

# Rəqəmsal dələduzluğun gizli tilovları

*Belə kiberhücumlardan necə qorunmaq olar?*



## Ekspert rəyi

**Fərid ƏMİROV,**  
kibertəhlükəsizlik mütəxəssisi

Sosial şəbəkələrdə müxtəlif məzmunlu mesajlar yayılır. Məsələn, onların bir qisminə kredit borcunun bağlanması, ərzaq yardımı, dövlət layihələri, hansısa dövlət qurumunun və ya vəzifəli şəxsin adından iş yerlərinin açılması, dəstək verilməsi ilə bağlı elanlar paylaşılır. Bu kimi hallar kiberdələduzluqdur və kibertəhlükəsizlik terminologiyasında sosial mühəndislik adlandırılır.

Hazırda bu cür kiberdələduzluqlar olduqca geniş yayılıb. Sosial şəbəkələrin əlçatan olması, hər kəs tərəfindən istifadə edilməsi kiberdələduzluqların yaranması və genişlənməsi üçün münbit şərait yaradır. Bəs belə bir vəziyyətdə kiberdələduzlar nə edirlər? Onlar, ilk növbədə, müxtəlif yollarla xeyriyyəçi, sponsor, dövlət layihəsi icraçısı, dövlət rəsmisi, hətta bəzən yüksək səviyyəli rəsmi şəxslərin adından istifadə edirlər. Müxtəlif kontentlər, videolar, səs yazıları, saxta sənədlər hazırlayaraq insanlarda etimad yaratmağa, təqdim etdikləri məlumatlarla inandırıcı görünməyə çalışırlar.

Sosial şəbəkələr və texnologiyalar sürətlə inkişaf edir. Bu gün bir şəxsin səsinə eyni formada başqa bir yerə köçürmək, onun videosunu istənilən mövzuda danışmış kimi yaratmaq mümkündür. Bu cür imkanlardan istifadə edərək vətəndaşlarda etimad formalaşdırılır. Kiberdələduzlar tərəfindən daha sonra isə vətəndaşlar haqqında məlumat toplamağa başlanılır, onların şəxsiyyət vəsiqəsi və bank kartları məlumatları, telefon nömrələri, WhatsApp hesabları, FİN kodları və digər şəxsi məlumatlar ələ keçirilir.

Növbəti mərhələdə isə artıq həmin şəxslərin adından müxtəlif üsullarla pul oğurluğu reallaşdırılır, bank kartlarından



vəsait çıxarılır, mobil bank tətbiqləri ələ keçirilir və digər qanunsuz əməllər törədilir.

Burada əsas diqqət yetirilməli məqam ondan ibarətdir ki, fırıldaqçılar şəxsi mesajlar vasitəsilə vətəndaşlara müraciət edirlər. Məsələn, “siz lotereyanın qalibi olmusunuz” və ya “təcili yazın, ilk 30 və ya 50 nəfərə xüsusi hədiyyə veriləcək” kimi mesajlar göndərilir. Daha sonra SMS və ya WhatsApp üzərindən göndərilən kodlar tələb olunur, hətta bir sıra hallarda bank kartlarının arxa hissəsindəki gizli kodlar istənilir.

Bəzən isə ilkin mərhələdə bu prosesin uduşlu və gəlirli kimi görünməsi üçün vətəndaşlara kiçik məbləğdə pul və ya digər vasitələrlə ödənişlər edilir, növbəti mərhələdə qazancın daha böyük olacağı bildirilir. Digər hallarda isə kiberdələduzlar tərəfindən özləri kiçik məbləğdə ödəniş tələb edilərək bunun uduşun bir hissəsi olduğu və sonradan daha böyük məbləğin veriləcəyi deyilir.

Bu kimi hallarda diqqətli olmaq vacibdir. Əgər hansısa şəxs müəyyən bir qurum adından danışarsa, mütləq həmin qurumun rəsmi məlumatlarını təqdim etməlidir. Məsələn, bank adından müraciət edilsə, rəsmi bank telefon nömrəsi olmalıdır və ya vətəndaş özü bankla əlaqə

saxlayaraq məlumatı dəqiqləşdirməlidir. Eyni zamanda, heç bir halda şəxsi məlumatlar paylaşılmamalıdır. FİN kodu, bank kartı məlumatları, SMS kodları, istifadəçi adı və şifrə kimi giriş məlumatları üçüncü şəxslərə verilməməlidir.

Ümumiyyətlə, sosial şəbəkələrdə şübhəli hesablar aşkar edildikdə həmin şəxslər bloklanmalıdır. Çünki bu cür fəaliyyətlər çox ciddi fəsadlara səbəb ola bilər. Əgər hər hansı halda bank kartı məlumatları qarşı tərəfə təqdim edilibsə, dərhal bankın mobil tətbiqi vasitəsilə və ya bankın rəsmi nömrəsinə zəng edərək kartın bloklanması tələb olunmalıdır. Bununla yanaşı, 102 xidmətinə – Cinayətkarlıqla Mübarizə Baş İdarəsinə məlumat verilməlidir. Eləcə də “e-gov” üzərindən müraciət mərkəzinə də şikayət etmək zəruri hesab edilir.

Mümkünsə, sübut kimi kiberdələduzlara aid ekran görüntüləri, yazışmalar, profil linkləri və mesaj tarixçələri saxlanılmalı və şikayət zamanı mütləq təqdim edilməlidir. Təcrübədə “qızıl qayda” ondan ibarətdir ki, sosial şəbəkələrdə tanımadığınızı şəxslər pul, yardım və ya dəstək tələb edirsə, bu halların 90 faizi dələduzluqdur və onlardan uzaq durmaq lazımