafiq yerlərə məlumat bildirmə vərdişlərinə dair hadisələrə işıq tutulması istiqamətində faydalı ola bilər.

"İşədüzəltmə şirkətlərindən birində marağımı ifadə edərək qeydiyyatdan keçdim. Bir nəfər mənə zəng edib, iş axtarmağım barədə məlumat aldı. O, qeydiyyatda olduğum işədüzəltmə şirkətinin nümayəndəsi deyildi və bir ad tələffüz etdi ki, mən hazırda həmin adı unutmuşam. İstənilən halda, sözügedən şəxs məndən 150 manat depozit tələb etdi. Əvvəlcə tərəddüdlü olmağıma və onunla şəxsən görüşərək qeyd edilən məbləği ödəməklə bağlı təkid etməyimə baxmayaraq, həmin şəxs məni olduqca yaxşı inandırdı. Bu səbəbdən kibercinayətkarlığı kimdənsə nəyisə oğurlamaq üçün yerinə yetirilən əməl kimi qəbul edirəm. Bəli, mən 150 manatı sözügedən şəxsə ödədim və bir neçə gün sonra bu adamla əlaqə saxlamaq istədikdə, o, telefona cavab vermədi… Polisə müraciət etdim. Təşəkkür edirəm ki, mənimlə əlaqə saxlayan insan tapıldı, lakin ödədiyim məbləğ artıq yox idi. Daha doğrusu, ölkədən kənardakı hesaba köçürüldüyü üçün polis onu geri ala bilmədi. (Kişi respondent, zərərçəkmiş qrup)

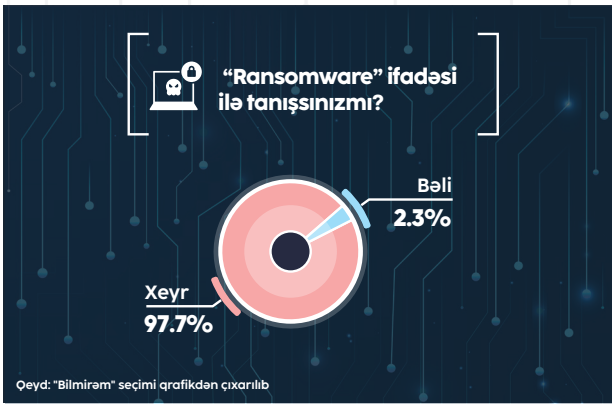
"Ucuz mobil telefon almaq üçün axtarış aparırdım. "Tap.az" (ölkədə tanınmış e-ticarət platforması) onlayn ticarət saytında endirimli olanına rast gəldim. Əlaqə saxladıqda, elan üzrə cavab verən şəxs 50 manat depozit istədi və biz bu məbləği ödədik. Daha sonra əlaqə saxlanılan şəxsi tapa bilmədik. Mən və qızım müraciət etsək də, məsələ ilə əlaqədar polis tərəfindən hər hansı müsbət reaksiyanın şahidi olmadıq. Bildirdilər ki, bu, onların işi deyil və başqa rayonun polis idarəsinə müraciət edilməlidir. Aydın idi ki, onlar bu yolla mövzudan yayınmaq istəyirdilər". (Qadın respondent, zərərçəkmiş qrup)

"Bu cür dələduzluğa məruz qalaraq pul itirməyimin səbəbi, əslində, oğlum idi. O, Amerikada tanımadığı insanlar tərəfindən həmin şəxslərə pul ödəyəcəyi halda, öz video oyunu ilə bağlı yaxşı geridönüşlər əldə edəcəyinə və "800 dollar qazanacaqsınız" və s. kimi vədlərə

inandırıldı. Mən yaşlı qadınam, bütün bu detallar barədə həqiqətən məlumatlı deyiləm. Oğluma 200 dollar təqdim etdim, o isə bu məbləği fırıldaqçılara görə itirdi". (Ümumi əhali qrupu)

5.4.2.3. Rənsamveə (ransomware)

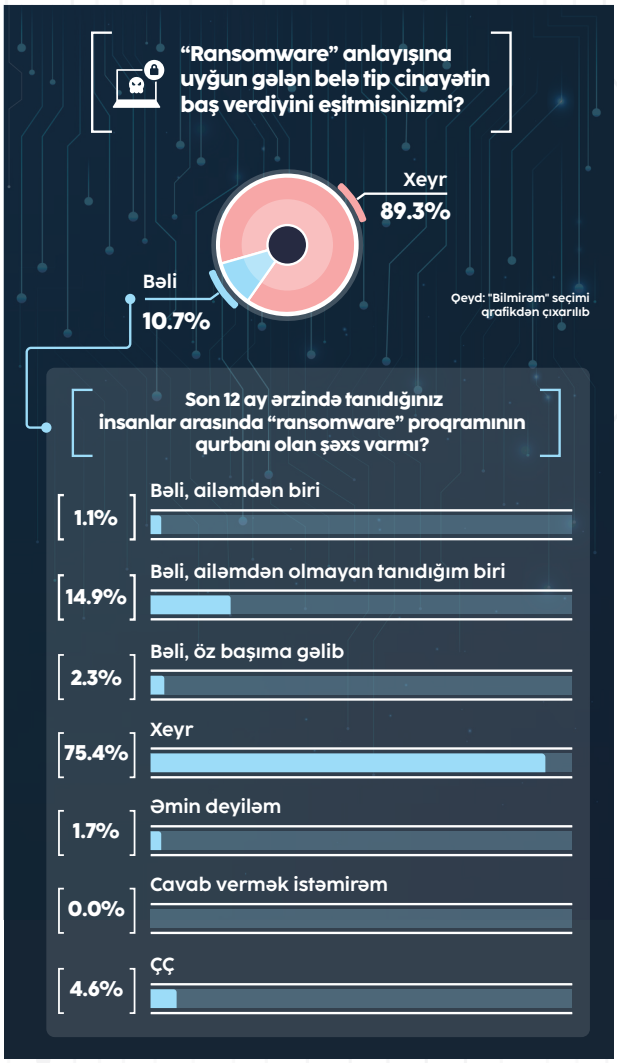
Rənsamveə (ransomware) kibercinayətkarlar tərəfindən istifadə edilən zərərli proqram növü olub, sistemə girişi bloklayır və ya məlumatları şifrələyir. *(Bunun qarşılığında qurbanlardan fidyə (haqq) tələb edirlər* - **red**.)



Ümumi olaraq, seçmədə iştirak etmiş respondentlərin 97,7%-i "rənsamveə" (məlumatların girov saxlanılması üçün zərərli proqramlar vasitəsilə kiberhücum) sözü ilə tanış olmadığını, cəmi 2.3%-i isə tanış olduğunu qeyd edib.

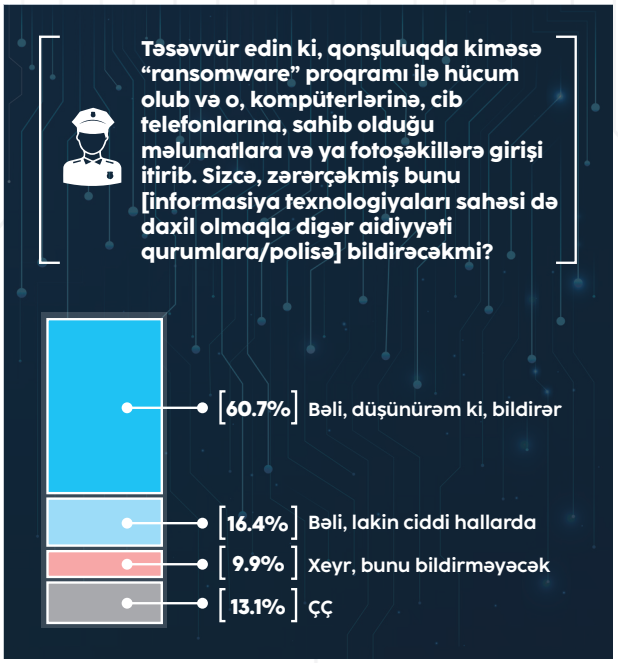
Onlara bu barədə müvafiq izah təqdim edildikdən sonra respondentlərin 89,3%-i belə cinayətin baş verdiyini eşitmədiyini, 10,7%-i isə eşitdiyini ifadə edib.

Respondentlərin 14.9%-i tanıdığı birinin, 1,1%-i ailəsindən birinin, 2,3%-i özünün son 12 ay ərzində rəmsamveə qurbanı olduğunu bildirib. Rəyi soruşulanların 4,6%-i bu suala cavab verməkdə çətinlik çəkib.

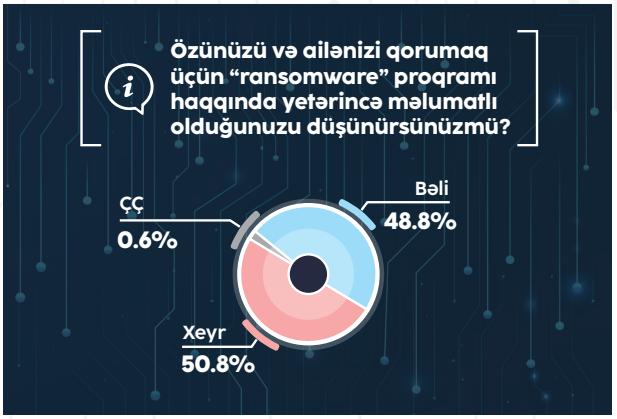


Bununla yanaşı, sorğuda iştirak edənlərin 60,7%-i hesab edir ki, qonşuluqda kiməsə bu tip hücum baş verərsə və onlar öz kompüterlərinə, mobil telefon və fotoşəkillərinə, yaxud digər məlumatlarına çıxışı itirsələr, zərərçəkmiş şəxslər bu barədə səlahiyyətli orqanlara/polisə məlumat verərlər. Respondentlərin 16,4%-i bu tip hücum baş verərsə, yalnız ciddi hallarda səlahiyyətli orqanlara/polisə məlumat verə biləcəklərini qeyd etdikləri halda, 9,9% respondent heç bir halda müraciət etməyəcəyini bildirib.

Sorğuda iştirak edənlərin 13,1%-i bu suala rəy bildirməyib.



Respondentlərin əksəriyyətinin fikrincə, rənsamveə (girov saxlama proqramlarının hücumları) insanlar üçün narahatlıq yarada və ya həyatlarına mənfi təsir göstərə bilər. Bu baxımdan, sorğuda iştirak edənlərin demək olar ki, yarısı Azərbaycanda qeyd edilən bu tip hadisələrin baş vermə səviyyəsindən olduqca narahatdır. Lakin nəticələrə əsasən, respondentlərin 48,8%-i inanır ki, özlərini və ailələrini belə hallardan qorumaq üçün kifayət qədər məlumatlıdır. Nəticə etibarilə, bu sual üzrə sorğu iştirakçılarının digər yarısı isə (50,8%) rənsamveə proqramı haqqında yetərincə məlumatlı olmadığını qeyd edib.



Lakin nümunələr arasında (həm sorğu, həm də fokus qruplar üzrə) rənsamveə proqramları ilə hücum cəhdlərinə məruzqalma təcrübəsinin çox az olmasını nəzərə alsaq, respondentlərin məsələyə dair risk qavrayışının dəqiqliyi və onların mövcud ehtimallardan həqiqətən lazımi səviyyədə qorunmasının mümkünlüyü özlüyündə sual doğuran məqamdır.

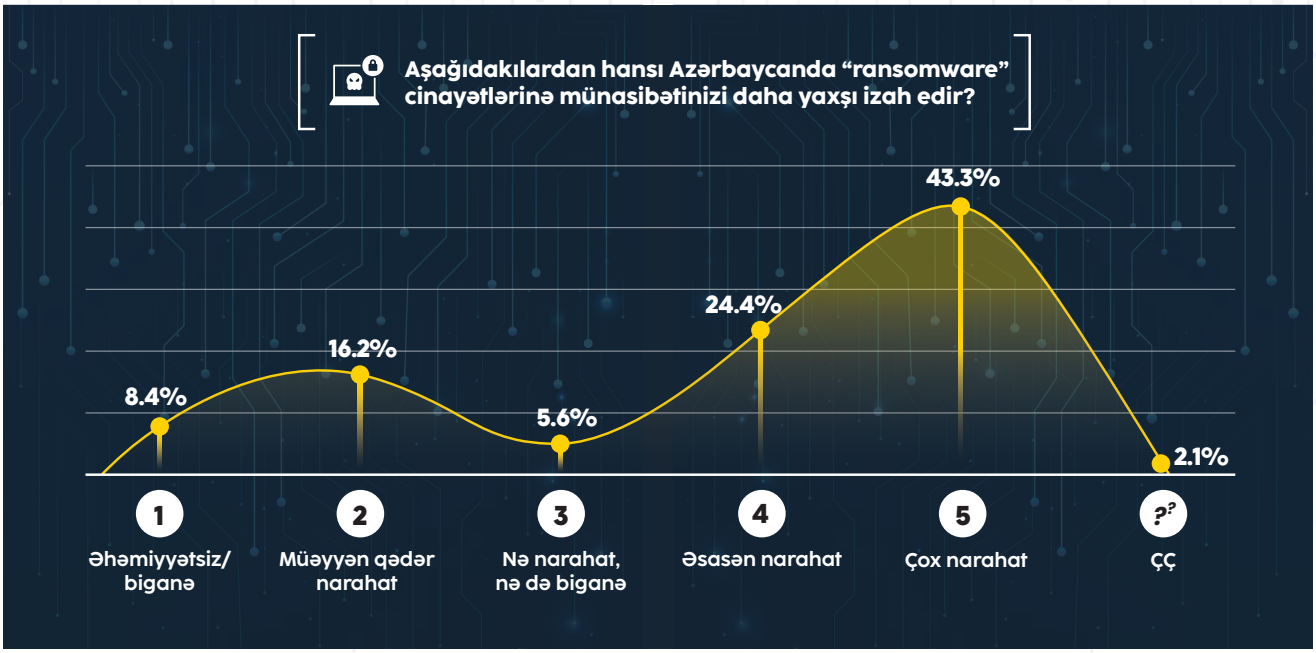
Bütün əhali qrupları üzrə heç bir respondentin müvafiq anlayış barədə onlara tərif təqdim edilməmişdən əvvəl yuxarıda sadalanan hallar haqqında məlumatlı olmadığı aydın olur (üçüncü qrupda əvvəllər bankda işləyən və mövzu üzrə müntəzəm seminarlarda iştirak etmiş bir nəfər xanım və birinci qrupda zərərçəkmiş tələbə istisna olmaqla). Ümumi olaraq, hər üç qrup üzrə yalnız 4 nəfər sonradan məsələyə dair nəyisə xatırladığını bildirib. Buna səbəb olan əsas amillər isə 1) terminin ingiliscə olması və 2) yerli miqyasda mövcud fəaliyyət növünün az yayılması hesab edilə bilər. Üstəlik, rənsamveə ifadəsinin hətta zərərçəkmiş respondentlər qrupunda belə bilinməyən (eşidilməyən) termin kimi müşahidə edilməsi faktı da mövcuddur. Hər üç qrupda ümumən iki zərərçəkmiş və bir təmsili qurban müəyyən edilib. Lakin onların heç biri girov saxlanılan məlumatların azad edilməsi üçün pul ödəmədiyini bəyan edib. Əvəzində, həmin şəxslər yeni cihaz aldıqlarını, yaxud əllərində mövcud olan cihaza yenidən proqramlar yazdıqlarını qeyd ediblər.

"Mən zərərçəkmiş deyiləm, lakin yaxın qohumumun telefonu onlayn hücuma məruz qalaraq bloklandı. O, girov vəsaitini ödəyə bilmədi və həmçinin, telefonunu təmir etmək mümkün olmadı. Beləliklə, qohumum yeni cihaz almalı oldu". (Ümumi əhali qrupu)

"İnstaqram hesabım təxminən 10 il əvvəl bloklanıb. Blok vəziyyətinin ləğvi üçün nə qədər vəsait tələb edildiyini bilmədim. Proqram mühəndisinə müraciət etdim və o, cihazı dəyişməyi təklif etdi. Mən də tövsiyəni icra etdim". (Ümumi əhali qrupu)

Ümumilikdə, seçmə üzrə bütün qruplar rənsamveənin məhdud miqyasda yayılmasına işarə edib. Lakin eyni zamanda maraqlıdır ki, Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzinin (KİMM) nümayəndəsi pandemiya zamanı bu kimi halların artan şəkildə yayılmasına diqqət çəkib:

"Mən fişinqin geniş vüsət alması fikri ilə tamamilə razıyam, onların bir çoxunda COVID-19 virusundan necə qorunmaq barədə mesajlar yer alır. Müşahidə etdiyimiz kimi, belə mesajların bəziləri rənsamveə ilə nəticələnib. Biz həmçinin özünü səhiyyə müəssisəsi kimi təqdim edən bir neçə saxta profil də aşkarlamışıq".



Respondentlərin 43,3%-i Azərbaycanda rənsamveə cinayətlərinin yayılmasından çox, 24,4%-i əsasən narahatdır. Rəyi soruşulanların 8,4%-i üçün bunun heç bir əhəmiyyəti yoxdur.

5.4.2.4. Hədə-qorxu, zorakılıq-təhqir və sui-istifadə

Respondentlərin demək olar ki, üçdə ikisi (59,9%) onlayn hədə-qorxu, zorakılıq-təhqir və sui-istifadə ilə bağlı suallara cavab verməkdən imtina edib. Sorğu iştirakçılarının cəmi 39,4%-i bu tip sullara cavb verməyə razılığını bildirib. Bu alt seçmənin nisbətən kiçik bir hissəsi (18,2%) isə müəyyən irqdən olan insanlara qarşı nifrət, ayrı-seçkilik və ya zorakılığın onlayn təbliğatının şahidi olduğunu, 81,3%-i isə bu cür halları müşahidə etmədiyini bildirib.

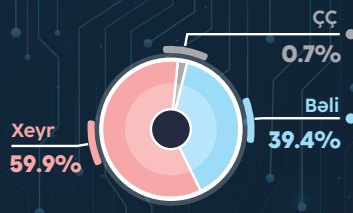
Sorğu iştirakçılarının 95,3%-i hesab edir ki, səlahiyyətli orqanlar/polis uşaqları internet mühitinin təhlükələrindən qorumaq üçün daha çox iş görməlidir. Respondentlərin cəmi 3,4%-i bunun əksini düşünür.

Bu suallara cavab verən 91% respondent onlayn hədə-qorxu, zorakılıq-təhqir və sui-istifadə halları ilə üzləşmədiyini qeyd edib. Sorğu iştirakçılarının 7,2%-i tanıdığı birinin, 0,2%-i ailəsindən birinin, 1,1%-i isə özünün onlayn zorakılıq halları ilə üzləşdiyini bildirib.

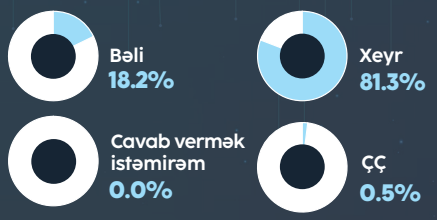
Respondentlərin 68,5%-i belə düşünür ki, qonşuluğunda kimsə onlayn hədə-qorxu, zorakılıq-təhqir və sui-istifadə hallarından zərər çəkmiş olsaydı, o, mütləq hüquq-mühafizə orqanlarına müraciət edərdi. Sorğu iştirakçılarının 17%-i belə hallarda qonşuluğunda kiminsə yalnız ciddi hallarda aidiyyəti orqanlara müraciət edəcəyini, 5,6%-i isə heç bir halda müraciət etməyəcəyini bildirib.

Sorğu iştirakçılarının 8,9%-i bu suala cavab verməkdə çətinlik çəkdiyini bildirib.

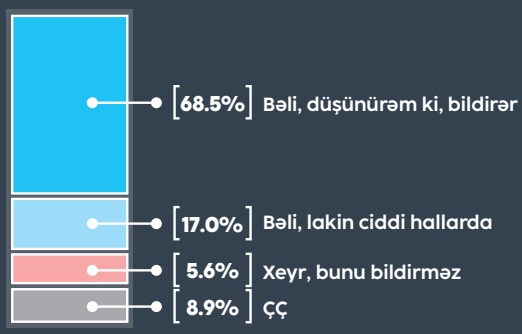
Onlayn hədə-qorxu və təhqirlə bağlı bir neçə suala cavab vermək istərdinizmi?



Son 12 ayda, müəyyən bir irq, rəng, mənşə və ya mənsubiyyətə malik insanlara qarşı nifrət, ayrı-seçkilik və ya zorakılığın hər hansı formada onlayn/internetdə təbliğinin şahidi olmusunuzmu?

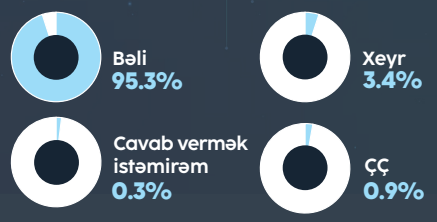


Sizcə, qonşuluğunuzda kimsə internetdə hədə-qorxu və sui -istifadə ilə bağlı cinayətlərdən zərər çəkmiş olsaydı, bunu [aidiyyəti qurumlara/ hüquq-mühafizə orqanlarına] bildirərdimi?



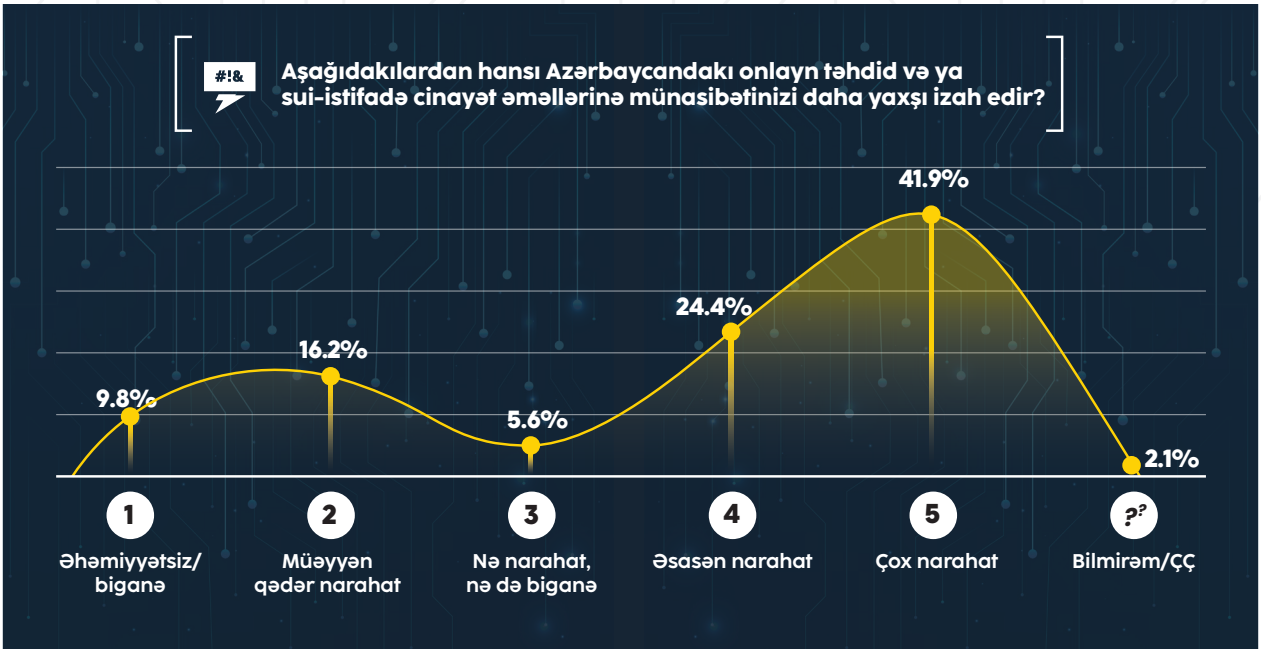
Bəzi onlayn ünsiyyətlər (əməliyyatlar) qorxulu ola bilər. Son 12 ay ərzində tanıdığınız insanlar arasında onlayn təhdid, təhqir və şantaja məruz qalan varmı?

Təəssüf ki, internet bəzən azyaşlılar üçün xoş olmayan bir yer ola bilər. Sizcə, aidiyyəti qurumlar onları onlayn qorumaq üçün daha çox iş görməlidirmi?



1 -dən 4 -ə qədər olan şkalada, son 12 ayda onlayn təhdid və ya təhqir həyatınıza nə dərəcədə təsir edib?

Respondentlərin 41,9%-i ölkədə onlayn təhdid, zorakılıq-təhqir/sui-istifadə hallarından çox, 24.4%-i isə əsasən narahatlıq keçirdiyini ifadə edib. Sorğu iştirakçılarının 9.8%-i bu cür halların onun üçün heç bir əhəmiyyət kəsb etmədiyini bildirib.



Özlərini və ailələrini müdafiə etmək üçün sorğu iştirakçılarının 63,7%-i onlayn hədə-qorxu, zorakılıq/təhqir və sui-istifadə barədə kifayət qədər məlumatlı olduğunu, 35.8%-i isə heç bir məlumata malik olmadığını bildirib.

Qeyd edək ki, bu rəqəm həm də artan məlumatlılıq və qabaqlayıcı tədbirlər üçün mövcud imkanların da göstəricisidir. Gənclərin çoxu özlərini və ailələrini qorumaq üçün onlayn hədə-qorxu və zorakılıq-təhqirə dair məlumata malik olduqlarını düşünür. Şəhər yerlərində yaşayanların özləri və ailə üzvlərinin mühafizəsi üçün yetərli dərəcədə məlumatlı olması daha çox nəzərə çarpır. Nəticələr həm də üzə çıxarır ki, respondentlər arasında təhsil səviyyəsi yüksəldikcə onların bu mövzuda məlumatlı olması ehtimalı da artır.

Fokus qruplara gəldikdə, burada iştirakçılar onlayn hədə-qorxu, zorakılıq/təhqir və sui-istifadə məsələsi ilə bağlı özünəməxsus yanaşmalar irəli sürüblər. İstər QHT nümayəndələri, istərsə də ümumi əhali qrupları arasında ortaq bir baxış müşahidə edilib: siyasi müzakirə və ya debatlarda fəal iştirak edənlər müəyyən vaxtlarda öz fikirlərinə görə onlayn hədə-qorxu, təhqir və sui-istifadəyə məruz qalıblar.

"Məşğul olduğum xüsusi fəaliyyətə görə bir həftə qarayaxma kampaniyasının hədəfinə çevrildim. Bu vəziyyət hücum edənləri ictimai şəkildə ifşa etməyimdən sonra dayandırıldı". (İT mütəxəssisləri və QHT qrupu)

5.4.2.5. Kibermüdaxilə (DDoS)

Respondentlərin 77,4%-i etibar etdikləri onlayn xidmətlərdən hər hansı birinin gözlənilmədən uzun müddətə əlçatmaz olması faktı ilə rastlaşmadığını, 9.9%-i isə rastlaşdığını qeyd edib. 12.8% respondent bu suala rəy bildirməkdə çətinlik çəkib.

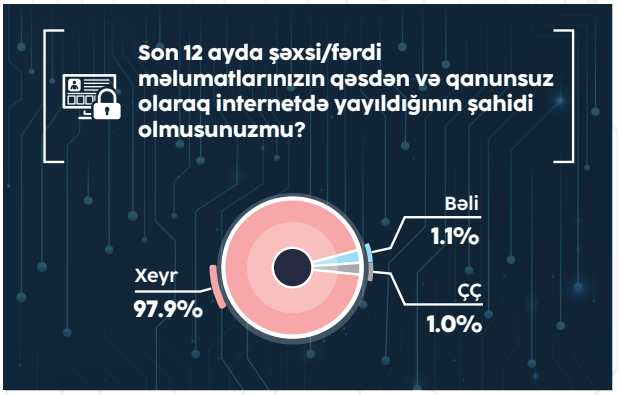
Fokus qruplar isə bununla bağlı fərqli fikirlər təqdim ediblər. Belə ki, onların cavablarına əsasən, onlayn bankçılıq sistemləri tez-tez çökməyə meyillidir və bu cür hallar təkcə xarici hücumlar səbəbindən meydana gəlmir.

5.4.2.6. Şəxsiyyət/kimlik (fərdi məlumatların) oğurluğu

Sorğunun nəticələrinə əsasən, respondentlərin əksəriyyəti (90,4%) son 12 ayda kimsə tərəfindən şəxsi hesablarına daxil olmaq və ya buna cəhd etmək halları ilə rastlaşmayıb. Sorğu iştirakçılarının 4,2%-i belə düşünür ki, buna cəhd edilib, lakin uğursuz olub.

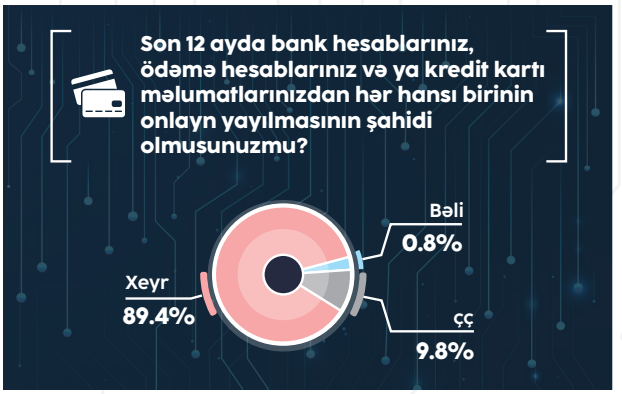
Respondentlərin 97,9%-i son 12 ay ərzində şəxsi məlumatlarının qəsdən və qeyri-qanuni şəkildə onlayn ələ keçirilməsi, internetdə yayılması ilə üzləşməyib.

Rəyi soruşulanların cəmi 1,1%-i bu cür halları müşahidə etdiyini bildirib.

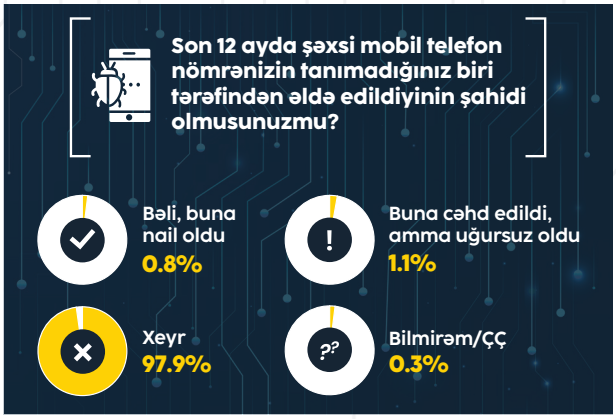


Rəyi soruşulanların 96%-i son 12 ayda şəxsi məlumatlarından sui-istifadə və ya onlara qarşı zorakılıq halları, yaxud belə cəhdlərlə qarşılaşmadığını deyib. Sorğu iştirakçılarının 2,6%-i qeyd edib ki, buna cəhd edilib, lakin uğursuz olub.

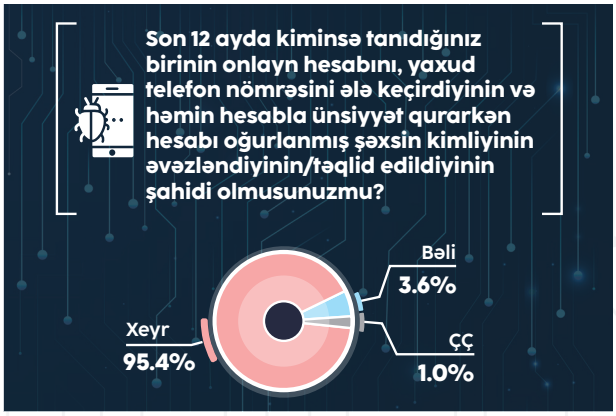
Sorğuda iştirak edənlərin 89,4%-i bank hesablarından hər hansı birinin, onlayn ödəniş hesabları və ya kredit kartı məlumatlarının onlayn şəkildə yayılmasının şahidi olmayıb. Respondentlərin 9,8%-i bu suala cavab verməkdə çətinlik çəkib.

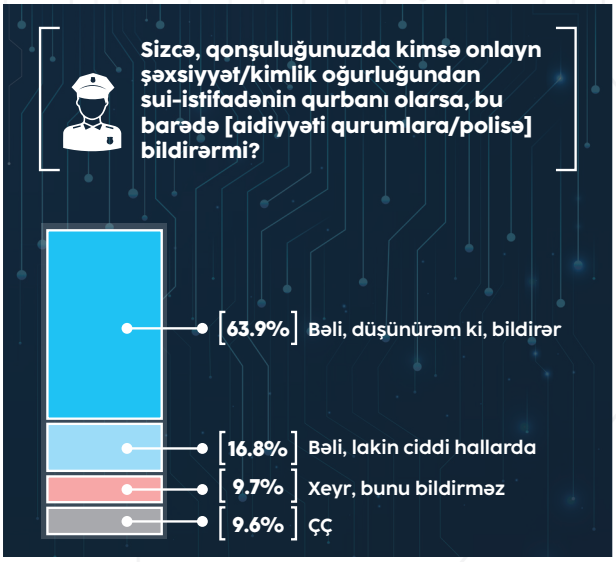


Demək olar ki, respondentlərin əksəriyyəti şəxsi mobil telefon nömrəsinin kənar (tanımadığı) şəxs tərəfindən ələ keçirilməsini müşahidə etməyib. Sorğu iştirakçılarının yalnız 1,1%-i bildirib ki, buna cəhd edilib, lakin uğursuz olub.



Respondentlərin yalnız 3,6%-i tanıdığı birinin telefon nömrəsi, yaxud onlayn hesabını ələ keçirən saxta istifadəçi/təqlidçi tərəfindən respondentin telefon nömrəsi və ya onlayn hesabı ilə əlaqə saxlanıldığını bildirib. Rəyi soruşulanların 95,4%-i isə bu cür hallarla rastlaşmadığını qeyd edib.

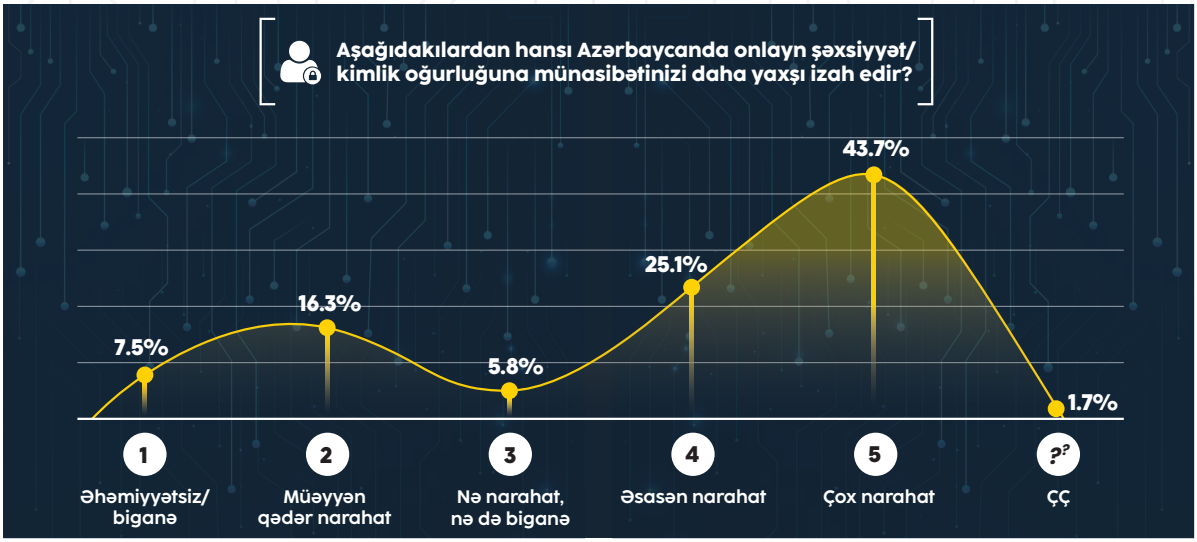




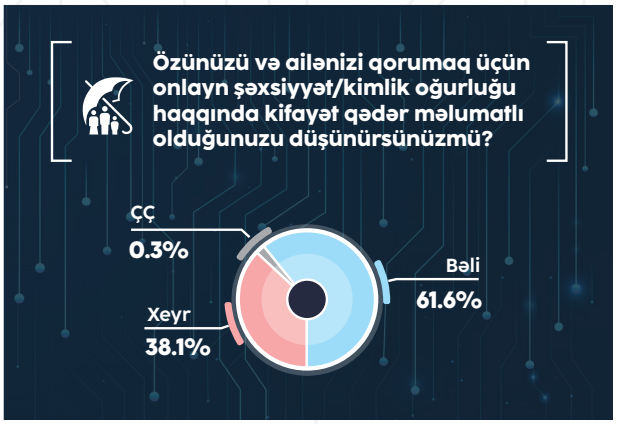
Respondentlərin 63,9%-i hesab edir ki, qonşuluqda kimsə onlayn şəxsiyyət/kimlik oğurluğunun qurbanı olarsa, zərərçəkmiş şəxslər bu barədə səlahiyyətli orqanlara/polisə məlumat verərlər. Sorğu iştirakçılarının yalnız 16,8%-i düşünür ki, yalnız ciddi hallarda məlumat verər. Respondentlərin 9,7%-i bunu bildirməyəcəyi qənaətindədir. Rəyi soruşulanların 9.6%-i isə bu suala cavab verməkdə çətinlik çəkdiyini bildirib.

Ümumiyyətlə, nəticələrə əsasən olduqca məhdud miqyasda yayılma halı ilə əlaqədar olaraq, təxminən 90% respondentin onlayn şəxsiyyət/kimlik oğurluğuna məruz qalmadığı məlum olur.

Təhlil əsasında göstəricilər sübut edir ki, seçmənin 43,7%-i ölkədə onlayn şəxsiyyət/kimlik oğurluğu hallarından çox, 25,1%-i isə əsasən narahatdır. Respondentlərin 7,5%-i bunun onun üçün heç bir əhəmiyyət kəsb etmədiyini bildirib.



Sorğu iştirakçılarının 61,6%-i özünü və ailəsini onlayn şəxsiyyət/kimlik oğurluğundan müdafiə etmək üçün lazımi səviyyədə məlumatlı olduğunu düşünsə də, 38,1%-i bu barədə kifayət qədər məlumatlı olmadığını qeyd edib.



Şəxsiyyət/kimlik oğurluğu məsələsi fokus qruplarla da geniş müzakirə edilib (4 respondent bank kartı oğurluğundan, 3 respondent isə sosial media hesabının sındırılmasından əziyyət çəkdiyini bildirib). Zərərçəkmiş şəxslərin nəql etdikləri hadisələr onların bu hallara necə məruz qalmasını işıqlandırmaq baxımından faydalıdır:

"Ödəniş etdiyim xarici şirkət öz sistemini effektiv şəkildə qoruya bilmədiyi üçün 500 dollar pul itirdim. Görünür, haker şirkətin bazasına hücum edərək bütün müştərilərin məlumatlarını ələ keçirmişdi. Səylərimə baxmayaraq, məbləğ bərpa edilmədi. Eyni zamanda, narahatedici bir zəng qəbul etdim. Əlaqə saxlayan şəxs bank hesabımdakı pul vəsaitinin miqdarı barədə dəqiq bilirdi. Bu səbəbdən zəng gələn telefon nömrəsini dərhal blok etdim" (Ümumi əhali qrupu).

(**QEYD**: respondent inamsızlıq səbəbindən polisə şikayət etməyib)

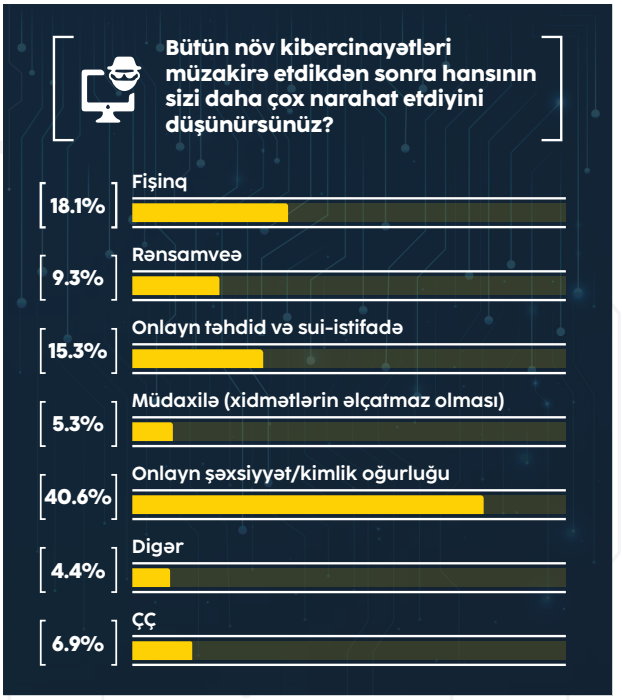
"Onlayn alış-veriş edə bilməsi üçün övladıma aid karta 1 dollar vəsait əlavə etdim. Lakin qısa vaxt ərzində məbləğ kartdan silindi (təxminən bir ay sonra). Bir müddət keçdikdən sonra həmin karta 20-30 dollar da əlavə etdim və əvvəlki hadisə təkrarlandı. Ümumilikdə, ailəvi olaraq sözügedən hesabı bağlayıb yenisini aktivləşdirənədək 100 dollar dəyərində pul itkisi ilə üzləşdik". (Ümumi əhali qrupu)

"Qardaşımın 200 manat pulu oğurlanıb. O, məbləğin itirildiyi kartdan 2-3 dollarlıq onlayn ödəniş etmək üçün istifadə edib. Təxminən bir ay sonra isə həmin kartdan 200 AZN oğurlanıb. Etimadsızlıq səbəbindən polisə məlumat vermədi. Bilirsiniz, niyə etibar etmirik (ehtimala əsasən, respondent açıq şəkildə polisi tənqid etməkdən çəkinirdi)". (Qadın respondent, zərərçəkmiş qrup)

"Oğlumun oyun hesabı oğurlandı. Çox ağladığı üçün hadisə hər birimizə təsir etdi. Bilirsiniz, onun hesabında oyun xalları, bonuslar və bu kimi elementlər var idi. Hamısını itirdi". (Qadın respondent, zərərçəkmiş qrup)

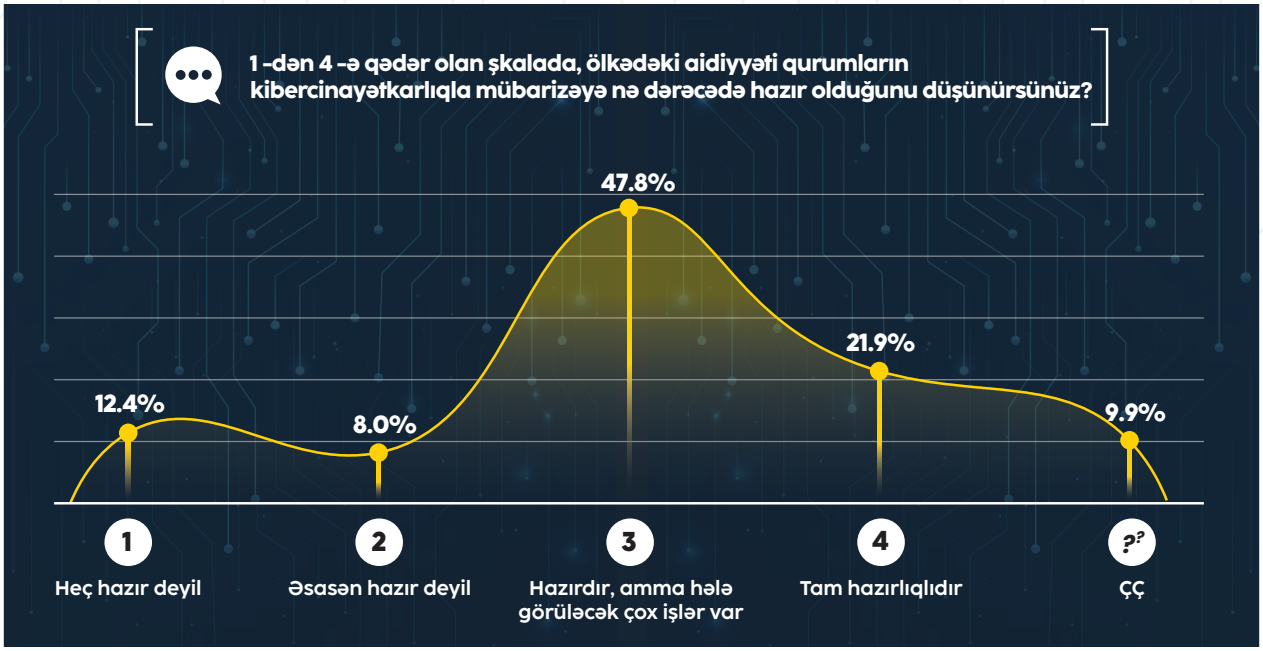
5.4.2.7. Kibercinayətkarlıq: narahatlıq və gözləntilər

Məlumat müdafiəsinin aşılması və onlayn şəxsiyyət/kimlik oğurluğu respondentlərin 40,6%-i üçün ən çox narahatlıq doğuran cinayət növü olsa da, maraqlıdır ki, bu hallardan sorğuda iştirak edənlərin yalnız cüzi bir hissəsi əziyyət çəkib. Oxşar məqam fişinqə də aiddir.



Rəyi soruşulanların 47,8%-i hesab edir ki, ölkədə səlahiyyətli qurumlar kibercinayətkarlıqla mübarizəyə hazır olsalar da, bu sahədə hələ görüləcək çox iş var. Respondentlərin 12,4%-i heç hazır olmadığını düşünür.

indi daha çox diqqət yetirirlər... Əslində, onlayn oğurluqların artması səbəbindən fiziki zərərlə nəticələnən cinayətlərin sayının azaldığını görə bilərik". (Ümumi əhali qrupu)



Kibercinayətlərin miqyasının gələcəyi ilə bağlı gözləntilərə dair nəticələr demək olar ki, bərabər şəkildə bölünür. Daha çox şəhər sakinləri, fəal internet istifadəçiləri və qadın respondent qrupu kibercinayətkarlığın artacağını düşünür. Dünya İqtisadi Forumunun (WEF) ekspertlərinin 2021-ci ili "Kiberpandemiya ili" adlandırmalarını nəzərə aldıqda, bu, olduqca maraqlıdır: *"Biz "kiberpandemiya"nın ortasındayıq. COVID-19 uzaqdan işləmə rejiminə keçidi sürətləndirdi və beləliklə, kiberhücumlar üçün istifadə edilən proqram təminatının icrası asanlaşdı, rənsamvеə hücumları sürətlə artdı və hələ də davam etməkdədir".*

Fokus qrup üzvlərinin məsələ ilə bağlı mülahizələri isə olduqca faydalıdır. İstisnasız olaraq, bütün qruplar elektron xidmətlərdən (e-gov və e-ticarət) istifadənin artmasına, eləcə də əvvəllər kağız üzərində olan məlumatların rəqəmsallaşdırılmasına görə kibercinayətkarlığın gələcəkdə daha da güclənəcəyi ilə bağlı ortaq qənaətə malikdir.

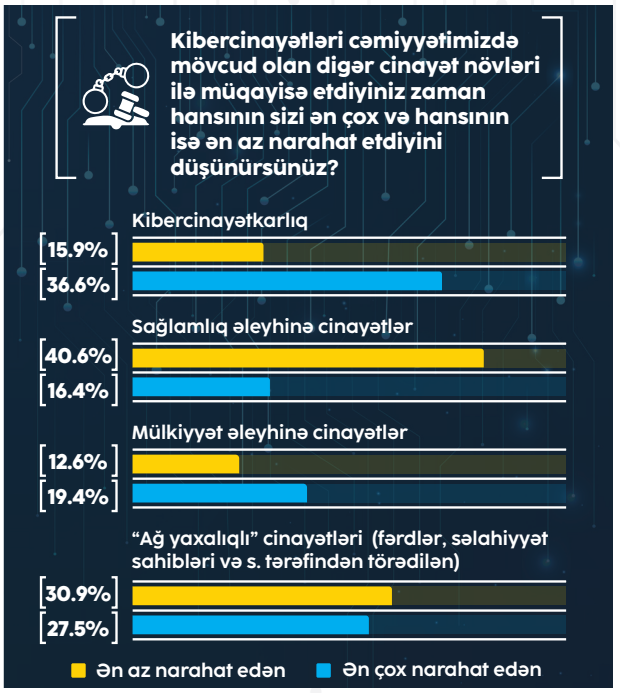
"Müasir dövrdə hər şey rəqəmsallaşdırılıb və biz rəqəmsal inqilabın astanasındayıq, beləliklə, bu problemin daha geniş yayılacağı çox aydındır. Dövlət orqanları kibercinayətlərlə mübarizə üzrə kadrların hazırlanmasına

"Bütün məlumatlarımızın rəqəmsal formada olduğu bir vaxtda özümüzü qorumaq üçün hər hansı gücümüz yoxdur". (Ümumi əhali qrupu)

"Ağıllı cihazlar, 5G, fiberoptikadan geniş istifadə, virtual reallıq – onların nə gətirəcəyini bilmirik". (Respondent öz fikrini şübhəçi üz ifadəsi ilə səsləndirib) (İT mütəxəssisləri və QHT qrupu)

"Smartfon və kompüterdən nə qədər çox istifadə etsək, təhlükə səviyyəsi müvafiq olaraq artacaqdır. Bu halda nə sığortaçı var, nə də sığortalanan. Hər kəsin bir-birinə qarşı şübhəsi günbəgün artır. Hamı təhdidə çevrilə bilər". (İT mütəxəssisləri və QHT qrupu)

Digər cinayətlərlə müqayisədə respondentlərin 36,6%-nin kibercinayətkarlığı ən narahatedici hüquq pozuntusu hesab etməsi onu göstərir ki, müzakirə edilən bir sıra kibercinayətlərə dair zərərçəkmə nisbəti çox aşağı olsa da, ümumilikdə, xeyli insan bu cinayət kateqoriyası üzrə kifayət qədər narahatlığa malikdir.



5.4.3. Nəticə

♦ Kəmiyyət göstəriciləri üzrə datalara əsaslanaraq müəyyən etmək olur ki, Azərbaycanda kibercinayətlərin bütün formaları nüfuz qazanmayıb və hətta daha çox yayılan növlər belə (sıravi vətəndaşlara qarşı məlumatları icazəsiz əldə etmə, onlayn şəxsiyyət/kimlik oğurluğu, təşkilatlara qarşı rənsamveə/DDoS cəhdləri) olduqca aşağı "uğur" səviyyəsinə malikdir.

♦ Tədqiqatda məlumatlara daxil olma və onlayn şəxsiyyət/kimlik oğurluğunun ən çox narahatlıq doğuran cinayətlər olması faktı həyəcan yaratsa da, bu növ əməllər üzrə zərərçəkmə nisbətinin olduqca aşağı miqyası məlumatlılıq və müdafiənin yaxşı nümunəsi kimi qeyd edilə bilər.

♦ Ümumən, əhalinin üçdə birindən çoxunun kibercinayətkarlığı ən çox narahat edən hüquqpozma kimi qəbul etməsi bu cinayət kateqoriyasının potensialının dərk edilməsindən xəbər verir.

♦ Növbəti tədqiqatlara zəmin yaradan maraqlı məqamlardan biri kibercinayətlərin gələcəyinə dair gözləntilərlə bağlı əhəmiyyətli fikir bölgüsünün meydana gəlməsidir.

♦ Mühafizə baxımından datalar müəyyən müsbət mənzərə əks etdirsə də, tədqiqatın vacib hissəsini əhatə edən respondentlər özlərini qorumaq üçün kifayət qədər hazırlıqlı olmadıqlarını düşünürlər. Bu isə, məsələn, KİMM tərəfindən təşkil edilən proqramlar kimi maarifləndirməyə ehtiyac olduğunu göstərir.

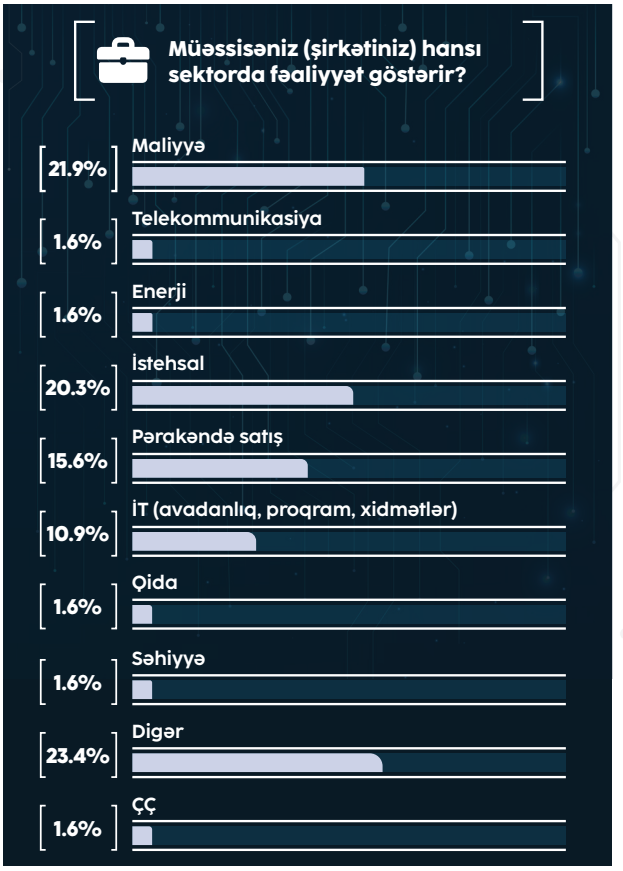
♦ Nəticələr belə deməyə əsas verir ki, respondentlərin dəqiq cavablar təqdim etdiklərini fərz etsək, istənilən halda onların qonşuluğunda bir çox kibercinayətlər diqqətdən kənarda qala bilər.

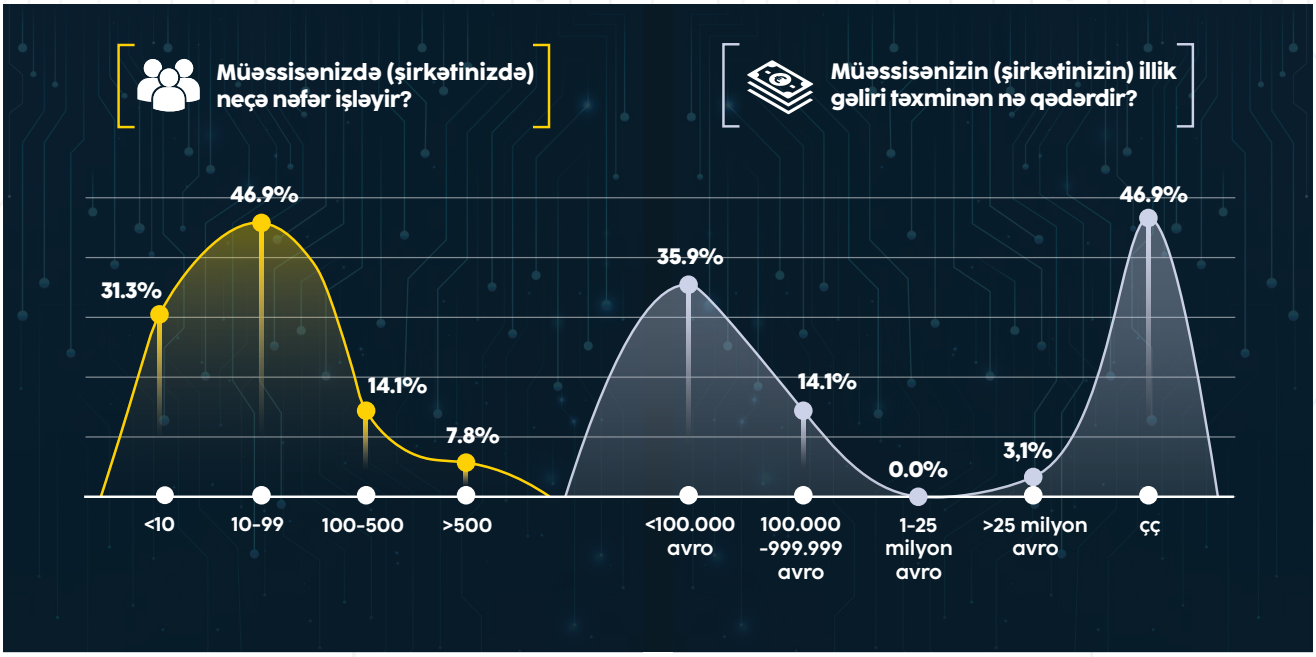
5.5. MÜƏSSİSƏLƏR/ŞİRKƏTLƏR

5.5.1. Təşkilati məlumat

Seçmədə nisbətən çox sayda təşkilatın maliyyə, istehsal və ticarət sektorlarını təmsil etməsi aydın görünür. Beləliklə, nəticələr üzrə göstəricilər bu cür məhdud müstəvi üzrə şərh edilməlidir. Coğrafi təmsilçilik baxımından paytaxt Bakı şəhəri və onun yerləşdiyi yarımada əhəmiyyətli hissəni (81,8%) əhatə edir. Sorğunun üstünlük təşkil edən faiz göstəricisi şəhərlərə aid olsa da, belə hal başadüşüləndir. Çünki əsasən şəhər bölgələrindəki şirkətlər biznes idarəçiliyi üçün internetdən yüksək miqyasda istifadə edirlər. Digər tərəfdən, tədqiqatda bir sıra iqtisadi rayonların ümumiyyətlə təmsil olunmadığı da nəzərə alınmalıdır.

Nəticələr əsasında daha konkret təhlil etsək aydın olur ki, sorğuya cəlb edilmiş müəssisələrin (qurumların/şirkətlərin) 21,9%-i maliyyə, 20,3%-i istehsal, 15,6%-i parakəndə satış, 10,9%-i İT (avadanlıq, proqram və xidmətlər), hər biri 1,6 % olmaqla səhiyyə, telekommunikasiya, enerji və qida, 23,4%-i isə digər sahələri əhatə edir.

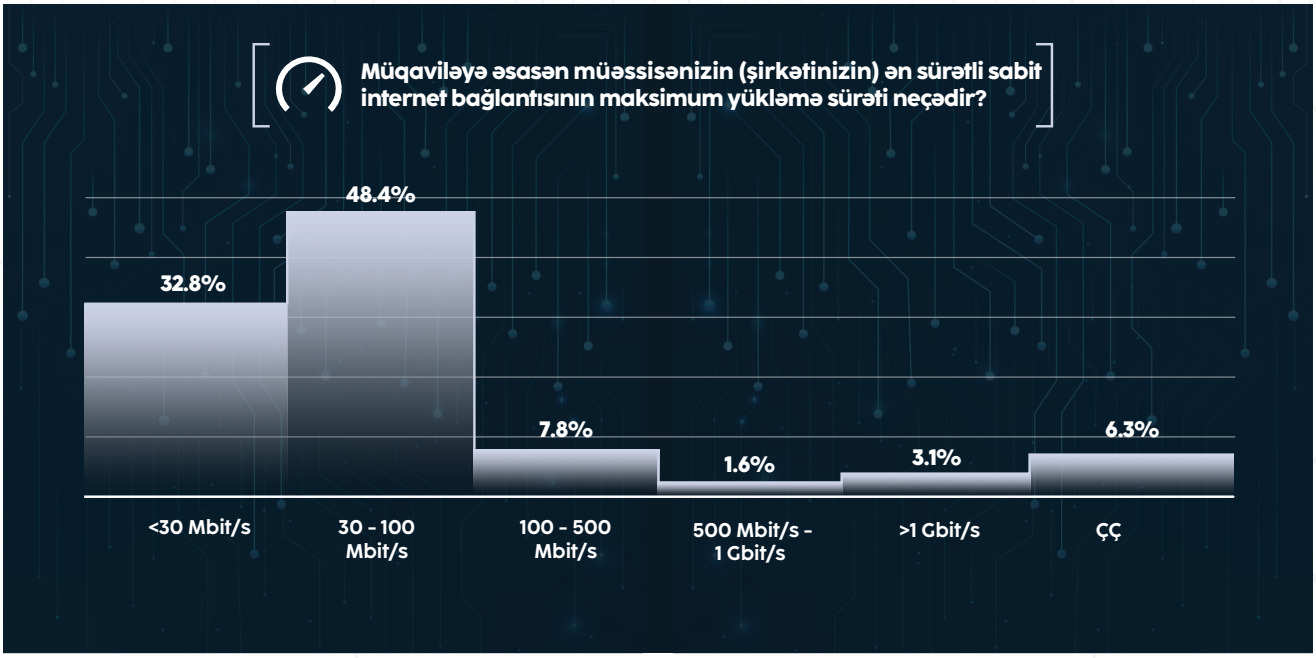




Seçmə üzrə təşkilatların əksəriyyəti 100-dən az işçi həddinə malik və yalnız 14,1%-i 100-500 arası, 7,8%-i isə 500-dən çox işçisi olan müəssisə və qurumlardır. Respondentlərin cavablarına əsasən, ümumən iştirakçı təşkilatların illik gəlirlərinin təxminən üçdə biri 100.000 avrodan aşağıdır. Oxşar sayda respondentlərin isə müvafiq rəqəmləri bilmədiyi (məsələn, İT departamentini təmsil etdikləri üçün), yaxud açıqlamaqdan imtina etdiyi aydın olur.

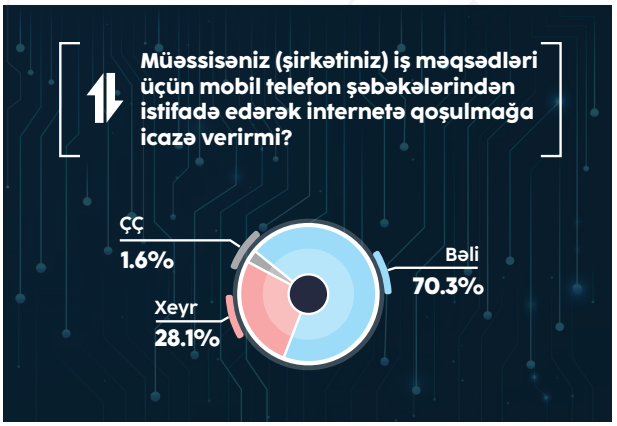
5.5.2. İnternetdən istifadə

Bütün qurum və şirkətlər internetə müəyyən sabit xətt bağlantısına malikdirlər. Ən sürətli stasionar internet bağlantısının müqavilə üzrə maksimum yükləmə sürəti isə ümumiyyətlə 100 Mbit/saniyədən aşağıdır.



Qurumların çoxu (70,3%) işçilərinin mobil telefon şəbəkələrindən istifadə etməklə iş məqsədləri üçün internetə qoşulmasına icazə verir ki, bu, özlüyündə həmin işçilərin cihazları vasitəsilə meydana gələ biləcək kibercinayətlərə qarşı həssaslığın artması üzrə narahatlıq mənbəyi ola bilər. Beləliklə, gəlinən nəticəyə əsasən, təşkilatların əhəmiyyətli hissəsi işçilərə şəxsi cihazlarından işlə bağlı istifadə etməyə hər zaman şərait yaradır.

Sorğunun nəticələrindən o da aydın olur ki, şirkətlərin (qurumların) 28,1%-i işçilərinə mobil telefon şəbəkələrindən istifadə etməklə iş məqsədləri üçün internetə qoşulmağa icazə vermir.



Əksər təşkilat və müəssisələrin veb-sayt (71,9%) və ya sosial media hesabları (78,1%) mövcuddur. Bu mənada bloq və ya mikrobloqlar müvafiq suala cavablar sırasında ən az yayılmış vasitə/platformadır (9,4%).

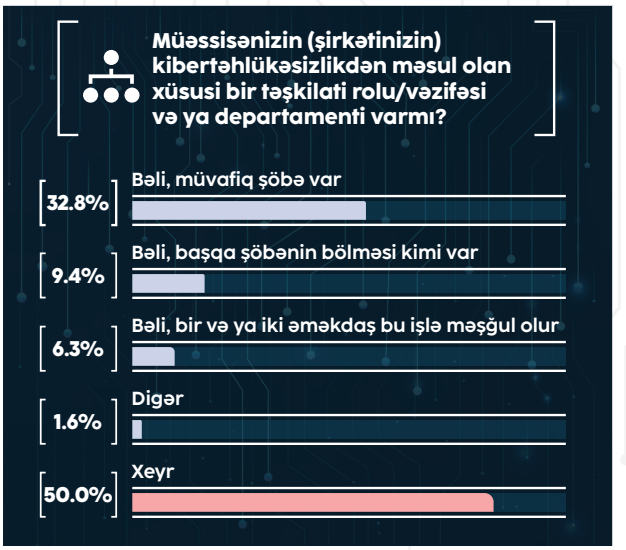
5.5.3. Kibertəhlükəsizlik üzrə bilik səviyyəsi

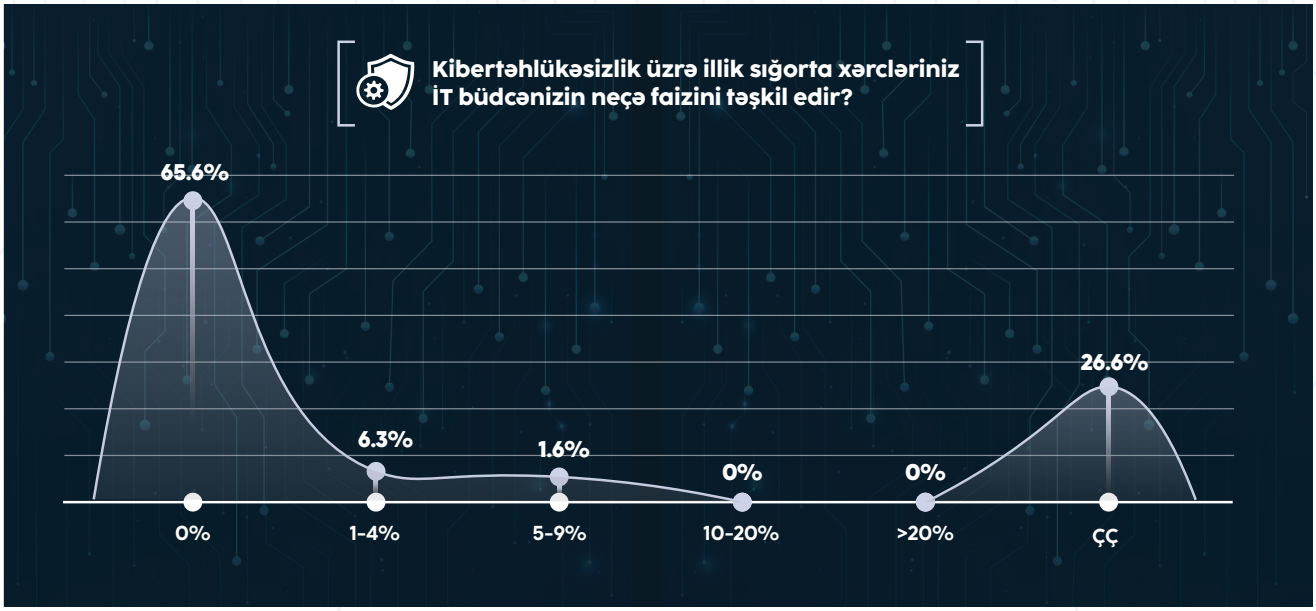
5.5.3.1. Kibertəhlükəsizliyin rolu

Müəssisə və təşkilatların əhəmiyyətli bir hissəsinin (50,0%) kibertəhlükəsizliyə cavabdeh xüsusi təşkilati rolu - vəzifə növü və ya şöbəsinin olmaması narahatedici faktdır. Maliyyə məsələləri burada önəm daşısa da, nəzərə almaq lazımdır ki, bütün müəssisələr (respondentlərin fikrincə) kibercinayətkarların diqqətini "çəkəcək" həssas/məxfi məlumatları idarə etmirlər.

Respondentlərin 32,8%-i təmsil etdiyi qurumda (müəssisədə) kibertəhlükəsizliyə cavabdeh xüsusi bir şöbənin olduğunu, 9,4%-i digər bir şöbənin bölməsi kim fəaliyyət göstərdiyini, 6,3%-i isə bir və ya iki əməkdaşın ayrıca bu işlə məşğul olduğunu qeyd edib.

Maliyyə sektorundakı şirkətlərin 64%-ində kibertəhlükəsizliyə məsul təşkilati rol/vəzifə və ya departament vardır, istehsal və informasiya texnologiyaları sahələri üzrə göstəricilər isə tədqiqat nəticələrinə müvafiq olaraq 23,1% və 57,2% təşkil edir. Qurumun miqyası burada vacib amildir – təhlillərə əsasən, müəssisənin böyüklüyü kibertəhlükəsizlik üzrə qurumun kadr ehtiyatının olması ehtimalını həmin ölçüdə artırır. Məsələn, 10-dan az işçisi olan təşkilatların yalnız 20%-i əlaqədar suala müsbət cavab verdiyi halda, işçi qüvvəsi 100-500 və 500-dən çox olan yerlərdə bu göstərici demək olar ki, 100%-dir.

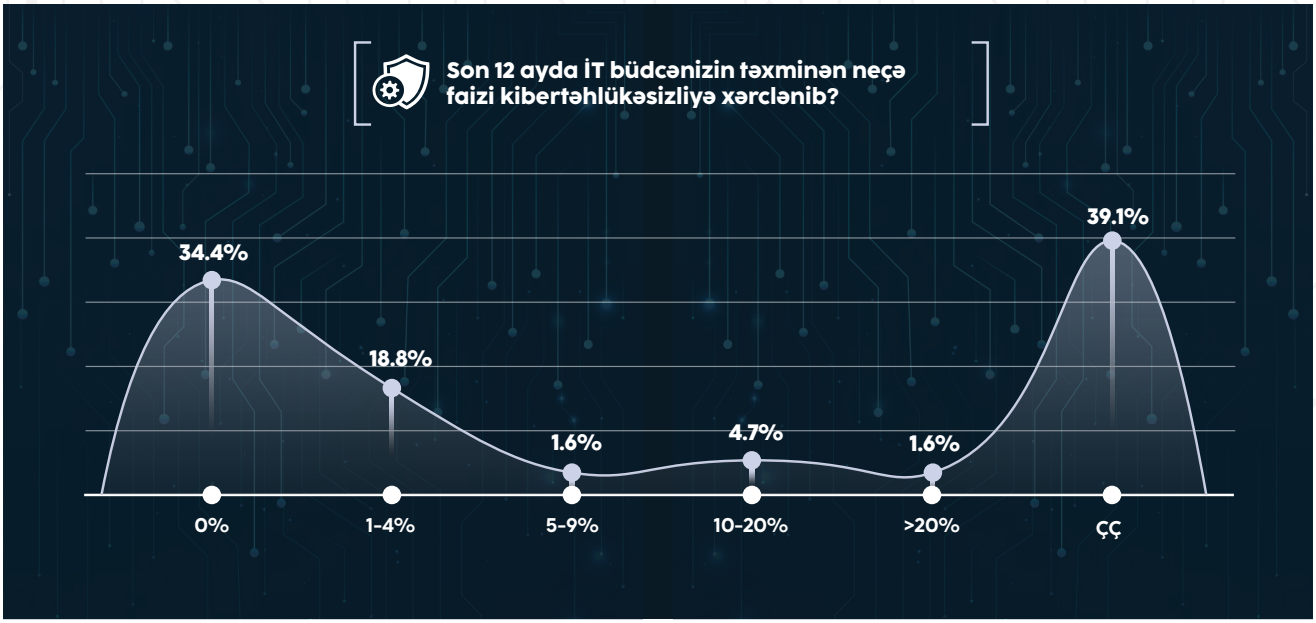




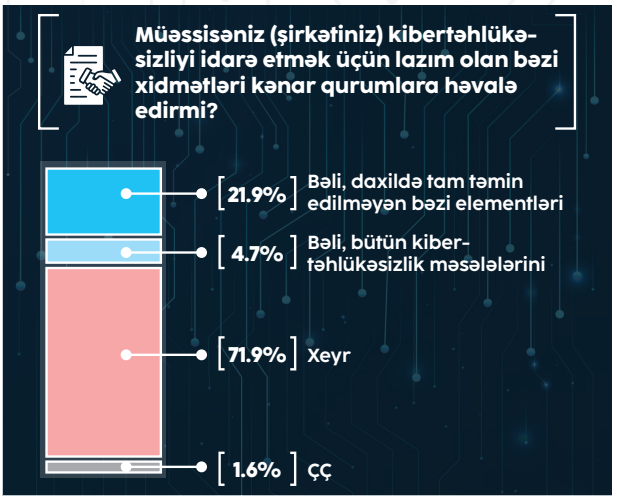
Respondentlərdən işlədikləri təşkilatda kibertəhlükəsizlik sığortasının həddini İT büdcəsi daxilində bildirmələri xahiş edildikdə məlum olub ki, əksər müəssisələrin (65,6%) sığortası yoxdur. Əslində, digər respondentlərin də İT departamentini təmsil etmələrinə baxmayaraq, məsələdən xəbərdar olmamalarına əsasən belə nəticəyə gəlmək olar ki, Azərbaycanda kibertəhlükəsizlik üzrə sığorta praktikası son dərəcə məhduddur və bu vəziyyətin sığorta sektoru (gələcəkdə nüfuz ediləcək bazar) üçün gələcək təsirləri vardır.

Müəssisə və təşkilatların nümayəndələrinin müvafiq suala cavablarına əsasən, onların 26,6%-i kibertəhlükəsizliyin idarə edilməsi üçün lazımi xidmətlərin bir hissəsi və ya hamısını kənar mənbədən təmin edir (outsourcing).

Təşkilatların İT büdcəsi daxilində kibertəhlükəsizliyə çəkdikləri xərclərin həcmi ümumiyyətlə aşağıdır. Respondentlərin əhəmiyyətli hissəsi (39,1%) bununla bağlı göstəricilər haqqında məlumatlı deyil (məsələn, İT departamentini təmsil etdiklərinə görə), ya da bilərəkdən müvafiq rəqəmi açıqlamayıb. Digər tərəfdən, maliyyə sektorunda fəaliyyət göstərən şirkətlərin 21,4%-i İT büdcəsinin 1-4%-ni kibertəhlükəsizliyin təminatına xərclədiyi halda, pərakəndə satış və istehsal sferasında müvafiq faizlər cüzi şəkildə yüksək müşahidə edilib (burada sektorları təmsil edən qurumların sayındakı mühüm fərq də nəzərə alınmalıdır).



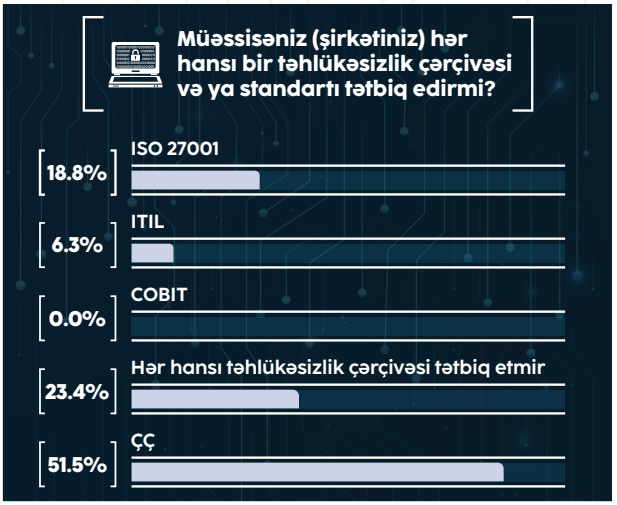
Sorğu iştirakçılarının 71,9%-i bildirib ki, təmsil etdiyi müəssisə (şirkət) kibertəhlükəsizliyi idarə etmək üçün lazım olan bəzi xidmətləri heç bir kənar quruma etibar etmir. Rəyi soruşulanların 21,9%-i qeyd edib ki, təmsil etdiyi qurum bu məqsədlə daxildə tam təmin edilməyən bəzi elementləri kənar qurumlara həvalə edir. Respondentlərin 4,7%-i bildirib ki, çalışdığı qurum kibertəhlükəsizliklə bağlı bütün məsələlərin idarə olunması məqsədilə kənar qurumların xidmətindən istifadə edir.



ISO 27001 standart seçmədə rast gəlinən ən yayılmış təhlükəsizlik çərçivəsi olmasına baxmayaraq (18,8%), xeyli sayda insanın mövcud çərçivədən xəbərsiz olması və ya istifadəsindən qeyri-əminliyi digər diqqət çəkən məqamdır (51,5%). Həmçinin qeyd etmək lazımdır ki, adı çəkilən standart müəyyən sahələrdə (bank sektoru) tənzimləyici mandatdır.

Respondentlərin 23,4%-nin qənaətinə görə, təmsil etdikləri müəssisə (qurum) hər hansı təhlükəsizlik çərçivəsi tətbiq etmir.

ISO 27001 standartı paytaxt Bakıda fəaliyyət göstərən və 100-500 nəfər işçisi olan şirkətlər tərəfindən daha çox tətbiq edilir.

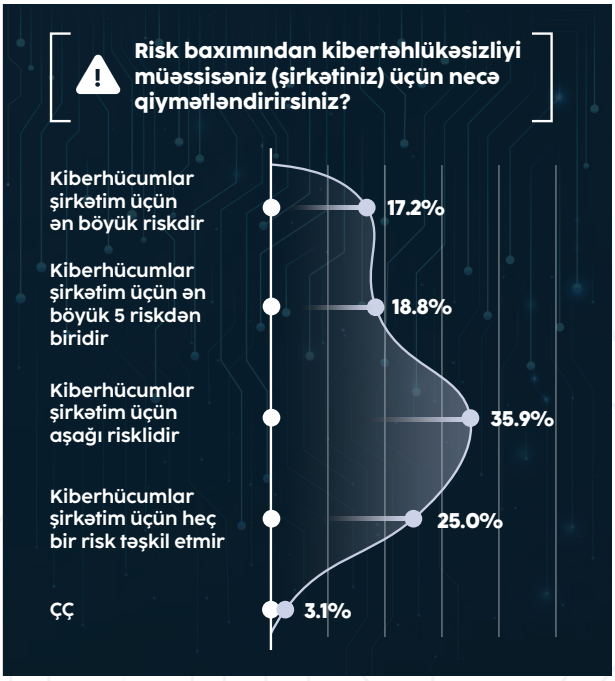


Qurum və təşkilatlarda istifadə edilən texnologiyalar soruşulduqda videokonfrans/görüş-iclas (70,3%), sosial media hesabları (68,8%) və veb saytlar (60,9%), bulud hesablama (34,4%) daha çox qeyd olunan cavablar olub. Bulud hesablamalarından istifadə edənlər kommersiya baxımından həssas məlumatları (18,8%), işçi qüvvəsi haqqında məlumatları (15,6%) və həssaslıq ehtiva etməyən digər məlumatları (20,3%) başqa datalara nisbətən daha çox saxlayırlar.

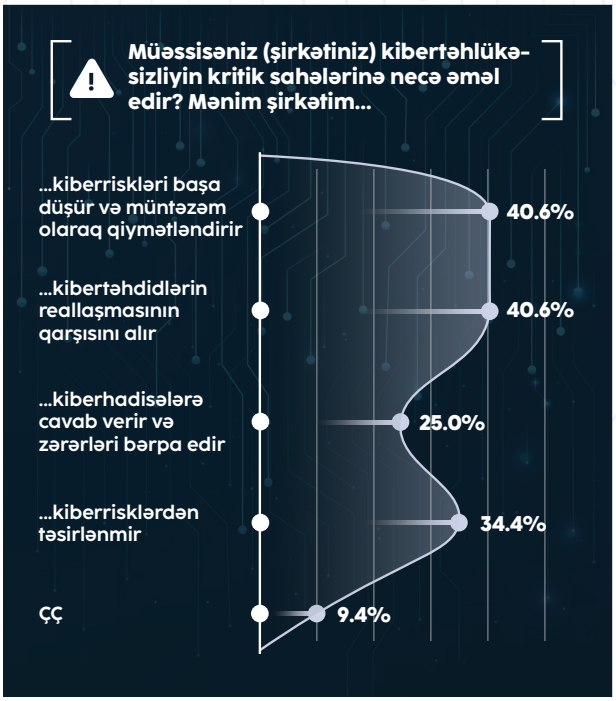
5.5.3.2. Ümumi prioritet və etibarlılıq

Seçmə üzrə ümumilikdə təşkilatların çoxu qurum daxilində kibertəhlükəsizliyi aşağı, ya da qeyri-mövcud səviyyədə qiymətləndirir. Digər tərəfdən, 100-500 və 500-dən çox işçi qüvvəsi olanların 80%-dən çoxu isə kibertəhlükəsizliyi ən ciddi – ilk beşlikdəki risklər sırasına daxil edir, kiçik şirkətlər üzrə bu rəqəm üç dəfədən daha aşağıdır. Maliyyə sektoru müəssisələrinin 64%-nə görə, kibertəhlükəsizlik ən vacib və ya 5 ən böyük risklərdəndir.

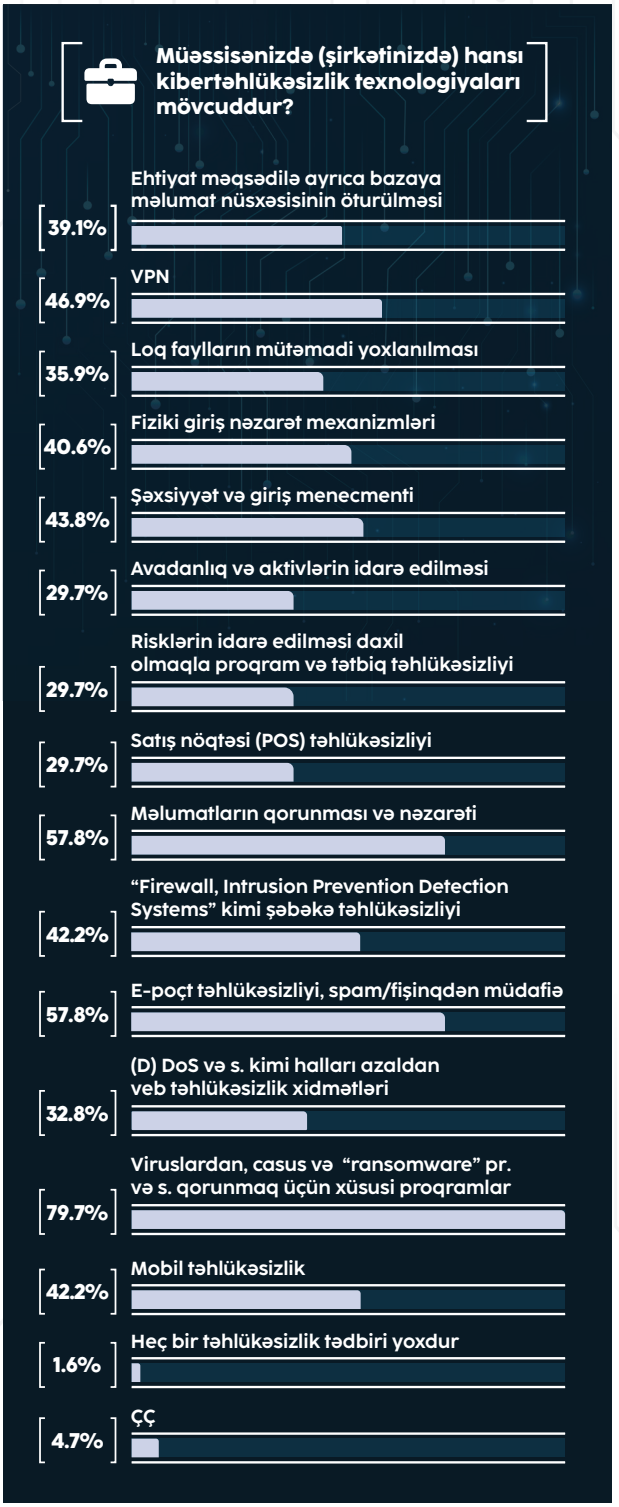
Suala verilən cavablar üzrə daha detallı qeyd etsək, respondentlərin 35,9%-nin fikrincə, kiberhücumlar təmsil etdiyi müəssisə (şirkət) üçün aşağı riskli,18,8% respondent üçün ən ciddi 5 riskdən biri, 17,2% respondent üçün ən böyük riskdir. Sorğu iştirakçılarının 25%-i bu fikri bölüşür ki, kiberhücumlar təmsil etdiyi qurum (müəssisə) üçün heç bir risk təşkil etmir. Respondentlərin 3,1%-i bu suala cavab verməkdə çətinlik çəkib.



Müəssisələr (şirkətlər) üçün kibertəhlükəsizliyin kritik sahələri barədə soruşulduqda, kiberrisklərin qavranılması və qiymətləndirilməsi, həmçinin həyata keçirilməsinin qarşısının alınması seçmə üzrə eyni səviyyədə rast gəlinən cavablardır (40,6%). Sonrakı sırada şirkətlərin (qurumların) kiberhadisələrə cavab tədbirləri və zərərləri bərpa etməsi (25%) gəlir.



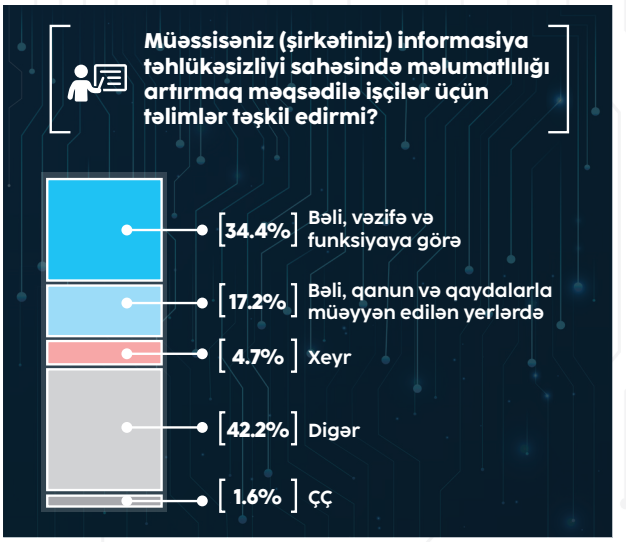
Cavablara əsasən, müəssisələrdə (şirkətlərdə) mövcud olan kibertəhlükəsizlik texnologiyaları sırasında viruslardan, casus proqramları və digər növlərdən müdafiə üzrə zərərli proqram əleyhinə həllərin (proqramların) istifadəsi üstünlük təşkil edir (79,7%). Bu baxımdan, məlumatların qorunması və nəzarət tədbirləri (57,8%), e-poçt təhlükəsizliyi, spam/fişinqdən müdafiə (57,8%), VPN (46,9%) mobil təhlükəsizlik (42,2%), ehtiyat məqsədilə ayrıca bazaya məlumat nüsxəsinin ötürülməsi (39,1%), loq faylların mütəmadi yoxlanılması (35,9%) və s. onlardan sonra gəlir.



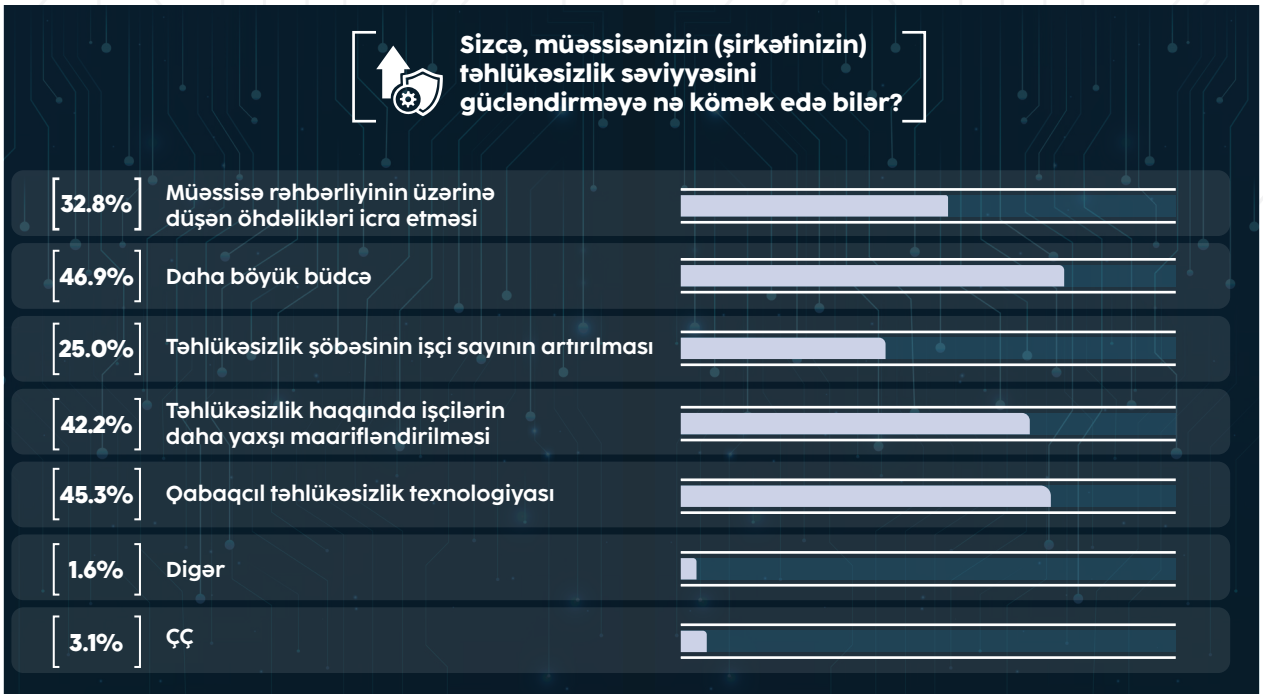
5.5.3.3. Məlumatlılığın artırılması

Müəssisə və şirkətlər informasiya təhlükəsizliyi üzrə məlumatlılığı artırmaq üçün işçilərə (vəzifə və funksiyasına görə) müəyyən ölçüdə təlimlər keçir. Respondentlərin 34,4%-i qeyd edib ki, təmsil etdiyi qurum (şirkət) bu məqsədlə təlimləri vəzifə və funksiyaya görə təşkil edir. Sorğu iştirakçılarının 17,2%-i təlimlərin qaydalarla müəyyən edilən yerlərdə keçirildiyini bildirib.Respondentlərin yalnız 4,7%-i bu məqsədlə heç bir təlimin keçirilmədiyini bildirsə də, 42,2%-i digər səbəbləri qeyd edib.

İşçi qüvvəsi 100-500 və 500-dən çox olan bütün müəssisələr (şirkətlər) təlim təşkil etdiyi halda, 10-99 say həddində işçiyə malik qurumların isə təxminən yarısının belə təlimlər keçirdiyi məlumdur. Sektor baxımından, maliyyə üzrə şirkətlərin üçdə birinin təlim keçirmədiyi faktı diqqət çəkir. Belə nəticə qəbul edilmiş seçmə yanaşmasına uyğun izah edilə bilər (təsadüfi olmayan seçmə tətbiq edilmişdir). Başqa bir səbəb həmin müəssisələr sırasında onların fəaliyyətinin müvafiq təlim tələb edə biləcək formada risk ehtiva etmədiyinə dair təsəvvürlərlə bağlıdır. Bu həm də çoxsaylı müəssisələrin internet istifadəsinə malik olduğu daha inkişaf etmiş iqtisadiyyatlarla müqayisədə Azərbaycanda kibercinayətkarlığın az yayılması aspektilə qismən əlaqəli ola bilər və belə qənaət əsasən şəxsi müşahidələrə söykənən mülahizədir.

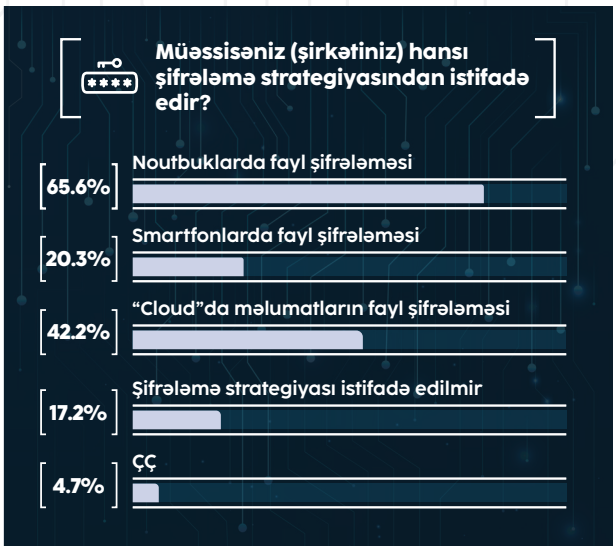


Müvafiq olaraq, 45,3% və 46,9% respondent mütərəqqi təhlükəsizlik texnologiyası və daha miqyaslı büdcələrin tətbiqinin təşkilatın təhlükəsizlik səviyyəsini yaxşılaşdırmağa kömək edəcəyini düşünür. Maraqlıdır ki, rəylərdə ən az ifadə edilən metod təhlükəsizlik şöbəsinin işçi sayının artırılmasıdır (25%). Kiberrisklərin effektiv idarə edilməsində əsas problemlər və ya maneələrin sadalanmasına baxdıqda, resurs çatışmazlığı və kibertəhlükələrin əsas prioritetlər sırasına daxil edilmədiyini bildirən cavablar da diqqəti cəlb edir.

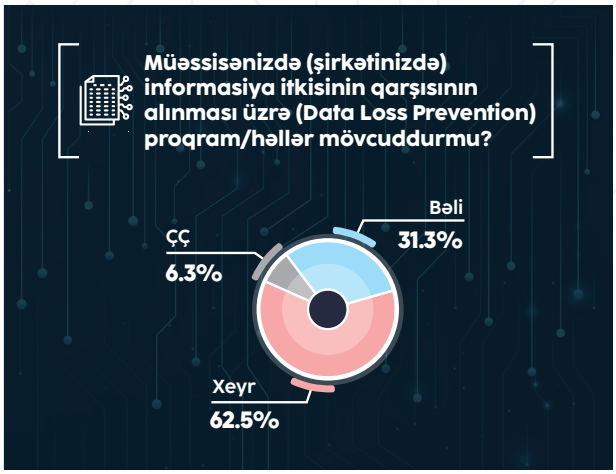


5.5.3.4. Autentifikasiya və şifrələmə

Tədqiqatın nəticələri sübut edir ki, müəssisələrin 65,6%-i qurum daxilində noutbuklarda faylların şifrələnməsini həyata keçirir. Sonrakı sıralarda kloudda məlumatların fayl şifrələməsi (42,2%) və smartfonlarda fayl şifrələməsi (20,3%) gəlir. Sorğuda iştirak edən müəssisələrin (şirkətlərin) 17,2%-i şifrələmə strategiyasından istifadə etmir.

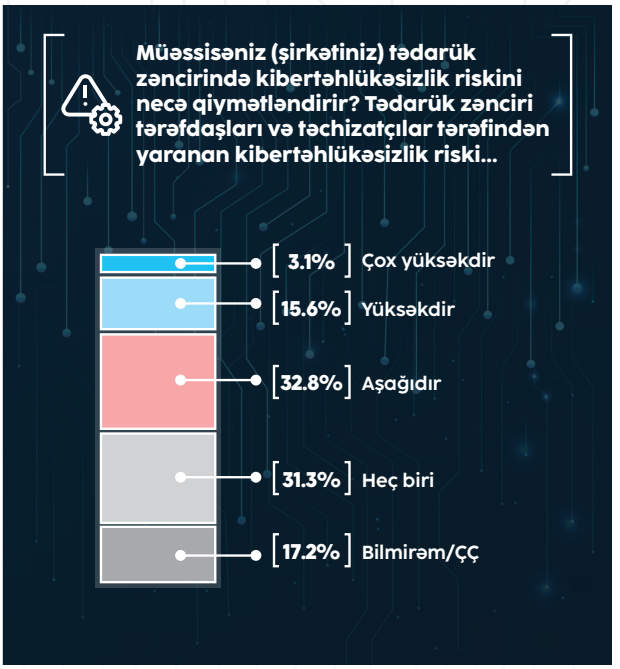


Qurum və müəssisələrdə məlumat itkisinin qarşısının alınması üçün həllər (proqram) geniş yayılmasa da (təşkilatların 62,5%-də istifadə edilmir), ikifaktorlu autentifikasiya cavablarda bir qədər çox rast gəlinən üsuldur (42,2%). Nəticələrə əsasən, təşkilatın miqyası genişdirsə, yuxarıda adı çəkilən proqramın (Data Loss Prevention) tətbiqi ehtimalı həmin səviyyədə yüksəkdir. Digər maraqlı fakt isə maliyyə sektorunu təmsil edən şirkətlərin 43%-də belə proqramın mövcud olmamasıdır.



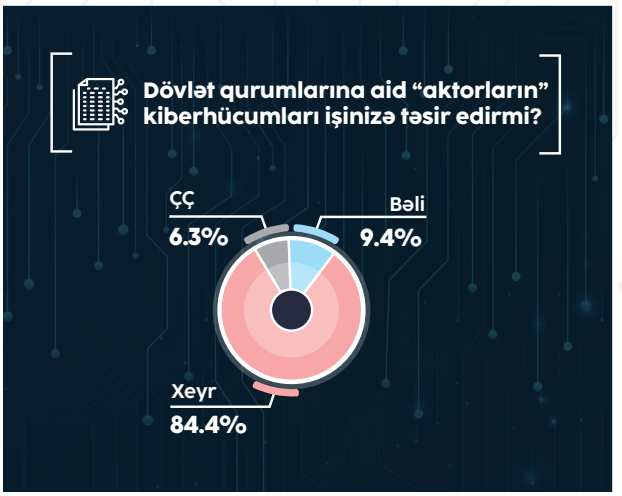
5.5.3.5. Tədarük/təchizat zənciri

Ümumilikdə, tədarük/təchizat zəncirində kibertəhlükəsizlik riski nümunələr üzrə respondent cavablarında kifayət qədər aşağı qiymətləndirilir. Müqavilədə informasiya təhlükəsizliyi məsələlərinin həlli və məxfilik, yaxud məlumatın açıqlanmaması ilə bağlı sənədlərin imzalanması bu istiqamətdə ən çox istifadə edilən müdafiə üsulları kimi tətbiq edilir.



5.5.3.6. Dövlətin/hökumətin rolu

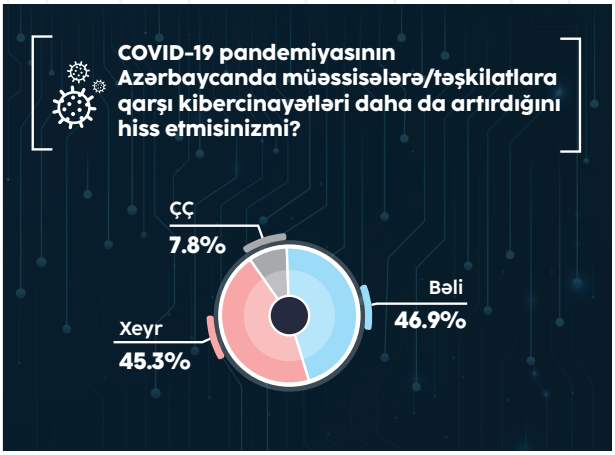
Soğunun nəticələrinə uyğun olaraq, dövlət aktorları tərəfindən həyata keçirilən, məsələn, xaricdən kiberhücumların seçmənin olduqca az hissəsinə təsir göstərdiyi qeydə alınıb (9,4%).



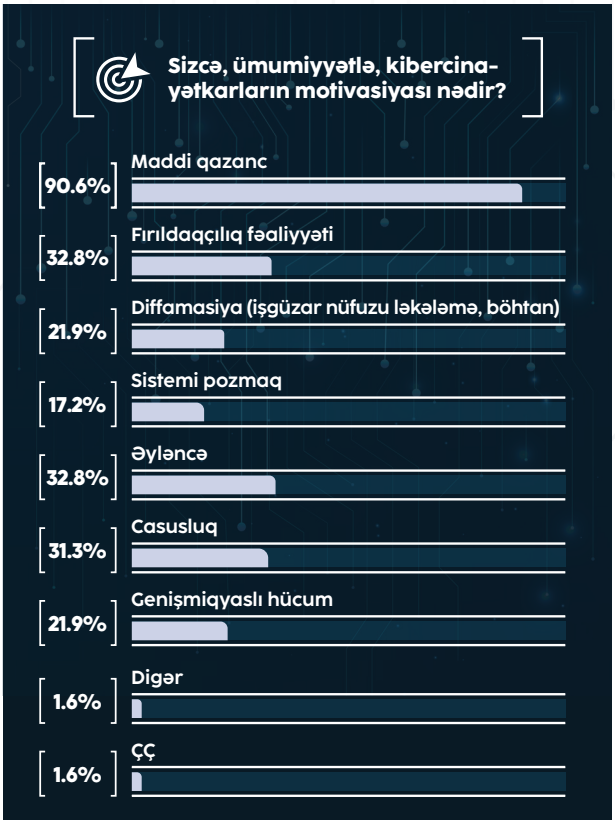
Respondentlərin yanaşmalarında kiber-risklərin idarə olunmasını təkmilləşdirmək üçün nəzərdə tutulmuş hökumət tərəfindən irəli sürülən qaydalara, qanunlara və sənaye standartlarına kifayət qədər müsbət münasibət mövcuddur. Respondentlərin 23,4%-i bunun çox effektli, 46,9%-i isə bir qədər effektli olduğunu düşünür. 10,9% respondent əks mövqedən çıxış edib.

5.5.3.7. Kibercinayətkarlıqla bağlı vəziyyət

Maraqlıdır ki, COVID-19 pandemiyasının qurum və müəssisələrə qarşı kibercinayətkarlığı intensivləşdirməsinə dair suallara cavablar, demək olar ki, "bəli" və "xeyr" variantları arasında bərabər şəkildə bölünüb (müvafiq olaraq 46,9% və 45,3%). Maliyyə sektorunda fəaliyyət göstərən təşkilatların 64,3%-də qeyd edilən sualla bağlı müvafiq artımı təsdiq edən fikirlər müşahidə edilsə də, istehsal müəssisələri üzrə bu göstərici 30,8% təşkil edib.

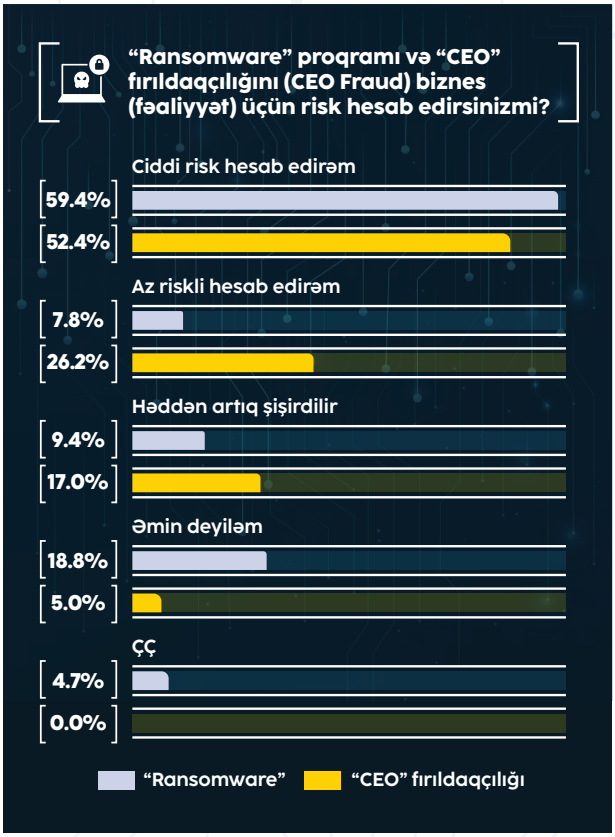


Kibercinayətlərin həyata keçirilməsində motivasiyaedici səbəb kimi ən diqqət çəkən cavab "maddi qazanc" ifadəsidir (90,6%).

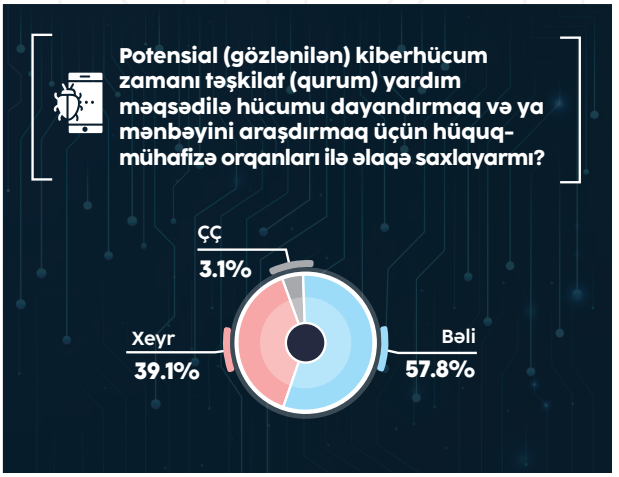


Sonrakı yerlərdə dələduzluq (fırıldaqçılıq) fəaliyyəti (32,8%), əyləncə (32,8%), casusluq (31,3%), genişmiqyaslı hücum (21,9%), diffamasiya (işgüzar nüfuzu ləkələmə, böhtan) (21,9%), sistemi pozmaq (17,2%) gəlir.

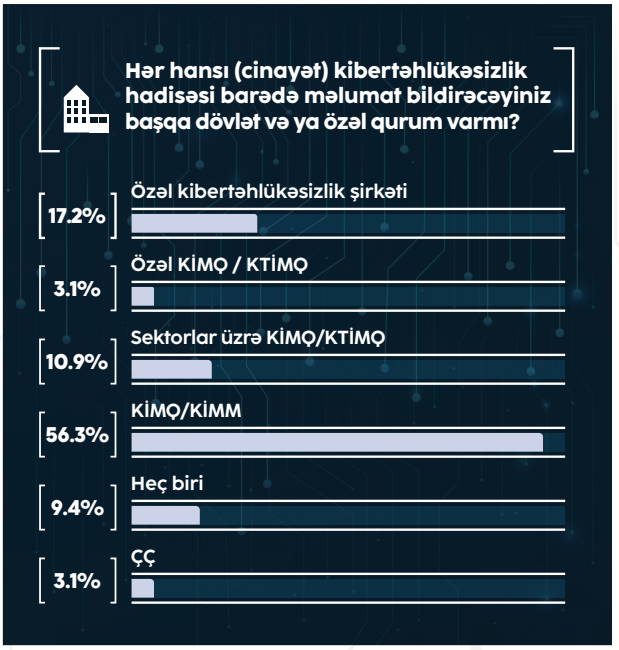
Zərərçəkmə ilə bağlı suallara verilən cavablar qurum və təşkilatlar arasında müvafiq göstəricinin olduqca aşağı həddini üzə çıxarır. Buna baxmayaraq, rənsamveə (59,4%) və "CEO" fırıldaqçılığının (vəzifəli şəxslərin adından icra edilən kibercəhdlər, poçt göndərmə və s.) (52,4%) yüksək risk səviyyələrinə dair respondentlərin rəyində ümumi fikir birliyi də qeydə alınan məqamdır.



Xeyli sayda təşkilat (şirkət) nümayəndəsi (57,8%) potensial və ya uğurlu hücumlar baş verərsə, yardım və ya hücumun mənbəyinin araşdırılması, yaxud dayandırılması üçün işlədiyi qurumun hüquq-mühafizə orqanları ilə əlaqə saxlayacağını bildirib.



Bu mənada cavablar üzrə ən seçilən hüquq-mühafizə təşkilatı Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzidir (KİMM) (56,3%). Digər tərəfdən, fokus qruplarla müzakirələrdə gəlinən nəticələrə oxşar şəkildə aydındır ki, seçmənin geniş hissəsi gələcəkdə kibercinayətlərin miqyasının artacağını düşünür.



5.5.4. Nəticə

Kibercinayətkarlığın qurbanı olma ilə bağlı suallara təqdim edilən cavablar müəssisə və qurumlar üzrə zərərçəkmə hallarının çox aşağı səviyyəsini üzə çıxarır. Halbuki fərdlər arasında fişinq və bank kartları oğurluğu kimi bəzi kibercinayətlərin geniş yayılmasını nəzərə aldıqda, qurumlarla bağlı vəziyyət müəyyən dərəcədə təəccüb doğurur. Digər tərəfdən, sorğular zamanı bəzi respondentlərin uğursuz kibercəhdlər barədə danışmaları da özlüyündə mövcud müdafiə sistemlərinin effektivliyinə işarə edir. Bu baxımdan, tədqiqatın nəticələri sübut edir ki, sorğuda iştirak etmiş hər hansı qurum və ya şirkət son 12 ayda kibercinayətkarlıq səbəbindən pul itkisinə məruz qalmayıb.

Müəssisələrin əhəmiyyətli hissəsinin kibertəhlükəsizliyə cavabdeh xüsusi təşkilati rolu/vəzifəsi və ya departamentinin olması olduqca narahatedici faktdır. Maliyyə məsələləri burada rol oynasa da, respondentlərin fikrincə, bütün qurumlar kibercinayətkarların diqqətini "çəkəcək" məxfi məlumatların idarə edilməsi işi ilə məşğul olmurlar. Üstəlik, kibercinayətkarlıq və ya təhlükəsizliyə görə məsuliyyət daşımamaq xüsusilə kiçik və orta sahibkarlıq subyektləri arasında geniş yayılmış təcrübədir.

İT büdcələri çərçivəsində kibertəhlükəsizlik sığortasının xərc çəkisi barədə respondentlərdən fikir bildirmələri xahiş olunduqda, oxşar mənzərə meydana çıxıb, çünki əksər müəssisələrdə sığorta sektoru üçün mümkün gələcək təsirləri olan bu tip sığorta proseduru tətbiq edilmir. Ümumilikdə, təhlillər belə deməyə əsas verir ki, qurum və şirkətlər arasında kibertəhlükəsizlik xərcləri İT büdcəsinin olduqca kiçik hissəsini təşkil edir.

Diqqətçəkən digər məqam zərərçəkmə səviyyəsi və kadr hazırlığı ilə bağlıdır. Nəticələr göstərir ki, bütün müəssisələr işçilərə kibertəhlükəsizlik üzrə təlim keçmirlər.

Dövlət aktorları tərəfindən həyata keçirilən, məsələn, xaricdən kiberhücumların seçmənin çox kiçik hissəsinə təsiri əlamətdar hal olsa da, sorğu zamanı bir neçə respondent 2020-ci ildə Ermənistanla müharibə dövründə xarici dövlətlərdən gələn kiberhücumların intensivliyi haqqında qeyd edib. Bu baxımdan, Azərbaycandakı mövcud qurumların başqa dövlə-

tin maliyyələşdirdiyi hücumlara qarşı həssas olmadığını, başqa sözlə ifadə etsək, möhkəm olduğunu demək erkən qənaətdir.

Dəstək göstərilməsi üzrə hüquq-mühafizə orqanları ilə əlaqə saxlamaqla bağlı sualda hər bir qurum və ya şirkət əməkdaşı lazım olduğu təqdirdə KİMM-ə məlumat verəcəyini qeyd edib ki, burada digər cavab variantlarının ümumiyyətlə seçilmədiyi (və ya az seçildiyi) nəzərə çarpıb. Beləliklə, sözügedən suala respondentlər tərəfindən təqdim edilən rəylər onu göstərir ki, xeyli sayda kiberhücum qeydiyyatdan kənarda qalıb (zərərçəkənlər aidiyyəti quruma (polisə və s.) məlumat bildirməyiblər).

QEYD: Müəyyən sualları olduqca həssas qəbul edən respondentlərin sayı da az deyil (28,1%). Bu cür vəziyyət qismən büdcə ilə bağlı suallara aiddir. Belə ki, bir çox respondent məxfilik səbəbindən müvafiq sualı cavablandırmayıb.

6. Keyfiyyət tədqiqatı

6.1. Xülasə

- Ümumi əhali qrupları (ÜƏQ) arasında respondentlərin müxtəlif tezliklərdə yalnız üç kibercinayət növü ilə rastlaşdıqlarına dair rəylər müşahidə edilib: onlayn hədə-qorxu, zorakılıq-təhqir və sui-istifadə; şəxsiyyət/kimlik oğurluğu və fişinq.
- Kibercinayətkarlığın qurbanı olma baxımından şəxsiyyət/kimlik oğurluğu həm tezlik, həm də təsir miqyası etibarilə fərqlənir. ÜƏQ-lər üzrə onlayn sui-istifadə/zorakılıq-təhqir (9 hal) şəxsiyyət oğurluğundan (4 bank kartı və 3 sosial media hesabı oğurluğu) bir qədər geniş yayılsa da, zərərçəkənlərə hansısa təsirinin olmadığı qeydə alınıb. Bütün iştirakçıların fişinq zəngləri və elektron poçt məktubları alması, lakin araşdırma zamanı yalnız iki zərərçəkmiş şəxsin müəyyən edilməsi faktı isə özlüyündə həmin kibercinayət növü üzrə yüksək məlumatlılıq və müdafiə səviyyəsini nümayiş etdirə bilər.
- Bütün digər kibercinayət növləri (rənsamveə, şəxsi məlumatların ifşası) son dərəcə məhdud yayılma səviyyəsinə malik olmaqla, hətta bəzi hallarda eşidilməyən hadisələr kimi qeydə alınıb.
- Əksər respondentlər onlayn rejimdə, smartfonlardan istifadə edərkən özlərini təhlükədə hiss edirlər. “Heç nə və heç bir yer təhlükəsiz deyil” ifadəsi sorğular zamanı üstünlük təşkil edən yanaşma kimi nəzərə çarpıb. Təhlükəsizlik amilinə gəldikdə, fokus qruplardan əldə edilən ən mühüm rəylərdən biri internet xidməti provayderlərinin (İXP) nümayəndələri tərəfindən irəli sürülüb. Belə ki, həyata keçirilən bütün ciddi tədbirlərə baxmayaraq, hətta onlar da özlərini tam təhlükəsiz şəraitdə hiss etmədiklərini bildiriblər. Çünki cavablarda da qeyd olunduğu kimi, istifadə edilən cihazlar və proqram təminatları tamamilə xaricdən idxal olunur.
- Kibercinayətin qavranılması üzrə “internet cinayətləri” və “informasiya cinayətləri” ifadələri ÜƏQ-lər arasında mövzunu tam əhatə edən anlayışlar kimi tez-tez səslənsə də, xüsusilə İT mütəxəssisləri və İXP nümayəndələri tərəfindən kəskin fərqli cavablar müşahidə edilib.
- Digər cinayət növlərinə münasibətdə kibercinayətlərin ciddilik dərəcəsi baxımından isə bu hallar potensial daha təhlükəli hesab edilib. Nəticələrə əsasən, kibercinayətlər daha geniş miqyasda cəmiyyətə təsir göstərə bilər, zorakılıq və mülkiyyət əleyhinə cinayətlər isə fərdlər və ya lokal səviyyədə bu imkana malikdir. İT mütəxəssisləri, İXP nümayəndələri və bəzi hüquq-mühafizə orqanlarının əməkdaşları mövzuya nisbətən geniş perspektivdən yanaşmaqla, zərər yetirilməsi məqsədilə başqasının avtomobilinin, yaxud "ağıllı ev" sisteminin asanlıqla qırılmasının mümkünlüyü haqqında fikirlər səsləndiriblər.
- Əksər ÜƏQ-lər və zərərçəkənlər arasında fişinq kibercinayətkarlığın ən çox narahatlıq doğuran növü kimi bəyan edilsə də, digər qruplarda bununla bağlı müxtəlif cavablar (DDoS, kritik infrastruktur sahələrinə hücum və s.) qeydə alınıb.
- Bütün respondentlərin “kibercinayət” sözü, həmçinin onlar üçün sadalanan cinayət növlərinin əksəriyyəti haqqında məlumatlı olmalarına baxmayaraq, fişinq və rənsamveə bu mənada demək olar ki, bilinməyən formalar kimi təsbit edilib. Sorğu iştirakçılarına müvafiq anlayışlarla bağlı izah və tərif təqdim edildikdən sonra onlar artıq sözügedən kibercinayət növlərini tanıdıqlarını ifadə ediblər.
- Yalnız zərərçəkənlər qrupunda bütün respondentlər fişinq hadisələrinin qurbanı olsalar da, həmin şəxslərin heç biri termin kimi fişinq anlayışını tanımayıb.
- Bir qrup respondent (18-21 yaş) gələcəkdə ehtimal şəklində kibercinayətkarlıqdan əziyyət çəkmə vəziyyətində polisi xəbərdar ediləcək bir təsisat kimi görsə də, digər ÜƏQ-lər, eləcə də QHT nümayəndələri polisə müraciəti istisna etməyərək, daha çox İT ekspertinə müvafiq sual ünvanlayacaqlarını bildiriblər. Başqa sözlə, belə respondentlər polisin sözügedən halları idarə etmək qabiliyyətinə aşağı səviyyədə etimad etdikləri üçün adıçəkilən quruma müraciətə yalnız son vasitə kimi yanaşırlar. Beləliklə, bu və yuxarıdakı digər nəticələr kibercinayətlərin müəyyən edilməsi və qeydə alınmasında İT sektoru ilə polis orqanları arasında sıx əməkdaşlığa zərurəti təsdiqləyən faktlardır.
- İstisnasız, bütün qrupların dominant baxışı xüsusən elektron xidmətlərdən (e-gov və e-ticarət) geniş istifadə və rəqəmsallaşma şəraitində kibercinayətlərin gələcəkdə güclənəcəyi ilə bağlıdır.

6.2. Texniki məlumat - respondentlərin strukturuna ümumi baxışı təmin etmək üçün diaqramlar təqdim edilir

Bax: Cədvəl 2 və 3

6.3. Tədqiqatın metodologiyası – tədqiqatla bağlı şərtlərdə təsbit edilib və bütün ölkə üzrə xüsusiyyətləri əhatə edir

Məlumatların toplanılması üsulu

İştirakçıların fikirlərinin öyrənilməsi məqsədilə onlara açıq sualların ünvanlanması və çevik müzakirə mühitinin yaradılması vacib sayıldığı üçün ümumi prosesdə buna zəmin yaradan fokus qrup formatı tətbiq edilib. Tədqiqatın aparılmasında ənənəvi sorğu metodu ilə müqayisədə bu cür üsuldan istifadə respondentlərdən ətraflı və daha detallı cavablar alınmasına şərait formalaşdırıb. Əslində, bütün qruplarda xüsusilə ümumi əhali üzrə sözügedən mühitin təşkili, alternativ qaydada toplanılması çətin cavabların ortaya çıxarılmasında olduqca təsirlidir. Belə ki, sorğu zamanı elə hallar meydana gəlib ki, eyni suala bir və ya iki cavab təqdim edildikdən sonra digər fikirlərin ardıcıl ifadəsi müşahidə edilib.

Sorğunun keçirilməsi zamanı anonimlik - cavabların məxfiliyinə dair iştirakçılara zəmanət təqdim edilib. Bununla yanaşı, müsahibəyə başlamamışdan əvvəl respondentlərdən müvafiq yazılı razılıq alınıb. Moderator köməkçisinin iştirakı ilə bütün müzakirələr səs yazısının qeydə alınması vasitəsilə aparılıb.

Müzakirələrin dördü (bütün ÜƏQ-lər, İXP nümayəndələri) otel konfrans zalında üzbəüz qaydada həyata keçirildiyi halda, üç müzakirə zum (zoom) proqramı ilə aparılıb. Zərərçəkmiş şəxslərin coğrafi baxımından müxtəlif ərazilərə yayılması səbəbindən zum platforması burada daha məqsədəuyğun seçim kimi müəyyənləşdirilib. Digər iki qrupda isə iştirakçıların iş qrafikləri onların ofis mühitindən kənara çıxmalarına maneə yaradan amil kimi ortaya çıxıb.

Son anda sorğuda iştirakdan imtina etmə səbəbindən (xüsusilə ali təhsil səviyyəsi aşağı olan potensial iştirakçılar tərəfindən) bütün ÜƏQ-lərdə qrup miqyası bəzi hallarda dəyişikliyə məruz qalıb. Bu halda müəyyən qruplar üzrə kvota tam yerinə yetirilməyib. Digər qruplarla əlaqədar yeganə problem isə İT mütəxəssisləri və QHT nümayəndələri ilə bağlı müşahidə edilib. Belə ki, onların işlədikləri yerdə gözlənilməz vəziyyət yarandığına görə üç İT mütəxəssisi prosesə qoşula bilməyib.

Seçmə

ÜƏQ-lər üzrə iştirakçılar (tədqiqatın aparılmasında "qartopu" texnikası istifadə edilməklə) başlıca olaraq iki istiqamətdə komplektləşdirilib: a) tədqiqat qrupunun tədris həyata keçirdiyi universitetlərin tələbələri və b) digər agentliklərlə əməkdaşlıq zamanı formalaşmış əlaqələr vasitəsilə. Sorğu nəticəsində zərərçəkmiş şəxslər əvvəlcədən müəyyən edilib. Mobil telefon nömrələri qeyd edilərək sonradan Sosial Tədqiqatlar Mərkəzinin (STM) sorğu qrupu tərəfindən onlarla əlaqə saxlanılıb. Digər tərəfdən, bir sıra hüquq-mühafizə orqanlarına rəsmi dəvət məktubları göndərilib. QHT nümayəndələri və İT sektorunun mütəxəssisləri isə həm rəsmi dəvət məktubu, həm də STM-in İT/Media departamenti tərəfindən birbaşa əlaqə saxlanılmaqla prosesə cəlb edilib.

Əlçatanlıq və xərc məsələləri ilə bağlı olaraq yalnız Bakı şəhəri seçim kimi müəyyənləşdirilib. İki nəfər zərərçəkmiş istisna edilməklə, zum iştirakçıları da Bakı ərazisini təmsil edənlər olub. Beləliklə, bu tədqiqatın coğrafi yayılma/təmsil olunma məhdudiyyətləri diqqətdə saxlanılaraq, nəticələri şərh edərkən oxucuların qeyd edilən amilləri nəzərə almaları vacibdir.

İşlərin icrasında sadəcə üz-üzə qrupların imzalı siyahısı mövcuddur, digər təsdiq materialları isə zum (zoom) ekran görüntüləri və bir votsap (WhatsApp) qrup zəngidir. Bütün təhlillər və s. tamamlandıqdan sonra yekun siyahı tərtib edilib. Yuxarıda qeyd edilən fotomateriallar, yaxud imzalı siyahılar isə ancaq rəsmi tələb qaydasında təqdim edilə bilər. Cins və yaş göstəricilərinin siyahısı üçün müvafiq cədvələ baxmaq tövsiyə edilir (*Bax: cədvəl 1, səh. 88).* Əlavə diqqət yetirilməli məqam odur ki, hüquq-mühafizə orqanları əməkdaşlarından ibarət fokus qrupda məxfilik aspekti nəzərə alınaraq sorğu zamanı istifadə edilən kompüterlərin kameraları işə salınmayıb.

Çətinliklər

Keyfiyyət datalarının toplanılması ilə bağlı problemlər baxımından ÜƏQ-lər üzrə respondentlərin əksəriyyətinin əhatə olunan bir çox cinayətlərdən xəbərsiz olması vacib məqamlardan biridir. Bu səbəbdən fokus qrupda iştirakçılıq forması əsasən qeyri-fəal olduqda xeyli fərqli şərait meydana gəlir. Bu problem xüsusilə gənclərin daha çox təmsil olunduğu

qrupda müşahidə edilib. Zərərçəkmiş şəxslər arasından dəvət olunan 11 nəfərdən 6-sı müzakirələrə qoşulsa da, onlardan birinin internet bağlantısı zəif olduğu üçün müzakirəni bir qədər gec bitirməli olub. Beləliklə, seçmə miqyasında müvafiq məhdudiyyətlərin mövcudluğu da qəbul edilməli digər haldır.

Hüquq-mühafizə orqanları ilə əlaqə saxlanılarkən sorğu aparılması prosesinin asanlığına baxmayaraq, bəzi nazirliklərin əməkdaşlarının fokus qruplarda iştirakı üçün rəsmi razılıqların alınması xeyli vaxt aparıb. İkincisi, hüquq-mühafizə orqanlarında kişi işçi qüvvəsi üstünlük təşkil etdiyinə görə bu qrupa yalnız bir qadın iştirakçı cəlb edilib. Eyni amil heç bir qadın iştirakçının qoşulmadığı digər qruplarla bağlı da qeyd edilə bilər. Belə vəziyyət işçi qüvvəsinin əhəmiyyətli hissəsinin kişilərdən ibarət olması ilə izah edilə bilər ki, bunun səbəbləri hazırkı tədqiqatın çərçivəsindən kənar mövzudur. Üçüncü məsələ prosesdə yalnız iki qurumun iştirak etməsidir.

Ümumilikdə, 70 nəfər iştirakçının toplanmasının mümkünsüzlüyü bu amillərlə bağlı olub: a) son anda prosesi tərk edənlərin mövcudluğu; b) həvəsləndirmənin olmaması və c) zum, yaxud digər oxşar tətbiqdən istifadə hər kəsə uyğun və rahat olmadığı üçün bir çox zərərçəkən şəxsin səyahət xərclərinə dair büdcə çatışmazlığı səbəbindən iştirakdan yayınma.

Müşahidələr göstərir ki, tədqiqat mövzusu vətəndaşların sorğuda iştirakla bağlı könülsüzlüyü üçün motiv təşkil etməyib. Lakin vacib məqam yalnız peşəkarlar qrupu və müəssisələr/şirkətlər arasında gender bölgüsündə əhəmiyyətli problemin nəzərə çarpmasıdır.

Sorğuya cəlb edilən müəssisə və təşkilatlarda İT departamentlərinin qeyri-mövcudluğu və ya İT ilə əlaqəli fəaliyyətlərin aparılmaması da prosesə təsir edən digər bir aspektdir. Kənd yerlərində bu hal çox ciddi bir məsələ kimi qarşıya çıxdığı üçün işin gedişatında diqqətin yalnız Bakı ərazisinə yönəldilməsi zərurəti yaranıb. Yetərli motivasiya tədbirlərinin olmaması isə iştirakçıların cəlb edilməsində çətinlik yaradan digər faktora çevrilib. Bu mənada, şəxsən əlaqə saxlanılan yalnız iki təşkilat/qurum tədqiqatda iştirak edib.

Dövlət təhlükəsizliyi xidmətləri və internet provayderləri arasında müəyyən suallara cavab verməkdən imtina halları da meydana gəlib. Belə ki, bəzi respondentlər həmin sualları həddən çox həssas və müdaxiləçi hesab ediblər. Həmçinin, ən gənc yaş qrupunu əhatə edənlər bir çox cinayətlərdən xəbərsiz olduqları üçün bu halda qrupun qeyri-fəallığı nəzərə çarpıb.

Təhlil

Kateqoriyaları sürətli və asan yaratma qabiliyyətinə və böyük verilənlər bazasını idarə etməsi baxımından təqdim etdiyi imkanlara görə hazırkı tədqiqatda “Nvivo” keyfiyyət təhlili proqramının tətbiqindən istifadə edilib.

Hazırlanma prosesinin ardınca bütün müsahibə stenoqramlarının moderator (layihənin keyfiyyət tədqiqatı hissəsinin meneceri) tərəfindən təhlili aparılıb. İxtisar edilmiş transkripsiya üsulundan istifadə edilməklə, burada söhbətin yalnız müvafiq hissələri yazı şəklində qeydə alınıb. Müsahibə stenoqramlarının tədqiqatı tematik təhlil üzrə həyata keçirilib (Braun & Clarke, 2006). Tematik təhlil data çərçivəsində nümunələr və mövzuların müəyyənləşdirilməsi, təhlil aparılması və hesabat təqdim edilməsi üsulu kimi konseptuallaşdırılıb. Hər bir transkriptdə açar sözlər qeyd olunmaqla və ortaya çıxan bütün mövzulara kod verilməsi nəticəsində onların digər transkriptlərdə mövcudluğunun yoxlanılması tətbiq edilib. İndividual şəkildə toplanan nəticələr sonradan hər bir suala əsas cavabların tapılması məqsədilə qruplaşdırılıb.

Tədqiqatda respondentlərin fikirlərinə də yer verilməsi üçün sitatlardan istifadə edilib. Hər bir sitata qısa adlar əlavə olunmaqla, anonimliyin qorunması üçün yalnız qrup nömrəsi (ÜƏQ üzrə) və ya ID nömrə (digər qruplar üzrə) göstərilib.

6.4. Ümumi Əhali Qrupu (ÜƏQ)

Qrup müşahidələri

Qrup 1 – əsasən 5-6 nəfərin dominant olduğu qrup daha çox tələbələrdən ibarətdir. Bu qrup daxilində yalnız bir neçə suala çox məhdud sayda cavab qeydə alınıb.

Qrup 2 – olduqca fəal qrupdur. Qarışıq peşə sahiblərindən ibarətdir.

Qrup 3 – olduqca fəal qrupdur. Qarışıq peşə sahiblərindən ibarətdir. Burada yalnız bir xanım respondent qeyri-fəal olmaqla, həm də yaşca ən böyük və ali təhsili olmayan iştirakçıdır. O, həmçinin digərlərindən daha məhdud internet istifadəsinə malikdir.

6.4.1. Onlayn fəaliyyətlər (ümumi istifadə)

Respondentlər qoşulduqları sosial media platformaları və onlardan gündəlik istifadə müddəti ilə bağlı rəylərində olduqca fərqlənib-lər. Xüsusilə jurnalistlər və tədqiqatçılar peşə-kar zərurət səbəbindən onlayn fəaliyyətlərinin yüksək həddə olmasını (gündəlik 10 saatdan çox) qeyd ediblər. Əslində, onlar üçün sosial media işlə bağlı istifadə edilən müstəvilər-dən biridir (yəni araşdırmalarını, müsahibələ-rini paylaşmaq üçün və s.). Tələbələr isə bu platformalardan həm təhsil, həm də qarşılıqlı əlaqə və paylaşımlar etmək məqsədilə demək olar ki, bərabər miqyasda istifadə edirlər. Həmçinin, bütün qruplar üzrə xəbərlərin oxun-ması baxımından sosial mediadan istifadə ikinci yerdə dayanır.

Onlayn rejimdə təhlükəsizlik məsələsinə gəldikdə, bir çoxları (n=12, 46%) narahatlıq-larını ifadə ediblər. Bu iştirakçılar daim zərər-çəkmə qorxusuna malik şəxslərdir. Qalan iştirakçıların isə müəyyən qədər həyəcanlı ol-maları müşahidə edilsə də, müxtəlif səbəblər-lə bağlı (məsələn, şəxsi məlumatlarını təqdim etmirlər, müəyyən veb-saytlara daxil olmurlar, ehtiyat tədbirləri görürlər və s.) eyni dərəcədə qorxu keçirmədikləri aydın olur. Beləliklə, təh-lükəsizlik aspekti üzrə respondentlər arasında ümumi əhval-ruhiyyə bir qədər şübhə doğuran yanaşmalar ehtiva edir. Başqa sözlə, demək olar ki, heç bir respondent özünü bu mənada tam müdafiədə hiss etmir.

Qrup 2 və Qrup 3 arasında "təhlükəsiz heç nə yoxdur", "gizlilik mümkün deyil" və "inter-netdə mövcud olan istənilən məzmun təhlükə riskləri ehtiva edir" kimi ifadələr respondentlə-rin lazımi müdafiənin təmin olunması ilə bağlı müəyyən acizlik hiss etdiklərini üzə çıxarır. İş-tirakçıların hər biri müvafiq risklərdən müda-fiənin necə mümkün ola biləcəyini müzakirə etməsələr də, nisbətən çox sayda respondent istifadəçilərin yalnız özləri tərəfindən mühа-fizənin mümkünlüyü barədə düşünürlər (yəni şəxsi məlumatlarını geniş şəkildə digər şəxs-lərlə bölüşməyərək). Əslində, iki respondent mövcud kiberməkanı cəmiyyətin "Orvellian təsviri" ilə eyniləşdirir. Mühafizənin haradan təmin olunmasına dair ümumi yanaşma həm istifadəçilərin, həm də provayderlərin (burada provayder dedikdə, məsələn, istifadəçilərə geniş onlayn ünsiyyət məkanı təqdim edən Feysbuk və s. kimi platformalar nəzərdə tu-tulur) öz rolunu icra etməsilə bağlıdır. Lakin rəylərə əsasən məlumdur ki, respondentlərin bir çoxu həmin şəraitdə də özlərini tamamilə təhlükəsizlikdə hiss etmirlər.

"Süni intellektin sosial mediada necə işlə-diyini dəfələrlə sınaqdan keçirmişəm. Haqqın-da düşündüyüm və axtardığım hər şey tez-tez kompüterimin ekranında görünməyə başlayır. Beləliklə, onlar ağlımızı oxuyur" (Bunu deyərkən üz ifadəsi və səs tonu qadın respon-dentin narahatlıq səviyyəsini nümayiş etdirib). Qrup 3

"Smartfon və ya hər hansı ağıllı cihaz sahi-bi olanlar həssas qrupa daxildir. Onlar özlərini təhlükəsiz hiss edə bilməzlər". Qrup 3

"İstifadə edərkən özümü təhlükəsiz hiss et-diyim yeganə platforma istifadəçi hesabı tələb etməyənlərdir. Deməli, xəbər agentlikləri buna bariz nümunədir". Qrup 2

"Heç bir sosial media platforması məlu-matlarımızın təhlükəsizliyinə zəmanət vermir. Beləliklə, burada özünü təhlükəsiz hiss etmək olmaz, lakin bu, insanın sosial tələbatıdır, orada profilə malik olmaq lazımdır". Qrup 1

"İstifadəçi blok edə, hansısa təhdid yaran-dıqda bank kartı məlumatlarını dondura, yaxud müdafiə üçün başqa növ addımlar ata bilər, la-kin bizdən asılı olmayan hallar da mövcuddur" (Fikrini bildirərkən respondentin çarəsiz ifadə ilə başını hərəkət etdirməsi müşahidə edilib). Qrup 3

"İcazə verin cavabımı dolayı yolla ifadə edim. Hesab yaratdıqda və ya kukiləri (coo-kies) qəbul etdikdə məlumatlarımıza giriş im-kanı təmin edirik. Əslində, biz onları heç vaxt oxumuruq. Fərdi məlumatlarımız mühüm əhə-miyyət daşımaya bilər, lakin bütün istifadəçilə-rin məlumatları toplandıqdan sonra bu, artıq vacib datadır. Amma qeyd etdiyim səbəbdən mənim üçün bu, böyük təhlükə deyil". Qrup 2

"Maraqlısı odur ki, texnoloji şirkətlərin mə-lumatlarımıza girişini məhdudlaşdıra bilərik, lakin onların istifadə üzrə şərtlərini qəbul et-məsək, proqramlar və ya sosial media bizim üçün istifadəyə açıq olmayacaq. Üstəlik, bir jurnalist kimi siyasətlə əlaqəli olduğum üçün hər dəfə internetə daxil olduqda və ya proqram yüklədikdə özümü kibercinayətkarlığa qarşı həssas kateqoriyada hiss edirəm". Qrup 2

"Fərdlər olaraq biz haqqımızda bütün məlumatları toplamaq üçün şirkətlərə hər imkanı vermişik". Qrup 3

"Bütün bank və maaş kartlarımız telefonumuzdadır. Ödənişləri və onlayn alış-verişi oradan edirik. Bəli, bu, məni bir az qorxudur". Qrup 3

Elektron hökumət (e-gov) xidmətlərindən 1-ci qrupun iştirakçıları arasında həm tətbiq motivləri, həm də ziyarətlərin tezliyi baxımından çox məhdud sayda istifadə səviyyəsi qeydə alınsa da, bütün digər respondentlər tərəfindən müntəzəm istifadənin olması müşahidə edilib. Əksəriyyət bu xidmətlərdən rüblük vergi və qazanc bəyannamələri, bəziləri isə müəyyən sənədlərin (şəxsi məlumatlar) yoxlanılması və çapı üçün istifadə edir. 1-ci qrupun iştirakçıları arasında əsas motiv təhsil haqqının ödənilməsidir. Ümumən, bütün seçmə üzrə geniş şəkildə ifadə edilib ki, dövlət mülkiyyətində olduğuna görə elektron hökumət xidmətlərindən istifadə edənlər (n=10, 38%) onun müdafiə sistemi ilə bağlı özlərini yüksək təhlükəsizlikdə hiss edirlər. Digər tərəfdən, yalnız dörd istifadəçi bu mənada narahatlığını bölüşüb:

"Heç kim təhlükəsizliyə yüz faiz zəmanət verə bilməz. Pandemiyanın erkən dövründə xarici hakerlər "e-gov"un bir hissəsi olmasına baxmayaraq, müvafiq sistemdən COVID-19-a yoluxmuş bütün xəstələrin siyahısını oğurlayıb ifşa etdilər". Qrup 3

Elektron ticarətlə bağlı, təxminən bütün respondentlər (1-ci qrupda bir nəfər istisna olmaqla) müxtəlif tezliklərdə ondan istifadə etdiklərini bəyan ediblər. Maraqlıdır ki, təhlükəsizliklə əlaqədar soruşduqda bir çox istifadəçi bu barədə hələ düşünmədiyini əsas gətirərək cavab verməkdə çətinlik çəkib. Müzakirə zamanı demək olar ki, bütün respondentlər sözügedən mövzuda çox az və ya heç bir risk görmədiklərini bildirib. Buna baxmayaraq, altı respondent elektron ticarət üçün xüsusi ehtiyat tədbirləri həyata keçirdiyini ifadə edib. Həmin ehtiyat tədbirləri kart hesabında az miqdarda pul saxlamaq və ya hər hansı məbləğ saxlamamaq, yaxud iki kartdan istifadə etməkdən ibarətdir (onlardan biri məhz elektron ticarət üçün nəzərdə tutulur). Yəni, adətən, məhz e-ticarət məqsədilə istifadə edilən kartа yalnız əməliyyat üçün tələb olunan məbləğ depozit edilir. Diqqətə çatdırılan əsas narahatlıq isə ödəniş həyata keçirildiyi halda heç bir əşyanın əldə olunmaması və ya keyfiyyətsiz əşyanın təqdim edilməsinə dair respondentlərin rast gəldiyi hadisələrdir.

"Məbləğ əsas məsələdir. E-ticarət platformasında hesabımda 100 manat olduqda düşünürəm ki, bu məbləği itirsəm sadəcə həmin qədər itirmiş olaram və tezliklə onu bərpa edə bilərəm. Ancaq hesabda 400-500 manat olsaydı, geri qaytarıla bilməyəcək itkiyə çevrilə bilərdi və şübhəsiz ki, belə vəziyyət məni daim narahat edərdi". Qrup 2

"Mən yalnız e-ticarət üçün ayrıca kart istifadə edirəm və ona sərf etdiyim məbləğ, adətən, az olur". Qrup 2

Onlayn rejimdə tətbiq edilən müdafiə tədbirləri baxımından fərqli platformalarda müxtəlif üsullar ortaya çıxır ki, onlara ayrıca nəzər yetirmək faydalıdır. Sosial mediaya diqqət etdikdə, respondentlərin yarısı (n=13, 50%) açıq tədbirlər gördüyünü bildirir ki, bunlardan bəziləri aşağıda ifadə edildiyi kimidir:

"Sosial media hesabımda ikifaktorlu identifikasiya funksiyasını aktiv etmişəm. Beləliklə, kimsə ona daxil olmaq istəyərsə, telefonuma xəbərdarlıq mesajı gəlir". Qrup 1

"Müdafiə tədbiri olaraq qəbul etdiyim addımlara tam inamım olmasa da, şifrəmi mütəmadi qaydada dəyişirəm". (Fikrini bildirərkən üz ifadəsi ümidsiz, aşağı etimad səviyyəsini təsdiqləyici şəkildə idi). Qrup 2

"Uzun və mürəkkəb şifrələrdən istifadə edirəm – 15-20 simvol, sözlər… Üstəlik, bütün sosial media hesablarımda ikifaktorlu identifikasiyanı qəbul edirəm". Qrup 2

"Vacib və həssas mövzularda Feysbuk vasitəsilə mesajlaşmıram. Hətta ürək simvolu kimi bəzi emojilərdən də istifadə etmirəm". Qrup 3

Cihazlarla bağlı müdafiə tədbirlərinin həyata keçirilməsi nöqteyi-nəzərindən bütün qruplar üzrə "Şifrə istifadə edirəm" ifadəsi üstünlük təşkil edir. Lakin yalnız dörd sorğu iştirakçısı əlavə vasitələr tətbiq etməsi (məsələn, ikifaktorlu identifikasiya) haqqında qeyd edib.

6.4.2. Kibercinayətkarlıq və kibertəhlükəsizlik üzrə bilik səviyyəsi

Respondentlərin əksəriyyəti pandemiyadan əvvəl və pandemiyadan sonra kibercinayətkarlığın dinamikası ilə bağlı sualın cavablandırılmasında çətinlik çəksələr də, bir neçə nəfər (xüsusilə, 36-65 yaş qrupu) eşitdikləri məlumatlar əsasında artım müşahidə etdiklərini qeyd ediblər. Beləliklə, müvafiq suala yalnız 5 respondent cavab verməklə, onların hamısı son 2-3 il ərzində kibercinayətkarlıq fəaliyyətinin genişləndiyini təsdiqləyib.

Bütün respondentlər müxtəlif kontekstlərdə (məktəb, bank təlimi, jurnalistika) olmaqla "kibercinayət" sözü haqqında eşitdiklərini ifadə ediblər. İstisna hal kimi iki respondent Ermənistanla müharibə zamanı bu haqda bildiyini qeyd edib. Beləliklə, respondentlərin 11-i (42%) bu terminlə ilk dəfə məktəbdə, yaxud universitetdə tanış olduğunu deməklə (9-u əsasən tələbələrdən ibarət 1-ci qrup iştirakçısıdır), yerdə qalan yaşlı respondentlər müvafiq anlayışı işdə, xəbərlərdə, yaxud 2020-ci ildə Ermənistanla müharibə zamanı eşitdiklərini səsləndiriblər.

Kibercinayətkarlıq və kibertəhlükəsizlik – spesifik hallar

Kibercinayətin mənasının necə anlaşılması ilə bağlı suala 1-ci qrupda yalnız 2 kişi və 1 qadın respondent cavab verməklə, digərləri bununla ya razılaşıb, ya da fikir ifadə etməyib. Bu qrupda öz yanaşmasını bölüşənlər kibercinayətkarlığı bu tərkibi formalaşdıran meyarlara uyğun gələn və virtual sferada baş verən istənilən akt kimi təsvir edib.

Buna baxmayaraq, ümumilikdə "internet cinayətləri" və "informasiya cinayətləri" ifadələrinə mövzunu əhatə edən anlayışlar qismində tez-tez rast gəlinib. Bəziləri (n=3) bunları ənənəvi cinayətlərin rəqəmsal versiyası kimi dəyərləndirib. Digər tərəfdən, özlərinin, ya da qohumlarının uşaqlarına zərər verdiyi üçün yalnız 3-cü qrupda müəyyən respondentlər (n=3) videooyunları kibercinayətkarlıq növü kimi ifadə ediblər. Paralel olaraq, respondentlərin yarıdan çoxu (n=16, 62%) bank kartlarının oğurlanması, DDoS (kibermüdaxilə, kiberhücum) və sosial media hesablarına giriş, eləcə də bütün onlayn fırıldaqçılığı kibercinayət nümunələri kimi təqdim edən cavabları dərhal səsləndiriblər. Ən çox bilinən cinayətlər bank kartları məlumatlarının oğurlanması (n=14, 53%), spam məktublar (n=4, 15%) və uşaqlara qarşı onlayn zorakılıqdır (n=3, 11%).

Kibercinayətin digər cinayətlərə münasibətdə ciddilik səviyyəsinə gəldikdə, qruplararası və qrupdaxili fərqlər müşahidə edilib. Bununla belə, ümumilikdə yalnız üç respondent sözügedən halları digər cinayətlərdən daha az ciddi forma kimi qəbul edib (və burada onlar yalnız zorakılıq cinayətlərini qeyd ediblər). Qalan respondentlərin hamısı bu barədə danışmasa da, onlardan 18-i (69%) hesab edib ki, kibercinayətlər təsir gücü baxımından digər cinayətləri asanlıqla üstələyə bilər. Bu mənada tez-tez səslənən fikir (n=20, 77%) kibercinayətlərin geniş cəmiyyətə təsir göstərə biləcəyi, zorakılıqla bağlı, yaxud mülkiyyət əleyhinə cinayətlərin isə fərdi və ya yerli-lokal səviyyədə olmasıdır.

"Kibercinayətin bərpa edilən nəticələri olur, lakin zorakılıq cinayətləri baş verdiyi təqdirdə dəyən zərər ödənilmir". Qrup 1

"Bəzi hallarda kibercinayət digərlərindən daha ciddidir. Məsələn, müharibə zamanı ölkəni məğlub etmək üçün hərbi sirləri oğurlamaq fərdi cinayətlərdən daha ciddi nəticələrə səbəb ola bilər". Qrup 1

"Bütün cinayətlər, fikrimcə, bərabərdir. Kibercinayət haqqında danışdıqda, şəxsi məlumatların oğurlanması zərərçəkmiş şəxsin hətta intiharı ilə nəticələnə, sosial-psixoloji sarsıntı hadisəsi meydana gətirə bilər. Bunu onlayn hədə-qorxu, zorakılıq-təhqirə də aid etmək olar". Qrup 3

"Kibercinayətlərin kütləvi ideoloji nəticələri yarana bilər. Dünən saxta xəbər eşitdim ki, milli qəhrəman olan generalımızı oğurlayıblar. Bu kimi halların millətin psixoloji vəziyyətinə ciddi təsiri olur". Qrup 3

"Bəzən bilərəkdən yalan xəbərlərin yayılması insanlara psixoloji və mənəvi zərər verə bilər". Qrup 2

"İcazə verin, sizə yaxın zamanların nümunəsi haqqında danışım. Son günlərdə narkotik böhranı yaşanır. Onların satışı İnstaqramda, eləcə də digər sosial media platformalarında həyata keçirilir. Daxili İşlər Nazirliyi bildirib ki, bütün belə əməliyyatlar kiberməkanda kriptovalyutalar vasitəsilə aparılıb. Görürsünüz, ki-

berməkanın yaratdığı imkanlardan çox sayda insan əziyyət çəkir". Qrup 3

Rəylərdə kibercinayətkarlıq motivlərinin ənənəvi cinayətlərdən fərqlənmədiyi ilə bağlı konsensus müşahidə edilib. Burada iki daha geniş yayılmış cavab nəzərə çarpıb - qazanc əldə etmək (n=7, 27%) və qisas almaq (revanş) (n=7, 27%). Lakin iştirakçıların hamısı bununla bağlı rəy bildirməyib.

"Eyni hallardır, sadəcə indi daha müasirləşib. Vasitələr dəyişib... Bu həm də cinayətkarları görünməz edir və onlara əlavə üstünlük qazandırır". Qrup 3

"Özünüreallaşdırma amili – əgər ailədə kimsə müəyyən səbəbdən təsirlənir, təhqir edilir və ya buna bənzər hansısa hala məruz qalırsa, bu zaman "sizə nə edə biləcəyimi görün" - qisas düşüncəsilə kibercinayətkarlıqdan özünü sübut etmə vasitəsi kimi istifadə edir". Qrup 2

"Bəzi insanların bunları məhz şəxsi düşmənçilik zəminində etdiyini görmüşəm. Yəni, məsələn, oğlanlar hansısa qızın hesabını oğurlamaq və onun nə ilə məşğul olduğunu öyrənmək və s. kimi oxşar məqsədlər üçün bu əməlləri edirlər. Həmçinin, muzdlu bir qatil kimi haker onu işə götürən müştərilərin (sifarişçi) tələbi ilə hesabların müdafiə sistemini qırmaq, kiməsə hücum etmək və bütün belə niyyətlər üçün deyilənləri icra edir". Qrup 2

"Asanlıqla və sürətli şəkildə pul qazanmaq istəyənlər üçün yaxşı vasitədir". Qrup 3

Kibercinayətlərin digər cinayətlərlə bənzərliyinə dair soruşduqda nəticələrin əvvəlki sualın cavabları ilə oxşarlığı aydın olub. Ümumi fikir ondan ibarətdir ki, kibercinayətlər xarakter etibarilə başqa cinayətlərdən çox fərqlənmir, bu cür cinayət "köhnə" əməlləri törətmək üçün sadəcə fərqli bir vasitədir. Bununla belə, hazırkı hesabatda yuxarıda qeyd olunduğu kimi, ümumi seçmənin üçdə ikisi kibercinayətlərin unikal xüsusiyyəti – daha geniş cəmiyyətə təsir etmək gücü barədə fikrə malikdir. Burada az sayda iştirakçı isə kibercinayətləri müqayisə edərkən "cinayətkarın görünməzliyi" ifadəsini sözlərinə əlavə edib.

Birinci qrupda əksər iştirakçılar kibercinayətkarlığın qurbanı olma ehtimalı üzrə hansı əhali kateqoriyasının daha həssas olması ilə bağlı fikir ifadə etməsə də, üçüncü qrupdakı respondentlərin bu məsələdən xüsusilə xəbərdar olması müşahidə edilib. Kibercinayətkarlıq hallarına məruz qalanların əsasən məxfi məlumatlara malik qurumların (yəni əsasən hərbi və kəşfiyyat orqanları) təşkil etməsi geniş yayılan düşüncədir. Ümumilikdə, bir neçə respondent (n=3, 11%) uşaqların bu mənada həssaslığına toxunaraq onlayn paylaşımlarının nəticələrini dərk etmədikləri üçün yüksək ehtimalla onların təhqiredici mesajlarla üzləşə biləcəklərini qeyd edib. Digər tərəfdən, ikinci qrupda dominant baxış belədir ki, kiberməkanın xüsusiyyətinə əsasən smartfon və ya ağıllı cihaz sahibi olan hər kəs oxşar təsirə məruz qala bilər. Bir neçə iştirakçı tərəfindən əlavə edilən yanaşma ilə müəyyən etmək olur ki, saxlanılan məlumatların səciyyəsinə görə dövlət aktorları və bank sektoru kibercinayətkarlıq hədəfinə çevrilmə baxımından olduqca həssas qrupu formalaşdırır. Dövlətlər arasında kiberhücumların bir neçə nümunəsi də iştirakçılar tərəfindən sadalanıb. Maraqlıdır ki, yaşlılarla bağlı vəziyyətə gəldikdə, bütün qruplardan fərqli olaraq bu qrupa daxil olan respondentlər hansısa mövqe bildirməyiblər.

6.4.3. Fişinq (phishing)

Birinci, ikinci və üçüncü qrupda respondentlərdən yalnız biri tərifin izahından əvvəl fişinq haqqında bilsə də, qruplara müvafiq olaraq dörd, səkkiz və yenə səkkiz nəfər iştirakçı anlayış haqqında məlumat təqdim edildikdən sonra bu kibercinayəti tanıyıb. Əslində, demək olar ki, heç kim zərər çəkməsə də, burada fişinq bütün müzakirə edilənlər arasında ən çox tanınan cinayət növüdür.

Əlaqə saxlanılmış, lakin sorğuda fəal iştirak etməyən şəxslərin hamısı (n=24, 92,3%) öz təcrübələrini bölüşüblər. Bir çoxları votsap (WhatsApp) mesajları ("10 nəfərə göndərməsən, öləcəksən" kimi mətnlərlə) və e-poçt məktubları ("Milyonlarla dollar miras qazanmısan, bizə kart məlumatlarını göndər nağd pul depozit edək") aldığını bildirib. İkinci və üçüncü qrup üzrə diqqət çəkən xüsusiyyət ondan ibarətdir ki, fişinq zəngləri əsasən Rusiya, Ukrayna və Avropadan, ani mesajlar və elektron məktublar isə daha çox ölkə daxilindən qəbul edilib. Bir çoxları onlayn satdıqları əşyanın saxta müştəri cəlb etməsi barədə qeyd edib. Bu kimi hallarda həmin saxta müştəri satıcıdan bank hesabını təqdim etməyi xahiş edir. Digər bir təcrübədə isə saxta onlayn satıcı ilə ünsiyyət səbəbindən pul itirmiş (80 manat, orta aylıq

əməkhaqqının 1/10-dən çoxu) 2-ci qrupdakı orta yaşlı qadın və bu qrupdakı oğlunun pulunu fırıldaqçılar mənimsəyən yaşlı bir xanım istisna olmaqla, respondentlər tərəfindən danışılan hadisələrdə, demək olar ki, heç bir kibercinayət cəhdinin uğurlu olmadığı məlum olub.

"Mən çoxsaylı şübhəli məktublar alıram, lakin media təmsilçisi kimi və İT sahəsində biliyə malik olduğuma görə belə halları öyrənmişəm, onları aşkar edə bildiyim üçün şübhəli məzmunları açmır və bu tipli mesajlara cavab vermirəm". Qrup 2

"Rus dilində çoxlu mesajlar almışam, lakin diqqət yetirmirəm. Həmçinin, səhər tezdən edilən bir çox zənglər, məncə, bir qədər pul əldə etmək məqsədi daşıyır. Mən onları heç vaxt cavablandırmıram". Qrup 3

"Bu cür dələduzluğa məruz qalaraq pul itirməyimin səbəbi, əslində, oğlum idi. O, Amerikada tanımadığı insanlar tərəfindən onlara pul ödəyəcəyi halda, öz video oyunu üçün geridönüşlər əldə edəcəyinə və "800 dollar qazanacaqsınız" və s. kimi vədlərə inandırıldı. Mən yaşlı qadınam, bütün bu detallar barədə həqiqətən məlumatlı deyiləm. Oğluma 200 dollar təqdim etdim, o isə bu məbləği fırıldaqçılara görə itirdi". Qrup 3

"Mən anayam. Qızımın müəllimi qeyd edilən həmin mesajlardan birini paylaşaraq sinifdə fişinq poçtu yayır (respondent öz fikrinə əsasən qorxuducu saxta mesajlara istinad edir). Ona görə də səlahiyyətli şəxslərə tövsiyə edirəm ki, məktəblərdə maarifləndirmə işləri aparsınlar". Qrup 3

Sorğu iştirakçılarından yalnız üç nəfər bu cinayətdən əziyyət çəkən kimisə tanıdığını bildirib.

Demək olar ki, bütün qrup iştirakçıları zənglərə və ya e-poçtlara laqeyd yanaşmaqdan başqa hər hansı tədbir görmürlər. Ümumilikdə, əsasən hər kəs müdafiə olunmaqla bağlı özlərini tam şəkildə məlumatlı hesab edib. Bu isə spam filtrlərinin quraşdırılması kimi əlavə üsullar tətbiq edən mütəxəssislərin baxışlarından fərqlənir.

Sorğuda iştirak edən ən gənc qrup üzvləri (18-21 yaş) fişinq haqqında necə maarifləncəkləri ilə bağlı məlumatlı deyil. Digər qrup (22-35 yaş) isə iştirak etmək üçün vaxt tələb edən xüsusi vebinarlara/seminarlara ehtiyac görmədiyini qeyd edib. Əvəzində onlar onlayn şəkildə paylaşılacaq faydalı brifinqlərin keçirilməsini üstün hesab ediblər. Başqa qrupun yeganə təklifi ölkə və məktəb səviyyəsində maarifləndirmə proqramlarının aparılması ilə bağlıdır ki, bütün bu təkliflər ya valideyn, ya da təhsil sektorunda fəaliyyət göstərən, ümumilikdə üç qadın və bir kişi respondent tərəfindən irəli sürülüb. Əslində, 3-cü qrupdakı bir qadın respondentin də bildirdiyi kimi, müəllimlər istəmədən fişinq məktublarının yayılmasında müəyyən rol oynaya bilərlər. Bu, məktəblərdə problemin ciddiliyini göstərə bilər və beləcə, yalnız valideynlərdən ibarət fokus qrupların yaradılmasına zərurət meydana çıxır.

6.4.4. Rənsamveə (ransomware)

Hər üç qrupda, demək olar ki, tərifi izah edilmədən rənsamveə haqqında eşidən respondentlərə rast gəlinməyib (3-cü qrupda əvvəllər bankda işləyən və bu problemlə bağlı müntəzəm seminarlarda iştirak edən bir qadın respondent və 1-ci qrupda zərər çəkmiş bir nəfər tələbə istisna olmaqla). Ümumiyyətlə, hər üç qrupda yalnız dörd nəfər sözügedən kibercinayəti sonradan tanıyıb. Bunun əsas səbəbləri 1) terminin ingiliscə olması və 2) yerli miqyasda qeyd edilən növdə cinayətin az yayılmasıdır.

Hər üç qrupda yalnız iki nəfər faktiki və bir təmsili zərərçəkən müəyyən edilib. Lakin bu qurbanların heç biri kibercinayətkar tərəfindən girov saxlanılan məlumatlarının geri qaytarılması üçün girov məbləği ödəməyib. Onlar yeni cihaz aldıqlarını, yaxud mövcud olanı formatladıqlarını ifadə ediblər.

"Mən zərərçəkən deyiləm, lakin yaxın qohumumun telefonu bağlandı (bloklandı). O, girov pulunu ödəyə, telefon ustası isə onun telefonunu təmir edə bilmədi. Bu səbəbdən yeni cihaz almalı oldu". Qrup 2

"İnstaqram hesabım təxminən 10 il əvvəl bloklanıb. Nə qədər pul tələb edildiyini bilmədim. Müraciət etdiyim proqram mühəndisi mənə cihazı dəyişməyi təklif etdi. Tövsiyəsinə əməl etdim". Qrup 2

6.4.5. Hədə-qorxu, zorakılıq-təhqir və sui-istifadə

Tədqiqatda digər cinayətlərlə müqayisədə onlayn hədə-qorxu, təhqir və sui-istifadə qurbanlarına bir qədər çox rast gəlinib. Bir qrupda üç respondent (18-21 yaş qrupu) onlayn

hədə-qorxu, təhqir və sui-istifadədən əziyyət çəksə də, 22-35 və 36-65 yaşlılar üçün müvafiq olaraq dörd və iki nəfər zərərçəkmiş qeydə alınıb. Demək olar ki, bütün onlayn hədə-qorxu, təhqir və sui-istifadə halları siyasi mövzular (digər sosial media istifadəçiləri ilə fikir ayrılığına görə) və Ermənistanla müharibə ilə (erməni istifadəçilərin hesabları vasitəsilə üzləşən zaman) əlaqəli olub. Beləliklə, məlumdur ki, hər hansı şəxs fəal müzakirə və ya debat iştirakçısıdırsa, daha çox onlayn hədə-qorxu, təhqir və sui-istifadə qurbanına çevrilə bilər.

İkinci və ya üçüncü qrupdakı bir neçə qadın iştirakçı (kişi iştirakçılardan heç biri bu məsələyə dair fikir bildirməyib) öz şagirdləri və ya uşaqları arasında müşahidə etdikləri onlayn hədə-qorxu, təhqir və sui-istifadə ilə bağlı narahatlıqlarını səsləndiriblər. Onlar bu barədə ətraflı məlumat təqdim etməyərək sadəcə müvafiq istiqamətdə məktəb proqramlarının icrasını təklif ediblər.

6.4.6. Şəxsiyyət/kimlik (fərdi məlumatların) oğurluğu

Şəxsiyyət/kimlik oğurluğu iştirakçıların dərhal və ən çox tanıdığı cinayətlər kimi cavablarda öz əksini tapıb. Bu tip cinayətlər sırasında tanımadığı şəxslərin onların sosial media və bank hesablarına daxilolma cəhdləri demək olar ki, respondentlərin qeyd etdiyi yeganə cinayət növüdür. Bu mənada sosial media hesabına daxilolma üzrə baş tutmuş üç uğurlu hücuma məruzqalma (hər biri 2-ci qrupda) və uğursuz iki hadisə (1-ci və 3-cü qrupda) haqqında respondentlərin təcrübələri qeydə alınıb. İnsanların bank hesablarını hədəf alan cəhdlərlə bağlı respondentlər tərəfindən qeyd olunan 8 hücumdan (30%) yarısı uğurlu olub.

"Onlayn alış-veriş etmək üçün övladıma aid karta 1 dollar vəsait əlavə etdim. Qısa vaxt ərzində məbləğ kartdan itdi (təxminən bir ay sonra). Yenidən həmin karta 20-30 dollar əlavə etdim və əvvəlki hadisə yenə təkrarlandı. Ümumilikdə, ailəvi olaraq sözügedən hesabı bağlayıb yenisini aktivləşdirənədək 100 dollar dəyərində pul itkisi ilə üzləşdik". Qrup 3

"Yaxın qohumlarım, daha dəqiq desəm, nənəm və babam bank kartı məlumatlarının oğurlanmasından əziyyət çəkirdilər. Məlum oldu ki, bunu onların nəvəsi edib, beləliklə, min dollardan çox vəsait mənimsənilib. Nağd pul hesabdan xərclənən kimi onlar dərhal polisə bu barədə məlumat vermişdilər, lakin davamlı surətdə oğurluq edən şəxsin kimliyini müəyyənləşdirmək çox vaxt apardı". Qrup 3

"Ödəniş etdiyim xarici şirkət öz sistemini effektiv şəkildə qoruya bilmədiyi üçün 500 dollar itirdim. Görünür, haker şirkətin sisteminə hücum edərək bütün müştərilərin məlumatlarını əldə etmişdi. Səylərimə baxmayaraq, vəsait bərpa edilmədi. Eyni zamanda, hədə-qorxu məzmunlu zəng də qəbul etdim. Zəng edən şəxs bank hesabımdakı pul məbləğinin miqdarı barədə dəqiq məlumatlı idi. Buna görə də həmin şəxsin telefon nömrəsini dərhal blok etdim". Qrup 3

(**QEYD**: respondent etimadsızlıq səbəbindən polisə şikayət etməyib)

Bank rekvizitlərinin ifşası (yayılması) ilə bağlı heç bir hal qeydə alınmayıb. Mobil telefon nömrəsinin oğurlanması üzrə də respondentlər tərəfindən təfərrüatları bölüşülən hər hansı hadisə yoxdur. Lakin iki respondent (2-ci və 3-cü qrupda) onların telefon nömrələri ilə votsap və instaqram hesabları yaratmaq məqsədilə hansısa şəxslər tərəfindən uğursuz cəhdlərin həyata keçirildiyini bildirib. Adıçəkilən proqramların bildiriş mesajı vasitəsilə sözügedən hala məruz qalan respondentlər vəziyyəti dərk edərək qanun pozuntusunun baş verməsinə imkan vermədiklərini ifadə ediblər.

6.4.7. Kibermüdaxilə (DDoS)

Bir çox iştirakçı bank sektorunda qeyri-funksional onlayn xidmətlərlə qarşılaşdığını desə də, bunun səbəbi əsasən kibercinayətkarlıqla deyil, texniki nasazlıqla bağlıdır.

Aparılan sorğu zamanı bütün jurnalistlər (n=3) internet saytlarında, yaxud tanınmış xəbər platformalarında belə hallarla üzləşdiklərini bildiriblər. İştirakçıların yarısından az hissəsinin (10 respondent tərəfindən bildirilmiş 20 hadisə) faktiki zərərə məruz qaldığını nəzərə alsaq, kibercinayətkarlığın qurbanı olduqdan sonra hüquq-mühafizə orqanlarına və digər aidiyyəti subyektlərə müraciətlə bağlı dataya diqqətlə yanaşılmalıdır. Təhlillər göstərir ki, qeyd edilən hallar üzrə yalnız bir nəfər polisə müraciət edib (bu müraciətin nəticəsi qeyri-qənaətbəxş olsa da), dörd nəfər isə İT eksperti, haker və ya işlə-

dikləri şirkətlərin müvafiq şöbəsi ilə əlaqə saxlayıb (nəticə nisbətən qənaətbəxş olub).

"Beş yüz dollar itirdikdə banka müraciət zamanı mənə bildirdilər ki, ödəniş etmək üçün kartımdan istifadə ilə ödəniş yolladığım şirkətlə əlaqə saxlamalıyam. Dedikləri kimi etsəm də, nəticə olmadı". Qrup 3

"Bir dəfə fişinqdən əziyyət çəkdikdə polisə şikayət etdiyim zaman polis yalnız bacardıqlarını etdiklərini və heç bir iz buraxmadığı üçün müəyyən məqamdan sonra cinayətkarı təqib etməkdə çətinlik çəkdiklərini qeyd etdi". Qrup 2

Ümumilikdə, bankların bu məsələlərlə məşğul olmaq üçün istəksizliyi, polisin cinayətkarları təqib etməklə bağlı acizliyi və təcrübəsinin olmaması ilə əlaqədar respondentlərin ciddi şikayətləri qeydə alınıb. Zərər çəkildiyi təqdirdə iştirakçıların necə davranacaqlarına baxaraq qeyd edilənləri anlamaq olar. Beləliklə, zərər çəkilən zaman hara müraciət edəcəkləri ilə bağlı suala qruplar arasında fərqli cavablar müşahidə edilib. Ümumilikdə, 12 nəfər bu sualda polisə istinad etsə də, qalan 14 nəfər qeyri-aktorlara (məsələn, İT mütəxəssisinə) müraciət edəcəyini bildirib. 22-35 yaş qrupundakı respondentlər ölkədə hüquq-mühafizə orqanlarında kadr çatışmazlığı amilini əsas gətirərək, demək olar ki, yekdilliklə özəl şirkətlərə və ya İT mütəxəssislərinə müraciətə üstünlük verəcəklərini ifadə ediblər. Lakin 36-45 yaş qrupunun iştirakçıları hüquq-mühafizə orqanlarına daha optimist münasibətə malikdir. Bu səbəbdən hətta bu qrupa daxil olan bəzi respondentlər buna könülsüz olmalarını etiraf etsələr də, digərləri kibercinayətkarlıq qurbanı olacaqları halda, bu barədə polisə bildirəcəklərini qeyd ediblər. Başqa sözlə, müəyyən iştirakçılar belə addım atmağı yalnız ona görə düşünür ki, cinayətkarın tapılmasında və dəymiş ziyanın bərpasında hüquq-mühafizə orqanlarına alternativ görmürlər. Əslində isə onlar polisi həqiqətən etibarlı və problemləri həll etmək üçün kifayət qədər bacarıqlı hesab etmirlər. Birinci qrupun rəylərində oxşar mənzərə olsa da, bu qrupdakı iştirakçılar məsələ ilə bağlı fikirlərini təfərrüatlı şəkildə açıqlamaqdan bir qədər çəkiniblər. Digər tərəfdən, bu qrupda da hər kəs müraciət üzrə polisi seçim olaraq müəyyən edib.

"Buradakı bir çox insanın fikirləri ilə razıyam, təhqiqatın ədalətli aparılması və polisin bacarığına inanmaya bilərəm, lakin yenə də onlara müraciət edərdim". Qrup 3

"Banklar hücumun mənbəyini tapmaq, öz təhlükəsizliklərini qorumaq və dəymiş ziyanı bərpa etmək kimi öhdəliklərini yerinə yetirmirlər. Beləliklə, banklara deyil, polisə müraciət edərdim. Əgər onlar da bununla məşğul ola bilmirlərsə, deməli, digər hüquq-mühafizə orqanları ilə əlaqə saxlanıla bilər. Cinayət əməli fişinqlə bağlıdırsa, bu, birmənalı olaraq bankın məsuliyyətidir. Mən müştəriyəmsə, onlar bu məsələni həll etməlidirlər". Qrup 3

"Polisdən çox İT mütəxəssisinə müraciət edərdim. Polis əməkdaşları, ümumiyyətlə, informasiya texnologiyaları ilə bağlı zəif məlumatlıdırlar. Onlara hadisə barədə bildirsəm də, polisin lazımi tədbirləri görməsindən asılı olmayaraq, İT mütəxəssisinə sual ünvanlayardım". Qrup 2

"Telefonum və ya hesabım girov götürülərsə, İT mütəxəssisinə müraciət edərdim". Qrup 3

6.4.8. Kibercinayətkarlıq: narahatlıq və gözləntilər

Ən narahatlıq doğuran kibercinayətlər baxımından 3-cü qrupda demək olar ki, bütün iştirakçılar fişinqi qeyd edib.

"Şübhəsiz ki, fişinq deyə bilərik və müşahidələrimə əsasən burada müzakirə olunan cinayətlərin əksəriyyətində də fişinq elementi var". Qrup 3

Mübarizə ilə bağlı yalnız səkkiz nəfər (30%) öz fikrini bildirib, digər tərəfdən, qalan şəxslərin bu məsələdə cavab verməkdə çətinlik çəkməsi məlumdur. Bu, kibercinayətkarlığın cəmiyyətimizdə nisbətən yeni bir hadisə olması ilə izah edilə bilər. Nəticə etibarilə, rəylər üzrə respondentlər bərabər qruplara bölünür – onların yarısı hesab edir ki, kibercinayətkarlıqla mübarizə faəliyyəti mövcuddur, lakin hələ də görülməli işlər çoxdur. Qalanlarına görə isə sözügedən istiqamətdə, demək olar ki, iş görülmür və beləliklə, təcrübənin olmaması burada ən böyük əngəldir.

"Bəli, görülən tədbirlər var, lakin kifayət deyil. Başımıza gəlmiş fişinq hadisəsi ilə bağlı polislə əlaqə saxladıq, lakin heç bir nəticə olmadı. Onlar cinayətkarı tapa bilmirlər... Bildir-

dilər ki, hansısa tədbirlər görsələr də, müəyyən vaxtdan sonra istintaqın davam etməsi mümkün deyil". Qrup 3

"İcazə verin (digər respondentə üz tutaraq) polisin cinayətkarları tapmaqdakı çətinliyi ilə bağlı narahatlıqlarınıza əlavə edim. Səbəb odur ki, hətta aidiyyəti dövlət orqanının daxilində belə ekspertiza yoxdur". Qrup 3

Hansı dövlət qurumlarının kibercinayətkarlıqla məşğul olduğuna dair rəylərə nəzər yetirdikdə, daha çox iş görülməsi və ekspertizanın təkmilləşdirilməsi kimi məsələlərə dair ümumi fikirlərin ortaya çıxmasının şahidi oluruq. Birinci qrupda bir nəfər iştirakçı kibercinayətlərlə məşğul olacaq qurumlararası orqanın yaradılması təklifini irəli sürüb. Daha konkret olaraq, ikinci qrupdakı maliyyə eksperti hesab edib ki, bütün hüquq-mühafizə orqanları bununla bağlı əməkdaşlıq etməli və xüsusi komissiya yaradılmalıdır.

İstisnasız, bütün qruplar üzrə üstünlük təşkil edən yanaşma ondan ibarətdir ki, xüsusən elektron xidmətlərdən (e-gov və e-ticarət) istifadə səviyyəsi getdikcə intensivləşdikcə və əvvəllər kağız üzərindəki məlumatların indi rəqəmsallaşdırılması nəticəsində kibercinayətlərin gələcəkdə artması mümkün ehtimal çərçivəsindədir.

"Artıq hər şey rəqəmsallaşdırılıb və biz rəqəmsal inqilaba keçid edirik, beləliklə, bu problemin daha da genişlənəcəyi aydındır. Hazırda dövlət orqanları kibercinayətlərlə mübarizə üzrə kadr hazırlığına çox diqqət yetirirlər... Əslində, onlayn oğurluqların artması səbəbindən fiziki zərərlə nəticələnən cinayətlərin sayında azalmanı görə bilərik". Qrup 1

"Bütün məlumatlarımızın rəqəmsal olduğu bir dövrdə özümüzü qorumağa gücümüz yoxdur". Qrup 3

6.5. Kibercinayət qurbanları

Qrup müşahidələri

Dəvət olunan 11 iştirakçıdan 6-sı sorğuya qoşulsa da, onlardan birinin internet bağlantısı zəif olduğu üçün müzakirəni bir qədər gec tərk etməli olub. Qrupda üç nəfər kişi və iki nəfər qadın iştirakçı olmaqla, üç paytaxt sakini və iki nəfər kənd ərazi vahidindən olan respondent təmsil olunub.

6.5.1 Onlayn fəaliyyətlər (ümumi istifadə)

İki iştirakçı işlə bağlı gün ərzində (saat 9.00-dan 18.00-dək) internetdən istifadə etdiyi halda, digərləri əsasən ünsiyyət və sosial media vasitəsi kimi istifadə edənlərdir.

Hər bir iştirakçı e-govdan faydalansa da, belə xidmətlərdən istifadənin intensivliyi iki iştirakçı arasında iş fəaliyyətlərinə əsasən (məsələn, yoxlama, sənədlərin göndərilməsi, qarşılıqlı əlaqə və s.) xüsusilə yüksək səviyyədə müşahidə edilib. Digərləri isə internetdən yalnız bəzi hallarda istifadə etdiklərini qeyd ediblər. Bundan başqa, bir nəfər qadın respondent istisna olmaqla, sorğu iştirakçılarının hamısının elektron ticarətdən istifadə etdiyi də təsbit edilib.

Platformalardan istifadə edərkən müdafiə məqsədilə görülən tədbirlər baxımından bir nəfər kişi iştirakçı elektron poçtunda mürəkkəb şifrələr, SMS bildiriş sistemi və filtrləmə tətbiq etməsi ilə seçilib. Digərləri isə spam mesajları açmamağı, e-ticarətdə iki kartdan istifadə etməyi və şübhəli mesaj göndərən şəxsləri bloklamağı özünüqoruma vasitəsi kimi qeyd edib. Özəl şirkətdə çalışan bir qadın iştirakçı çalışdığı müəssisədə hər bir spam mesajının yönləndirildiyi xüsusi şöbənin olması haqqında danışıb.

Bir nəfər kişi iştirakçıdan başqa mövzu üzrə digərlərinin müəyyən qədər narahatlığı da müşahidə edilib. Məlum olduğu kimi, bu, ilk növbədə özlərinin və başqalarının zərərçəkən olması ilə əlaqədardır. Qadın respondentlərdən biri dostlarının dələduzlar tərəfindən aldadılmasından (onlara pul verməsindən) sonra onlayn alış-veriş etməyi dayandırdığını bildirib.

6.5.2. Kibercinayətkarlıq və kibertəhlükəsizlik üzrə bilik səviyyəsi

Ötən il ərzində fokus qrupun onlayn rejimində yeganə dəyişiklik evdən işləmək səbəbindən e-ticarət və internetdən istifadənin artması ilə bağlı olub. Lakin son vaxtlar kibercinayətkarlıq dinamikasında hər hansı artımın olması fikri isə qəbul edilmir. Qrup daxilində hər bir iştirakçının məktəb təhsili dövründən sonra "kibercinayətkarlıq" sözü ilə tanışlığı respondentlərin yaş ortalamasının nisbətən yüksək olması baxımından başadüşüləndir.

Kibercinayətin mənasının qavranılması ilə bağlı respondentlərdən biri (kişi) "Mən kibercinayəti ustalıqla aldatma və manipulyasiya aktı

kimi qəbul edirəm, sizi inandırıb tələyə salırlar" cavabını irəli sürüb. Digər bir kişi respondent isə hesab edir ki, başqa insanların şəxsi materiallarının (video, şəkillər) oğurlanması kibercinayətkarlıq faktını təsdiq edir və bu kimi hallar çox geniş yayılıb. Bir qadın respondentin da cavabı belədir: "Kibercinayətkarlıq - kiminsə mükafat (gəlir/mənfəət) qazanacağı ilə bağlı aldadılması və beləliklə, kartından onlayn şəkildə pul mənimsənilməsidir". Qalan iştirakçıların mülahizələri onlayn kart oğurluğu ilə bağlı olsa da, onlar bu barədə ətraflı məlumat verməyiblər. Faktlara əsasən demək olar ki, bütün iştirakçıların fikirləri birbaşa olaraq özlərinin zərərçəkmə təcrübələri ilə əlaqəlidir. Bu baxımdan, təqdim edilən kibercinayətkarlıq nümunələrinə dair onlayn kart oğurluğu ən çox rast gəlinən cavab kimi meydana çıxır.

Motivlərlə bağlı cavablara baxdıqda, qazanc əldə edilməsi burada üstünlük təşkil edən yanaşmadır. Həssas kateqoriya haqqında soruşulduqda isə respondentlər tərəfindən konkret qrup qeyd olunmayıb. Daha doğrusu, sözügedən mənada ardıcıl səslənən fikir hər kəsi əhatə edən "xalq" sözü ilə ifadə olunub. Kibercinayətin ciddiliyi nöqteyi-nəzərindən bəziləri zorakılıq cinayətlərini ağır hesab etsə də, nisbətən az sayda respondent psixoloji təsirinə görə kibercinayətləri eyni dərəcədə və ya daha ciddi qiymətləndirib.

6.5.3. Fişinq (phishing)

Əslində, fişinqin nə olduğunu bilməsələr də, respondentlərin hər biri bundan əziyyət çəkib. Təhlilin gedişatını asanlaşdırmaq üçün hesabatlılıq baxımından qurbanların təcrübələri də burada mətnə əlavə edilir. Beləliklə, üç respondentin fikirlərini təqdim edirik:

"İşədüzəltmə şirkətlərindən birində maraığımı ifadə edərək qeydiyyatdan keçdim. Bir nəfər mənə zəng edib, iş axtarmağım barədə məlumat aldı. O, qeydiyyatda olduğum işədüzəltmə şirkətinin nümayəndəsi deyildi və bir ad tələffüz etdi. Mən hazırda həmin adı unutmuşam. İstənilən halda, sözügedən şəxs məndən 150 manat depozit tələb etdi. Əvvəlcə tərəddüdlü olmağıma və onunla şəxsən görüşərkən qeyd edilən məbləği ödəməklə bağlı təkid etməyimə baxmayaraq, həmin şəxs məni olduqca yaxşı inandırdı. Bu səbəbdən mən kibercinayətkarlığı kimdənsə nəyisə oğurlamaq üçün yerinə yetirilən əməl kimi qəbul edirəm. Bəli, mən 150 manatı ödədim və bir neçə gün sonra bu adamla əlaqə saxlamaq istəyəndə o, telefona cavab vermədi… Polisə müraciət etdim. Təşəkkür edirəm ki, sözügedən şəxs tapıldı, lakin ödədiyim məbləğ artıq yox idi. Daha doğrusu, ölkədən kənardakı hesaba köçürüldüyü üçün polis onu geri ala bilmədi".

***MODERATOR:** Sizə hansı növ iş təklif edildiyini bilmək olar?*

"Maaşı 800-900 AZN civarında olan özəl şirkətdə sürücü vəzifəsi". (Kişi respondent)

"Ucuz mobil telefon almaq üçün internet üzərindən axtarış edirdim. Tap.az (ölkədə tanınmış e-ticarət platforması) onlayn ticarət saytında endirimli olanına rast gəldim. Əlaqə saxladıqda, elan üzrə cavab verən şəxs 50 manat depozit istədi və biz bu məbləği ödədik. Daha sonra əlaqə saxlanılan şəxsi tapa bilmədik. Mən və qızım müraciət etsək də, məsələ ilə əlaqədar polis tərəfindən hər hansı müsbət reaksiyanın şahidi olmadıq. Bildirdilər ki, bu, onların işi deyil və başqa rayonun polis idarəsinə müraciət edilməlidir. Aydın idi ki, onlar bu yolla mövzudan yayınmaq istəyirdilər" (Qadın respondent).

"Özünü işədüzəltmə şirkətinin əməkdaşı kimi təqdim edən şəxs pulumu mənimsədi. Qadın olduğum üçün polis məmurlarının mənə eyham edəcəklərini düşündüm və onlara bu haqda məlumat verərək vaxtımı itirmək istəmədim (qadın respondent).

Ümumilikdə, yalnız bir nəfər zərərçəkmiş şəxs polisin reaksiyasından razı qalıb və respondentlərin yalnız biri (qadın respondent) polisə müraciət etmədiyini bildirib.

Müvafiq halların başvermə səbəblərinə gəldikdə, kişi iştirakçı bunu iki amillə - fırıldaqçının ustalıqla ifadə etdiyi nitqinin qurbanı olması və iş tapmaq ehtiyacı ilə əlaqələndirib. Sözügedən respondent fırıldaqçının tələbini yerinə yetirməkdən əvvəlcə imtina etdiyini desə də, sonuncunun danışıq üslubunun onun fikrini dəyişdiyini qeyd edib. Demək olar ki, eyni vəziyyətdən əziyyət çəkən qadın respondent isə bu cür cinayət halları haqqında məlumatsızlığını gənc olması ilə əlaqələndirib. Digər respondentlər eyni şəkildə məlumatsızlıq amili və fırıldaqçıların "etibarlı görünən" imicinə

diqqəti yönəldiblər.

Kibercinayətlərin zərərçəkənlərə təsiri baxımından təcrübələrə nəzər yetirdikdə, oğlunun oyun hesabını itirməsindən sonra e-ticarətdə iki kartdan istifadə etməyə başlayan yaşlı qadın, dostlarının fırıldaqçılara pul itirməsindən sonra narahatlıq keçirməklə internetdən əşya almağı dayandıran digər qadının qeyd etdikləri də məlumdur. İşədüzəltmə şirkətindən zəng edərək onunla əlaqə saxlanılması səbəbindən zərər çəkən kişi respondentin cavabı isə belədir: *"Hələ də inana bilmirəm. Bu hadisə mənə çox təsir etdi, çünki kibercinayətkarlığın şiddətini dərk etdim və buna görə həmişə digər insanları ehtiyatlı olmaq barədə məlumatlandırmağa çalışıram".*

6.5.4. Rənsamveə (Ransomware)

Respondentlərə müvafiq termin izah edilməmişdən əvvəl heç kimin rənsamveə haqqında məlumatı olmadığı, anlayışın izahından sonra isə yalnız bir iştirakçının onu tanıması təsbit edilib. Bununla bağlı hər hansı zərərçəkmiş şəxs isə qeydə alınmayıb.

6.5.5. Hədə-qorxu, zorakılıq-təhqir və sui-istifadə

Yalnız bir onlayn hədə-qorxu/sui-istifadə və zorakılıq-təhqir halı müəyyən edilib ki, burada təmsili (nəql edilən) zərərçəkmə təcrübəsi mövcuddur.

"Oğlum onlayn hədə-qorxu ilə üzləşib. O, bəzi internet saytlarından "öləcəksən", "get özünə zərər ver", "sonrakı həyatda cənnət səni gözləyir" kimi mesajlar alıb. Dərhal mənə bu barədə bildirdi və saxta mesajlar olduğunu anladım. Lakin hadisə oğlum üçün olduqca qorxuducu idi". (Qadın respondent)

6.5.6. Şəxsiyyət/kimlik (fərdi məlumatların) oğurluğu

Zərərçəkmiş qurbanlardan birinin (kişi respondent) dediyinə əsasən bank kartına edilən hücum nəticəsində onun müəyyən pul vəsaiti (45 manat) mənimsənilib və bu barədə özü bu sözləri deyib: *"Ciddi bir məsələ olmadığına görə polisə xəbər vermədim"*. Digər zərərçəkmiş qismində çıxış edən qadın respondentin qardaşının kartı hücuma məruz qalaraq 200 manat məbləğində pulu oğurlanıb, lakin onlar da inamsızlıq səbəbindən hadisə haqqında polisə bildirməyiblər. Oğullarının oyun hesabı ələ keçirilmiş, yaxud oğurlanmağa cəhd edilmiş digər qadın respondentlər tərəfindən iki oxşar zərərçəkmə hadisəsinə dair qeydlər də mövcuddur. Sözügedən vəziyyətlərlə əlaqədar yalnız bir respondent kartları üçün 3D təhlükəsizlik sistemindən istifadə etdiyini vurğulayıb ki, bu da maraqlı faktlardan biridir. Əslində, özünün ifadə etdiyi kimi, qismən kartındakı 3D təhlükəsizliyə görə bank kartı oğurluğu hadisəsi ilə üzləşməyib. Digər tərəfdən, mövzu üzrə bir nəfər respondent öz sosial media hesabının təhlükəsizilik səddinin aşılması istiqamətində uğursuz cəhdə məruz qaldığını səsləndirib.

"Qardaşımın 200 AZN pulu oğurlandı. O, məbləğin itdiyi kartdan 2-3 dollar onlayn ödəniş etmək üçün istifadə edirdi. Təxminən bir ay sonra 200 AZN itirildi. Etimadsızlıq səbəbindən polisə xəbər vermədi. Bilirsiniz ki, niyə etibar etmirik" (burada respondent yüksək ehtimalla polisi ictimai şəkildə tənqid etməkdən narahat idi). (Qadın respondent)

"Oğlumun oyun hesabı ələ keçirildi. Bu səbəbdən onun çox ağlaması hamımıza təsir etdi. Bilirsiniz, həmin hesabında xallar, bonuslar, bu kimi elementlər var idi və hamısını itirdi". (Qadın respondent)

6.5.7. Kibermüdaxilə (DDoS)

Bununla bağlı ifadə edilən hər hansı hal mövcud deyildir.

6.5.8. Kibercinayətkarlıq: narahatlıq və gözləntilər

Müzakirə edilən bütün kibercinayətkarlıq növləri arasında fişinq ölkədə ən çox rast gəlinən və narahatedici hadisə olaraq qeyd edilib. Müvafiq cavabları formalaşdıran əsas səbəbləri isə respondentlərin öz təcrübələri, həmçinin başqalarının zərər çəkməsi ilə bağlı müşahidəsi təşkil edir.

Gələcək oxşar hallar zamanı bu barədə şikayət bildirilməsi baxımından iştirakçı qrup demək olar ki, eyni baxışa malikdir. Kişi respondentlər istisna olmaqla, iştirakçıların çoxu polisə müraciətə üstünlük vermir. Maraqlıdır ki, onlar buna sadəcə laqeyd yanaşırlar. Etibar amili burada əsas səbəb kimi çıxış edir. Bununla bağlı iki qadın respondent müəyyən

təklif də irəli sürüb:

"Məncə, dövlət kibercinayətkarlığa dair internet saytı yaratmalıdır ki, burada insanlar həm özlərinin, həm də digərlərinin zərər çəkməsi barədə məlumat bölüşə bilərlər. Bu yolla daha çox insan təhlükələrdən xəbərdar olar". (Qadın respondent).

Yuxarıdakı respondentin şərhinə istinadla, digər qadın respondent bildirir:

"Bəli, razıyam. Belə proqram həm də sosial media vasitəsilə başladıla bilər. Rusiyada oxşar sayt nümunəsi görmüşəm".

Bundan başqa, digər qruplardakı bəzi valideynlər və müəllimlər kimi, bu qrupda da övladları olan iki qadın və bir kişi respondent uşaqları risk qrupuna aid etdikləri üçün məktəbdə maarifləndirmə proqramının zəruriliyi haqqında söhbət açıblar.

Zərərçəkmiş respondentlərdən biri isə rastlaşdığı hadisə barədə səlahiyyətli orqana xəbər vermək əvəzinə maarifləndirmə işləri ilə məşğul olacağını bildirib: *"Mən sosial şəbəkələrdəki hesabları və insanların məruz qaldıqları (danışdıqlarımıza oxşar) fırıldaqçılıq təcrübələrini paylaşdıqları səhifələri izləyirəm. Özüm də maarifləndirmə məqsədilə mütəmadi məlumatlandırıcı postlar paylaşıram".*

Bütün qruplarda olduğu kimi, bu qrup iştirakçılarının da ümumi qənaəti belədir ki, texnologiyanın inkişafı ilə paralel kibercinayətkarlıq halları da daha geniş vüsət alacaq.

6.6. İT mütəxəssisləri

Qrup müşahidələri

Sorğular zamanı qrup iştirakçılarının eyni dərəcədə fəallığı müşahidə edilib. Burada üç İT şirkətini təmsil edən dörd nəfər və bir media (TV) təşkilatının nümayəndəsindən ibarət qrupu öz qurumları daxilində müxtəlif vəzifələr tutan şəxslər təşkil edib. Təəssüf ki, beş nəfərin fikirləri ümumən İT mütəxəssislərinin rəy müxtəlifliyini mümkün şəkildə geniş əhatə etmir. Dəvət olunan digər üç ekspert isə çalışdıqları təşkilatda internet şəbəkəsində yaranmış problemi əsas gətirərək son məqamda sorğuda iştirak edə bilməyəcəklərini bildiriblər. Respondentlər sırasında yer alan insan haqları üzrə üç QHT nümayəndəsindən ikisi ölkədə tanınmış simalardır. Digəri isə internet və İT sektoru üzrə ixtisaslaşıb.

6.6.1 Onlayn fəaliyyətlər (ümumi istifadə)

Tətbiqi həyata keçirilməyib - N/A (non-applicable)

6.6.2. Kibercinayətkarlıq və kibertəhlükəsizlik üzrə bilik səviyyəsi

Orta göstərici əsasında qrup iştirakçılarının "kibercinayət" sözü ilə ilkin tanışlığı müxtəlif kontekstlərdə (internet klublarında və işlə bağlı) təxminən 20-22 il əvvəl meydana gəlib. QHT nümayəndəsi olan iki respondent isə 1990-cı illərin əvvəllərində Azərbaycanda internet istifadə edilməyə başlanılan vaxtlarda bu termin haqqında eşitdiyini bəyan edib. İT mütəxəssisləri üçün sözügedən anlayış, demək olar ki, ancaq təhsil və ya iş fəaliyyətilə əlaqədar aktuallaşmağa başlayıb.

Qrup üzvləri arasında fişinqin ölkədə ən çox yayılan kibercinayət olmasına dair yekdil fikir mövcuddur. Müzakirə zamanı demək olar ki, hər bir iştirakçı fişinq fırıldaqçıları tərəfindən hədəfə çevrilən bank sferasında qarşılaşılan ən son hallara istinadlar ediblər.

İT mütəxəssislərinin kibercinayətkarlığa baxışı ümumi əhali qrupunun müvafiq anlayış haqqında düşüncələrindən tamamilə fərqlənir. Sözügedən respondentlər üçün kibercinayətkarlıq cəhd deyil, məqsədə nail olunan istənilən cinayətdir. Həmçinin, bu iştirakçılar kibercinayətkarlığın çox mürəkkəb və təkmil təfərrüatları haqqında fikirlər də bildiriblər. Beləliklə, qeyd edilən iştirakçılar müzakirə edilən bütün cinayət kateqoriyaları üzrə dərin biliklərə malikdirlər.

"Mənim üçün əsl kibercinayət bütün sistemlərə – antivirus proqramlarına, bizim qurduğumuz müdafiəyə (firewall) nüfuz edən hallardan ibarətdir. Bizi çarəsiz və ümidsiz edən vəziyyəti əsl kibercinayətkarlıq hesab edirəm. Özümüz, yaxud sistemimizin hər gün üzləşdiyi kiçikmiqyaslı hücumlar və ya problemlərdən söhbət gedirsə, onlar ciddi əhəmiyyət kəsb etmir". R1

"Kibercinayət fəaliyyətləri və buna dair potensial hər yerdə mövcuddur. İnternet məkanı, bankomatlar, kart ödəniş terminalları və s. burada əsas yer tutur. Əgər sistemlərin idarə edilməsində insan faktoru, yəni idarəedici məsul şəxs varsa, bu halda təhlükəsiz heç nə

yoxdur və sistemin işində boşluğun yaranmasına meyillilik istisna deyil". R2

"Məlumatların daxil edilməsi və çıxış imkanı olan müstəvidə kibercinayətkarlıq potensialı mövcuddur". R3

Digər tərəfdən, QHT nümayəndələrinin kibercinayətkarlıq anlayışı əsasən ümumi əhalinin mövzu üzrə fikirlərinə oxşardır. Bu baxımdan, onların nitqində "internet vasitəsilə törədilən cinayətlər" ifadəsi üstünlük təşkil edir.

Həssaslıq amili ilə bağlı qrup üzvlərinin rəylərində bölünmə müşahidə edilir. Belə ki, üç iştirakçı yaşlıları kibercinayətkarlıq qurbanı olma üzrə həssas kateqoriya kimi görsə də, digər halda gənclər qeyd edilir. İştirakçılar kibertəhlükələri aşkar etməkdə yaşlı insanların biliklərinin olmamasına istinad edirlər. Gəncləri kibercinayətkarlığın qurbanı olmaqla bağlı həssas qrupa daxil edən rəylərdə isə respondentlər onların yüksək onlayn fəallığına əsaslanırlar. İstənilən halda məsələ kibertəhlükələrdən xəbərdar olmaqla əlaqəlidir. Bu mənada İT mütəxəssisləri və QHT nümayəndələri yaşından asılı olmayaraq məlumatlılıq və maarifləndirmə üzrə çatışmazlığı həssaslığa yol açan əsas faktor kimi qiymətləndirirlər. Lakin təhsil-məlumatlılıq aspekti diqqət mərkəzində olsa da, həm də hesab edilir ki, yaş amili təbii korrelyasiya yaradır. Başqa sözlə, internetdən nisbətən intensiv istifadə edən gənclər olduğuna görə onlar məsələyə dair daha məlumatlı olurlar və yaxud əksinə.

"Fikrimcə, həssaslıq məsələsi yaşla deyil, biliklə bağlıdır. Bu səbəbdən insanlar maarifləndirilməli, onlara müvafiq təlimlər keçirilməli, konfranslar təşkil edilməlidir". R2

"Zərərçəkmənin səbəbini bilik çatışmazlığında görmürəm. Çünki hesab edirəm ki, risk qrupunu ən çox təşkil edən gənclər daha çox onlayn olduqları üçün bəzi səhvlərə yol verməyə və zərər çəkməyə meyillidirlər. Buna görə də bu, yaşla bağlı məsələ deyil". R3

"Ümumiyyətlə, İKT sahəsində bilik səviyyəsi və istifadəçilərin yeni vərdişlərinin yaranması mühüm məsələdir. Uşaqlar və qocalar daha həssas təbəqələrdir. Gender bölgüsünə baxdıqda isə qurbanlar arasında qadınlar çoxluq təşkil edir". QHT

Respondentlər həssaslıq baxımından özlərini necə qiymətləndirirlər? İştirakçıların görülən tədbirləri sadalamalarına baxmayaraq, hamıda kibercinayətkarlığa dair qorxu hissi müşahidə edilib və onlar buna onlayn məkanın qaçılmaz nəticəsi kimi yanaşırlar.

"Mühafizə tədbiri olaraq, tam oflayn rejiminə əminlik üçün yayım cihazlarını şəbəkədən ayırırıq. Onları yalnız lazım olduğu təqdirdə, qısa müddətə şəbəkəyə qoşuruq. Siqnal göndərilməsi üçün isə VLAN, optik xətdən istifadə edirik". R4

"Əlbəttə, kibercinayətkarlığı nə qədər çox anlasam, bir o qədər özümü müdafiəsiz hiss edirəm. Mənim vəzifəm şirkətin serverinin, işçi qüvvəsinin, özümün və infrastrukturun mühafizəsini əhatə edir... Bütün proqram təminatı və həlləri çatışmazlıqlar səbəbindən mütəmadi qaydada yenilənir. Buna görə də insan özünü həmişə təhlükədə hiss edir". R1

"Şirkətimizdə hər kəs bu məsələlərə həssas yanaşır. İstənilən halda həmişə boşluqlar olur. Biz proqramları yeniləyirik, lakin bir müddət sonra orada çatışmazlıq görürük. Beləliklə, müdafiəni davam etdirmək üçün mümkün qədər ən son texnologiyalardan istifadə etməliyik". R3

"Smartfon və kompüterdən çox istifadə etsək, təhlükə səviyyəsi müvafiq şəkildə artacaq. Bu halda nə sığortaçı, nə sığortalanan var. Hər kəsin bir-birinə qarşı şübhələri günbəgün artır. Hamı təhdidə çevrilə bilər". QHT

Görülən ümumi mühafizə tədbirləri ilə bağlı rəylərdə hazırkı qrupu bütün ümuməhali qruplarından əsaslı şəkildə fərqləndirən çoxlu sayda təsbitlər müəyyən edilib. Bu qrup daxilində "hər yerdə təhlükə mövcuddur" kimi ifadələr xeyli ölçüdə səslənib. Ağıllı qurğular və ev sistemləri, eləcə də rəqəmsallaşma hamını həssas vəziyyətə gətirib və hər kəs üçün təhlükə formalaşdırır. Bu baxımdan, aşağıdakı yanaşmaları nəzərdən keçirmək maraqlıdır:

"Proqramlara çoxlu yeniliklər daxil olur. Hər dəfə mən bu halı işçilərimizə izah etməli oluram. Məsələn, hesab edək ki, Maykrosoftun (Microsoft) mövcud proqramı hipotetik olaraq 500 peşəkar tərəfindən hazırlanıb. Bu o deməkdir ki, 10 milyard insan var ki, onların arasında potensial hakerlər sistemi qırmağa çalışır. Proqramların mükəmməllik səviyyəsindən asılı olmayaraq, onların hər bir yenilənmə

hadisəsi problemlərin, boşluqların mövcudluğundan da xəbər verir. Mən bu yeniləmələri belə izah edirəm". R2

"Görüləsi elementar müdafiə tədbirləri vardır. Spam filtrlərini aktivləşdirmək, müəyyən veb-saytlara daxil olmamaq, şübhəli e-poçtlara cavab verməmək və s. Mən bunların hamısına əməl edirəm və indiyədək heç bir problem yaşamamışam". QHT

Ümumilikdə, bütün respondentlər kibercinayətkarlıq dinamikasının pandemiyadan sonrakı dövrdə dəyişməsi mülahizəsi ilə razıdır. Onları belə düşünməyə vadar edən isə konkret data deyil, şəxsi müşahidələridir.

Kibercinayətin ciddilik səviyyəsinin digər hüquqpozmalara münasibətdə qavranılması baxımından qrup üzvləri vahid düşüncədədir. Belə ki, birinci potensial olaraq ikincidən daha təhlükəlidir. Bütün qruplarda bir çox iştirakçının toxunduğu məqamlar kimi ciddilik səviyyəsini izah edən kibercinayətin özünəməxsus xüsusiyyətlərinə istinad edilib. Əslində, iki respondent müxtəlif cinayətlərlə müqayisə apararkən kibercinayətkarlıq haqqında "müqayisəolunmaz" ifadəsini səsləndirib. Onların yanaşmaları aşağıdakı sitatlarda öz əksini belə tapır:

"Kibercinayətkarlıq daha ciddidir, çünki bu vasitə ilə terror aktı törədilə bilər. Müasir ölkələrdə sərnişindaşıma dəmir yolları rəqəmsal sistem əsasında idarə edilir. Hansısa kibermüdaxilə qatarın toqquşmasına səbəb ola bilər... Belə cinayət əməlləri fiziki həyata keçirilsə, böyük miqdarda maliyyə gücü tələb edir, halbuki bunun üçün kibercinayətkarlıq daha rahat yoldur". R3

"Siz bir və ya iki nəfərin pul kisəsini oğurlaya bilərsiniz, lakin bir veb-sayta giriş əldə etməklə eyni vaxtda 200-300 müştərinin kart məlumatlarını əldə etmək mümkündür... Yaxud zərər məqsədilə hər hansı elektrik stansiyasına fiziki şəkildə yalnız 3-5% miqyasında xətər yetirilməsi ilə müqayisədə kibercinayətkarlıq qaydasında bütün ərazinin fəaliyyətini bloklamaq olur". R4

"Kibercinayətlərin mümkün təsirləri adi qanun pozuntuları ilə müqayisə edilə bilməz". QHT

Respondentlərin rəylərində kibercinayətkarlıqla bağlı hüquqpozmalara aid müxtəlif motivlər qeyd olunub. İki iştirakçı hər kəsin, xüsusən bəzi gənclərin (18-21 yaş) bunu cinayət hesab etmədiyini müdafiə edir. Əksinə, kibercinayətlər onlara polisin diqqətini çəkmədən (məsələn, başqalarının xahişi ilə sosial media hesablarının müdafiəsini qırmaq) özlərini digərlərinə nümayiş etdirmə fürsəti təqdim edir. Kibercinayətkarlığın motivlərinin ənənəvi cinayətlərdən (mənfəət əldə etmək, qisas almaq və s.) fərqlənmədiyinə dair yekdil qənaət mövcuddur.

"Daha çox 16-22 yaşlılar kibercinayət törədirlər. Səbəb odur ki, bir qədər azyaşlı və ya yeniyetmə olduqları üçün onların sürətli pul qazanmaq istəkləri vardır və kibercinayətkarlıq buna imkan yaradır". R1

"Kiminsə pul kisəsindən oğurluq etmək bank kartından oğurluq etmək kimidir. Bunlar bərabərdir və eyni cəzaya layiqdir". R4

Hər biri müxtəlif şirkətləri təmsil edən üç respondent şirkət siyasətləri, məsələn, bütün işçilər üçün fərdi olaraq girişin dəyişdirilməsi, şəxsi cihazlar vasitəsilə vayfaya (Wi-Fi) qoşulmağa qadağaların tətbiqi və s. haqqında ətraflı fikirlər ifadə edib. Əslində, həmin iştirakçılar belə strategiyanın sərtliyinə dair qurumların öz işçiləri tərəfindən olan şikayətlər barədə də danışıblar. Lakin yalnız bir respondent işlədiyi şirkətdə kibertəhlükəsizliklə bağlı müntəzəm seminarların təşkili haqqında qeyd edib. Digər halda, təlimatlar yalnız işçilər şirkətdə işə qəbul edildikləri zaman onlara təqdim olunur. Sözügedən şirkətlərdə şübhəli onlayn e-poçt/dəvətlə əlaqədar necə və kimə məlumat veriləcəyinə dair də bir sıra ətraflı qaydalar mövcuddur. Bu qrupda respondentlər kibercinayətkarlıqdan yayınmaq üçün daha çox məlumata ehtiyac duyulduğunu deməsələr də, ümummilli səviyyədə, xüsusən yaşlılar arasında maarifləndirmə proqramlarının aparılmasını təklif ediblər.

6.6.3. Fişinq (phishing)

İştirakçı şirkətlərdən birinin spam qutusunda təxminən 12.000 fişinq e-poçtu olması, digərində isə belə halların demək olar ki, qeyri-mövcudluğu tədqiqat prosesində toplanan məlumatlar sırasındadır. Hazırkı qrup daxilində bildirilən yeganə kibercinayət növü fişinqdir, lakin bunların şirkətdə hər hansı təsir yaratmadığı da məlum olur. Beləliklə, sorğuda iştirakçı şirkətlərin heç birində zərərçəkən aşkarlanma-

yıb. Cavablara əsasən, şübhəli məktubların filtrasiyası üçün bütün şirkətlərin elektron poçt sistemlərində spam filtrləri tətbiq edilir.

Digər tərəfdən, QHT nümayəndəsi olan bir respondent fişinqdən əziyyət çəkdiyini, ardınca isə sosial media və e-poçt hesabının müdafiəsinin qırıldığını qeyd edib. O, maddi ziyana məruz qalmasa da və İT mütəxəssisinin köməyi ilə hesabını bərpa etmək mümkün olsa da, demək olar ki, bütün elektron məktubları silinib. QHT nümayəndələrinə görə, əsas müdafiə mexanizmi şübhəli e-poçtları oxumamaq və onlara qarşı onlayn hədə-qorxu, zorakılıq-təhqir, yaxud sui-istifadə tətbiq edənləri sosial mediada bloklamaqdır.

6.6.4. Rənsamveə (ransomware)

Tədqiqat zamanı bununla bağlı birbaşa zərərçəkən müəyyən edilməyib. İT sektorunda olmasına baxmayaraq, yalnız iki respondent başqasının başına gəlmiş hansısa rənsamveə hadisəsi haqqında eşitdiyini qeyd edib. Sorğu iştirakçıları qismində QHT nümayəndələri isə heç bir rənsamveə fəaliyyəti ilə qarşılaşmadıqlarını ifadə ediblər.

6.6.5. Hədə-qorxu, zorakılıq-təhqir və sui-istifadə

İT sektorunun iştirakçıları onlayn təhdid, zorakılıq-təhqir, yaxud sui-istifadə ilə üzləşmədiyi halda, bütün QHT nümayəndələri bir neçə dəfə belə kibercinayətlərdən əziyyət çəkdiklərini bildiriblər. Onların fikrincə, bu, bəzən başqaları ilə ziddiyyət təşkil edən siyasi mövcudluqları və fəaliyyətləri ilə əlaqədar yaranan normal haldır. Həmin məqam ÜƏQ-lər arasında da oxşar şəkildə müşahidə edilən vəziyyətdir. Belə ki, onların sırasında da QHT nümayəndələri kimi siyasi müzakirə və ya debatlarda fəal iştiraka görə yuxarıda qeyd edilənlərə məruz qalan respondentlər vardır.

“Məşğul olduğum xüsusi fəaliyyət səbəbindən bir həftə qarayaxma kampaniyasının hədəfinə çevrildim. Sonra belə onlayn hücum edənləri ictimaiyyətə açıqladıqdan sonra mənə qarşı kampaniya dayandırıldı”. QHT

6.6.6. Şəxsiyyət/kimlik (fərdi məlumatların) oğurluğu

Bir nəfər QHT nümayəndəsi (yuxarıda qeyd olunduğu kimi) istisna olmaqla, hər hansı iştirakçı və ya onlarla işləyən şəxslər kimlik (fərdi məlumatlar) oğurluğu hadisəsi ilə rastlaşmayıb. Yalnız bir respondent (həm də fişinqdən əziyyət çəkən QHT nümayəndəsi) sosial media hesabının oğurlanması üzrə uğurlu və uğursuz cəhdlərə məruz qalıb. Bank rekvizitlərinin ifşası ilə bağlı isə respondentlər tərəfindən hər hansı təcrübə bölüşülməyib. Eyni zamanda, rəylərə əsasən mobil telefon nömrəsinin oğurlanması üzrə də hansısa hallar yaşanmayıb.

6.6.7. Kibermüdaxilə (DDoS)

İT sferasının nümayəndələri DDoS hadisəsi ilə rastlaşmadıqlarını qeyd ediblər və bunu işlədikləri şirkətin strateji əhəmiyyət daşımaması ilə əlaqələndiriblər.

6.6.8. Məlumatların pozulması

Respondentlərin heç biri belə kibercəhdlərlə üzləşməyib.

6.6.9. Rəhbər şəxslərin (CEO) adından istifadə edilməklə dələduzluq/ Biznes e-poçtu riskləri (BEC)

Respondentlərin heç biri belə bir kibercinayətlə üzləşməyib.

6.6.10. Kibercinayətkarlıq: narahatlıq və gözləntilər

Ümumilikdə, İT mütəxəssisləri tərəfindən korporativ zərər barədə məlumat verilməyib. İnsan hüquqları üzrə fəaliyyət göstərən QHT-lərin üç nümayəndəsindən (hər birinin üzləşdiyi onlayn zorakılıq-təhqir/sui-istifadə halları istisna olmaqla) yalnız biri zərərçəkmiş respondentdir.

İştirakçıların gələcəkdə kibercinayətkarlığa məruz qalması barədə kiməsə məlumat vermə ehtimalları ilə bağlı rəylərdə yekdil razılıq vardır. Burada bütün cavablarda “vəziyyətdən asılıdır” ifadəsi qarşımıza çıxır. Yəni respondentlər kibercinayətlərə iki kateqoriyada yanaşırlar: bacarıqlarına əsasən təkbaşına həll edəcəkləri hallar (məsələn, DDoS) və onların həlletmə imkanları və ya qabiliyyətindən kənar vəziyyətlər (məsələn, şəxsi məlumatların gizliliyi və ya onlayn təhdid).

QHT nümayəndələri ciddi hallarda polisə müraciət ehtimalını istisna etməyərək, əsasən

bu sahə ilə bağlı digər mütəxəssislərə sual ünvanlamağa üstünlük verilməsi üzrə ortaq baxışa malikdirlər. Bununla belə, yalnız bir respondentin rəyi ən azı iki səbəbə görə digər iştirakçıların fikirlərindən tamamilə fərqlənib. Bu, ilk növbədə belə cavabın bütün tədqiqat üzrə yalnız bir respondentə - QHT nümayəndəsinə aid olması, ikinci tərəfdən isə kibercinayətkarlıqla mübarizədə qeyri-rəsmi sosial nəzarətin rolunu üzə çıxarması ilə bağlıdır. Həmin QHT nümayəndəsi bildirib ki, kibercinayətkarların istifadə etdiyi yeni üsullar və cəhdlər haqqında bir neçə quruma, xüsusən də Elektron Təhlükəsizlik Xidmətinə məlumat verib. Onun fikrincə, respondent aidiyyəti qurumlar tərəfindən daha çox qabaqlayıcı tədbirlərin görülməsi işində müəyyən rol oynayır.

"İstifadəçi hesablarını bloklayaraq onlayn təhlükə kimi kiçik məsələlərlə məşğul oluruq. Bu kimi işlərin öhdəsindən özümüz asanlıqla gələ bilərik". QHT

"Hansısa təhlükə və ya şübhəli fəaliyyət görəndə mən sadəcə İT mütəxəssisləri ilə məsləhətləşirəm". QHT

Bütün kibercinayətlər arasında məlumat oğurluğu və kənar/yad şəxsin kameraya müdaxiləsi QHT nümayəndələri tərəfindən qeyd edilən hallardır. DDoS və məlumat oğurluğu İT sektorunun nümayəndələri arasında daha çox yayılmış cavablardır. Məlumat oğurluğu hadisələrinə istinad edən QHT nümayəndəsi iddia edir ki, onlar bir çox aktorlar və dövlət qurumları ilə daim danışıqlar apardıqları üçün həssas məzmunlu sənədləri tez-tez göndərir və qəbul edirlər. Buna görə də belə məlumatların kiberəməllər nəticəsində itirilməsi narahatlıq yaradır. İT sektoru üzvləri isə irəli sürür ki, DDoS-u qeyd etmələrinə səbəb bu kibercinayət növünün onların fəaliyyətini qeyri-müəyyən müddətə məhdudlaşdırması ilə bağlıdır. Lakin maraqlıdır ki, onlar yenə də DDoS-un başvermə ehtimalını aşağı səviyyədə qiymətləndirirlər.

İstisnasız olaraq, bütün qrupların dominant baxışı xüsusilə elektron xidmətlərdən (e-gov və e-ticarət) getdikcə daha çox istifadə və əvvəllər kağıza əsaslanan məlumatların indi rəqəmsallaşdırılması səbəbindən kibercinayətlərin gələcəkdə intensivləşəcəyi ilə əlaqəlidir. Bütün ÜƏQ-lərdə də məhz bu ortaq düşüncə mütləq müşahidə edilib.

"Hazırda bütün dünya analoq sistemdən rəqəmsal sistemə keçid edir. Xəstələrə dərmanların tətbiqindən təhlükəsizlik sisteminə qədər hər cür fəaliyyət artıq rəqəmsallaşdırılıb. Zaman keçdikcə insan asanlıqla uzaqdan başqalarına zərər yetirəcək gücə malik olacaqdır". R1

"Nə qədər rəqəmsallaşsaq, kibercinayətlər o qədər geniş yayılacaq". QHT

"Ağıllı cihazlar, 5G, fiberoptikadan daha çox istifadə, virtual reallıq – onların nə gətirəcəyini bilmirik (bu fikri çatdırarkən respondentin üz ifadəsinin skeptikləşməsi qeydə alınıb). R3

6.7 İXP (internet xidməti provayderləri) mütəxəssisləri

Qrup müşahidələri

Burada dörd qurum (3 özəl şirkət və 1 dövlət agentliyi) təmsil olunub. Özəl şirkətlər telekommunikasiya və internet təminatı sektoruna aid olmaqla, digər təşkilat onlayn təhlükəsizliyə cavabdeh dövlət qurumunu təmsil edib. Qrup kişi respondentlərdən ibarət olub. Sorğular zamanı bütün iştirakçılar eyni dərəcədə fəallıq nümayiş etdiriblər. Qrup ümumilikdə fəaliyyət göstərdikləri təşkilatlar daxilində müxtəlif vəzifələr tutan şəxslərdən təşkil olunub. Bir neçə sual istisna olmaqla (ehtiyat məlumatların saxlanılması – bir çoxu bunu paylaşmaq üçün məxfi məlumat kimi qiymətləndirib) respondentlərin məsələlərin müzakirəsindən məmnun qaldıqları müşahidə edilib.

6.7.1 Onlayn fəaliyyətlər (ümumi istifadə)

Tətbiqi həyata keçirilməyib - N/A (non-applicable)

6.7.2 Kibercinayətkarlıq və kibertəhlükəsizlik üzrə bilik səviyyəsi

Bu qrupun kibercinayətkarlıq anlayışının ümumi əhalidən xeyli fərqlənməsi respondentlərin qurumların nümayəndəsi kimi işlədikləri təşkilatları sözügedən fəaliyyətlərdən qorumaq vəzifəsi daşıyan şəxslər olması ilə izah edilə bilər. Özəl sektorda çalışan respondentlərin baxışlarında müəyyən ifadələrin yer alması bu qrupda xüsusi rezonans yaradıb: reputasiya və mənfəət itkisi. Demək olar ki, bütün iştirakçılar tərəfindən səslənən kiber-

hallar məlumat itirilməsidir ki, bu, onlar üçün verilənlər bazasından vacib dataların oğurlanması və ya gizli saxlanılması deməkdir. Qeyd edilənlərin ətraflı izahı soruşulduqda, aşağıdakı fikirlər meydana çıxıb:

"Bizim üçün bu, mənfəət və nüfuz itkisidir. Hücumlar səbəbindən sistem sıradan çıxanda telefonlarımıza gələn zənglər dayanmır. Mən elə hallar görmüşəm ki, şirkətlər saatlarla fəaliyyəti dayandırmalı olublar". R1

"Kibercinayətkarlıq ənənəvi cinayətlərin virtual məkanda törədilməsidir. Siz oflayn rejimdə olduğu kimi kimisə kibercinayətkarlıq yolu ilə öldürə bilərsiniz, məsələn, onları intihar edəcək səviyyəyə qədər qorxudaraq, insanları qeyri-qanuni işlər görməyə və qanunsuz əşyalar almağa təhrik edə bilərsiniz". R2

"Mən bunu məxfi məlumatların sızması kimi qiymətləndirirəm". R3

Təşkilatların təhlükəsizliyi baxımından respondentlərin özlərini müdafiədə hiss etmələri məsələsinə gəldikdə, təhlükənin daim mövcudluğu amili qeyd edilsə də, bəzi iştirakçılar müxtəlif cavablar səsləndiriblər. Müzakirələrdə "biz özümüzü 24/7 rejimində kibertəhlükələrdən mühafizə edirik" ifadəsi geniş şəkildə səsləndirilib.

Təhlükəsizlik haqqında danışarkən hər kəsin qeyd etdiyi əsas mövzu aydın olub. Belə ki, deyilənlərə əsasən, görülmüş bütün tədbirlərə baxmayaraq, Azərbaycanda əksər qurumların "Axilles dabanı" var. Başqa sözlə, burada istifadə olunan cihazlar və proqram təminatı tamamilə xaricdən idxal olunur. Dövlətdən fərqli olaraq, özəl sektor nümayəndələri, təhlükəsizlik səviyyəsinin yaxşılaşdırılmasında maliyyə çatışmazlığına tez-tez istinad ediblər. Ümumilikdə, bir çox respondent təhlükəsizlik məsələsini təsvir etmək üçün "50/50" ifadəsinə yer verib. Yəni mühafizə üçün çoxsaylı addımlar atdıqları halda (öz sözləri ilə desək, mümkün olanların 50%-ni) işin yarı hissəsinin onların nəzarəti xaricində olduğunu bildiriblər.

"Nəzərə alsaq ki, hətta Feysbuk kimi şirkət sistemindəki boşluqlardan zərər çəkib. Əlbəttə, biz də eyni şəkildə, məsələn, məlumatların pozulmasından ziyan görə bilərik. İstifadə etdiyimiz əməliyyat sistemi, eləcə də işlətdiyimiz cihazlar öz məhsulumuz deyil. Beləliklə, risk səviyyəsini 50% olaraq qiymətləndiririk". R3

Ölkədə ən çox yayılmış kibercinayətlərə dair rəylərdə də fərqli yanaşmalar müşahidə edilib. İki respondent fişinq növünü qeyd etsə də, başqa heç bir kibercinayət bir dəfədən artıq ifadə olunmayıb.

Sektorlar baxımından bir nəfər respondent istisna olmaqla, bütün iştirakçılar eyni fikirdədir ki, bank sferası yüksək risk daşımaqla, hücumlara ən çox məruz qalan sektordur. Banklar və maliyyə şirkətləri adından edilən fişinq zənglərinin və göndərilən məktubların son vaxtlar artması iştirakçılar tərəfindən qeyd edilən digər bir məqamdır. Yuxarıdakı fikirlərlə razılaşmayan bir nəfər respondent isə telekommunikasiyanı ən həssas sektor kimi cavablarına əlavə edib.

Kibercinayətkarlıqla bağlı hüquqpozmalara dair respondentlər tərəfindən müxtəlif motivlər qeyd olunub. İştirakçılardan üçü qazanc əldə etməyin əsas amil olduğunu, digər üçü isə ənənəvi cinayətlərin törədilməsində kibercinayətlərə alət kimi baxdıqlarını bildiriblər. Digər qruplardan fərqli olaraq, burada bir cavab mütləq surətdə seçilib (n=4) – casusluq və xalqlar arasında gizli məlumatların toplanılması.

Zərərçəkmə ilə bağlı həssaslığa gəldikdə, qrup daxilində cavablar fərqlidir. Dörd iştirakçının fikrinə görə, təhsil və məlumatlılıq səviyyəsi həssas kateqoriyanın formalaşmasını müəyyən edir. Beləliklə, onlar düşünürlər ki, yaşlılar nisbətən az məlumatlı olduqlarından sözügedən hallardan daha çox əziyyət çəkirlər. Digər beş iştirakçı isə hesab edir ki, 12-16 yaşlı gənclər ciddi formada risk qrupunu təşkil edir. Həmin respondentlər öz arqumentlərini aşağıdakı kimi əsaslandırıblar:

"Cinsindən asılı olmayaraq, 12-16 yaşda kibercinayətlərin qurbanı olma ehtimalı artır. Belə desək, bu yaşdakılarda riskli veb-saytlardakı məzmunlara maraq yarana bilər. Onlardan mikrofonu, kameranı, olduğu yeri və s. aktiv etmək tələb edilə bilər. Yaşları az olduğu üçün bu qrup potensial təhlükələri təsəvvür edə bilmir". R2

"Yeniyetmə oğlanların oyunlara böyük marağı var. Onlar çox vaxt kibercinayətkarlar tərəfindən oyunlarda qurulan tələlərə düşürlər". R5

Digər qruplardan fərqli olaraq, burada rəqəmsal cihazlarla bağlı məsələ müzakirə zamanı meydana çıxan həssas faktorlardandır

(n=3). Korporasiyaların həssaslıq səviyyəsindən danışarkən, respondentlər hesab edirlər ki, bir çox qurumların müdafiə üçün lazımi avadanlıq alınması üzrə maliyyə resursları çatışmır. Kiberhücumlara qarşı həssaslıqla bağlı digər amillər kimi qadın kateqoriyasından olmaq (n=1), satıcılarla işləmək (n=1) və ağıllı cihazlardan istifadə (n=2) qeyd edilib. "Satıcılarla işləmək" cavabının əsası əməkdaşlıqlar (biznes-ticarət və s .) zamanı kibertəhlükəsizlik tədbirləri/səviyyəsi, həmçinin risklər haqqında məlumatsızlıqla bağlıdır.

Fəaliyyət göstərdikləri təşkilatlar tərəfindən görülən ümumi müdafiə tədbirləri istiqamətində respondentlərin əksəriyyəti mövzunun dərinliyi haqqında danışmasalar da, çox sayda tədbirlər barədə söhbət açıblar.

İT ekspertlərindən ibarət qrupda olduğu kimi, müdafiə səddi (firewall), antivirus proqramları və spam filtrlərinə dair fikirlər səslənib. Bununla yanaşı, bu qrupun fərqləndirici xüsusiyyəti ondan ibarətdir ki, iştirakçıların hamısı virtual mühafizə sisteminə əlavə olaraq server və avadanlıqların fiziki təhlükəsizliyi haqqında da danışıblar. Artıq istifadə olunmayan cihazların fiziki olaraq məhv edilməsi üzrə oxşar bir yanaşma belədir:

"Bizim həm virtual, həm də fiziki müdafiəmiz mövcuddur, çünki serverlərimiz 24/7 nəzarət edilən xüsusi yerdə yerləşir. Həmin əraziyə daxil olma və ya oradan çıxış zamanı giriş üçün şifrələr, şifrə rekvizitləri diqqət etdiyimiz vacib elementlərdir ki, bunlar müdafiəmizi təşkil edir". R7

"Elektron məlumatlardan xilas olmağın özü ayrıca məsələdir. Lakin biz binamızdakı xüsusi otaqda cihazların fiziki məhvini də həyata keçiririk". R6

Bu qrupun kibercinayətlərin ciddilik dərəcəsini qavrama səviyyəsi nisbidir. Respondentlər düşünür ki, heç bir cinayət təkbaşına yalnız ciddilik amilinə görə qiymətləndirilə bilməz – daha doğrusu, konkret zorakılıq və ya mülkiyyət cinayəti ilə əlaqəli olan hansısa kiberfəaliyyətin ölçüsünü müəyyən etmək lazımdır. Bir neçə iştirakçı onlayn zorakılıq-təhqir və ya sui-istifadə kimi kibercinayətlərdə qurbanın intiharına şərait yaradan nümunələr misal göstərməklə, bəzi hallarda bu kimi iki cinayətin üst-üstə düşməsi haqqında danışıblar. Yalnız bir respondent zorakılıq cinayətini birmənalı olaraq daha ciddi hesab edib (müqayisə edilən kibercinayətin fiziki zərər daşımadığı hallarda). Ümumilikdə, belə yanaşma bütün qruplar tərəfindən ifadə edilən cavaba olduqca oxşardır.

Hər bir iştirakçı qurumun nümayəndəsi mütəmadi olaraq sistemə nüfuzetmə testləri keçirdiklərini bəyan edib. DTX təmsilçisi isə qeyd edib ki, bu, onların vəzifə borcudur və bütün dövlət qurumları üçün ildə iki dəfədən az olmayaraq belə tədbirlər həyata keçirirlər.

"Data mərkəzimizdə xüsusi proqram təminatı mövcuddur. O, sistem istifadəçilərini müntəzəm şəkildə izləyir və təhlil edir. Məsələn, deyək ki, X (iks) istifadəçinin gündəlik giriş və çıxış vaxtının xəritəsi vardır və onun şəxsi şifrəsi bu və ya digər formadadır. İstifadəçi haqqında parametrlərdən hər hansı biri dəyişərsə, sistem belə halı şübhəli fəaliyyət kimi işarələyərək məlumat verir". R5

6.7.3 Kibercinayətkarlıq və kibertəhlükəsizliyə dair İXP ilə əlaqədar xüsusiyyətlər

Cavablardan aydın olduğu kimi, iştirakçı təşkilatlar tərəfindən toplanılan yeganə məlumatlar mənbə və təyinat nöqtəsinin izlənilməsindən ibarətdir. Başqa sözlə, trafikin haradan gəldiyi və hansı veb-sayta daxil olunması haqqında informasiya qeydə alınır. İstifadəçi profilləri ilə bağlı isə heç bir məlumat yığılmır. Məlumatların silinməsinə gəldikdə, qurumdan asılı olaraq, hər 3, 6, 12 ayda bir toplanılanların silinməsi prosesi aparılır. Respondentlər məlumatların silinməsi üzrə indiyədək müraciət qəbul etmədiklərini yekdilliklə bildiriblər. Bəziləri isə bu kimi məlumatların cinayətkarları aşkar etməkdə hüquq-mühafizə orqanlarına faydalı olduğunu söyləyiblər.

Qrupdakı hər hansı bir şirkətin nümayəndəsi müştəri məlumatlarını satmadığını iddia edərək belə əməli qanunazidd olaraq qiymətləndirib. Əslində, məlumatların saxlanılmasından danışarkən, bütün təşkilatlar bunu icra etmək istədiklərini, lakin saxlama vasitələrinin olmamasını maneə kimi qeyd ediblər.

"Provayderlər tərəfindən məlumatların toplanılması düzgün deyil, çünki bu, böyük həcmdə investisiya tələb edən məsələdir. Toplanıla bilən məlumatlar və bununla bağlı bizim

gördüyümüz işlər isə belədir: İP ünvanlarının qoşulma vaxtı, daxil olunan veb-saytlar və onlayn rejimdən çıxış saatının müəyyən edilməsi. İnanıram ki, daha çox təfərrüat toplanılmalıdır, ona görə ki, mövcud vəziyyətə əsasən hansısa dövlət qurumu kiminsə haqqında məlumat tələb etdikdə, İXP-lər onlara lazımi cavab verməkdə çətinlik çəkirlər". R5

"Məlumatların toplanılması və idarə edilməsi həm maliyyə, həm də texnoloji baxımdan asan iş deyil. Üstəlik, ölkədəki internet provayderlərinin 90%-i belə fəaliyyət aparmır". R3

"Müəyyən məlumatları toplayırıq. Verilənlər (meta-data) iki qrupa bölünür. Hansısa məlumatların yığılması səbəblərindən biri dövlət təhlükəsizliyi ilə bağlıdır, belə ki, cinayət hallarında cinayətkarı bu vasitə ilə tapa bilərik. Digər halda isə məqsəd müştərilərin login trafiki və müddətini qeyd etməkdir".

Yalnız dövlət sektorunda çalışan bir respondent təmsil etdiyi təşkilatda ISO/IEC 27001-ə riayət etdiklərini ifadə edib. Əlavə olaraq qeyd edib ki, onlar özləri tərəfindən hazırlanmış daxili standartlara da əməl edirlər.

6.7.4. Fişinq (phishing)

Hər hansı zərərçəkən müəyyən edilməyib.

6.7.5. Rənsamveə (ransomware)

Zərərçəkən mövcud olmasa da, sadəcə illər əvvəl bir neçə cəhdin həyata keçirilməsi haqqında cavab qeydə alınıb.

6.7.6. Hədə-qorxu, zorakılıq-təhqir və sui-istifadə

Heç bir iştirakçı (özəl sektordan bir nəfər respondent istisna olmaqla) kibermüstəvidə "imtiyazların eskalasiyası" hücumu ilə üzləşməsə də, bu kibercinayət növü çoxlarının həyəcanına səbəb olub. Əslində, yalnız DDoS və adıçəkilən əməl respondentlərin bədən dilində qrup miqyaslı və aydın müşahidə edilən narahatlığı üzə çıxarıb. Bu baxımdan, aşağıdakı fikirlər həmin narahatlıqları əks etdirir:

"Əlbəttə, imtiyazların eskalasiyası hücumu ciddi bir haldır. Sistemimizə adi "istifadəçi" kimi qoşulur, administrator səviyyəsinədək yüksəlməklə sonda istədiklərini etməyə çalışırlar".

"DTX-də audit qrupu vasitəsilə özümüzü imtiyazların eskalasiyası hücumundan qoruyuruq. Komanda ildə iki dəfə həm daxili sistemimizi, həm də hökumət veb-saytlarımızı izləyir və ya skan edir. İstənilən halda, bu əməllərin daxildən baş verməsi də yüksək ehtimaldır".

6.7.7. Şəxsiyyət/kimlik (fərdi məlumatların) oğurluğu

Yalnız özəl sektorda çalışan bir iştirakçı məlumatların müdafiə səddinin aşılmasından əziyyət çəkdiyini ifadə edib. O, bununla bağlı təcrübəsini bölüşüb:

"Məlumatların "qırılması" hadisəsi ilə qarşılaşmışıq. Belə hal sadəcə bir ehtiyatsız hərəkətlə də meydana gələ bilər. Mühasib əməkdaşımız şəxsi fləşkartını (yaddaş kartı) şirkətimizin kompüterlərindən birinə daxil edib. Növbəti gün texniki direktorumuzdan bununla bağlı mənə zəng gəldi. Çünki hər bir işçinin şifrəsi və istifadəçi adı onun masasında idi. Gördüyümüz kimi, hadisə sürətlə baş verdi və bir fləşkart təhlükəsizliyimizi pozmağı bacardı".

6.7.8. Kibermüdaxilə (DDoS)

Demək olar ki, bütün respondentlər DDoS ilə müntəzəm surətdə qarşılaşdıqlarını bildirir və bunu fəaliyyət göstərdikləri şirkət, yaxud təşkilatların xarici agentlərin hədəfi olması ilə əlaqələndirirlər. Bu baxımdan, DDoS iştirakçıların hər biri tərəfindən ən çox rast gəlinən hücum kimi qeyd olunub. Bu hal başadüşüləndir, çünki iştirakçılardan altısı telekommunikasiya və internet təminatına cavabdeh şirkətlərdə, digər üçü isə ölkədəki bütün dövlət orqanlarının onlayn təhlükəsizliyinin qorunmasına məsul dövlət qurumunda çalışır. Uzunmüddətli iş təcrübəsinə əsaslanaraq, onlar DDoS-da yeni xüsusiyyətin yaranmasına diqqəti yönəldiblər. Daha dəqiq desək, mütəxəssislər bildiriblər ki, DDoS ölçüsü 10-12 il əvvələdək nadir hallarda 1 giqabayta çatırdısa, indi o, asanlıqla 1 terabaytı keçir. Xüsusən, meqa idman və ya mədəni tədbirlər, yaxud siyasi hadisələrdən əvvəl DDoS hücumlarının tezliyi və ciddilik səviyyəsinin artmasına dair geniş yayılmış fikir də cavablar sırasındadır.

"DDoS hücumu nəticəsində bu yaxınlarda

müştərilərimizə internet təminatı dayandı. Rəhbərlik, texniki direktor və digərləri tərəfindən telefonuma fasiləsiz zənglərin gəlməsi davam edirdi. Sistemi bərpa etmək bir neçə dəqiqə çəksə də, tanıdığım başqa bir internet provayderdə oxşar hadisə zamanı vəziyyət 6 saata düzəlmişdi".

"DDoS böyük maliyyə itkisinə səbəb olmaqla, həm də müştəri məmnuniyyətini azaldır, çünki xidmət səviyyəsi aşağı düşür. Beləliklə, bu hal bizi həmişə ayıq-sayıq vəziyyətdə saxlayır"

6.7.9 Kibercinayətkarlıq: narahatlıq və gözləntilər

Kibercinayətkarlıqdan zərər çəkilərsə, bu halda məlumat çatdırılması üzrə suallara cavablar baxımından qeyd edilməlidir ki, üç iştirakçı (hər biri dövlət təşkilatını təmsil edir) işlədiyi yerin ərizə veriləcək qurum olduğunu ifadə edib, yəni analoji hallarda onlar özləri başqa təşkilata xəbər vermirlər. Digər iştirakçılar isə (hər biri özəl sektorda çalışır) iki cür cavab təqdim ediblər: məsələnin daxili yolla həll edilməsi və ya fokus qrupda təmsil olunan dövlət təşkilatına hesabat verilməsi. Əslində, müzakirə müddətində və hətta müsahibədən əvvəl və sonra da sorğuda respondent kimi iştirak edən dövlət və özəl qurum nümayəndələrinin dialoqu müşahidə edilib. Özlərinin də qeyd etdikləri kimi onlar sözügedən mövzularla bağlı daimi ünsiyyət yaradırlar.

İştirakçıların gələcəkdə kibercinayətkarlığa məruzqalma zamanı bu barədə hansısa struktura məlumatvermə ehtimalına dair suallara cavablar ümumilikdə İT ekspertlərinin müvafiq baxışları ilə eynilik təşkil edib. Bütün cavablarda "vəziyyətdən asılıdır" ifadəsi üstündür. Başqa sözlə, iştirakçılar bu baxımdan cinayətləri kateqoriyalaşdırırlar: bacarıqlarına əsasən təkbaşına həll edəcəkləri hücumlar (məsələn, DDoS) və imkanlarından kənar hadisələr (məsələn, şəxsi məlumatların oğurlanması və ya onlayn hədə-qorxu).

Qrupun dominant mövqeyi kimi kibercinayətlərin gələcəkdə güclənməsinə inam, xüsusən həyatımızın bütün sahələrində smart cihazların getdikcə artan istifadəsi ilə bağlıdır. Bu mənada, bir çox respondent "ağıllı evlər"ə istinad edərkən təhlükə səviyyəsini izah etmək üçün belə qeyd edib: *"Kimsə bacarsa və istəsə, birinin evini uzaqdan partlada bilər"* (yəni cihazların idarəetməsini ələ keçirməklə başqalarına hər cür ziyan yetirilə bilər). Qeyd edilən digər narahatlıq DDoS-un artan meydanagəlmə səviyyəsi və onlardan müdafiənin çətinliyidir.

Ən çox diqqət çəkən kibercinayətlər sırasında daxildən olan hücumlar da yer tutur. Ətraflı təsvir edildikdə, iki cavab mövcuddur: məxfi məlumatları əldə etmək və paylaşmaq üçün kənar şəxslə gizlin əməkdaşlıq edən işçinin davranışı, ya da işçi səhvi nəticəsində daxili təhlükəsizliyin ifşası və pozulması. "Troya atı" belə kibercinayətlər sırasında ikincidir. Müvafiq narahatlığı dilə gətirənlər Maykrosoft və Sisko şirkətlərinə istinad edərək izah edirlər ki, əgər onlar "Troya atı" hadisəsindən əziyyət çəkirlərsə, respondentlərin işlədikləri qurumlar da asanlıqla qurbana çevrilə bilər.

"Ölkədə provayderlər arasında ciddi problem sistemi xarici təhdidlərdən qorumağa dair narahatlıq səviyyəsidir. Çünki onlar daxili təhdidlərə laqeydliyə meyillidirlər. Məsələn, işçi şəxsi telefonu vasitəsilə şəbəkəyə qoşula bilər ki, bu, özlüyündə təhlükə amilidir". R3

"DTX olaraq dövlət orqanlarında sistemlərin və rabitə xətlərinin xarici təhlükələrdən qorunmasını təmin edirik. Bu, asandır, çünki müdafiəni quraraq hücumun baş verməsini gözləmək və dəf etmək mümkündür. Halbuki, daxili faktorlar da təhlükə yarada bilər. Qurumların parametrləri və kommunikasiya xətlərini mühafizə etsək də, hər təşkilatın öz şəbəkəsində baş verənlərə nəzarət edə bilmirik". R2

"Bəli, daxili mənbələrdən yaranan problemlərlə üzləşmişik. Məsələn, işçilərdən biri məlumat bildirməyərək nəyisə "yumşaq" formada dəyişmişdi, beləliklə, biz vəziyyətdən xəbərdar olanadək və sistemi sınaqdan keçirməmişdən əvvəl dəyişiklik xeyli müddət fəaliyyət göstərmişdi". R4

6.8. Hüquq-mühafizə orqanları (HMO)

Qrup müşahidələri

Təşkilatlar bu qrupda məhdud sayla (Dövlət Təhlükəsizliyi Xidməti – 5, Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi – 1, Daxili İşlər Nazirliyi – 1, Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Xidməti – 1) təmsil olunub.

6.8.1.Onlayn fəaliyyətlər (ümumi istifadə)

Kiberrisk nöqteyi-nəzərindən ümumi əhali üçün ən təhlükəli hesab edilən onlayn fəaliyyətlər baxımından e-ticarət və fişinq respondentlər tərəfindən ən riskli əməllər kimi fərqləndirilib. KİMM nümayəndəsi qeyd edir: *"Bizə bildirilən hadisə hesabatlarına əsasən, İnstaqram və digər e-ticarət platformalarında satışlar risk daşıyır. Burada hesabların müdafiəsi mütəmadi olaraq qırılır. Bank sferasında da insidentlər barədə tez-tez məlumat verilir".*

Eyni məqamı Daxili İşlər Nazirliyinin nümayəndəsi də ifadə edib. Dövlət Təhlükəsizliyi Xidmətinin əməkdaşı bunlarla yanaşı, kiçik müəssisələrə diqqəti yönəldərək onların onlayn müdafiə mexanizmlərinin iri tərəfmüqabilləri ilə müqayisədə daha məhdud səviyyədə olması, beləliklə, tez-tez hədəfə çevrilməsini fikirlərinə əlavə edib. Pandemiya və kibercinayətkarlıq məsələlərinin müzakirəsində də geniş əhali üçün ən təhlükəli hesab edilən onlayn fəaliyyətlərə dair peşəkarların baxışları mövcuddur. DTX əməkdaşının qeyd etdiyi maraqlı məqam belədir:

"Çoxsaylı xarici ölkələrlə müqayisədə kibercinayətkarlıq bank işi istisna olmaqla, ciddi qəbul olunmur. Bizdə yüksək səviyyədə olmasa da, xaricdə xeyli miqyasda kibercinayətkarlarla insayder (daxili) əməkdaşlıq təcrübəsi vardır".

Sektorların kiberhücumlara qarşı həssaslığı baxımından hər bir respondent kritik infrastruktur sahələrini, iki respondent isə bank sənayesini qeyd edib. Bütün iştirakçıların fikrincə, kritik infrastruktur sahələrinə hücumlar ən qorxuducu hadisə kimi müəyyən edilib. Daxili İşlər Nazirliyi nümayəndəsinin fişinq və e-ticarət (bank rekvizitlərinin əldə edilməsi və ya depozit tələbi) hüquqpozmalarını ən çox yayılan hal kimi qeyd etməsilə yanaşı, Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin əməkdaşının cavabı belədir: *"Məlumatlar və pul əldə edilən hər bir sektorda zərərçəkmə ehtimalı daha yüksəkdir".* KİMM-dən olan bir respondent isə fikrini belə ifadə edib: "*Əvvəl bildirdiyim və digər iştirakçılar tərəfindən də ifadə edildiyi kimi, İnstaqram və digər e-ticarət platformalarında aparılan onlayn ticarət, həmçinin bank fəaliyyətləri bu mövzuda olduqca həssasdır".*

6.8.2. Kibercinayətkarlıq və kibertəhlükəsizlik üzrə bilik səviyyəsi

Qrup iştirakçılarının nəzərində hüquqi məcəllədən irəli gələn kibercinayətin vahid tərifi belədir: *"Kibercinayət kompüter sistemlərinin sındırılması və saxlanılan məlumatların əldə edilməsi, yaxud zədələnməsi ilə bağlı fəaliyyətdir".* Bəziləri isə öz yanaşmalarına əlavə edib ki, istehsalçılarına gəlir gətirən zərərli proqramların dövriyyəsi də kibercinayətdir.

Digər tərəfdən, bütün qruplardan fərqli olaraq, burada respondentlər kibercinayətin tərifi ilə bağlı müəyyən bir problemə də diqqət çəkiblər. Belə ki, onların fikrincə, kibercinayətkarlıqla mübarizədə ən vacib məsələlərdən biri ümumi qəbul edilmiş izahın olmamasıdır. Məsələn, "kiberdələduzluq" ifadəsinin geniş yayılmasına baxmayaraq, hüquqi qaydada kibercinayət kimi müəyyən edilmir. Bu, sadəcə İKT vasitələri ilə həyata keçirilən dələduzluq növüdür.

"COVID-19" pandemiyasından sonra kibercinayətkarlığın təbiətində və intensivliyində meydana gələn dəyişikliklə bağlı isə rəylərdə yekdil qənaət müşahidə edilib. Buna dair bir sıra misallar aşağıda sadalanıb:

"COVID-19 pandemiyası zamanı üç mühüm dəyişiklik aşkar etdik. Birincisi, evdən işləmə rejimi işçilərin şirkətlərin təhlükəsizlik şəbəkəsindən kənar qalması demək idi. Belə ki, hər dəfə şirkət şəbəkəsinə başqa yerdən qoşulduqda bu, korporativ sistem üçün təhlükə yaradırdı. İkincisi, onlayn ticarətin artması daha çox onlayn məlumat mövcudluğu deməkdir. Üçüncüsü, fişinq daha geniş yayılıb və mən burada "pandemiya xəritəsi" tələsini qeyd etmək istərdim. Özünü sağlamlıq müəssisəsi kimi təqdim edən təşkilatlar internet istifadəçilərinə COVID-19-un yayılmasının yenilənmiş təsvirini əks etdirən xəritələr göndərirdilər. Bu xəritələri açanlar dələduzların tələsinə düşürdülər. Əslində, belə hücumlar çoxsaylı dövlət qurumlarını hədəf almışdı". XRİTDX

"Mən fişinqin daha geniş yayıldığı fikri ilə tamamilə razıyam və bu halların çoxunda COVID-19 virusundan qorunma haqqında mesajlar da yer alır. Müşahidələrimizə əsasən, bəziləri hətta rənsamvеə ilə nəticələnən hadisələrdir. Özünü səhiyyə müəssisəsi kimi təqdim edən bir neçə saxta profil də aşkar etmişik". KİMM

"Bank sektorunda kibercinayətlərin artdığı-

nı müşahidə etmişəm. Saxta bank profilləri yaradılaraq insanlara evdən çıxmadan hesab açıb əməliyyatlarını həyata keçirməyi təklif edirlər. Belə şəxslərə etibar edənlər dialoq şəraitində onlara (qondarma banka) öz bank rekvizitlərini təqdim edirlər. Zərərçəkmişlər tərəfindən bankla bağlı qeyd edilən məsələlərlə əlaqədar Nazirliyimizə xeyli sayda hesabatlar daxil olur." DİN

Kibercinayət və kibertəhlükəsizlik – ümumi

İştirakçıların eşitdikləri əsas kibercinayətkarlıq növləri baxımından cavablar sırasında fişinq diqqəti çəkir. Bununla yanaşı, DTX-nin əməkdaşları olan respondentlər biznes dilerləri hədəf alan "ortadakı adam" (tərəflər arasında və ya gedişatda fəaliyyətindən istifadə edilən şəxs, casus və s.) cinayətini və banklar adından edilən saxta çağırışları nəinki getdikcə geniş yayılan, həm də qurbanlar üçün çətin anlaşılan hallar kimi qiymətləndiriblər.

Respondentlər fişinqin çoxsaylı növlərini qeyd ediblər. Çünki bu, fəaliyyətləri çərçivəsində, adətən, məşğul olduqları əsas cinayət növüdür. Yuxarıda qeyd olunduğu kimi, "ortadakı adam" hallarına da getdikcə daha çox rast gəlinir və DTX-ya daxil olan müraciətlərdə öz əksini tapır. Qurumu təmsil edən respondentlərin sözlərinə görə, belə cinayətlər zərərçəkənlərə milyonlarla dollar və ya avro itkisinə başa gəlir.

Kibercinayətin ciddiliyinə münasibətə nəzər saldıqda, demək olar ki, birmənalı surətdə bu əməllər potensial daha təhlükəli hesab olunub. Hücumların kritik infrastruktur sahələrini hədəfseçmə imkanlarını nəzərə aldıqda, onların ənənəvi cinayətlərlə edilə bilməyən kütləvi ziyana səbəbolma xüsusiyyəti və buna görə daha təhlükəli xarakter daşıması aydındır. Bununla belə, maraqlı məqam Cinayət Məcəlləsinin kibercinayətlərə cəza təyin etməsilə bağlıdır. DTX əməkdaşı qeyd edib ki, mühüm infrastruktur sahələrinə hücum qanunla kibercinayətin ən ağır növü hesab edilsə də, cinayətkar maksimum 6 il həbs cəzası ala bilər.

Kibercinayətkarlığın qurbanı olmaqla bağlı müraciət üzrə geniş yayılmış düşüncə isə ondan ibarətdir ki, Azərbaycan vətəndaşları ümumiyyətlə kibercinayətkarlıqdan zərər çəkdikləri zaman hara məlumat verilməsinə dair xəbərsizdirlər, çünki bizdə kibercinayət qurbanlarının problemləri ilə məşğul olan xüsusi təşkilat fəaliyyət göstərmir. Əksinə, belə qurumların sayı çoxdur. Məsələn, həm DİN, həm də DTX sözügedən hadisələrlə bağlı təhqiqat aparır. Vətəndaşların kiberəməllər haqqında məlumat vermədikləri hallara dair səbəblər isə respondentlər tərəfindən belə ifadə edilib:

"İstintaq prosesində problem yaradan vəziyyətlərdən biri odur ki, bizə hər növ şikayətlər, o cümlədən araşdırılmalı olan çox kiçikmiqyaslı hadisələr barədə məlumatların daxil olması iş yükümüzü artırır. Məsələn, maliyyə cinayətləri üzrə təhqiqata cavabdeh orqanlar tərəfindən müəyyən edilməli məsələni həmin orqanlar məhz bizə yönləndirirlər, çünki onlar bizi bu mənada daha bacarıqlı hesab edirlər. Beləliklə, burada "ilkin cavabdeh qurum" anlayışına dair problem meydana çıxır". DTX

"Təcrübəmə əsasən araşdırmalar zamanı yaranan əsas problemlərdən biri kibercinayətkarların bilik səviyyəsinin artması ilə bağlıdır. Onlar oğurladıqları pulların izini, məsələn, xarici hesablara köçürməklə necə itirəcəkləri haqqında indi daha məlumatlıdırlar". DİN

"Bəzən zərərçəkmiş şəxslər məlumat bildirmir, bəziləri isə hadisə haqqında olduqca gec şikayət edirlər. Digər hallarda hesabat düzgün ünvana getmədiyinə görə həmin orqanın və ya qurumun işi bizə təhvil verməsi çox vaxt aparır. Sosial media hesablarımız vasitəsilə də zərərçəkmə hadisələri barədə müraciətlər alırıq. Zərərçəkənlər ofisə baş çəkdikdə isə onlardan hadisənin təfərrüatları haqqında soruşanda natamam cavablara, yaxud "(detalları-sübutları) skrinşot etməmişəm" (cinayətkarla ünsiyyət izləri və ya kompüterin ekran görüntüsü mövcud deyil - **qeyd.**) *kimi ifadələrə rast gəlirik. Bütün bunlar araşdırmanın ləngiməsinə səbəb olur". DTX*

Lakin iki qurumun nümayəndəsi bəzi hallarda insanların faktiki cinayət törədilmədən (kibercinayətə məruz qalmadan) öncə şübhə əsasında dərhal onlarla əlaqə saxladıqları vaxt bunun yaranan müsbət tərəflərini qeyd ediblər.

Bütün respondentlər razılaşır ki, zərərçəkənlərin şikayət ərizələrini yazmaq və səmərəli nəticə əldə etmələrini asanlaşdırmaq üçün hesabat-şikayət ərizəsi təqdimetmə mexanizmləri daha aydın (yəni şəxs hara və necə məlumat veriləcəyini bilməlidir) və az bürokratik olmalıdır.

Kibercinayət və kibertəhlükəsizlik – xüsusi

Qrup üzvləri tərəfindən qeyd olunan kibercinayətkarlıq motivləri demək olar ki, başqalarının təqdim etdiyi cavablarla üst-üstə düşür: özünütəsdiq, mənfəət, təxribat, casusluq və qisas (məsələn, narazı işçi tərəfindən). Geniş yayılmış maraqlı yanaşma isə kiberməkanın təklif etdiyi imkanları qeyd edir: anonimlik və potensial qurbanların daha böyük platforması.

Müxtəlif qrupların kibercinayətlərə həssaslıq səviyyəsi ilə bağlı sual da fərqli fikirlər doğurub. Üç respondent məlumatlılığın həlledici faktor kimi çıxış etməsi ilə bağlı yekdil fikrə malikdir. Onlardan ikisi məlumatlılıq səviyyəsini yaşla da əlaqələndirərək yaşlıların kiber "tələlər" haqqında zəif bilikləri olması səbəbindən daha həssas təbəqə olduğunu qeyd edib. İki respondent isə onlayn fəaliyyət səviyyəsini həssaslıq dərəcəsinin vacib nisbəti kimi görür. Başqa sözlə, onların fikrincə, onlayn rejimdən nə qədər çox istifadə edilərsə, ziyan çəkmək riskləri bir o qədər arta bilər. Bu respondentlər onlayn fəaliyyəti həm də yaş aspekti ilə əlaqələndirərək, gənclərin və orta yaşlı şəxslərin kibercinayətkarlığa daha meyilli olduğunu deyiblər:

"Əlbəttə ki, məlumatlılıq səviyyəsi aşağı olanlar kibercinayətkarlıq hallarına məruz qalmağa daha meyillidirlər. Kompüter və İKT-dən çox istifadə edənlər isə hansı e-poçtun cavablandırılması, göndərilən keçidlərin (link) açılması kimi məsələlərlə olduqca yaxşı tanışdırlar. Buna görə də yeni istifadəçilərin, xüsusilə də yaşlıların internetdə hər oxuduqlarına inanmaları onların zərərçəkmə ehtimalını artırır. Əslində, biz yaşlı insanların bilmədən yaydığı saxta xəbərlərdə çoxunu görmüşük". DTX

"Məlumat bazamız kibercinayətkarlığa məruzqalma hadisələrinin şəhər yerlərində nisbətən daha çox meydana gəlməsini üzə çıxarır. Biz bunu əslində məlumatlılıq səviyyəsi ilə izah edirik. Belə ki, insanların mövzu üzrə daha çox məlumatlı olması onların hesabat (şikayət ərizəsi) təqdim etmə ehtimalının yüksək olması deməkdir. Kənd yerlərinə nisbətdə daha çox paytaxtda müraciətlərin şahidi oluruq. Bu mənada, düşünürəm ki, həssaslıqla bağlı suala da cavab verdim". DTX

"Bank kartlarından istifadə formasını düzgün başa düşməyən çox sayda insan vardır. Fikrimi fərqli şəkildə izah edim: əgər siz kredit kartınızın bütün detallarını, o cümlədən bank kartının digər hissəsindəki təhlükəsizlik nömrəsi və telefonunuza göndərilən OTP kodunu harasa təqdim edirsinizsə, bu halda bankınız sizi qorumaq üçün nə edə bilər?" DİN

6.8.2.1. Əlaqələndirmə

Qeyd: Sualların məzmununa görə müsahiblərin şəxsiyyəti gizli saxlanılır.

Təhlillər nəticəsində aydın olub ki, biri istisna olmaqla, sorğularda iştirak edən bütün qurumlar işlərə (ərizələrə) baxılması üzrə prioritetləşdirmə mexanizmindən istifadə edib. Onlar qanunla hər bir şikayətə eyni dərəcədə ciddi yanaşmağa borclu olduqlarından, "kritik infrastrukturun hədəf alınması faktı hər hansı vətəndaş və ya zərərəçəkənin nisbətən az əhəmiyyətli hesab edilən müraciətlərinin ciddiliyini, ya da mahiyyətini kiçiltmir" ifadəsi qurumun müəyyən yanaşmasını əks etdirir. Halbuki, digər iştirakçı təşkilatların prioritetləşdirmə faəliyyəti də məlumdur. Belə ki, respondentlərdən biri qurumdaxili siyasətlərini "işlərə yanaşmamız kibercinayətin hədəfindən, onun kritiklik dərəcəsi və növündən asılıdır" kimi təsvir etsə də, digəri belə ifadə edib:

"Hadisə haqqında məlumat daxil olduqda zərərin qarşısını almaq üçün təcili müdaxilə vacibdir. Prioritetlər təyin edilməlidir. Kibertəhlükəsizlik agentliklərində bu nəzərə alınır. Müraciətlərə qanunvericiliklə müəyyən edilmiş müddətdə cavab verilməlidir. Hər hansı bir ziyan önlənəcəksə, biz həmin müraciətləri əhəmiyyətinə görə sıralayırıq. Bəzən cəmiyyətin elə qrupları var ki, onlar daha həssas təbəqədir. Nisbətən həssas kateqoriyaya aid müraciətçilərə və ya zərərçəkənlərə mümkün müddətdə tez cavab verilməsi üçün belə qrupları aydınlaşdırırıq. Bəzi hallarda məlum olur ki, dəymiş ziyanın fəsadları ciddi olmasa da, vətəndaş bunu əhəmiyyətli hesab edir".

Bütün iştirakçı təşkilat nümayəndələri kibercinayətkarlıqla bağlı lazımi məlumatların toplanılmasına dair problemləri səsləndiriblər. Müəyyən müsbət şərhlər olsa da, bir çox məsələlər məlumat toplanılmasına maneə törədən hallarla əlaqəlidir. Ortaya çıxan ümumi məqamlardan biri kibercinayətkarlıqla

üzləşən təşkilatların müvafiq dövlət qurumlarına məlumat bildirməkdən yayınmalarıdır ki, respondentlərdən birinin yanaşmasına əsasən bu vəziyyət "maarifləndirmə proqramları vasitəsilə dəyişdirilə bilər". Bir çox kibercinayətlər belə problemə görə qeydə alınmadığından, müvafiq hal hüquq-mühafizə orqanlarının çəkindirici təsirini də zəiflədən faktora çevrilir. Başqa bir respondent diqqəti zərərçəkmiş şəxslərin onlarla əməkdaşlıq edə bilməməsinə yönəldib. Başqa sözlə, qurbanlar hara müraciət edilməli olduğunu bilmədikləri və cinayətkarla ünsiyyət izlərini saxlamadıqları üçün bu vəziyyət şikayətə baxan qurumun (respondentin fəaliyyət göstərdiyi cavabdeh təşkilat) istintaq işini çətinləşdirir. Aşağıdakı sitatlarda qeyd edilənlərə aid bəzi nümunələr təqdim edilir:

"Burada iki məsələ var ki, onlardan biri daxili məlumatların toplanılması ilə bağlıdır. Bu baxımdan, əslində, heç bir çətinlik yoxdur, onları əldə edə bilərik. Məsələn, bank məlumatları. Ancaq bəzi hallar var ki, məsələ ölkə hüdudlarından kənara çıxır. Misal üçün, başqa ölkəyə məxsus İP (internet protokol ünvanı) aşkarlandıqda cinayətkarın kimliyi dəqiqləşdirilməlidir. Bu, həmişə uğurlu alınmır. Ərizə əsasında tapmaq mümkün olsa da, bəzən İP bir neçə şəbəkədən keçdiyi üçün itir və onun müəyyən edilməsi çox çətinləşir. Eyni zamanda, digər ölkələr bizim müraciətlərimizə heç də həmişə cavab vermirlər. Məsələn, kibercinayət nəticəsində 10 min manat pul oğurlanıbsa, bu, xarici həmkar qurumlar üçün əhəmiyyət daşımayan hadisədir. Bu halda onlar sorğumuza cavab verməyə bilərlər. Lakin, əksinə, ortada aqressiya, insan ölümü faktı varsa, onda müraciəti cavablandıra bilərlər. Əslində, 30-50 min manat dəyərində kiberoğurluq hadisələri beynəlxalq səviyyədə ağır cinayət sayılmadığı üçün xaricdən məlumat almaq bu mənada olduqca mürəkkəb məsələdir".

"Hər iki sahədə çətinliklər mövcuddur: həm texniki, həm də hüquqi. Hüquqi nöqteyi-nəzərdən məsələ ondan ibarətdir ki, qanunvericiliyimizdə kibercinayətlərin araşdırılması üzrə zəruri prosessual hüquqi tədbirlərin həyata keçirilməsi üçün ayrıca kiberxüsusi müddəalar yoxdur. Bu halda məcburən kibercinayətlərin təhqiqatına ənənəvi prosessual hüquq normalarını tətbiq etməli oluruq. Kibercinayətləri təsnif etmək də asan deyil, çünki cəmiyyət üçün təhlükə yaratmayan nisbətən az ağır cinayət hesab olunur. Biz işin gedişatında məhkəmə qərarı almaq, məlumat əldə etmək və məzmunu nəzərdən keçirmək məcburiyyətindəyik. Məlumatı açıqlamaq üçün isə əlimizdə məhkəmə qərarı olmalıdır. Leqallaşdırma ilə bağlı qanunvericilik bizə məhdudiyyətlər tətbiq edir, bu da kibercinayətlərin araşdırılmasını qəlizləşdirən amildir. Əlavə olaraq, burada bəzi texniki çətinliklər də vardır".

"Yalnız məhkəmə qərarı olarsa, biz məlumat toplaya bilərik. Başqa amillərlə də qarşılaşırıq. İlk növbədə, əldə edilən məlumatları təsnif etmək lazımdır. Onları iki hissəyə bölmək olar: sabit və dəyişən məlumatlar. Məlumat alındıqdan və araşdırma aparıldıqdan sonra cinayətin kim tərəfindən və hansı səbəbdən törədildiyini müəyyən etmək mümkündür. Lakin məlumatların şifrələnməsi kimi maneələrlə də rastlaşırıq. İstənilən vasitə ilə şifrələrin açılması uzun müddət vaxt apara bilər. Yaxud bu prosesin qısa müddət tələb etdiyi obyektiv məlumatlar da olur. Digər hallarda həddindən çox informasiya problemə çevrilir (bəzən məlumat çoxluğu terabaytlıq həcm təşkil edə bilər). Bu məlumatların yalnız kiçik bir hissəsi istintaqa gərəklidir. Yekun olaraq, deyə bilərik ki, biz məlumat toplaya bilərik, lakin nəticə əldə etməkdə çətinliklər qalmaqda davam edir".

Digər ölkələrlə (məsələn, Aİ ölkələri) əməkdaşlıq bütün iştirakçılar tərəfindən qeyd edilib. Respondentlərdən birinin təmsil etdiyi təşkilat qlobal miqyasda 20-dən çox mərkəzlə əməkdaşlıq edir və 6 beynəlxalq təşkilatın tamhüquqlu üzvüdür. Nümayəndənin sözlərinə görə, onlar beynəlxalq müzakirələrdə iştirak etməklə və həmin təşkilatlarla iş nəticəsində vacib mövzular haqqında öyrənsələr də (göstəricilərin mübadiləsi, təhdidlərin prioritetləşdirilməsi, qlobal tendensiyalar, yeni kibercinayətlərlə tanışlıq və s.), cinayət axtarışı həyata keçirmək səlahiyyətinə malik deyillər. Oxşar fikri digər bir respondent də səsləndirib. Bu iki iştirakçıdan fərqli olaraq, növbəti respondent əməkdaşlıq etdikləri təşkilatların/dövlətlərin sayını bildirməsə də, cinayət təhqiqatında iştirak etmək səlahiyyətinə malik olduqlarını və lazım gəldikdə beynəlxalq həmkarlardan cinayətin detalları ilə bağlı məlumat tələb edə biləcəklərini bildirib. Buna baxma-

yaraq, həmin iştirakçı xaricdən cavabların gəlməsində həddən çox gecikmələrin olmasından şikayətlənərək qeyd edib ki, belə hallar araşdırma aparılmasında maneəyə çevrilə bilər. Respondent bu kimi münasibətin (gecikmədən əlavə aşağı səviyyədə dəstək hallarına da rast gəlinir) Budapeşt Konvensiyasına zidd olduğuna diqqət çəkib. Bütün bunlarla yanaşı, iştirakçılar tərəfindən bildirilən başqa bir mövzu aşağıdakı sitatla qısa şəkildə ümumiləşdirilə bilər:

"Bəzi ölkələr informasiya sorğularına olduqca laqeyd yanaşırlar. Onlar Konvensiyanın tələblərinə əməl etmir, müddəalara diqqət yetirmirlər. Sorğuların icrası ilə bağlı səthi yanaşmaların şahidi oluruq. Məsələn, bir neçə hal üzrə sorğu göndərdikdə bəzən yalnız biri haqqında məlumat təqdim edirlər və belə münasibət mövzuya dair dolğun cavab almağa imkan vermir. Bu kimi vəziyyətləri hər hansı konvensiya nizamlaya bilməz. O, hər bir ölkənin daxili qanunvericiliyindən asılıdır və ona əsaslanır. Beləliklə, beynəlxalq konvensiyaya o qədər əhəmiyyət verilmədiyi müşahidə olunur. Ona görə də kibercinayətkarlıq məsələlərinin ən zəif halqası da hüquqi yardım sorğularıdır. Texniki tərəfləri əhatə edən xeyli məlumat əldə etdiyimiz halda, qarşı tərəfin aidiyyəti qurumları araşdırma zamanı başqa problemlər yaradır... Elə olur ki, bəzən onlardan cavab aylarla gəlməyə bilər. Konvensiyalarda sorğuların icrası üçün konkret müddət müəyyən edilməyib. Yaxşı olardı ki, tərəflər vaxtında öhdəlik qəbul etsinlər, məsələn, sadə problemi bir ay ərzində, mürəkkəb məsələlərin həllini isə daha uzun müddətə həyata keçirsinlər".

Geniş məlumatlar - "Big Data" bazaları ilə əlaqədar onu qeyd edə bilərik ki, bu tədqiqatda öz nümayəndələri ilə təmsil olunan qurumlardan birinin belə məlumatları müəyyən üsullarla tərtib edən və onlara təqdim edən "qidalanma" mərkəzlərinin xidmətindən istifadə etməsi məlumdur. Bu tipli geniş verilənlər bazası, adətən, təhdidlər və yeni tendensiyaların formalaşması ilə bağlıdır. Cavablara əsasən məlum olur ki, hər bir dövlət təşkilatı kibercinayətkarlıqdan müdafiə olunmaq üçün mütəmadi qaydada müvafiq məlumatlarla təmin edilir və burada "Big Data" mühüm rola malikdir. Digər bir təşkilat üzvü bildirib ki, cinayət təhqiqatında əhəmiyyətli sayılan məlumatları deşifrə etmək üçün "onlayn borulardan" (ödənişli və ödənişsiz olmaqla) faydalanırlar. Qalan qurumlar isə (n=2) böyük məlumatlar (big data) üzrə repozitoriyalarından (yəni məlumat bazalarından) istifadə etmirlər.

Azərbaycan Aİ-nin Ümumi Məlumatın Mühafizəsi Qaydalarının (ÜMMQ) yurisdiksiyasından kənar olduğu üçün tədqiqatda iştirak edən təşkilatların heç biri təlimat kimi ona əməl etməsə də, hər biri Cinayət Məcəlləsinə və qaydalara riayət edirlər (**QEYD**: bir respondentin məlumatına əsasən, yerli qaydaların ÜMMQ-yə uyğunlaşdırılması istiqamətində hazırda işlər aparılır). Digər tərəfdən, respondentlər qeyd ediblər ki, fərdlərin şəxsi məlumatları ilə bağlı qanunların mövcudluğuna baxmayaraq, onlar ÜMMQ qədər əhatəli və təfərrüatlı deyil. İştirakçılardan biri kibercinayətlərin araşdırılması zamanı insan hüquqlarına dair qanunlara əməl edilməsi ilə bağlı geniş problemə münasibət bildirib:

"Bizdə şəxsi həyatın toxunulmazlığının qorunması haqqında qanun var. Lakin məzmunu hələ ÜMMQ qədər müfəssəl deyil. Bu həm özəl sektorun, həm də üçüncü tərəfin əməkdaşlarının kifayət qədər təlim keçmədiyi vəziyyətlə əlaqəlidir. Məsələn, nəzarət jurnalı var: deyək ki, mən sübutu əldə etdim və növbəti işçiyə ötürdüm, o isə başqasına göndərdi. X (iks) işçisi də onu məhkəməyə yönləndirir. Bu, təhlükəsizlik məqsədlərilə həyata keçirilən prosedurdur. Nəzarət jurnalında müvafiq tarix, məlumatın qarşıya kim tərəfindən və hansı dəyişikliklə çatdırıldığı əks olunur. Bütün bunlar insan haqları ilə bağlı məsələlərdir. Bunun səbəbləri məhkəmələrdə hakimlərin, prokurorluq, istintaq idarəsi və əməliyyat tərəfinin yanaşmasına əsaslanır. Ümumiyyətlə, biz hüquq-mühafizə orqanları, məhkəmələr və prokurorlar səviyyəsində dövrün çağırışlarına tam uyğunlaşa bilmirik. Yalnız kibercinayətkarlıq təhlükəsi yarandıqda onunla mübarizəyə başlayırıq və bu zaman proses, əlbəttə, tələblərə ciddi riayət edilməklə aparılmalıdır. Ümid edirəm ki, gələcəkdə nəsə dəyişəcək".

İştirakçılar tərəfindən toxunulan digər məsələ Cinayət-Prosessual Məcəllə ilə bağlıdır. Bildirilib ki, Cinayət Məcəlləsininin Budapeşt Konvensiyasına uyğunlaşdırılmasına baxmayaraq, Cinayət-Prosessual Məcəlləsinə hər hansı dəyişiklik edilməyib. Beləliklə, bu hal elektron sübutlarla

davranışlara dair problemlər yaradır.

"Məlumatların əldə edilməsi və saxlanılmasının texniki aspektləri haqqında danışmaq istəyirəm. Məlumatların dəyişkən olması faktı nəzərə alınmaqla, daxili qaydalarımıza uyğun olaraq informasiyanın əldə olunmasında əsas prinsip belədir ki, məlumat dəyişdirilə və ya düzəliş edilə bilməz. Bu səbəbdən məlumat heç vaxt birbaşa qeyd edilmir, adətən, onun şəkli çəkilir və bayt surəti alınır. Ümumiyyətlə, məlumatın nə vaxt, harada və hansı həcmdə əldə olunması və s. bir sıra daxili qaydalarla tənzimlənən məsələlərdir".

Artıq qeyd edildiyi kimi, özəl sektorun kiberfəaliyyətlərlə bağlı aidiyyəti dövlət qurumlarına məlumat təqdim etməsi könüllü əsasda baş verir. Beləliklə, respondentlər qeyd edir ki, özəl sektordan məlumat qəbul edən zaman şirkətlər maarifləndirməyə ehtiyac olduğunu bildirirlər. Respondentlərdən biri kibercinayətlərə qarşı mübarizədə aidiyyəti dövlət qurumları ilə özəl banklar arasında bir növ vasitəçi rolunda çıxış edən Mərkəzi Bankla (MB) sıx əməkdaşlıq haqqında danışıb. Belə ki, MB özəl banklara və maliyyə institutlarına kibercinayətkarlıqdan hansı qaydada müdafiə olunacaqları ilə bağlı məlumatlar təqdim edir. Müzakirələrdə "onurğa provayderlər"lə tərəfdaşlıq da yada salınan digər məqamdır, çünki qeyd edilib ki, onlar "insidentlərin ölkə daxilində yayılması zamanı lazımi işlər görürlər". Bundan başqa, qurum nümayəndələri əlavə ediblər ki, maliyyə sektorunda fəaliyyət göstərən bir çox təşkilatlarla müntəzəm məlumat mübadiləsi aparılır. Bu kimi rəylər iştirakçıların hər birinə aiddir. Bir qurumdan olan əməkdaş fikirlərinə davam edərək bildirib ki, onların təşkilatı da maarifləndirmə işləri ilə bağlı seminarlar keçirir və hər il müvafiq jurnallar nəşr etdirirlər. Əslində, KİMM və DTX məktəblərdə və ümumi əhali arasında fişinq və digər riskli fəaliyyətləri izah etmək üçün maarifləndirmə proqramlarına malikdir.

İstintaq zamanı konkret hüquq-mühafizə və məhkəmə proseslərinin tətbiqinə gəldikdə, iki qurumun üzvləri istintaq səlahiyyətlərinə malik olmadıqları üçün kibercinayətkarlıqla bağlı bəzi işləri DTX-yə yönləndirdiklərini qeyd ediblər. Beləliklə, respondentlərin cavablarına əsasən, araşdırmalar zamanı hüquq-mühafizə və məhkəmə proseslərinə dair addımların yerinə yetirilməsini yalnız DTX həyata keçirib.

6.8.2.2. Kibercinayətlərin qarşısının alınması

İlk olaraq kimin başlatmasından asılı olaraq, istintaq baxımından ibtidai araşdırmaları DTX və ya DİN həyata keçirə bilər. Adıçəkilən qurumlar və KİMM vətəndaşlardan məlumat qəbul etsələr də, sonuncunun araşdırma aparmaq səlahiyyəti yoxdur. Ona görə də bu qurum lazım olduğu təqdirdə işi aidiyyəti qurumlara yönləndirir. İstənilən halda, KİMM həm zərərçəkənlər, həm də qeyri-zərərçəkən şəxslər arasında məlumatlılığın artırılmasında mühüm rol oynayır.

İddia edildiyi kimi, Cinayət-Prosessual Məcəllə kibercinayətkarlığın spesifikasiyasına uyğunlaşdırılmadığı üçün DTX bu sahədə klassik cinayət kəşfiyyatı və istintaq üsullarına müraciət etməli olur. Aşağıdakı sitat bu məqamı izah edir:

"Prosessual qanunvericiliyimiz kifayət qədər kiberspesifik olmadığı üçün klassik istintaq tədbirlərinə istinad etmək məcburiyyətindəyik. Digər tərəfdən isə "Kibercinayətkarlıq haqqında" Konvensiyaya qoşulduqdan sonra bizə lazım olan çevikliyi təmin etmək üçün məlumatların dondurulması üzrə birbaşa səlahiyyət tətbiq etmək imkanımız mövcuddur. Beləliklə, məlumatlar dondurulur və saxlanılır. Məhkəmə qərarı ilə dondurulmuş məlumatları istifadə edə bilirik. Təbii ki, belə təcrübə digər klassik cinayətlərə şamil edilmir. Bu hal yalnız kiberspesifikdir. Lakin hələ də Prosessual Məcəlləmiz köhnə yanaşmalar təqdim etdiyi üçün yalnız həmin üsullardan istifadə etməliyik".

Qeyd olunanlara əsasən, sözügedən işlərdə klassik cinayət kəşfiyyatı və təhqiqat üsullarından istifadəyə baxmayaraq, digər cinayət sübutlarından fərqli mahiyyətinə görə elektron dəlillərə son dərəcə diqqətli yanaşmaq lazımdır. Respondent tərəfindən buna dair maraqlı nümunə misal gətirilib:

"Müstəntiq heç vaxt mütəxəssisin adından qərar qəbul edə bilməz. O, yalnız mütəxəssislə məsləhətləşir, öz taktikasını dəyərləndirir və lazımi formada peşəkarla işləyir. Cinayətkarların böyük bir qrupu həbs edilmiş ola bilər. Kompüter sisteminə baxmaq burada ənənəvi üsuldur (DNT, barmaq izi yoxlanılması). Daxili sistemdəki müəyyən istifadəçi məlumatlarından da şəxsin nə tətbiq etdiyini bilmək mümkündür. Ancaq sübutların təsdiqi üçün DNT

və barmaq izi testləri mütləq aparılır. Bunlar klassik üsullardır. Kibercinayətkarlıqda isə konkret metodlar üstündür. Bu halda, sahə ilə tanış olmayan müstəntiq sübutların aradan qaldırılmasından xəbərsiz ola bilər. Məsələn, operativ yaddaşda hansı məlumatın saxlanıldığını bilmir və kompüteri idarəetmə otağına aparmaq və təhlil etmək üçün söndürür. Beləliklə, əsas sübutların yerində məhv edilməsi baş verir. Çünki kompüterdə saxlanılan məlumatlar daimi yaddaşa yazılmaya bilər. Bu kimi ssenarilərdə necə davranılması barədə müstəntiq mütləq məlumatlandırılmalıdır".

Davam edən kibercinayətlərin qarşısının alınmasından söz açan bir respondent "gov.az.info" domeninin qeydiyyatı prosesində şübhəli fəaliyyət sezdiklərini qeyd edərək vəziyyətə diqqət yetirmələri haqqında misal gətirib. Həmçinin bildirib ki, onların dövlət qurumlarına göndərilən fişinq mesajlarını izləmək, təhlil etmək və əks tədbir görmək üçün texniki və hüquqi imkanları mövcuddur. Digər respondent isə xarici ölkə mənşəli zərərli proqram (malware) və "mining" kiberfəaliyyəti proseslərindən danışıb. Mütəxəssislər belə halları aşkarlayan kimi cəhdlərin qarşısını almaq üzrə sübutlar toplamaqla İP ünvanını (internet protokolu ünvanı) uğurla müəyyənləşdirməyə nail olublar. Ümumilikdə, bu haqda məlumat verən respondent İP ünvanı müəyyən edildiyi müddətdə kibercinayətləri pozmağın asanlığını ifadə edərək, ölkənin "müdafiə divarına" *(yəni kiberhallardan müdafiə edən texnoloji sistemlərin qurulması və vasitələrin tətbiqi)* blokların tətbiqi üsuluna da toxunub.

6.8.2.3. Zərərçəkənlərə qayğı göstərilməsi

Bütün respondentlər zərərçəkənlərə müxtəlif dərəcədə qayğı göstərildiyini ifadə ediblər. Daha əvvəl də qeyd edildiyi kimi, bir qurum nümayəndəsi söyləyib ki, onların təşkilatı məlumatlılığın artırılması üçün hər il seminarlar təşkil edir və jurnallar dərc etdirir. Məktəblərlə iş və televiziya yayımları da proses çərçivəsində əhatə olunur. Digər respondent iki fərqli orqanla birgə başladıqları Kibergigiyena layihəsi haqqında söhbət açaraq maarifləndirmə kampaniyasının tərkib hissəsi kimi 10.000 nəfər hədəf kütləsinə çatmağın nəzərdə tutulduğunu deyib. Başqa bir qurumun üzvü olan respondent də bildirib ki, qəbul etdikləri hər bir zərərçəkən şəxslə konsultativ fikir mübadiləsi aparırlar. Bütün bunlarla yanaşı, əlavə fərqli tədbirlər haqqında məlumat bölüşülməyib. Digər tərəfdən, kiberhədəfə çevrilən şəxslərin məlumatları əsasında hüquq-mühafizə orqanlarının həyata keçirəcəkləri işlərin keyfiyyətinə dair zərərçəkənlərin əminlik ehtimalları üzrə müzakirələr isə vaxt məhdudiyyəti səbəbindən sorğularda yer almayıb.

6.8.2.4. Kibercinayətlərin qarşısının alınmasında preventiv yanaşma

Üç iştirakçı təşkilatdan nümayəndələr kibercinayətləri ilk dəfə törədən gənc hüquqpozucuların bacarıqlarına xüsusi maraq göstərdiklərini və bu bacarıqlardan istifadə etdiklərini qeyd ediblər. Bütün qrup üzrə ümumi fikir odur ki, müvafiq qurumlar "karyera" sahibi (peşəkar) cinayətkarlara çevrilməmişdən əvvəl həmin şəxslərin qabiliyyətlərindən yaxşı formada faydalanmaq lazımdır. Aşağıdakı sitatlar bu mənada sözügedən baxışları ifadə edir:

"Yetkinlik yaşına çatmayanlarla bağlı işlər xüsusi maraq dairəsindədir. Əvvəla, bizi maraqlandıran odur ki, yeniyetmənin cinayəti törətməsinə şərait yaradan onun öz İT biliklərini və hakinq bacarıqlarını tətbiq etməsi, yoxsa qarşı tərəfin bu sahədəki məlumatsızlığıdır? Əksər hallarda məsələ İT biliklərinin olması ilə bağlı deyil. Yəni cinayətkar sadəcə insanların məlumatsızlığından istifadə edən dələduzdur".

"Artıq kibercinayət əməllərinin törədilməsində peşəkarlaşan və məqsədyönlü addımlar atan şəxslər əvəzinə, gənc kiberhüquqpozucuların biliyini doğru istiqamətə çevirmək daha səmərəlidir. Erkən yaşda onları (kibercinayətkarları) müəyyən etmək və biliklərini düzgün yönəltmək nisbətən asandır".

6.8.2.5. Kiberpotensial, kiberqabiliyyətlər

Respondentlərdən biri istedadlı gənclərin işə götürülməsi ilə bağlı ümumi çətinlikləri və kibercinayətlərə qarşı mübarizədə ölkə üzrə hazır kadr çatışmazlığını qeyd edib. Buna baxmayaraq, istedadlı kadrların yetişdirilməsində əsas mərkəz kimi DTX-nin tərkibindəki akademiya və ali məktəblərin hüquq fakültələri göstərilib. Rəylərə əsasən, işə qəbuldan sonra kadrlar bir neçə təlim və sınaqdan keçməli olurlar. Burada respondentlərdən biri müvafiq şəxslərin seçilə biləcəyi müsabiqələrə

də diqqət yönəldib. Digər respondentin aşağıdakı sözləri isə prosesin maliyyə xarakterli problemlərini qısa şəkildə əhatə edir:

"Ölkəmizdə kadr tapmaq çətindir. Səbəblər isə məlumdur. Əvvəla, potensial işçi normal olaraq daha yüksək maaş tələb edə bilər, lakin məvaciblər tamamilə qurumdan asılı olmayıb Maliyyə Nazirliyinə bağlı məsələdir və bir çox səbəbdən həmişə arzulanan məvacib imkanı yaranmır. Elə insanlar var ki, onlar üçün maaş problem olmasa da, azad və ya daha rahat şərait və iş qrafiki tələb edirlər. Hazır kadrla rastlaşmaq müşkül haldır, lakin yetişdirilə bilən kadr tapmaq nisbətən asandır. Belə şəxslər universitetlərdə yüksək bal toplayanlar ola bilər. Onlar yaxşı qavrayışa, öyrənmə qabiliyyətinə malikdirlər. Bu kimi istedadlı kadrları kafedralar özləri hazırlamalı, kurslara (xaricdə və ya ölkədaxili) cəlb etməlidirlər".

6.8.3. Kibercinayətkarlıq: narahatlıq və gözləntilər

Digər qruplarda olduğu kimi, bu qrup daxilində də rəqəmsallaşma səviyyəsi, internetə qoşulan cihazların sayının artması və ümumilikdə texnoloji inkişaf nəticəsində kibercinayətkarlığın gələcəkdə intensivləşəcəyinə dair yekdil rəy mövcuddur.

6.9. Nəticə

❖ Əhali sorğusunun nəticələri ilə fokus qruplarda iştirak edən respondentlərin rəyləri arasındakı fərqlərdən biri odur ki, fokus qruplara daxil olan bütün respondentlər kibercinayətin nə olduğunu bildiyi halda, sorğuda iştirak edən ümumi əhalinin yalnız üçdə biri kibercinayət haqqında məlumatlıdır. Belə nəticə qismən sorğu nümunələrinin hər birində tətbiq edilən müxtəlif seçmə metodları ilə izah edilə bilər.

❖ Kibercinayətkarlığın qavranılması ilə bağlı "internet cinayətləri" və "informasiya cinayətləri" ifadələri ÜƏQ-lər ilə yanaşı, QHT nümayəndələri tərəfindən də mövzunu hər yöndə əhatə edən fikirlər şəklində tez-tez qeyd olunub. Digər tərəfdən, İT mütəxəssisləri və hüquq-mühafizə orqanlarının əməkdaşları arasında kibercinayətkarlıq anlayışı ümumi əhalinin yanaşmalarından əsaslı surətdə seçilib. Belə ki, birincilər üçün kibercinayətkarlıq cəhd deyil, məqsədə çatan istənilən cinayətdir. Onların cavablarına əsasən, İT sektorunda xeyli sayda polisə və digər səlahiyyətli qurumlara bildirilməyən kibercinayət hücumlarının olması faktı mövcuddur. Həmçinin, bu respondentlər kibercinayətkarlığın olduqca mürəkkəb və qarışıq detalları haqqında da danışıblar. Beləliklə, həmin iştirakçıların müzakirə edilən bütün cinayət kateqoriyaları üzrə dərin biliklərə yiyələnməsi aydın olub. Hüquq-mühafizə orqanlarının üzvləri üçün isə kibercinayətkarlıq başqa cihazlardakı məlumatlara giriş və müdafiənin aşılması, eyni zamanda informasiya sistemlərinin bütövlüyünün pozulması deməkdir.

❖ Kibercinayətin yalnız məhdud növləri (əsasən şəxsiyyət/kimlik oğurluğunun bəzi formaları, fişinq və DDoS) ölkənin kibermə-kanına nüfuz edib. Lakin həm fokus qruplar, həm də sorğu məlumatlarının üzə çıxardığı nəticəyə əsasən ümumi respondentlərin rastlaşdıqları çoxsaylı cəhdlərə (xüsusən, fişinqlə bağlı) baxmayaraq, kibercinayətkarlığın qurbanı olma səviyyəsi kifayət qədər aşağıdır. Əslində, həm İT mütəxəssisləri, həm də hüquq-mühafizə orqanlarının təmsilçiləri tərəfindən ifadə edilənlərə uyğun olaraq, daha inkişaf etmiş ölkələrlə müqayisədə yeni yaranması və onlayn fəaliyyətlərdən nisbətən az istifadə səbəbindən Azərbaycanda kibercinayətkarlıq hələ cəmiyyətin ümumi narahatlığına çevrilməyib. Digər tərəfdən isə texnologiya və onlayn qarşılıqlı əlaqələrin getdikcə yüksək istifadəsi nəzərə alınmaqla, yaxın gələcəkdə kibercinayətlərin narahatlıq doğuracağını təsəvvür etmək mümkündür.

❖ Sorğuda iştirak edən həm əhali, həm də fokus qrup üzvlərinin rənsamveə ilə bağlı olduqca aşağı məlumatlılıq səviyyəsi müşahidə edilib, lakin hər iki hədəf qrupu üzrə müəyyən qədər insanın bu cinayət növünün baş verməsi haqqında xəbərdar olması da məlumdur. Ən narahatedici kibercinayət növü hesab edilməsinə baxmayaraq, şəxsi məlumatların ifşasına (yayılmasına) dair respondent təcrübələri hər iki hədəf qrupunda, demək olar ki, müəyyən edilməyib.

❖ Təhlillər sübut edir ki, fokus qruplarından fərqli olaraq, ümumi sorğuda iştirak edən respondentlərin hamısı fişinq cəhdləri ilə qarşılaşmayıb. Faktiki olaraq, yalnız 22% iştirakçı qeyd edilən hallarla üzləşib.

❖ Əhali ilə keçirilən sorğunun nəticələrinin

fokus qruplarla müzakirələrdəki yanaşmalardan digər mühüm fərqi onlayn hədə-qorxu, zorakılıq-təhqir və sui-istifadə ilə bağlıdır. Fokus qruplarda respondentlərin təxminən üçdə biri bundan əziyyət çəksə də, sorğuda demək olar ki, hər hansı şəxs sözügedən cinayəti qeyd etməyib. Bu vəziyyət qismən fokus qruplar üzrə nümunənin xüsusiyyəti ilə izah edilə bilər, belə ki, bəzən ideyaları əks mövqelilər tərəfindən onlayn hədə-qorxu və zorakılıq-təhqirə məruz qalan çox sayda politoloq, jurnalist və fəallar burada iştirak ediblər.

❖ Kibercinayətkarlıqdan müdafiə baxımından müəyyən zərərçəkmə hadisələri qeyd edilsə də, ümumilikdə, toplanmış data mühafizə üzrə məlumatlılığın mövcud olduğunu deməyə əsas yaradır. ÜƏQ-lərin bildirişləri ilə məşğul olan hüquq-mühafizə orqanlarına münasibətdə respondentlərin skeptik düşüncələrinə baxmayaraq, bu strukturların fokus qruplardakı üzvləri də zərərçəkənlərin özləri ilə bağlı bir sıra ciddi problemləri ifadə ediblər: məsələn, kiberhücum faktları barədə gec xəbər verilməsi, banklar tərəfindən təqdim edilən təhlükəsizlik təlimatlarını oxumamaq və ya onlara əməl etməkdə laqeydlik (fişinq və bank kartı oğurluğu kontekstində qeyd edilib). Digər tərəfdən, hüquq-mühafizə orqanlarının fokus qrup iştirakçıları təhqiqatların aparılması zamanı gecikmə və başqa problemlərin olmasını qəbul ediblər. Bütün zərərçəkənlər və yalnız qurbanlardan ibarət fokus qrup üzvlərinin iddialarına görə, onlar hüquq-mühafizə orqanları ilə əlaqə saxlayarkən bir çox məsələlərin şahidi olublar: məsələn, ərizəçinin məruzəsinə ləyaqətlə yanaşılmadığı və işin ciddi qəbul edilmədiyi hallar, yaxud araşdırmaların aparılması və cinayətkarların tapılmasında çətinliklərin etiraf edilməsi və s. Beləliklə, yekun qənaətə əsasən, müvafiq orqanlara kiberhadisələrlə bağlı məlumat bildirilməsi özlüyündə problem ehtiva etməsə də, insanları müraciətdən çəkindirən və ya qənaətbəxş nəticəyə maneə yaradan aidiyyəti qurumların ərizələrə münasibəti və təhqiqatın aparılmasındakı münasibətidir

❖ Kibercinayətlərə qarşı həssaslıq məsələsi üç mühüm və müəyyən qədər bir-biri ilə əlaqəli aspekt formalaşdırıb: yaş, təhsil səviyyəsi, yaxud kibercinayətkarlıq haqqında məlumatlılıq və onlayn fəaliyyət həddi. Bəzi iştirakçılar üçün həssaslıqlarını təyin edən ilk növbədə onların təhsil səviyyəsi və ya məlumatlılıqdır. Digər düşüncəyə görə, burada yaş amili təsiredicidir, belə ki, gənclər yaşlılara nisbətən onlayn potensial təhlükələr haqqında daha çox bilik sahibidirlər. Lakin alternativ fikirlərə əsasən, məlumatlılıq və ya yaşdan asılı olmayaraq insanların onlayn fəaliyyət dərəcəsi mövzu etibarilə müəyyən rol oynayır.

❖ Yuxarıda qeyd edilən məqam həm də uşaqlarla əlaqəli vəziyyəti ön plana çıxarır. Fokus qrupun bir sıra iştirakçıları valideyn olduqları üçün ekran qarşısında və qadcetlərlə (texnoloji alətlər) çox vaxt keçirən uşaqlara dair narahatlıqlarını ifadə ediblər.

❖ Həssaslıq amili ilə bağlı məktəblilərin qarşılaşdığı risklərin qeyd edilməsi də vacibdir. Fokus qruplardan birinin iştirakçısı ümummilli və məktəb səviyyəsində maarifləndirmə proqramlarının icrasını təklif edib ki, bütün belə təkliflər valideyn olan və ya təhsil sektorunda fəaliyyət göstərən üç qadın və bir kişi respondent tərəfindən irəli sürülüb. Bu vəziyyət məktəblər arasında problemin ciddiliyinə işarə edə bilər, beləliklə, gələcəkdə yalnız valideynlər üçün nəzərdə tutulmuş fokus qrupların təşkilinə zərurət yaranır. Bir nəfər qadın respondentin qeyd etdiklərinə əsasən, müəllimlər istəmədən fişinq məktublarının yayılmasında iştirak edə bilərlər. Şagirdlər arasında smartfon və planşetlərdən yüksək istifadə amilini nəzərə aldıqda, sözügedən alt qrupda kibercinayətkarlığın əhəmiyyətli rola malik "qaranlıq (bilinməyən) rəqəm"lərinin mövcudluğu mümkün ehtimala çevrilir.

❖ ÜƏQ-lərdə bəzilərinin, digər qruplarda isə demək olar ki, bütün respondentlərin bildirdiyi kimi, bank sektoru kibercinayətkarlığa məruz qalmaqla bağlı həssas kateqoriyaya daxildir.

❖ Kibercinayətlərin digər cinayətlərə münasibətdə təsirinin ciddiliyi baxımından isə bütün qruplar tərəfindən bu fəaliyyətlər potensial daha təhlükəli hesab edilib. Mülahizələrə uyğun olaraq, kibercinayətlər geniş cəmiyyətə təsir imkanı daşıdığı halda, zorakılıq və ya mülkiyyət əleyhinə cinayətlər fərdlər səviyyəsində, yaxud məhdud ictimai çərçivədə təzahür edir. Hüquq-mühafizə orqanlarının respondentləri belə düşünür ki, kibercinayətkarlığın xüsusi narahatedici keyfiyyəti kritik infrastruktura zərər yetirmə və beləliklə, qarışıqlığa səbəb olma xüsusiyyətidir. Müəyyən qruplarda kibercinayətlərin hədə-qorxu kimi bəzi hallarda intiharla nəticələnə biləcəyinə dair geniş yayılmış cavablar da diqqətdən ya-

yınmayıb.

❖ Kibercinayətkarlıq hadisələri haqqında məlumat bildirilməsi baxımından çox az sayda respondentin polislə əlaqə saxladığı məlum olsa da, cavablara əsasən onların bu cür hesabatlılıq təcrübəsinin nəticəsinin qeyri-qənaətbəxş olması müəyyən edilib. Gənclərdən ibarət fokus qrup iştirakçıları istisna olmaqla, ümumən respondentlər arasında kibercinayətkarlığın qurbanı olduqda İT mütəxəssislərinə müraciət etməyə meyillilik müşahidə edilib. Təəssüflə qeyd edilməlidir ki, tədqiqat zamanı toplanan data öz növbəsində İT mütəxəssislərinin sözügedən halları, yaxud zərərçəkənləri polisə yönləndirməsinə dair xülasə əldə etməyə və ya baxış formalaşdırmağa imkan vermir.

❖ Təhlilin nəticələrinə əsasən, İT mütəxəssisləri, İXP və QHT nümayəndələrinin kibercinayət halları ilə bağlı polisə məlumat bildirmə ehtimalı ÜƏQ-lər ilə müqayisədə daha azdır.

❖ Hüquq-mühafizə orqanlarının əməkdaşları və zərərçəkmiş şəxslərin də ifadə etdiyi kimi, yerli aidiyyəti qurumlar cinayətkar axtarışının əsasən qeyri-mümkün olduğu çoxsaylı hallarla üzləşiblər.

❖ İstisnasız, sorğunun keçirildiyi bütün beş qrupda respondentlər elektron xidmətlərdən (e-gov və e-ticarət) istifadənin artması və əvvəllər kağız üzərində toplanan məlumatların hazırda rəqəmsallaşdırılması nəticəsində kibercinayətlərin gələcəkdə kəskinləşəcəyinə dair ümumi yanaşmaya malikdir. Buna baxmayaraq, ümumi əhali sorğusunun göstəriciləri və fokus qruplarla müsahibələrin nəticələri arasında təəccüb yaradan fərq də kibercinayətkarlıqla bağlı gözləntilərlə əlaqəlidir. Demək olar ki, fokus qruplarda iştirak edən bütün respondentlər kibercinayətkarlığın intensivləşəcəyinə inansa da, ÜƏQ-lər ilə keçirilən sorğuda iştirakçıların təxminən yarısı bu fikrin əksini düşünür. Belə müxtəlif mövqenin meydana gəlməsi müəyyən qədər seçmə metodlarına əsasən izah edilə bilər. Başqa sözlə, fokus qruplar üçün iştirakçılar seçilərkən bəzi kriteriyalar (məsələn, internetdən fəal istifadə, İT və ya İXP sektorunu təmsil etmə və s.) tətbiq edilib. Beləliklə də, hazırkı fərq yaranıb. Lakin ÜƏQ-lər ilə keçirilən sorğu təsadüfi seçmə qaydasında təşkil edilib.

7. Ümumi nəticələr

▶ Kibertəhlükəsizliyə dair məlumatlılıq səviyyəsi, problemi dərketmə, dünyagörüş boşluğunun, "qavrayış (həssaslıq) uçurumunun" (perception gap)[29] aşkara çıxarılması qabaqcıl və hərtərəfli kibertəhlükəsizlik siyasətinə kəskin ehtiyacın mövcudluğunu, müvafiq dövlət siyasətinin və ictimai fəaliyyətin gücləndirilməsini diktə edir;

▶ Tədqiqat əhalinin müxtəlif hədəf qrupları arasında yaş, cins, peşə, təhsil və s.-dən asılı olaraq kibertəhlükələrə qarşı müxtəlif münasibətlərin formalaşmasını üzə çıxarıb. Kibercinayətlərin qavranılması baxımından ən ümumi təsəvvürlər "internet cinayətləri" ifadəsi kimi əksini tapır. Ümumi Əhali Qrupu (ÜƏQ), eləcə də QHT nümayəndələri arasında da "informasiya cinayətləri" mövzunu əhatə edən ifadə kimi qeyd tez-tez olunub. Bununla yanaşı, İT mütəxəssislərinin və hüquq-mühafizə orqanları (HMO) nümayəndələrinin kibercinayətkarlıq anlayışı ümumi əhalidən köklü surətdə fərqlənir, eləcə də sorğu və fokus qrupları ilə tədqiqatın bəzi nəticələri bir-birindən fərqlidir. Buna misal olaraq, kibercinayətkarlıq gözləntiləri ilə bağlı anket sorğusu və fokus qrup nəticələri arasında məlumatlılıqla bağlı müxtəlif nəticələri göstərmək olar. Demək olar ki, fokus qruplarda iştirak edən hər bir respondent kibercinayətkarlığın gələcəkdə artacağını gözləsə də, sorğuda iştirak edənlərin demək olar ki, yarısı azalma gözləyir. Baxmayaraq ki, bu fərq fokus qrupları üçün iştirakçıların seçilməsi meyarları ilə izah edilir;

▶ Hazırkı hesabatda qeyd edilən rəsmi statistikaya əsasən, Azərbaycanda botnet və fişinq hücumları 2021-ci ildə ən çox qeydə alınan kibercinayətlər olub. Keçirilmiş sorğunun nəticələri göstərir ki, ölkədə kibercinayətlərin bütün mövcud formaları geniş yayılmayıb. Həm fərdi, həm də təşkilati səviyyədə bir çox kibercinayətlər üzrə zərərçəkənlərin (qurbanların) sayı olduqca aşağıdır. Başvermə cəhətdən nisbətən daha çox yayılmasına baxmayaraq, respondentlərin əksəriyyəti, məsələn, "fişinq" terminindən xəbərsizdir. Ümumilikdə, sorğu nəticəsində bankların fişinq və ya konkret bank kartı oğurluğu ilə bağlı kibercinayətlərlə məşğul olmaq istəməməsi, polisin cinayətkarları tapmaqda üzləşdiyi problemlər, hərtərəfli qanunvericiliyin olmaması, ciddi təcrübə çatışmazlıqları və s. məsələlər aşkara çıxıb. Birmənalı olaraq, fokus qruplar arasında kibercinayət digər cinayət növlərindən potensial daha təhlükəli hesab edilib. Anket sorğusu iştirakçılarının xeyli hissəsi də kibercinayəti digər cinayətlərdən daha təhlükəli hesab edib;

▶ Kibercinayətkarlığın səviyyəsinə adekvat olan yeni "onlayn kiberdüşüncə tərzinin" (online cybermindset) formalaşmasının müəyyən dərəcədə gecikdiyi reallıqdır. Bu istiqamətdə əsas maneə cəmiyyətin kibercinayətkarlıq haqqında düşüncələri ilə təhlükənin reallığı arasında mövcud olan əhəmiyyətli qavrayış, dünyagörüş boşluğudur (perception gap). Bu qavrayış boşluğunun nəticəsi ondan ibarətdir ki, ictimaiyyətin bir çox üzvlərinin onlayn təhlükəsizliyə qeyri-həssas yanaşması, onu öz həyatının prioritetləri sırasına daxil etməməsi cəmiyyəti kibercinayətin qurbanı olmaq riski ilə üz-üzə qoya bilər;

▶ Kibercinayət terminin əhali arasında hələ də geniş istifadə edilməməsi bu sahədə daha çox maarifləndirmə aparılmasını zəruri edir. Xatırladaq ki, 2021-ci ildə Azərbaycanda 10 minə yaxın vətəndaşın zərər çəkdiyi beynəlxalq kiberfırıldaqçılıq kripto piramidası (Ponzi sxemi) ifşa edilmişdi. Bu faktın özü əhalinin kibercinayətkarlıq haqqında tam məlumatlı olması qənaətinə ziddir;

▶ Digər tərəfdən, kibercinayətkarlıqla bağlı artan narahatlıq fonunda viktimizasiya - cinayət qurbanlarının statistikası ilə bağlı aşağı rəqəmlərin özü də ciddi uyğunsuzluq hesab edilməlidir. Bu, effektiv əks tədbirlərin görülməsi üçün mühüm əsas yaradır. Bir tərəfdən kibertəhlükənin sürətlə artan tempi, digər tərəfdən ictimai rəyin qeyri-adekvat münasibəti görüləcək tədbirlərin miqyasını və əhəmiyyətini göstərir. Səbəblərdən biri də bu, ola bilər ki, Azərbaycanda kibercinayətkarlığın bütün formaları yayılmayıb. Həmçinin, ən çox yayılan fişinq və məlumatların oğurlanması halları da hələlik ən təhlükəli səviyyəyə çat-

[29] Məlum olduğu kimi, sosial-psixoloji tədqiqatlarda "qavrayış-həssaslıq boşluğu, yaxud uçurumu" 3 əsas mif üzərində qurulur:
1."Kibercinayətkarlıq mənim üçün narahatedici məsələ deyil"; 2."Kibercinayətkarlıq real həyat cinayəti deyil"; 3." Kibercinayətkarlıq özümü qorumaq üçün həlletmə imkanlarımdan kənar haldır ".
Bir çoxları kibertəhlükəsizliyi şəxsi məsuliyyət kimi qəbul etmək əvəzinə, bunun "başqasının problemi" olduğunu və ümumi gözləntiləri səthi şərh etməklə məsuliyyətdən kənarda qaldığını düşünür.

mamış ola bilər;

▶ Tədqiqat nəticəsində müəyyən edilib ki, hazırda ötən illərlə müqayisədə həm inkişaf, həm də kibertəhlükəsizliyin təmin edilməsində və kibercinayətkarlıqla mübarizədə problemlər var. Belə ki, hədəf qrupları arasında keçirilən sorğunun nəticələri ümumilikdə əhali arasında kibercinayətkarlıq haqqında məlumatlılıq səviyyəsinin artdığını göstərib. Xüsusilə də, pandemiyanın başlanğıcından bəri kibertəhlükəsizlik mövzusu cəmiyyətdə daha da əhəmiyyət qazanıb. Belə ki, onlayn fəaliyyətlər hədsiz dərəcədə sürətlənib və ötən illərə nisbətən ictimai məlumatlılıq artıb;

▶ İnformasiyanın qorunması baxımından sorğunun nəticələri müsbət mənzərəni təqdim edir. Bununla yanaşı, hədəf qrupların əhəmiyyətli hissəsi kibertəhlükələrdən kifayət qədər müdafiə olunmadıqlarını hiss edir. Bu da, KİMM tərəfindən təşkil edilən maarifləndirmə proqramlarının faydalılığını sübut etsə də, eyni zamanda onun coğrafi əhatəliliyinin intensivləşdirilməsinə ehtiyacı üzə çıxarır.

Hədəf qruplarının - müəssisələrin/təşkilatların kibertəhlükəsizlik və təhdidlərə münasibətinə dair təkliflər

▶ Müəssisələr/təşkilatlar arasında keçirilən sorğunun nəticələri kibertəhlükəsizlik və təhdidlərin qavrayışı sahəsində tam bir boşluğun mövcudluğunu aşkara çıxarıb. Azərbaycanda sahibkarlıq subyektlərinin sayı (2021-ci il oktyabrın 1-nə olan məlumata görə) 1.306.490 nəfər təşkil edib. Qeydə alınmış statistik vahidlərin 136.743-ü mikro (93%), 6832-si kiçik (4,7%), 2652-si orta və 603-ü (1,8%) iri biznes subyektləridir;

▶ Kiçik və orta biznes müəssisələrinin (KOB) kibertəhlükəsizliyə münasibətlə bağlı rəyinə, bilik və məlumatlılıq səviyyəsinə gəldikdə, sorğunun nəticələri göstərdi ki, respondentlərin əhəmiyyətli bir hissəsi kibercinayətkarlıq riskini kifayət qədər ciddi qiymətləndirmir, yaxud da özlərini ondan qorunmaqda qeyri-məsul, aciz hesab edirlər. Geniş yayılmış "miqyas önəmlidir" düşüncələrinə əsasən hesab edilir ki, kibercinayətkarlar kiçik biznesi, "adi" insanları deyil, yalnız böyük bizneslərə hədəf alırlar. Bu da, öz növbəsində kibercinayətin qurbanı olmaqla bağlı yanlış təsəvvürlərə, təhlükəli atalətə gətirib çıxaran amildir;

▶ Sorğu gedişində sektorlar baxımından bank sənayesinin (böyük biznes aktorları kimi) ən böyük risk və ən çox hücumlarla üzləşməsi ilə bağlı reallıq da ortaya çıxıb;

▶ Son 2 ildə banklar və maliyyə şirkətləri adından edilən fişinq zənglərinin, göndərilən məktubların sayının olduqca artması da qeyd edilib;

▶ Kiberrisklərin səmərəli idarə edilməsində əsas problemlər və ya maneələr barədə soruşulduqda, respondentlərin ən çox istinad etdiyi məqam texnloji təminat çatışmazlığı olub. Kiçik və orta biznes (KOB) sahibləri yeni təhlükəsizlik texnologiyalarının tətbiqi və bunun üçün müvafiq büdcənin artırılmasını qurum və təşkilatların təhlükəsizlik səviyyəsinin yüksəldilməsində həlledici amil sayır. Bu isə kibertəhlükəsizlikdə texnoloji həllərin əsas hesab edilməsinin, eyni zamanda strateji sayılan insan amilinin rolu və kadr probleminin əhəmiyyətinin KOB sahibləri tərəfindən adekvat dəyərləndirilmədiyini aydın göstərir;

▶ Xeyli sayda sahibkarlıq və s. müəssisələrdə kibertəhlükəsizliyə cavabdeh hər hansı bir departamentin və ya təhlükəsizliyə məsul şəxsin və xüsusilə kiçik və orta müəssisələrdə (KOB) kibertəhlükəsizlik sığortasının olmaması nəzərə alınarsa, yaxın gələcəkdə bu sahədə böyük problemlər yarana bilər. (Məlum olduğu kimi, əksər qabaqcıl ölkələrdə analoji departament, yaxud məsul şəxs ştatları mövcuddur). Ümumi olaraq, müəssisələrə qarşı törədilən kibercinayətlərin miqyası və getdikcə artan dinamikası fonunda yaranacaq problemlərin daha ciddi şəkildə insanlara çatdırılmasına ehtiyac üzə çıxır;

▶ Kibertəhlükəsizliklə bağlı "qavrayış boşluğu"nun mövcudluğu, müəssisələrdə minlərlə insanın ən sadə onlayn təhlükəsiz davranış vərdişlərinə malik olmaması özlərini, bizneslərini və bütövlükdə infrastrukturu kiberhücumlarla bağlı həssaslığa məruz qoyur. Halbuki, kibercinayətkarlar qlobal korporasiyaları və ya mikro KOB-ları hədəf almaqlarından asılı olmayaraq, bütövlükdə kibertəhlükəsizlik mühitinin zəifliyindən istifadə edirlər. Beynəlxalq təcrübələr göstərir ki, şirkətlər digər təşkilatların və ya müştərilərinin zəif kibertəhlükəsizliyi nəticəsində yaranan pozuntulara görə də ictimai şəkildə günahlandırıla bilər. Hazırkı tədqiqat müəssisələrdə təhlükəli qavrayış boşluğunu aradan qaldırmaq üçün birlikdə işləmək, fərdləri, təşkilat və biznesi, bütövlükdə cəmiyyəti qorumaq üçün tədbirlər görməyə təşviq etməyin önəmini ortaya çıxarıb;

▶ Burada diqqət çəkən digər bir məsələ də sorğu gedişində müxtəlif hədəf qruplarının bütün məsələlərin dövlət tərəfindən həll ediləcəyi ilə bağlı gözləntiləridir. Əksəriyyət hesab edir ki, dövlət və ya milli hakimiyyət orqanları kibercinayətkarlıqla mübarizəyə məsuldur, lakin hələ də bəzi işlər görülməlidir. Bu durum, təbii olaraq, cəmiyyətdə kibertəhlükələrə qarşı birgə mübarizədə milli səfərbərliyin, vətəndaş cəmiyyətinin, hər bir şəxsin yeri və rolunun prosesdə dəyərləndirilməsində çatışmazlıqları göstərir.

İT (informasiya texnologiyaları) və İXP (internet xidməti provayderləri) mütəxəssisləri hədəf qruplarının kibercinayətkarlıq və kibertəhlükəsizliyə münasibətinə dair təkliflər

▶ Sorğunun nəticələri: İT və İXP peşəkarları hədəf qruplarının kibercinayətkarlıq və kibertəhlükəsizliklə bağlı qavrayış, bilik səviyyəsi və kibercinayətkarlıqla bağlı narahatlıqları və gözləntilərinin təhlili həm ümumi, həm də ölkəyə xas olan nəticələri ortaya qoydu;

▶ Tədqiqatda qeyd edildiyi kimi, dünyada milli kibertəhlükəsizliyin təmin edilməsində ümumi prinsip belədir ki, ölkədə İKT-nin, e-dövlət infrastrukturunun inkişafı ilə kibertəhlükəsizliyin səviyyəsi təxminən eyni olmalıdır. Həmçinin, güclü təhlükəsizliyin təmin edilməsində, kibertəhlükələrə qarşı şüurlu və informasiya mədəniyyətinə malik cəmiyyətin formalaşmasında maraqlı olan ölkə bütün bu sadalanan istiqamətlərə eyni dərəcədə diqqət yetirməlidir. Bu sahələr balanslaşdırılmalıdır;

▶ Tədqiqat hazırda Azərbaycanda İKT-nin və bu sahədə kibertəhlükəsizliyin inkişafı arasında balansın deyil, "uçuruma" yaxın boşluğun mövcudluğunu göstərdi. Bu boşluğun minimuma endirilməsi günün tələbidir. Elektron idarəetməyə keçid prosesində zəif bəndləri və riskləri minimuma endirmək üçün təhlükəsizlik dizaynı təmin edən xidmətlər və həllər hazırlanmalıdır. İKT və kibertəhlükəsizlik sahəsində mövcud qanunvericilik bazasının qabaqcıl təcrübəyə əsasən modifikasiyası da eyni əhəmiyyətli vəzifələrdəndir. Bu baxımdan hədəf qrupunun - İT və İXP mütəxəssislərinin bütün sistemlərinin potensialının artırılması Azərbaycanda kibertəhlükəsizlik idarəçiliyinin prioritetinə çevrilməlidir;

▶ Kibercinayətkarlıqla mübarizədə hüquqi-qanunverici əsaslar həm effektiv cinayət mühakiməsi, həm də dövlətin kibertəhlükəsizlik siyasətinin vəhdətinə söykənir. Müasir dövrdə bütün növ cinayətlər, məsələn, mütəşəkkil cinayətkarlıq, iqtisadi cinayətlər, şəxslərə qarşı cinayətlər də internetdə elektron sübutlara, yaxud da qanunsuz gəlirlərə çıxışla bağlı effektiv dəlillər tələb edir. Bu baxımdan məhkəmə, özəl təşkilatlar, o cümlədən informasiya xidməti təminatçıları arasında əməkdaşlıq labüddür. Hüquq-mühafizə orqanlarının maraqlarını təhqiqat və təqib əhatə etsə də, provayderlərin prioritetləri isə interneti istifadəçilər üçün təhlükəsiz etmək, müştəri məmnuniyyəti və s. olsa da, ümumi məqsədlər eynidir;

▶ Kibertəhlükəsizlikdə əsas məqamlardan biri ən yeni texnoloji innovasiyaların risklərlə mübarizə potensialının artırılmasıdır. Texnoloji inkişafdan asılı olaraq, hər il yeni kibertəhlükələr və onlarla bağlı yeni kiberhücum üsulları yaranır. Bu da, müasir təhlükəsizlik siyasəti, qanunlar, standartlar, kibermüdafiə məhsulları, həllərin hazırlanması deməkdir;

▶ Tədqiqatda əldə edilən nəticələrdən biri də budur ki, İT və İXP peşəkarlarının kibertəhlükəsizlik imkanları üzrə potensialının artırılması bu gün özəl qurumlar və dövlət üçün vacib tələbə çevrilib. Həmçinin, bütün dünyada mövcud olan trend - bu sahədə də ixtisaslı kadr çatışmazlığı ilə bağlı ciddi problemlər vardır. Kibertəhlükəsizlik sahəsində tələb olunan ixtisaslı insan resurslarını inkişaf etdirmək üçün milli və beynəlxalq layihələrin, magistratura və doktorantura səviyyəli proqramların, tədqiqat institutları və test mərkəzlərinin, sertifikatlaşdırma proqramlarının yaradılması dövlət tərəfindən təşviq edilməlidir. Bundan əlavə, kibertəhlükəsizlik üzrə təlim kursları təşkil edilməli və insanlara aşağı səviyyədən yüksək səviyyəyə qədər bilik və bacarıqlar çatdırılmalıdır;

▶ Ölkədəki İXP-lər arasında problemlərdən biri daxili mənbəli təhlükələrə məhəl qoymadan sistemləri xarici təhlükələrdən qorumağın vacibliyi düşüncəsidir. Halbuki, məsələn, iş yerlərində çalışanlar şəxsi telefonu vasitəsilə şəbəkəyə qoşulur ki, bu da kibertəhlükələrə şərait yarada bilər. Mövcud reallıq kibertəhlükəsizlik siyasətini inkişaf etdirmək üçün həm infrastrukturu, həm də resurs potensialını gücləndirməyi tələb edir. Kibertəhlükəsizlik arxitekturasının, maliyyələşdirilmə amilinin, məlumat mübadiləsi mexanizmlərinin və s.

daha da təkmilləşdirilməsi, vətəndaşların kibertəhlükəsizlik mədəniyyətinin formalaşması kimi məsələlər bir-biri ilə əlaqədardır.

Hüquq-mühafizə orqanları ilə fokus qrupların kibertəhlükəsizliyə münasibətinə və görüləcək tədbirlərə dair təkliflər

- Kibertəhlükəsizlik haqqında məlumatlılığın artırılmasına, cari risklər və xüsusi tədbirlər haqqında ictimaiyyətə daha geniş məlumatın təqdim edilməsinə ehtiyac var. Aidiyyəti qurumlar - Xüsusi Rabitə və Informasiya Təhlükəsizliyi Dövlət Xidməti, DİN və s. maarifləndirmə üçün əhəmiyyətli səylər göstərsə də, xüsusilə müvafiq kadrların yetişdirilməsi və daha səmərəli istintaq tədbirləri aparmaq baxımından daha çox iş görülməlidir;
- Dəyərlərlə bağlı münasibətə sistemli nəzər salmaq vacibdir: məsələn, təhlükəsizlik, məxfilik və ya hər hansı digər amil arasında seçim edilməsinin izahına ehtiyac var. Onların hər hansı biri müstəsna olmayıb, hazırkı mövzu istiqamətində hamısı eyni dərəcədə önəmlidir;
- Milli və beynəlxalq qanunvericiliyin unifikasiyası gündəlikdə durur, belə ki, beynəlxalq və milli qanunlardakı fərqlər əməkdaşlığın həyata keçirilməsinə təsir edir;
- Kibercinayətkarlıq kritik infrastruktur sahələrini hədəfə ala bildiyindən ənənəvi cinayətlərdə rast gəlinməyən kütləvi ziyana səbəb ola, buna görə də potensial olaraq daha təhlükəli ola bilər. Bununla belə, maraqlı məqam isə yerli Cinayət Məcəlləsinin bu cür kibercinayətlər üçün cəzanı necə təyin etməsidir. Dövlət mühafizə xidmətindən olan respondent qeyd edib ki, mühüm infrastruktur sahələrinə hücum qanunla kibercinayətin ən ağır növü hesab edilsə də, cinayətkar maksimum 6 il müddətinə azadlıqdan məhrum edilə bilər;
- Kibercinayətlərin dekriminalizasiyası məsələsi aktualdır. Məsələn, respondentlər xırda dələduzluq üçün cəzanın sərtləşdirilməsini təklif edib. Belə ki, hazırda 500 AZN-dən çox zərərçəkmişə ziyan dəydikdə cinayət təqibi başlayır. Bu səbəbdən, az miqdarda itki ilə bağlı vətəndaşlar şikayət etmir və kibercinayətkarların məqsədləri də elə məhz buna hesablanıb. Prosesin uzanması və vaxt itkisini də nəzərə alan vətəndaşlar şikayət etməkdən çəkinirlər. Kibercinayətlərin artması fonunda viktimizasiya faizinin aşağı olması da bununla bağlıdır. Halbuki, dəymiş ziyanın az və ya çox olmasından asılı olmayaraq vətəndaşların şikayət etmələri vacibdir və mövzunun araşdırılması üzrə faydalı olardı;
- Tədqiqatda hüquq-mühafizə orqanlarının nümayəndələrindən ibarət hədəf qrupunun əsas hesab etdiyi göstəricilərin əksəriyyəti ümumi təhlükəsizlik və məxfilik məsələlərinə aiddir. Buna görə də digər dəyərləri əhatə etmək, bəzi konkret məsələləri araşdırmaq üçün əlavə empirik sorğulara/tədqiqatlara ehtiyac var;
- Azərbaycanda fərdi məlumatlarla bağlı yerli qaydalarla yanaşı, beynəlxalq qaydaların da tətbiqi nəzərə alına bilər. 25 may 2018-ci il tarixində qüvvəyə minən “Ümumi Məlumatların Qorunması Qaydası"na (ÜMQQ, ingilis dilində: General Data Protection Regulation (GDPR)) əsasən, bu cür məlumatları emal, əldə və ya idarə edən qurumların rezidentliyi (qeydiyyat ünvanı) nəzərə alınmayaraq, sadəcə Aİ rezidentlərinin məlumatlarının qorunmasına diqqət yetirilir. Sözügedən tənzimləmənin bu cür ekstraterritorial təsiri transmilli biznes fəaliyyətinə malik olan təşkilatlar, xüsusən də iş yerindən asılı olmayaraq bütün dünyada xidmət göstərən qurumlarla bağlı nəzərə alınmalıdır;
- Araşdırmalar göstərir ki, bankların yalnız kiçik bir hissəsi ÜMQQ-nin tələblərinə əməl edib. Böyük əksəriyyəti isə müəyyən tələbləri pozub. Azərbaycan qanunvericiliyi maliyyə xidmətləri göstərən hüquqi şəxsləri ÜMQQ-nin tələblərinə əməl etməyə məcbur etmir. Bununla belə, hər hansı bir bank Avropadan ən az bir müştərinin məlumatlarını saxlayırsa, birbaşa olaraq ÜMQQ-nin təsir dairəsinə daxil olur. Bundan əlavə, ÜMQQ-nin tələblərinə uyğunluq maliyyə xidmətləri üçün tərəfdaş axtaran potensial təşkilatlar (xüsusilə Aİ-dən olanlar) üçün həlledici amil ola bilər;
- Hazırda kibertəhlükəsizlik sahəsində özəl sektor, biznes və startaplar inkişaf etməkdədir. Hətta Azərbaycanda qabaqcıl ölkələrin (ABŞ və s.) xidmət üçün müraciət etdiyi kibertəhlükəsizlik subyektləri mövcuddur. Aidiyyəti qurumların bu sahədə qanuni tənzimləmə məsələlərinə həssaslıq göstərməsi önəmlidir.

Respondentlərin kibercinayətlər və kibertəhlükəsizliyə dair münasibətinin formalaşmasına təsir göstərə biləcək sosial və mədəni kontekstlə bağlı yekun və təkliflər

▶ Azərbaycanda gedən proseslər demək olar ki, ənənəvi cəmiyyətdən müasir cəmiyyətə keçid, postmodern mərhələyə qədəm qoyulması kimi səciyyələndirilə bilər. Qlobal informasiya inqilabı burada öz mühüm təsirini arzuolunmaz kibertəhlükələr şəklində göstərir. İnformasiya cəmiyyətinin şəffaflıq meyarlarının artırılması zərurətə çevrilir. Sorğu zamanı müəyyən edilən maliyyələşmənin kifayət qədər olmaması, kibertəhlükəsizlik büdcəsinin qeyri-şəffaflığı, onun əhəmiyyətinin dərk edilməməsi ilə bağlı bəzi cavablar ölkədə şəffaflığın hələ tam formalaşmaması ilə bağlıdır;

▶ Nisbətən çox rast gəlinən rəy bundan ibarətdir ki, kibercinayətlər daha geniş cəmiyyəti əhatə etdiyi halda, real həyatdakı zorakılıq cinayətləri, mülkiyyət cinayətləri dar sahəni, fərdi və ya icma səviyyəsini əhatə edir;

▶ Coğrafi amildən danışarkən, 10 milyondan çox əhalisi olan Azərbaycanda sürətli urbanizasiya artmaqda davam edir. Ümumi əhalinin 56%-i şəhərlərdə və ya şəhərətrafı ərazilərdə yaşayır (Dünya Bankı, 2020), qeyri-rəsmi olaraq bu rəqəm daha yüksək ola bilər. Bundan başqa, paytaxt və regionlar arasında iqtisadi və sosial bərabərsizliklərlə yanaşı, rəqəmsal disbalans də başqa problemdir. Neft və digər biznes sektorları hesabına ÜDM-in 70%-i paytaxt Bakının payına düşür. Bu, şəhər və kənd əhalisinin kiberməziyyətlə bağlı qavrayışına təsir göstərir. Kibercinayətlər və real həyatda baş verən cinayətlərin miqyası və təsiri ilə bağlı fərqli fikirlərin ifadə edilməsi müəyyən amillərlə şərtlənib. Burada coğrafi, yaş, cins, təhsil və s. amillər özünü göstərir. Məsələn, əsasən şəhər sakinləri, aktiv internet istifadəçiləri və qadınlar kibercinayətkarlığın artdığını düşünür;

▶ Kibertəhlükəsizliyin formalaşmasına müsbət təsir göstərə biləcək sosial və mədəni amillərə gəldikdə, bu sırada Azərbaycanda ənənəvi ailə dəyərlərini qeyd etmək olar. Ailələr uşaqların kibertəhlükəsizlik probleminə həssasdır. Fokus qrup iştirakçıları olan valideynlər pandemiya zamanı ekranlar qarşısında və cihazlarla çox vaxt keçirdikləri üçün uşaqlarla bağlı narahatlıqlarını vurğulayıblar. Hətta növbəti tədqiqatlarda yalnız valideynləri hədəf qrupu kimi seçməklə fokus qrupların formalaşdırılmasına ehtiyac olduğu qeyd edilib. Bu təkliflərin qısa vaxtda reallaşdırılması faydalı olardı;

▶ Məlumdur ki, maraqlı qüvvələr Azərbaycan gəncləri arasında yad dini-ideoloji təbliğatda yeni texnologiyalardan istifadə edirlər. Müxtəlif məqsədləri, hədəfi olan virtual məkan burada sui-istifadə edilir. Bir çox faktlar göstərir ki, əsasən İrandan yönəldilən, uşaq və gəncləri hədəfə alan məqsədyönlü fəaliyyətlər çoxluq təşkil edir;

▶ Respondentin məsələləri qavramasına təsir edən digər sosial və mədəni kontekst internetdə “qürur, şərəf, ləyaqət, təhqir və s. ilə bağlı intihara səbəb ola biləcək, ənənəvi dəyərlərə, mentalitetə xas olan “şərəf/namus kibercinayətləri”dir ("honor cybercrimes").

Kibertəhlükəsizlik haqqında məlumatlılığın artırılması yönündə təlim, maarifləndirmə, təhsil və akademik tədqiqat proqramlarının reallaşdırılmasına dair təkliflər

▶ Hazırda xarici dövlətlərin himayə etdiyi kibercinayətlərin təhlükələri siyasi qeyri-sabitlik, sosial iğtişaşlar və iqtisadi tələtümlər yaratmaq və istənilən dövlətin rəqəmsal infrastrukturuna ziyan vurmaq potensialına malikdir. Rəqəmsal əsrdə bir ölkənin həssas kiberməkanı təkcə iqtisadi böhrana, siyasi qeyri-sabitliyə və təhlükəsizliyin deqradasiyasına deyil, həm də “kiberterrorizm” səviyyəli hücumlarla sosial iğtişaşlara səbəb ola bilər. Buna görə də kiberhücum ehtimalını aradan qaldırmaq və ya minimuma endirmək üçün əks tədbirlər bütün dövlətlərin siyasətində kibertəhlükəsizliyin vacib tərkib hissəsinə çevrilib;

▶ Əksər insanlarda belə bir yanlış təsəvvür formalaşıb ki, onlayn məkanda aparılan bütün fəaliyyətlər haradasa anonim/naməlumdur. Cəmiyyəti kibertəhlükəsizlik sahəsində maarifləndirmək üçün aidiyyəti qurumların, bütün sektorların, təhsil müəssisələrinin, özəl və dövlət qurumlarının üzərinə böyük məsuliyyət düşür;

▶ İKT sənayesinin tədqiqi və inkişafı üçün İKT təhsilinin inkişafı, virtual təlim mərkəzləri və kompüter proqram təminatı mühəndisliyi mərkəzlərinin milli səviyyədə təşviqindən ibarət kompleks planın effektiv şəkildə həyata keçirilməsinə ehtiyac var;

▶ Azərbaycanın kiberqüdrətini artırmaq

üçün universitetlərdə-akademik mühitdə kibertəhlükəsizliyin dərki yönündə tədqiqatların aparılmasına, maarifləndirici və informasiya fəaliyyətlərinin güclü şəkildə təşviqinə ehtiyac var. Akademik institutlarda kibertəhlükəsizlik mərkəzlərinin yaradılması cəmiyyətdə kibermüdafiə və fövqəladə hallar siyasətinin formalaşdırılmasına kömək edə bilər;

- Kibertəhlükəsizlik yönümlü tədqiqatlar aparan ayrıca qurumun, akademiya və s. təsis edilməsi Azərbaycanın kibertəhlükəsizlik üzrə ekspertlərinin yetişməsinə təkan verə bilər;
- Kibercinayətkarlıqla mübarizə üzrə güclü və operativ ixtisaslaşdırılmış bölmələr, "kiberordular", "kiberkönüllülər" formatında resursların hazırlanması ictimai gündəliyə daxil edilməlidir. Mövzu ilə bağlı milli müzakirə forumları, dinləmələr kibercinayətkarlıqla bağlı real durumun dərk edilməsinə, ictimai rəyin diqqətinin yönəlməsinə maksimum şərait yaratmağa kömək edə bilər;
- Araşdırmadan da göründüyü kimi, Azərbaycanda ali təhsil müəssisələrində kibertəhlükəsizliklə bağlı heç bir bakalavr və magistr proqramları təklif olunmur və bu sahə mövcud proqramlara daxil edilmir. Fraqmentar məzmunlu müəyyən mühazirələr oxunsa da, bu, ölkədə kibertəhlükəsizlik sahəsində yeni mütəxəssislərin hazırlanmasında, fundamental problemlərin həllində çarə sayıla bilməz. Bir çox özəl təhsil şirkətləri kommersiya məqsədilə Azərbaycanda müxtəlif mühazirələr və kurslar təqdim edirlər. Bunlara həm yerli, həm də xarici kurslar daxildir.

Dövlətin kibertəhlükəsizlik sahəsində siyasətinin təkmilləşdirilməsinə dair təkiflər

- Kibertəhlükəsizlik siyasətinin mövcud vəziyyətinin təhlili Azərbaycanda sahənin inkişafına qeyri-taraz, disbalans yanaşmanın mövcudluğunu göstərir, milli kibertəhlükəsizlik strategiyasının qəbul edilməsinə təcili ehtiyac olduğunu üzə çıxarır. Sürətlə inkişaf edən informasiya infrastrukturu fonunda kibertəhlükəsizlik məsələlərinə diqqətli baxışın nisbətən ləngiməsi mənzərəsi mövcuddur;
- Azərbaycanın İKT-nin inkişafı ilə bağlı milli siyasəti və strategiyası var. Lakin Azərbaycanın milli kibertəhlükəsizlik strategiyası, sahənin qanunvericilik bazası ilə bağlı siyasət sənədi hələlik yoxdur. Hazırda milli kibersiyasət qərarları maraqlı tərəflər və kibertəhlükəsizlik ekspertləri tərəfindən obyektiv siyasət qiymətləndirməsi olmadan qəbul edilir. Effektiv kibertəhlükəsizlik siyasəti və strategiyasının işlənib hazırlanması üçün tədqiqatın müxtəlif aspektləri düzgün nəzərə alınmalıdır. Kibertəhlükəsizlik siyasətinə ciddi şəkildə riayət edilməlidir ki, hər bir ölkə və təşkilat gələcəkdə artan kibertəhlükəsizlik təhdidlərinin müxtəlif formalarını tanıya və onlara hazırlaşa bilsin;
- Azərbaycanda Milli Kibertəhlükəsizlik Strategiyasının məqsədlərinin həyata keçirilməsinin ləngiməsi ölkədə təhlükəsizliyin təmin edilməsi istiqamətində daha aydın trayektoriyanın müəyyənləşdirilməsinin zəruriliyini diktə edir;
- İnsan hüquqları və qanunun aliliyi komponenti davamlı dövlət-özəl dialoq, İXP tənzimləyiciləri və məlumatların mühafizəsi orqanları ilə iş və vətəndaşların təhlükəsizliyinə diqqət yetirmələri baxımından kibercinayətkarlığa dair davamlı açıqlamalar, hesabat sistemlərinin təqdimi və müzakirəsi ayıq-sayıqlığın artması, kibercinayətkarlıqla mübarizədə vətəndaş iştirakının, nəzarətin gücləndirilməsinin və tədbirlərin görülməsinin təkmilləşdirilməsi baxımından məqsədəuyğun ola bilər;
- Tədqiqatın nəticələri göstərir ki, İKT-nin və təhlükəsizlik infrastrukturunun inkişafı strategiya və qanunvericiliklə tarazlaşdırılmalıdır. Səlahiyyətli şəxslər kibertəhlükəsizlik siyasətlərinin və strategiyalarının effektivliyinə dair vaxtaşırı təhlillər aparmalıdırlar. Kiberhücumların dağıdıcı təsiri bir çox ölkələrin, o cümlədən Azərbaycanın milli təhlükəsizlik strategiyalarını təhlükə altına qoyur. Azərbaycanın ənənəvi milli təhlükəsizlik çərçivəsi dövlətin sürətlə artan e-infrastrukturunun təhlükəsizliyini təmin etmək üçün yeni elektron müdafiə mexanizmlərini özündə birləşdirərək müasir kiber islahatların aparılmasını tələb edir;
- Bir sözlə, kiberqanunvericiliyin, texnoloji inqilabın, adekvat təhlükəsizlik standartlarının qəbul edilməsi, kibertəhlükəsizlik mərkəzlərinin yaradılması və təhlükəsizlik aparatının, ölkənin kiberməkanda mövqeyinin gücləndirilməsi son nəticədə Azərbaycana çoxşaxəli və çoxmənbəli kiberhücumlara effektiv şəkildə müqavimət göstərə bilən "kiberqalxanı" (cyber-shield) formalaşdırmağa imkan verə bilər.

8. ƏLAVƏLƏR

8.1. Demoqrafik göstəricilər

Cədvəl 1. Sorğunun/anketin nümunə profili

İqtisadi rayon	Respondentlərin sayı	Faiz
Bakı	400	25,0
Abşeron	100	6,3
Gəncə-Qazax	220	13,8
Şəki-Zaqatala	120	7,5
Lənkəran	160	10,0
Quba-Xaçmaz	100	6,3
Aran	360	22,5
Dağlıq Şirvan	60	3,8
Yuxarı Qarabağ	80	5,0
Yekun	1600	100,0
Yaşayış məntəqəsinin növü		
Şəhər		53,7
Kənd		46,3
Gender		
Kişi	788	49,3
Qadın	812	50,7
Təhsil		
Kvalifikasiya yoxdur	7	0,4
Peşə/ixtisas təhsili	331	20,7
Ümumi orta təhsil	99	6,2
Tam orta təhsil	734	45,9
Bakalavriat	385	24,1
Magistratura	35	2,2
Doktorantura	7	0,4
Postdoktorantura	1	0,1
Bilmirəm/ÇÇ	1	0,1
Yaş		
18-24	201	12,5
25-34	366	22,8
35-44	474	29,6
45-54	285	17,8
55-65	274	17,1

Cədvəl 2. Fokus qrupların nümunə profili

Nəticələr: fokus qrup - İT ekspertləri və QHT		
		Gender
	30	Kişi
	35	Kişi
	30	Kişi
	35	Kişi
	31	Kişi
	53	Kişi
	50	Kişi
	45	Kişi
	Qrup 1 (18-21) nəticələri	
	18	Kişi
	20	Kişi
	21	Qadın
	19	Kişi
	20	Kişi
	19	Qadın
	22	Kişi
	20	Qadın
	19	Kişi
	19	Qadın
	Qrup 2 (22-35) nəticələri	
	25	Kişi
	23	Qadın
	27	Kişi
	32	Kişi
	35	Qadın
	33	Qadın
	24	Qadın
	26	Kişi
	Qrup 3 (36-65) nəticələri	
	55	Qadın
	35	Qadın
	45	Kişi
	40	Qadın
	39	Qadın
	50	Kişi
	38	Qadın
	38	Kişi
	HMO və QHT	
	NA (non-applicable)	Kişi
	NA	Kişi

	NA	Kişi
	NA	Kişi
	NA	Kişi
	NA	Kişi
	NA	Kişi
	NA	Qadın
	İnternet xidməti provayderləri	
	NA	Kişi
	NA	Kişi
	NA	Kişi
	NA	Kişi
	NA	Kişi
	NA	Kişi
	NA	Kişi
	NA	Kişi
	NA	Kişi
	Qurbanlar (zərərçəkənlər)	
	54	Kişi
	65	Qadın
	45	Kişi
	40	Kişi
	29	Qadın

Cədvəl 3. Qrup tərkibi və müzakirələrin davametmə müddəti

	Qrup növü	Qrup miqyası	Müddət	Gender	
Qrup 1	Ümumi əhali (18-21)	10	1 saat 00 dəqiqə	6 K	4 Q
Qrup 2	Ümumi əhali (22-35)	8	1 saat 16 dəqiqə	4 K	4 Q
Qrup 3	Ümumi əhali (36-65)	8	1 saat 15 dəqiqə	3 K	5 Q
Qrup 4	Zərərçəkənlər	6	45 dəqiqə	2 K	4 Q
Qrup 5	İXP	9	1 saat 40 dəqiqə	9 K	0 Q
Qrup 6	Hüquq-mühafizə orqanları	8	3 saat 14 dəqiqə	7 K	1 Q
Qrup 7	İT və informasiya təhlükə-sizliyi ekspertləri / insan hüquqları müdafiəçiləri	8	1 saat 38 dəqiqə	8 K	0 Q
Orta müddət					
Yekun		57	73 dəqiqə / 14 saniyə		

8.2. Anket

8.2.1 Sorğu

KİBERCİNAYƏT VƏ KİBERTƏHLÜKƏSİZLİK BAROMETRİ SORĞU

Əsas idarəetmə məlumatı

M-1. Müsahibənin aparıldığı ay _____

M-2. Müsahibənin aparıldığı tarix _____

M-3. Region_____

1. 2. 3. 4. 5. 6. 7. 8.

M-4. **Yaşayış məntəqəsi:** 1. Kənd ərazisi 2. Şəhər ərazisi

M-5. **Bölgənin/Bələdiyyənin kodu**

1. Paytaxt	9.	17.	25.	33.
2.	10.	18.	26.	34.
3.	11.	19.	27.	35.
4.	12.	20.	28.	36.
5.	13.	21.	29.	37.
6.	14.	22.	30.	38.
7.	15.	23.	31.	39.
8.	16.	24.	32.	40.

M-6. Müsahibəni aparanın kodu _____

M-7. Müsahibənin aparılma müddəti _____

PROSEDUR NÜMUNƏSİ

1. Müsahibə üçün ailə seçdikdən sonra aşağıdakı addımları yerinə yetirin:
2. Müsahibənin aparıldığı günə/aya ən yaxın doğum günü olan şəxsi seçin.
3. Seçilmiş şəxs onunla müsahibə aparılmasından imtina edərsə və ya kimsə müsahibənin aparılmasına maneə yaradarsa, proses dayandırılmalı və digər bir ailə ilə davam etdirilməlidir.
4. Yaşı 18-dən yuxarı olan ailə üzvlərinin adları, cinsi və yaşları barədə soruşun. Davam edərək, həmin şəxslərin doğum günləri haqqında məlumat əldə edin:

No.	İnisiallar	Gender	Yaş	Doğum tarixi (gün/ay/il)
1.	_____	_____	_____	_____
2.	_____	_____	_____	_____
3.	_____	_____	_____	_____
4.	_____	_____	_____	_____

5. _____ _____ _____ _____ _____
6. _____ _____ _____ _____ _____
7. _____ _____ _____ _____ _____
8. _____ _____ _____ _____ _____
9. _____ _____ _____ _____ _____

Özümüzü necə təqdim edək?

Sabahınız xeyir! / Günortanız xeyir!

Mən _____(ad/soyad) _____, _____əməkdaşıyam.

Müstəqil layihə əməkdaşı kimi hökuməti, siyasi və beynəlxalq qurumları təmsil etmirik.

Tədqiqatda (sorğuda) iştirak etməyi qəbul etdiyiniz üçün təşəkkür edirik. Bu tədqiqat layihəsinin məqsədi kibertəhlükəsizliyə və kibercinayətkarlığa qarşı milli münasibətə dair məlumat toplanılmasından ibarətdir. Sözügedən fəaliyyət Avropa Şurası və Avropa İttifaqının əməkdaşlığı istiqamətində "Kiber Şərq" və "Kibertəhlükəsizlik – Şərq" layihələri çərçivəsində yerinə yetirilən araşdırma işidir.

Sorğuda iştirakınız könüllüdür və seçiminizdən asılıdır. İştirak etmək qərarınız varsa, istənilən vaxt bu barədə fikrinizi dəyişdirə bilərsiniz. Sorğu təqribən 30-40 dəqiqə vaxtınızı alacaq anket suallarının cavablandırılmasını əhatə edir.

Avropa İttifaqının Ümumi Məlumatların Qorunması Qaydası (ÜMQQ) və məlumatların mühafizəsi yönündə milli qanunvericiliyə uyğun olaraq, yuxarıdakı layihələr bütün şəxsi məlumatların məxfiliyi ciddi qorunmaqla həyata keçiriləcəkdir. Əlaqə məlumatlarınız müvəqqəti qaydada yalnız məlumatları toplayan qurumun və layihənin databazasında olacaqdır. Adınız və əlaqə məlumatlarınız sorğu nəticələrinin nəşr edilməsindən əvvəl, 2 fevral 2022-ci il tarixindən gec olmayaraq databazadan silinəcəkdir. Bütün cavablarınızın gizliliyi təmin edilir. İstənilən şəxsi identifikasiya haqqında göstəricilərəriniz cavablarınızdan ayrı qorunur. Əmin ola bilərsiniz ki, sorğunun nəticələri ancaq məcmu səviyyədə və sadəcə tədqiqat məqsədləri üçün istifadə edilir. Sorğu suallarına cavablarınızla kimliyiniz anonim saxlanılır.

Qeyd edilən şərtlərlə razısınızsa, xahiş olunur, sorğuya keçid etmək üçün “BƏLİ” düyməsinə basın (və ya “bəli” söyləyin).

Təşəkkür edirik!

I BLOK.
Texnoloji təqdimat

1. Yaşadığınız evdə sizin və ya digərlərinin internetə çıxışı varmı? **VARİANTLAR OXUNMUR / SORĞU İNTERNETƏ ÇIXIŞI OLANLARLA KEÇİRİLMƏLİDİR**

a. Bəli
b. Xeyr (sorğu dayandırılsın: cavab statistik məlumat toplamaq üçün qeydə alınsın)
c. Əmin deyiləm (sorğu dayandırılsın: cavab statistik məlumat toplamaq üçün qeydə alınsın)
d. Cavab verməkdə çətinlik çəkirəm

2. Aşağıdakı cihazlardan hansını müntəzəm olaraq şəxsi ehtiyaclarınız üçün istifadə edirsiniz? **BİR NEÇƏ VARİANT**

a. Smartfon
b. Tablet
c. Noutbuk
d. Masaüstü kompüter
e. Smart TV
f. Oyun konsolları
g. Digər: (...) **CAVABI QEYD EDİN**
h. Cavab verməkdə çətinlik çəkirəm

3. Şəxsi zamanınızın ümumilikdə nə qədər hissəsini (onlayn olub-olmamasından asılı olmayaraq) rəqəmsal cihazlarla keçirirsiniz? Zəhmət olmasa rəqəmsal cihazların (smartfon, tablet və kompüterin) istifadəsinə sərf etdiyiniz ümumi vaxtı qeyd edin

a. Bir saatdan az
b. 1-2 saat
c. 2-3 saat
d. 3-4 saat
e. 4-5 saat
f. 5-6 saat
g. 6-7 saat
h. 7-8 saat
i. 8-9 saat
j. 9-10 saat
k. 10 saatdan çox

4. Gündəlik olaraq nə qədər şəxsi zamanınızı cihazlar vasitəsilə onlayn müstəvidə keçirirsiniz? Zəhmət olmasa bütün cihazlar üzrə ümumi vaxtı qeyd edin.

a. Bir saatdan az
b. 1-2 saat
c. 2-3 saat
d. 3-4 saat
e. 4-5 saat
f. 5-6 saat
g. 6-7 saat
h. 7-8 saat
i. 8-9 saat
j. 9-10 saat
k. 10 saatdan çox

5. İnternetdə mütəmadi olaraq hansı fəaliyyətlərlə məşğul olursunuz? **BİR NEÇƏ VARİANT ÜNSİYYƏT ÜÇÜN**

a. E-mail göndərmək /qəbul etmək
b. İnternet vasitəsilə ünsiyyət (videozənglər daxil olmaqla) – məsələn, Skype, Messsenger, Whatsapp, Facetime, Viber, Snapchat ilə
c. Sosial şəbəkələrdə fəaliyyət göstərmək (istifadəçi profili yaratmaq, Facebook, Twitter, Instagram, Snapchat və s. şəbəkələrdə mesajlar göndərib qəbul etmək, yaxud məzmun paylaşmaq)

İNFORMASİYAYA ƏLDƏ ETMƏK ÜÇÜN

d. Məhsullar, iş və ya xidmətlərlə əlaqədar məlumat axtarmaq
e. İnternet saytlarında/qəzetlərdə/jurnallarda xəbərləri oxumaq

YARADICILIQ ÜÇÜN

f. Hazırladığınız fotoların, mahnı və ya mətnlərin veb-saytlar, yaxud aplikasiyalar üzərindən paylaşılması

ƏYLƏNMƏK ÜÇÜN

g. Musiqiyə qulaq asmaq və ya musiqi yükləmək
h. İnternet TV izləmək (canlı, yaxud catch-up proqramlar) (məsələn, [milli nümunələr göstərmək]).
i. Video on Demand (istənilən anda istənilən videoya baxmaq imkanı) kommersiya xidmətlərindən videolar izləmək (misal üçün, Netflix, HBO, GO, Amazon Prime və s.)
j. Müəyyən sosial platformalardan/şəbəkələrdən videolar izləmək (məsələn, YouTube)
k. Oyunlar oynamaq və ya yükləmək

DİGƏR ONLAYN XİDMƏTLƏR

l. Veb-sayt və ya aplikasiyalar üzərindən məhsulların və ya xidmətlərin satışı
m. Onlayn bankçılıq
n. Elektron hökumət xidmətləri

II BLOK.
Ümumi istifadə və davranışlar

6. “Kibercinayət” ifadəsi barədə məlumatınız varmı?
a. Bəli
b. Xeyr
c. Əmin deyiləm
d. Cavab verməkdə çətinlik çəkirəm

Bu müsahibə üçün “kibercinayət” dedikdə bir kompüteri, kompüter şəbəkəsini və ya şəbəkəyə qoşulmuş cihazı hədəf alan və ya sui-istifadə edən cinayət əməli başa düşülür.

7. Bu tərifə uyğun olaraq, aşağıdakı cümlələrin hansı ilə daha çox razılaşdığınızı qeyd edin
a. Kibercinayətkarlıq olduqca nadir bir haldır və ümumiyyətlə, şübhəli fəaliyyətlərlə məşğul olan müəssisələr və / və ya şəxslərə qarşı törədilir; "normal" insanlar üçün ciddi bir risk deyil.
b. Kibercinayət insanların rifahı üçün əsl təhdiddir və bu gün hər kəs ondan zərər çəkmək riski ilə üz-üzədir.

8. Özünüzü kibercinayətdən necə qoruyursunuz? **BİR NEÇƏ VARİANT SEÇİLƏ BİLƏR**
a. Cihazlarımdan istifadə edərkən nə etdiyimə diqqətlə yanaşıram. Məsələn, şübhəli poçtu açmıram və s. **9-CU SUALA KEÇİN**
b. Cihazlarıma girişi məhdudlaşdırıram. Məsələn, şifrələrdən (paroldan) istifadə etmək və s. **10-CU SUALA KEÇİN**
c. Təhlükəsizlik proqramlarından istifadə edirəm. Məsələn, antivirus/zərərli təsirə qarşı proqram və s. **11-Cİ SUALA KEÇİN**
d. Yuxarıdakılardan heç biri **12-Cİ SUALA KEÇİN**
e. Əmin deyiləm
f. Cavab verməkdə çətinlik çəkirəm

9. YALNIZ 8-Cİ SUALIN a VARİANTINI SEÇƏNLƏR ÜÇÜN AÇILIR. Cihazlarınızı istifadə edərkən ehtiyat/qorunmaq üçün aşağıdakılardan hansını tətbiq edirsiniz? **BİR NEÇƏ VARİANT.**

a. Şübhəli mesajları silirəm
b. Şübhəli mesajları açıram, amma onlara cavab vermirəm və üzərinə klik etmirəm
c. Şübhəli saytlardan çəkinirəm / istifadə etmirəm
d. Qanunsuz və ya pirat məzmun yaymaqla məşğul ola biləcək saytlardan istifadə etmirəm
e. Şəxsi məlumatlarımı üçüncü şəxslərə vermirəm / imtina edirəm
f. Pulsuz simsiz şəbəkələrdən (məsələn, WiFi) istifadə etmirəm
g. Yuxarıdakılardan heç biri
h. Əmin deyiləm
i. Cavab verməkdə çətinlik çəkirəm

10. YALNIZ 8-Cİ SUALIN b VARİANTINI SEÇƏNLƏR ÜÇÜN AÇILIR:
Şəxsi cihazlarınıza girişi necə məhdudlaşdırırsınız? **BİR NEÇƏ VARİANT.**

a. Şifrə/Parol
b. PİN
c. Biometrik - barmaq izi, üz tanıma
d. İkifaktorlu identifikasiya (parolla yanaşı, göz, barmaq və ya üz izinin tələb edilməsi)
e. Yuxarıdakılardan heç biri
f. Əmin deyiləm.
j. Cavab verməkdə çətinlik çəkirəm

11. YALNIZ 8-Cİ SUALIN c VARİANTINI SEÇƏNLƏR ÜÇÜN AÇILIR: Hansı cihazlarınızda təhlükəsizlik proqramı quraşdırılıb? a və d bəndləri üçün, **BİR NEÇƏ VARİANT.**

a. Smartfon
b. Tablet (planşet)
c. Noutbuk
d. Masaüstü kompüter
e. Yuxarıdakılardan heç biri
f. Əmin deyiləm
g. Cavab verməkdə çətinlik çəkirəm

12. YALNIZ 8-Cİ SUALIN d VARİANTI ÜÇÜN. Kibercinayətlərdən qorunmaq üçün bu vasitələrdən heç birini istifadə etməməyinizin bir səbəbi varmı? (Əgər belədirsə, səbəb nədir?) **AÇIQ SUAL**

a. […….] **CAVABI QEYD EDİN**

13. Nə vaxtsa sizə qarşı onlayn formada cinayət əməli olduğunu hiss etdiyiniz bir cəhdlə hədəf alındığınızı hiss etmisinizmi?

a. Bəli
b. Xeyr
c. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

14. COVID-19 pandemiyası ərzində [ölkə] vətəndaşlarına qarşı kibercinayətlərin daha da artdığını hiss etmisinizmi?

a. Bəli
b. Xeyr
c. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

Fişinq (phishing)

15. Son 12 ay ərzində özünü texnologiya şirkətinin nümayəndəsi kimi təqdim edən və sizi canlı yayıma dəvət edən bir şəxs sizinlə əlaqə saxlayıbmı?
a. Bəli
b. Xeyr
c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

16. "Fişinq" (phishing) sözü ilə tanışsınızmı?
a. Bəli
b. Xeyr
c. Əmin deyiləm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

Bu müsahibədə fişinq (phishing) cinayətkarların digər tərəfləri əvəzləmək/təqlid etmək üçün telefon, e-poçt, mətn mesajları və ya sosial şəbəkələr vasitəsilə uzaqdan əlaqə qurmaqdır. Cinayətkarlar özlərini başqası kimi göstərir və istifadəçini aldadaraq zərərli proqramlar quraşdırmağa, pul və ya şəxsi məlumat göndərməyə çalışırlar.

17. Bu tərifə uyğun olaraq bu növ cinayətlərin ətrafınızda və ya haradasa baş verdiyini eşitmisinizmi?
a. Bəli
b. Xeyr. **22-ci SUALA KEÇİN**
c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

18. Son 12 ay ərzində hər hansı bir fişinq mesajı və ya zəngi almısınızmı?
a. Bəli
b. Xeyr. **22-ci SUALA KEÇİN**
c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

19. Son 12 ay ərzində aşağıdakı formalardan hansı ilə şəxsi cihazlarınızdan və ya hesablarınızdan fişinq (phishing) mesajı almısınız? **BİR NEÇƏ VARİANT.**
a. E-mail/elektron poçt ilə
b. Telefonda mətn mesajı (sms, iMessage) ilə
c. Telefonda ünsiyyət/söhbət tətbiqləri (məsələn, WhatsApp, Telegram) ilə
d. Sosial şəbəkə (məsələn, Facebook, Instagram, TikTok, Vkontakte) ilə
e. Səsli və ya video zəng ilə
f. Tanımadığın bir nömrədən cavabsız zəng ilə (qarşı tərəfin geri zəng etməsinə çalışır)
g. Digər […] **CAVABI QEYD EDİN.**

20. Son 12 ay ərzində bunlardan hər hansı birini etmisinizmi: zəng edənə inanaraq onunla söhbət etmək, eyni zamanda kiminsə göndərdiyi linkə və ya proqramlara daxil olmaq (üzərinə klikləmək).
a. Bəli
b. Yox
c. Əmin deyiləm
d. Bu barədə danışmaq istəmirəm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

21. 1-dən 4-ə qədər olan bal sistemi ilə qiymətləndirsək fişinq (phishing) (əvvəllər müzakirə edildiyi kimi) son 12 ay ərzində həyatınıza nə dərəcədə təsir etdi?

a. 1 = mənə heç təsir etmədi
b. 2 = bir az narahat etdi
c. 3 = müəyyən qədər narahat etdi
d. 4 = həyatıma mənfi təsir etdi
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

22. Necə düşünürsünüz, qonşuluğunuzda kimsə fişinq (phishing) mesajı alarsa və daha sonra bunun qeyri-qanuni əməl olduğunu bilərsə, bu əmələ məruz qaldığını aidiyyəti qurumlara (polisə) bildirərmi?
a. Bəli, düşünürəm ki, bildirər
b. Bəli, lakin yalnız ciddi hallarda
c. Xeyr, bunu bildirməz
d. Əmin deyiləm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

23. Aşağıdakılardan hansı Azərbaycanda fişinq (phishing) cinayətlərinə münasibətinizi daha yaxşı izah edir?
a. Əhəmiyyətsiz/biganə
b. Müəyyən qədər narahat
c. Nə narahat, nə də biganə
d. Əsasən narahat
e. Çox narahat
g. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

24. Özünüzü və ailənizi qorumaq üçün fişinq (phishing) haqqında kifayət qədər məlumatınız olduğunu düşünürsünüzmü?
a. Bəli
b. Xeyr
c. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

“Rənsamveə” (ransomware):

25. “Rənsamveə” (ransomware) ifadəsi ilə tanışsınızmı?

a. Bəli
b. Xeyr
c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

Müəyyən məbləğ ödənilənə qədər kompüter, mobil telefon və onların saxladığı data sisteminə daxil olmağa maneə törətmək üçün hazırlanmış zərərli proqram növü.

26. Bu tərifə uyğun gələn belə tip cinayətin baş verdiyini eşitmisinizmi?

a. Bəli
b. Xeyr **29-CU SUALA KEÇ**
c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

27. Son 12 ay ərzində tanıdığınız insanlar arasında “rənsamveə” (ransomware) proqramının qurbanı olan şəxs varmı?

a. Bəli, ailəmdən birini
b. Bəli, ailəmdən olmayan tanıdığım birini
c. Bəli, öz başıma gəlib
d. Xeyr **29-CU SUALA KEÇ**
e. Əmin deyiləm **29-CU SUALA KEÇ**
f. Cavab vermək istəmirəm **29-CU SUALA KEÇ**
g. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

28. Bunu eşitməyimə pis oldum. Bu mövzuda bir texniki sualımız var ki, insanların çoxu buna cavab verə bilmir. Sizə qarşı istifadə edilən “ransomware” (rənsamveə) proqramının növünü bilirsinizmi? **AÇIQ SUAL**
a. [……] **CAVABI QEYD EDİN**

29. Təsəvvür edin ki, qonşuluqda kiməsə “rənsamveə” (ransomware) proqramı ilə hücum olub və o, kompüterlərinə, cib telefonlarına, sahib olduğu məlumatlara və ya fotoşəkillərə girişi itirib. Sizcə, zərərçəkmiş bunu [aidiyyəti qurumlara/polisə] bildirərmi?
a. Bəli, düşünürəm ki, bildirər
b. Bəli, lakin ciddi hallarda
c. Xeyr, bunu bildirməz
d. Əmin deyiləm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

30. Bir anlığa təsəvvür edək ki, sizə bir “rənsamveə” (ransomware) proqramı ilə hücum edilib. Əhəmiyyətli miqdarda pul ödəmədiyiniz təqdirdə ən sevdiyiniz kompüter, telefon, məlumat və ya fotoşəkillərə girişiniz mümkünsüz olacaq. 1-4 ballıq sistem miqyasında bu, sizə nə dərəcədə təsir edərdi?
a. 1 = Mənə heç təsir etməzdi
b. 2 = Bu, məni bir az narahat edərdi
c. 3 = Bu, məni narahat edərdi
d. 4 = Həyatıma mənfi təsir edərdi
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

31. Aşağıdakılardan hansı Azərbaycanda “rənsamveə” (ransomware) cinayətlərinə münasibətinizi daha yaxşı izah edir?
a. Əhəmiyyətsiz/biganə
b. Müəyyən qədər narahat
c. Nə narahat, nə də biganə
d. Əsasən narahat
e. Çox narahat
g. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

32. Özünüzü və ailənizi qorumaq üçün “rənsamveə” (ransomware) proqramı haqqında yetərincə məlumatlı olduğunuzu düşünürsünüzmü?
a. Bəli
b. Xeyr
c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

Hədə-qorxu, zorakılıq-təhqir və sui-istifadə

Anketdə onlayn hədə-qorxu, zorakılıq-təhdid və sui-istifadə ilə bağlı bir neçə sual var. Heç bir təfərrüatlar barədə soruşmayacağıq. Xatırlatmaq istərdik ki, cavab vermək məcburiyyətində deyilsiniz.

33. Onlayn hədə-qorxu, zorakılıq-təhdid və sui-istifadə bağlı bir neçə suala cavab vermək istərdinizmi?
a. Bəli
b. Xeyr, **39-CU SUALA KEÇ**
c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

34. Bəzi onlayn ünsiyyətlər (əməliyyatlar) qorxulu ola bilər. Son 12 ay ərzində tanıdığınız insanlar arasında onlayn təhdid, təhqir və şantaja məruz qalan şəxs varmı?
a. Bəli, ailəmdən biri
b. Bəli, ailəmdən olmayan tanıdığım biri
c. Bəli, öz başıma gəlib
d. Xeyr
e. Əmin deyiləm
f. Cavab vermək istəmirəm
g. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

35. Son 12 ayda müəyyən bir irq, rəng, mənşə və ya mənsubiyyətə malik insanlara qarşı nifrət, ayrı-seçkilik və ya zorakılığın hər hansı formada onlayn/internetdə təbliğinin şahidi olmusunuzmu?
h. Bəli
i. Xeyr
j. Əmin deyiləm
k. Cavab vermək istəmirəm
l. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

36. Təəssüf ki, internet bəzən azyaşlılar üçün xoş olmayan bir yer ola bilər. Sizcə, [aidiyyəti qurumlar/hüquq-mühafizə orqanları] onları onlayn qorumaq üçün daha çox iş görməlidirmi?
a. Bəli
b. Xeyr
c. Əmin deyiləm
d. Cavab vermək istəmirəm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

37. Sizə internetdə hədə-qorxu gəlmək və sui-istifadə ilə bağlı bir neçə sual verdim. Qonşuluğunuzda kimsə bu cür cinayətlərdən zərər çəkmiş olsaydı, sizcə, bunu [aidiyyəti qurumlara/hüquq-mühafizə orqanlarına] bildirərdimi?
a. Bəli, düşünürəm ki, bildirər
b. Bəli, lakin ciddi hallarda
c. Xeyr, bunu bildirməz
d. Əmin deyiləm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

38. 1-dən 4-ə qədər olan şkalada, son 12 ayda onlayn hədə-qorxu, zorakılıq-təhdid və sui-istifadə həyatınıza nə dərəcədə təsir edib?
a. 1 = mənə heç təsir etməyib
b. 2 = məni bir az narahat edib

c. 3 = məni müəyyən qədər narahat edib
d. 4 = həyatıma mənfi təsir edib
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

39. Aşağıdakılardan hansı Azərbaycandakı onlayn hədə-qorxu, zorakılıq-təhdid və sui-istifadə cinayət əməllərinə münasibətinizi daha yaxşı izah edir?
a. Əhəmiyyətsiz/biganə
b. Müəyyən qədər narahat
c. Nə narahat, nə də biganə
d. Əsasən narahat
e. Çox narahat
g. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

40. Özünüzü və ailənizi qorumaq üçün onlayn hədə-qorxu, zorakılıq-təhdid və sui-istifadə haqqında kifayət qədər məlumatlı olduğunuzu düşünürsünüzmü?
i. Bəli
j. Xeyr
k. Əmin deyiləm
l. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

Kibermüdaxilə (DDoS)

Bəzən bir problem səbəbindən onlayn xidmətlər əlçatmaz ola bilər. Digər tərəfdən, cinayətkarlar onlayn xidmətlərə daxil olmağa maneə törədə bilər.

41. Son 12 ayda istifadə etdiyiniz onlayn xidmətlərdən hər hansı biri gözlənilmədən uzun müddət əlçatmaz olubmu?
a. Bəli
b. Xeyr
c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

Şəxsiyyət/kimlik (fərdi məlumatların) oğurluğu

42. Son 12 ayda şəxsi hesabınıza giriş məlumatlarınızın internetdə yayılması hadisəsi ilə qarşılaşmısınızmı?
a. Bəli
b. Xeyr
c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

43. Son 12 ayda icazə vermədiyiniz halda kimsə tərəfindən şəxsi hesabınıza daxil olmaq və ya buna cəhd edildiyinin şahidi olmusunuzmu?
a. Bəli, buna nail oldu
b. Buna cəhd edildi, lakin uğursuz oldu
c. Xeyr
d. Əmin deyiləm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

44. Son 12 ayda şəxsi/fərdi məlumatlarınızın qəsdən və qanunsuz olaraq internetdə yayıldığının şahidi olmusunuzmu?
a. Bəli
b. Xeyr

c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

45. Son 12 ayda şəxsi məlumatlarınızdan sui-istifadə və ya buna cəhd edildiyinin şahidi olmusunuzmu?
a. Bəli, buna nail oldu
b. Buna cəhd edildi, lakin uğursuz oldu
c. Xeyr
d. Əmin deyiləm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

46. Son 12 ayda bank hesablarınız, ödəmə hesablarınız və ya kredit kartı məlumatlarınızdan hər hansı birinin onlayn yayılmasının şahidi olmusunuzmu?
a. Bəli
b. Xeyr
c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

47. Son 12 ayda bank hesablarınız, onlayn ödəmə hesablarınız və ya kredit kartı məlumatlarınızın yad biri tərəfindən istifadə edildiyinin və ya edilməsinə cəhdin şahidi olmusunuzmu?
a. Bəli, buna nail oldu
b. Buna cəhd edildi, amma uğursuz oldu
c. Xeyr
d. Əmin deyiləm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm.

48. Son 12 ayda şəxsi mobil telefon nömrənizin tanımadığınız biri tərəfindən əldə edildiyinin şahidi olmusunuzmu?
a. Bəli, buna nail oldu
b. Buna cəhd edildi, lakin uğursuz oldu
c. Xeyr
d. Əmin deyiləm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

49. Son 12 ayda kiminsə tanıdığınız birinin onlayn hesabını, yaxud telefon nömrəsini ələ keçirdiyinin və həmin hesabla ünsiyyət qurarkən hesabı oğurlanmış şəxsin kimliyinin əvəzləndiyinin şahidi olmusunuzmu?
a. Bəli
b. Xeyr
c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

50. Cinayətkarların özlərini başqa şəxs kimi təqdim etməyə calışdıqları üsulların bir neçə növünü müzakirə etdik. Bu, onlayn şəxsiyyət/kimlik - fərdi məlumatların oğurluğu adlandırılır və kibercinayətin əsas komponenti hesab edilir. Qonşuluğunuzda kimsə onlayn şəxsiyyət/kimlik oğurluğundan sui-istifadənin qurbanı olarsa, sizcə, bu barədə [aidiyyəti qurumlara/polisə] bildirərmi?
a. Bəli, düşünürəm ki, bildirər
b. Bəli, lakin ciddi hallarda
c. Xeyr, bunu bildirməz
d. Əmin deyiləm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

51. 1-dən 4-ə qədər olan şkalada, son 12 ayda onlayn şəxsiyyət/kimlik oğurluğu həyatınıza nə dərəcədə təsir edib?

a. 1 = Mənə heç təsir etməyib
b. 2 = Məni bir az narahat edib
c. 3 = Məni müəyyən qədər narahat edib
d. 4 = Həyatıma mənfi təsir edib
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

52. Aşağıdakılardan hansı Azərbaycanda onlayn şəxsiyyət/kimlik oğurluğuna münasibətinizi daha yaxşı izah edir?
a. Əhəmiyyətsiz/biganə
b. Müəyyən qədər narahat
c. Nə narahat, nə də biganə
d. Əsasən narahat
e. Çox narahat
g. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

53. Özünüzü və ailənizi qorumaq üçün onlayn şəxsiyyət/kimlik oğurluğu haqqında kifayət qədər məlumatlı olduğunuzu düşünürsünüzmü?
a. Bəli
b. Xeyr
c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

54. Bütün növ kibercinayətləri müzakirə etdikdən sonra hansının sizi daha çox narahat etdiyini düşünürsünüz?
a. Fişinq
b. Rənsamveə
c. Onlayn hədə-qorxu, təhqir və sui-istifadə
d. Kibermüdaxilə (DDoS)
e. Onlayn şəxsiyyət/kimlik (fərdi məlumatların) oğurluğu
f. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

55. Kibercinayətləri cəmiyyətimizdə mövcud olan digər cinayət növləri ilə müqayisə etdiyiniz zaman hansının sizi daha çox və hansının isə ən az narahat etdiyini düşünürsünüz?

VARİANTLAR TƏSADÜFİ QAYDADA DƏYİŞİK FORMADA TƏQDİM EDİLSİN

a. Kibercinayətkarlıq
b. Sağlamlıq əleyhinə cinayətlər, məsələn, soyğunçuluq, talan və s.
c. Mülkiyyət əleyhinə cinayətlər, məsələn, oğurluq, avtomobil oğurluğu və s.
d. "Ağ yaxalıqlı", vəzifə və səlahiyyət sahibi olan şəxslər tərəfindən törədilən cinayətlər (kibercinayətlər istisna olmaqla), məsələn, fırıldaqçılıq, rüşvət və s.

56. 1-dən 4-ə qədər olan şkalada, ölkədəki aidiyyəti qurumların kibercinayətkarlıqla mübarizəyə nə dərəcədə hazır olduğunu düşünürsünüz?
a. 1 = heç hazır deyil
b. 2 = əsasən hazır deyil
c. 3 = hazırdır, amma hələ görüləcək çox işlər var
d. 4 = tam hazırdır
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

57. Növbəti 5 il ərzində kibercinayətkarlıq fəaliyyətinin necə olacağını gözləyirsiniz?
a. Kəskin azalacaq
b. Nisbətən azalacaq
c. Nisbətən artacaq

d. Kəskin artacaq
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

Demoqrafik göstəricilər

58. Cinsiniz?
a. Kişi
b. Qadın

59. Yaşınız?
_____

60. Təhsiliniz?
a. Heç bir ixtisasım yoxdur
b. Orta ümumtəhsil
c. Ali təhsil
d. Bakalavriat
e. Magistratura
f. Doktorantura
g. Postdoktorantura
h. Bilmirəm /Cavab verməkdə çətinlik çəkirəm

Zəhmət olmasa, müsahibəni belə bir fikirlə yekunlaşdırın:
"Bu sorğuda iştirak etdiyiniz üçün təşəkkür edirik! Bizə hər hansı sualınız varmı? Sizinlə bu sorğunu apardığımı təsdiq etmək məqsədilə rəhbərimin əlaqə saxlaması üçün telefon nömrələrinizdən hər hansı birini təqdim edə bilərsinizmi?"

Ad və soyad:_____
Telefon nömrəsi:_____

MÜSAHİBƏNİ APARAN ŞƏXS TƏRƏFİNDƏN TAMAMLANMALIDIR:

Sualların hər hansı biri həssas və ya cavab vermək üçün çətin idi?
1. Bəli **2.** Xeyr

Müsahibənin aparılması müddətinə dair respondentlərin şikayəti olubmu?
_____

"Bu müsahibənin düzgünlüyünü təsdiq edirəm"
Ad və soyad_____
İmza_____

SAHƏ RƏHBƏRİ TƏRƏFİNDƏN TAMAMLANMALIDIR:

Müsahibənin aparılması prosesinə rəhbərlik edilibmi?
_____

Cavab "Bəli"dirsə, hansı yolla həyata keçirilib?
1. Telefon vasitəsilə
2. Müsahibənin aparılmasında iştirak etməklə

Ad _____
İmza _____

Müəssisələr / Şirkətlər

KİBERCİNAYƏT VƏ KİBERTƏHLÜKƏSİZLİK BAROMETRİ SORĞU

Əsas idarəetmə məlumatı

M-1. Müsahibənin aparıldığı ay _____

M-2. Müsahibənin aparıldığı tarix _____

M-3. Region_____

1. 2. 3. 4. 5. 6. 7. 8.

M-4. Müəssisənin miqyası: 1. Böyük 2. Orta 3. Kiçik

M-5. Region/Bələdiyyə kodu:

1. Paytaxt	9.	17.	25.	33.
2.	10.	18.	26.	34.
3.	11.	19.	27.	35.
4.	12.	20.	28.	36.
5.	13.	21.	29.	37.
6.	14.	22.	30.	38.
7.	15.	23.	31.	39.
8.	16.	24.	32.	40.

M-6. Müsahibəni aparan şəxsin kodu_____

M-7. Müsahibənin aparılma müddəti_____

Özümüzü necə təqdim edək?

Sabahınız xeyir! / Günortanız xeyir!
Mən _____(ad/soyad) _____, _____əməkdaşıyam.
Müstəqil layihə əməkdaşı kimi hökuməti, siyasi və beynəlxalq qurumları təmsil etmirik.

Tədqiqatda (sorğuda) iştirak etməyi qəbul etdiyiniz üçün təşəkkür edirik. Bu tədqiqat layihəsinin məqsədi kibertəhlükəsizliyə və kibercinayətkarlığa qarşı milli münasibətə dair məlumat toplanılmasından ibarətdir. Sözügedən fəaliyyət Avropa Şurası və Avropa İttifaqının əməkdaşlığı istiqamətində "Kiber Şərq" və "Kibertəhlükəsizlik – Şərq" layihələri çərçivəsində yerinə yetirilən araşdırma işidir.

Sorğuda iştirakınız könüllüdür və seçiminizdən asılıdır. İştirak etmək qərarınız varsa, istənilən vaxt bu barədə fikrinizi dəyişdirə bilərsiniz. Sorğu təqribən 30-40 dəqiqə vaxtınızı alacaq anket suallarının cavablandırılmasını əhatə edir.

Avropa İttifaqının Ümumi Məlumatların Qorunması Qaydası (ÜMQQ) və məlumatların mühafizəsi yönündə milli qanunvericiliyə uyğun olaraq, yuxarıdakı layihələr bütün şəxsi məlumat-

ların məxfiliyi ciddi qorunmaqla həyata keçiriləcəkdir. Əlaqə məlumatlarınız müvəqqəti qaydada yalnız məlumatları toplayan qurumun və layihənin databazasında olacaqdır. Adınız və əlaqə məlumatlarınız sorğu nəticələrinin nəşr edilməsindən əvvəl, 2 fevral 2022-ci il tarixindən gec olmayaraq databazadan silinəcəkdir. Bütün cavablarınızın gizliliyi təmin edilir. İstənilən şəxsi identifikasiya haqqında göstəricilərinizcavablarınızdan ayrı qorunur. Əmin ola bilərsiniz ki, sorğunun nəticələri ancaq məcmu səviyyədə və sadəcə tədqiqat məqsədləri üçün istifadə edilir. Sorğu suallarına cavablarınızla kimliyiniz anonim saxlanılır.

Qeyd edilən şərtlərlə razısınızsa, xahiş olunur, sorğuya keçid etmək üçün "BƏLİ" düyməsinə basın (və ya "bəli" söyləyin).

Təşəkkür edirik!

I BLOK.
Müəssisənin/şirkətin təqdimatı/məlumat

1. Müəssisəniz/şirkətiniz hansı sektorda fəaliyyət göstərir?

- Maliyyə
- Telekommunikasiya
- Enerji
- Avtomobil
- Logistika (yükdaşıma) və nəqliyyat
- İstehsal
- Pərakəndə satış
- İnformasiya texnologiyaları (avadanlıq, proqram, xidmətlər)
- Qida
- Səhiyyə
- Daşınmaz əmlak
- Digər […]
- Bilmirəm/Cavab verməkdə çətinlik çəkirəm

2. Müəssisənizdə/şirkətinizdə işləyən bütün şəxslərin (əsas işçilərin) iş məqsədləri üçün internetə çıxışı varmı? (bura sabit xətt və/və ya mobil əlaqə daxildir).

VARİANTLAR OXUNMUR

a. Bəli
b. Xeyr (sorğu dayandırılır)
c. Bilmirəm/Cavab verməkdə çətinlik çəkirəm (sorğu dayandırılır)

3. Müəssisəniz/şirkətiniz internetə hər hansı bir sabit xətt bağlantısı istifadə edirmi? (ADSL, SDSL, VDSL, fiberoptik texnologiyası (FTTP), kabel texnologiyası və s.)

a. Bəli
b. Xeyr
c. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

4. Müqaviləyə əsasən müəssisənizin/şirkətinizin ən sürətli sabit internet bağlantısının maksimum yükləmə sürəti neçədir?

a. 30 Mbit/s-dən azdır
b. ən azı 30, lakin 100 Mbit/s-dən az
c. ən az 100 Mbit/s, lakin 500 Mbit/s-dən az
d. ən az 500 Mbit/s, lakin 1 Gbit/s-dən azdır
e. ən azı 1 Gbit/s
f. Əmin deyiləm

g. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

5. Müəssisəniz/şirkətiniz iş məqsədləri üçün mobil telefon şəbəkələrindən istifadə edərək internetə qoşulmağa icazə verirmi? **VARİANTLAR OXUNMUR**

a. Bəli
b. Xeyr
c. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

6. Müəssisəniz/şirkətiniz aşağıdakı onlayn vasitələrdən birini istifadə edirmi?

a. Korporativ sayt
b. Sosial şəbəkələr (məsələn, LinkedIn, Facebook, Odnoklassniki, Vkontakte, Xing və s.)
c. Müəssisənin bloqu və ya mikrobloqları (məsələn, Twitter və s.)
d. Multimedia paylaşım saytları və ya tətbiqləri (məsələn, YouTube, Flickr, SlideShare,Instagram, Pinterest, Snapchat və s.)
e. Wiki əsaslı məlumat mübadiləsi vasitələri
f. Digər: […]
g. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

II BLOK.
Müəssisənin/şirkərin kibertəhlükəsizlikdə rolu

7. Müəssisənizin/şirkətinizin kibertəhlükəsizlikdən məsul olan xüsusi bir təşkilati rolu/vəzifəsi və ya şöbəsi varmı?

a. Bəli, müvafiq şöbə var
b. Bəli, amma başqa bir şöbənin bölməsi kimi var
c. Bəli, bir və ya iki əməkdaş bu işlə məşğul olur
d. Digər [...]
e. Xeyr
f. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

8. Müəssisəniz/şirkətiniz kibertəhlükəsizliyi idarə etmək üçün lazım olan bəzi xidmətləri kənar qurumlara həvalə (outsource) edirmi?

a. Bəli, daxildə tam təmin edilməyən bəzi elementləri
b. Bəli, bütün kibertəhlükəsizlik məsələlərini
c. Xeyr
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

9. Son 12 ayda İT büdcənizin təxminən neçə faizi kibertəhlükəsizliyə xərcləndi?
CAVAB VARİANTLARI OXUYUN

a. 0 %
b. 1-4%
c. 5-9%
d. 10-20%
e. > 20%
f. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

10. Kibertəhlükəsizlik üzrə illik sığorta xərcləriniz İT büdcənizin neçə faizini təşkil edir?
BİR NEÇƏ VARİANT

a. Kibertəhlükəsizlik sığortası yoxdur
b. 1-4%
c. 5-9%
d. 10-20%
e. > 20%
f. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

11. Müəssisəniz/şirkətiniz hər hansı bir təhlükəsizlik çərçivəsi və ya standartı tətbiq edirmi?
BİR NEÇƏ VARİANT
a. ISO 27001
b. ITIL
c. COBIT
d. Digər […] **CAVAB YAZIN**
e. Hər hansı təhlükəsizlik çərçivəsi tətbiq etmir
f. Cavab vermək istəmirəm
g. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

12. Hazırda biznesinizdə aşağıdakılardan hansını istifadə edirsiniz? **VARİANTLAR TƏSADÜFİ QAYDADA DƏYİŞİK FORMADA TƏQDİM EDİLSİN, BİR NEÇƏ VARİANT**
a. İşiniz üçün veb sayt
b. İşiniz üçün sosial media hesabları
c. Elektron ticarət platformaları və həlləri
d. Veb əsaslı tətbiq
e. Açıq mənbə proqramı
f. Bulud hesablama (cloud computing) və ya saxlama (yəni məlumatlarınız sizin girişinizin olduğu başqa mənbədə saxlanılır və istənilən cihazdan ora daxil olmaq mümkündür)
g. İnternetə bağlı smart cihazlar və ya Əşyalar İnterneti (IoT)
h. İntranet
i. Blokçeyn texnologiyaları
j. Kriptovalyutalar (məsələn, bitcoin)
k. İnternet üzərindən səs protokolu (VoIP) xidmətləri
l. Video / canlı ünsiyyət və konfrans
m. Yuxarıda göstərilənlərdən heç biri
n. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

13. Biznesinizdə Cloud Computing, yaxud saxlama servislərində hansı növ datanı saxlayırsınız? Backup'ı (ehtiyat nüsxəsi) olan məlumatlar da daxildir. **BİR NEÇƏ VARİANT**
a. İşçilərin məxfi məlumatları
b. Müştərilər, təchizatçılar, tərəfdaşlar və ya digər üçüncü şəxslər haqqında məxfi məlumatlar
c. Gizli iş məlumatları
d. Ticarət baxımından həssas məlumatlar
e. Həssas olmayan və ya ictimai məlumatlar
f. Biznesimdə Cloud Computing və ya saxlama xidmətlərində məlumat saxlanılmır
g. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

14. Müəssisənizdəki/şirkətinizdəki hər hansı əməkdaş müntəzəm iş fəaliyyəti ilə bağlı smart telefon, planşet, noutbuk və ya kompüter kimi şəxsi cihazlardan istifadə edirmi?
a. Bəli, hər zaman
b. Bəli, amma nadir hallarda, istisna olaraq
c. Xeyr
d. Xeyr və bu, şirkət siyasəti ilə açıq şəkildə qadağandır
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

III BLOK.
Ümumi prioritet və etibarlılıq

15. Risk baxımından kibertəhlükəsizliyi müəssisəniz/şirkətiniz üçün necə qiymətləndirirsiniz?
a. Kiberhücumlar müəssisəm/şirkətim üçün ən böyük riskdir
b. Kiberhücumlar müəssisəm/şirkətim üçün ən böyük 5 riskdən biridir
c. Kiberhücumlar müəssisəm/şirkətim üçün aşağı risklidir

d. Kiberhücumlar müəssisəm/şirkətim üçün heç bir risk təşkil etmir
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

16. Müəssisəniz/şirkətiniz kibertəhlükəsizliyin kritik sahələrinə necə əməl edir?
BİR NEÇƏ VARİANT
Mənim şirkətim:
a. kiberriskləri başa düşür və müntəzəm olaraq qiymətləndirir
b. kibertəhdidlərin reallaşmasının qarşısını alır
c. kiberhadisələrə reaksiya (cavab) verir və zərərləri bərpa edir
d. kiberrisklərdən təsirlənmir
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

17. Müəssisənizdə/şirkətinizdə hansı kibertəhlükəsizlik texnologiyaları mövcuddur?
BİR NEÇƏ VARİANT
a. Mobil təhlükəsizlik
b. Viruslardan, casus və rənsamveə proqramlarından və s. qorunmaq üçün xüsusi proqramlar
c. Kibermüdaxilə (DDoS) və s. kimi halları azaldan veb təhlükəsizlik xidmətləri
d. E-poçt təhlükəsizliyi, spam/fişinqdən müdafiə
e. “Firewall, Intrusion Prevention Detection Systems” kimi şəbəkə təhlükəsizliyi
f. Məlumatların qorunması və nəzarəti
g. Satış nöqtəsi (POS) təhlükəsizliyi
h. Risklərin idarə edilməsi daxil olmaqla proqram və tətbiq təhlükəsizliyi
i. Avadanlıq və aktivlərin idarə edilməsi
j. Şəxsiyyət və giriş menecmenti
k. Fiziki giriş nəzarət mexanizmləri
l. VPN
m. Ehtiyat məqsədilə ayrıca bir bazaya məlumat nüsxəsisinin öturülməsi
n. Biznesimizin heç bir kibertəhlükəsizlik tədbiri yoxdur
o. Digər [...]
p. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

IV BLOK.
Məlumatlılığın/sayıqlığın artırılması

18. Müəssisəniz/şirkətiniz informasiya təhlükəsizliyi sahəsində məlumatlılığı artırmaq məqsədilə işçilər üçün təlimlər təşkil edirmi?
a. Bəli, vəzifə və funksiyaya görə
b. Bəli, ancaq qanun və qaydalarla müəyyən edilən yerlərdə
c. Digər [...]
d. Xeyr
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

19. Sizcə, müəssisənizin/şirkətinizin təhlükəsizlik səviyyəsini gücləndirməyə nə kömək edə bilər? **VARİANTLAR TƏSADÜFİ QAYDADA DƏYİŞİK FORMADA TƏQDİM EDİLSİN, BİR NEÇƏ VARİANT**
a. Müəssisə rəhbərliyinin üzərinə düşən öhdəlikləri icra etməsi
b. Daha böyük büdcə
c. Təhlükəsizlik şöbəsinin işçi sayının artırılması
d. Təhlükəsizlik haqqında işçilərin daha yaxşı maarifləndirilməsi
e. Qabaqcıl təhlükəsizlik texnologiyası
f. Digər [...]
g. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

20. Müəssisənizin/şirkətinizin səmərəli kiberrisk idarəçiliyində üzləşdiyi əsas çətinliklər və ya maneələr nələrdir?
a. Səlahiyyətin olmaması
b. Resursların olmaması
c. İdarəçilər tərəfindən dəstək olmaması
d. Prioritetləşdirmə
e. Digər [...]
f. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

V BLOK.
Autentifikasiya və şifrələmə

21. Müəssisəniz/şirkətiniz hansı şifrələmə strategiyasından istifadə edir?
BİR NEÇƏ VARİANT
a. Noutbuklarda fayl şifrələməsi
b. Smartfonlarda fayl şifrələməsi
c. "Cloudd"a məlumatların fayl şifrələməsi
d. Digər....., qeyd edin
e. Şifrələmə strategiyası istifadə edilmir
f. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

22. Müəssisənizin/şirkətinizin məlumat itkisinin qarşısının alınması üzrə Data Loss Prevention proqram həlləri mövcuddurmu?
a. Bəli
b. Xeyr
c. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

23. Müəssisəniz/şirkətiniz ikifaktorlu identifikasiyadan istifadə edirmi?
a. Bəli, əksər istifadəçilər üçün istifadə olunur
b. Bəli, az sayda istifadəçiyə paylanır
c. Onu istifadə etməyi düşünürük / planlaşdırırıq
d. Xeyr
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

VI BLOK.
Tədarük/təchizat zənciri

24. Müəssisəniz/şirkətiniz tədarük zəncirində kibertəhlükəsizlik riskini necə qiymətləndirir?
Tədarük zənciri tərəfdaşları və təchizatçılar tərəfindən yaranan kibertəhlükəsizlik riski...
a. Çox yüksəkdir
b. Yüksəkdir
c. Aşağıdır
d. Heç biri
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

25. Şirkətiniz üçüncü şəxslər üzərindən adekvat/ uyğun informasiya təhlükəsizliyi səviyyəsini necə təmin edir? **BİR NEÇƏ VARİANT**
a. İnformasiya risklərinin qiymətləndirilməsi çərçivəsində üçüncü tərəflərlə əlaqəli riskləri müəyyən edir
b. İnformasiya təhlükəsizliyi məsələlərini müqaviləyə daxil edir
c. Məxfilik və/və ya konfidensiallıq müqavilələrini imzalayır
d. Üçüncü tərəflərə korporativ təhlükəsizlik siyasəti və nəzarət tətbiq edir
e. İcazə verilən yerdə şirkətin keçmişi və digər cəhətləri barədə yoxlamaları həyata keçirir

f. Üçüncü tərəflərin sistemlərə və məlumatlara girişinə nəzarət edir
g. Üçüncü tərəflərin xidmətlərini mütəmadi olaraq izləyir və qiymətəndirir
h. Digər […]
i. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

VII BLOK.
Dövlətin/hökumətin rolu

26. Dövlət qurumlarına aid ‘‘aktorların’’ kiberhücumları işinizə təsir edirmi?
a. Bəli
b. Xeyr
c. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

27. Hökumətin kiberrisklərin idarə edilməsini yaxşılaşdırmaq məqsədi daşıyan qaydaları, qanunları və sənaye standartları...
a. Çox effektlidir
b. Bir qədər effektlidir
c. Effektli deyil
d. Hətta bəzən əks-təsir göstərir
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

VIII BLOK.
Kibercinayətkarlıqla bağlı vəziyyət

28. COVID-19 pandemiyasının Azərbaycanda müəssisələrə qarşı kibercinayətləri daha da artırdığını hiss edirsinizmi?
a. Bəli
b. Xeyr
c. Əmin deyiləm
d. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

29. Son 12 ayda cinayətkarlar müəssisənizdən/şirkətinizdən və ya müştərilərinizdən ödəniş məlumatları oğurlayıb və/və ya sui-istifadə edibmi?
a. Bəli
b. Xeyr
c. Əmin deyiləm
d. Cavab vermək istəmirəm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

30. Son 12 ay ərzində çalışdığınız müəssisə/şirkət məqsədli DDoS hücumlarına məruz qalıbmı?
a. Bəli, ehtiyacımız olan xidmətlərə etibar edə bilmədik
b. Bəli, əvvəlki xidmətləri təmin edə bilmədik
c. Xeyr
d. Əmin deyiləm
e. Cavab vermək istəmirəm
f. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

31. "Rənsamveə" proqramını biznes üçün risk hesab edirsinizmi?
a. Ciddi riskdir
b. Kiçik riskdir

c. Həddindən artıq şişirdilir
d. Əmin deyiləm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

32. Rəhbər şəxslərə (CEO) qarşı dələduzluğunu, biznes e-poçtu risklərini (BEC) biznes üçün risk hesab edirsinizmi?
a. Ciddi riskdir
b. Kiçik riskdir
c. Həddindən artıq şişirdilir
d. Əmin deyiləm
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

33. Son 12 ayda çalışdığınız müəssisə/şirkət neçə dəfə kibercinayətkarlığın qurbanı olub?
a. Heç vaxt. **36-cı suala keçin**
b. 1 dəfə
c. 2-5 dəfə
d. 5 dəfədən çox
e. Cavab vermək istəməzdim **36-cı suala keçin**
f. Bilmirəm/Cavab verməkdə çətinlik çəkirəm **36-cı suala keçin**

34. Son 12 ay ərzində çalışdığınız müəssisəyə/şirkətinizə hansı növ kibercinayətlər təsir edib? **BİR NEÇƏ VARİANT**
a. Kibermüdaxilə (DDoS)
b. Hacking cəhdi (yəni başqasının sisteminə ondan icazəsiz daxil olmaq)
c. Fişinq emaili
d. Zərərli proqram və troyanlar (bu viruslar sistemə daxil olandan sonra onu tədricən ələ keçirir)
e. Casus proqramı / gizli proqram (sizin razılığınız olmadan sisteminizə daxil olaraq, məlumatları üçüncü tərəfə, məsələn, şirkət və ya dövlət qurumuna ötürür)
f. Fırıldaqçı e-maillər (məsələn, CEO Fraud)
g. Helpdesk / Tech fırıldaqçılıq (yəni özünü tanınmış şirkətin əməkdaşı kimi təqdim edib, sizə kompüter dəstək xidməti göstərməyi təklif edən dələduz)
h. Rənsamveə
i. Rəhbər şəxslərin (CEO) adından istifadə etməklə dələduzluq/ Biznes e-poçtu riskləri (BEC)
j. Şəxsiyyət oğurluğu (kimliyiniz barədə məlumatları ələ keçirir və müxtəlif işlər üçün, məsələn, onlayn alış-verişdə istifadə edir)
k. Digər […]
l. Cavab vermək istəmirəm. **36-cı SUALA KEÇİN**
m. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

35. Cinayət(lər) müəssisənizə/şirkətinizə necə təsir etdi? **BİR NEÇƏ VARİANT**
a. Veb sayt və ya digər onlayn xidmətlər oflayn müstəviyə keçirildi
b. Təşkilatla əlaqədar məlumatlar sızdırıldı
c. Pul naməlum bank hesabına köçürüldü
d. Nəzərdə tutulmayan ödənişlər edildi
e. IP və ya işçilər haqqında məlumatlar internetə sızdırıldı
f. Şəxsi məlumatlar oğurlandı
g. Blackmail (qarayaxma, təhdid, şantaj və s.) cəhdi edildi
h. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

36. Sizcə, ümumiyyətlə, kibercinayətkarların motivasiyası nə olur? **BİR NEÇƏ VARİANT**
a. Maddi qazanc
b. Dələduzluq fəaliyyəti

c. Diffamasiya (işgüzar nüfuzu ləkələmək, böhtan)
d. Sistemi pozmaq
e. Əyləncə
f. Casusluq
g. Genişmiqyaslı hücum
h. Digər […]
i. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

37. Son 12 ay ərzində çalışdığınız müəssisə/şirkət kibercinayətlər səbəbindən nə qədər pul itirib?
a. Heç nə qədər
b. İllik gəlirimizin <0.1%-i
c. İllik gəlirimizin <1.0%-i
d. İllik gəlirimizin <10%-i
e. <100% illik gəlirimiz
f. İllik gəlirimizdən çox
g. Əmin deyiləm
h. Cavab vermək istəmirəm
i. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

38. Kibercinayətkarlığın son 12 ay ərzində müəssisəniz/şirkətiniz üzərində necə təsirləri oldu?
a. Heç bir təsiri olmadı
b. Kiçik narahatlıq yaratdı
c. Proseslərə ciddi mane oldu
d. Əməliyyatlarımıza ciddi təsir etdi
e. Əmin deyiləm
f. Cavab vermək istəmirəm
g. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

39. Son 12 ay ərzində cinayətkarlar kibercinayətlər vasitəsilə müəssisənizdən/şirkətinizdən pul almağa cəhd ediblərmi?
a. Bəli, rənsamveə vasitəsilə: cihazlara girişi bloklamaqla
b. Bəli, rənsamveə vasitəsilə: məlumatları şifrələməklə
c. Bəli, oğurlanmış məlumatları dərc edib təhdid etməklə
d. Bəli, uzun müddət davam edən DDoS hücumunu dayandırmaq üçün pul istəməklə
e. Bəli, həssas şəxsi görüntülərdən istifadə etməklə
f. Digər […]
g. Xeyr. **41-ci SUALA KEÇİN**
h. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

40. Cinayətkarlara nə qədər pul sərf edildi?
a. Heç bir məbləğ
b. İllik gəlirimizin <0.1%-i
c. İllik gəlirimizin <1.0%-i
d. İllik gəlirimizin <10%-i
e. <100% illik gəlirimiz
f. İllik gəlirimizdən çox
g. Əmin deyiləm
h. Cavab vermək istəmirəm
i. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

41. Potensial (gözlənilən) kiberhücum zamanı müəssisəniz/şirkətiniz yardım məqsədilə hücumu dayandırmaq və ya mənbəyini araşdırmaq üçün hüquq-mühafizə orqanları ilə əlaqə saxlayarmı?
a.Bəli
b. Xeyr. **42-ci SUALA KEÇİN**

42. Niyə əlaqə saxlamazsınız?
a. Kimlə əlaqə saxlayacağımı bilmirəm
b. Keçmişdə kömək edilmədi
c. Məsələ daxildə həll edilir
d. Bunun kömək edə biləcəkləri bir hal olduğunu bilmirdim
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

43. Hər hansı (cinayət) kibertəhlükəsizlik hadisəsi barədə məlumat verəcəyiniz başqa dövlət və ya özəl qurumlar varmı?
a. Özəl kibertəhlükəsizlik şirkəti
b. Özəl kompüter hücumlarına qarşı hazırlıq komandası/kompüter təcili müdaxilə qrupu (kompüter təhlükəsizliyi hadisələrini idarə edən bir mütəxəssis qrupu)
c. Sektorlar (məsələn, enerji və ya nəqliyyat) üzrə kompüter hücumlarına qarşı hazırlıq komandası/kompüter təcili müdaxilə qrupu (kompüter təhlükəsizliyi hadisələrini idarə edən bir mütəxəssis qrupu)
d. Milli kompüter hücumlarına qarşı hazırlıq komandası/kompüter təcili müdaxilə qrupu (kompüter təhlükəsizliyi hadisələrini idarə edən bir mütəxəssis qrupu)
e. Heç biri
f. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

44. Növbəti 5 il ərzində təşkilatları hədəf alan kibercinayətkarlıq əməllərinin hansı istiqamətdə dəyişəcəyini düşünürsünüz?
a. Kəskin azalacaq
b. Nisbətən azalacaq
c. Nisbətən artacaq
d. Kəskin artacaq
e. Bilmirəm/Cavab verməkdə çətinlik çəkirəm

Müəssisə/şirkətlə bağlı məlumat

45. Müəssisənizdə/şirkətinizdə neçə nəfər işləyir? **VARİANTLARI OXUYUN**
a. < 10
b. 10 – 99
c. 100 – 500
d. > 500

46. Müəssisənizin/şirkətinizin illik gəliri təxminən nə qədərdir? **VARİANTLARI OXUYUN**
a. <100.000 avro
b. 100.000 – 999.999 avro
c. 1-25 milyon avro
d. > 25 milyon avro

Zəhmət olmasa, müsahibəni belə bir fikirlə yekunlaşdırın:
"Bu sorğuda iştirak etdiyiniz üçün təşəkkür edirik! Bizə hər hansı sualınız varmı? Sizinlə bu sorğunu apardığımı təsdiq etmək məqsədilə rəhbərimin əlaqə saxlaması üçün telefon nömrələrinizdən hər hansı birini təqdim edə bilərsinizmi?"

Ad və soyad:_____
Telefon nömrəsi:_____

MÜSAHİBƏNİ APARAN ŞƏXS TƏRƏFİNDƏN TAMAMLANMALIDIR:

Sualların hər hansı biri həssas və ya cavab vermək üçün çətin idi?
1. Bəli **2.** Xeyr
Müsahibənin aparılması müddətinə dair respondentlərin şikayəti olubmu?
_____

"Bu müsahibənin düzgünlüyünü təsdiq edirəm"
Ad və soyad_____
İmza_____

SAHƏ RƏHBƏRİ TƏRƏFİNDƏN TAMAMLANMALIDIR:
Müsahibənin aparılması prosesinə rəhbərlik edilibmi?
_____

Cavab "Bəli"dirsə, hansı yolla həyata keçirilib?
1. Telefon vasitəsilə
2. Müsahibənin aparılmasında iştirak etməklə

Ad_____
İmza_____

QEYD ÜÇÜN

Avropa İttifaqının, Avropa Şurasının və
Sosial Tədqiqatlar Mərkəzinin birgə layihəsi

AZƏRBAYCANDA KİBERCİNAYƏT VƏ
KİBERTƏHLÜKƏSİZLİK BAROMETRİ

Ölkə üzrə kibercinayətlərə və kibertəhlükəsizliyə
ictimai rəydə münasibətin kəmiyyət və keyfiyyət əsaslı təhlili

Redaktor: Aqşin Məmmədov
Tərcüməçi: Aytən Babayeva
Dizayner: Qurban Cəlilov
Babək Cəfər

Ünvan:
Azərbaycan Respublikası, AZ 1073, Bakı şəhəri,
Yasamal rayonu, İsmayıl bəy Qutqaşınlı küçəsi, 18.
Sosial Tədqiqatlar Mərkəzi

Telefon: (+994 12) 510-70-78
(+994 12) 510-23-75
(+994 12) 510-70-69

E-poçt: info@stm.az
İnternet ünvanı: www.stm.az

Çapa imzalanıb: 09.12.2022
Fiziki çap vərəqi: 14.25
Sifariş: 35
Tiraj: 500

"MM-S" müəssisəsinin mətbəəsində çap edilmişdir.
Ünvan: Azərbaycan Respublikası, AZ 1102, Bakı şəhəri,
Nəsimi rayonu, A.Tağızadə küçəsi, ev 13.
Telefon: (+994 12) 431 11 00
(+994 50) 314 09 37

Azərbaycan Respublikası, AZ 1073, Bakı şəhəri, Yasamal rayonu, İsmayıl bəy Qutqaşınlı küç., 18

Telefon: (+994 12) 510 70 78; (+994 12) 510 23 75; (+994 12) 510 70 69

info@stm.az www. stm.az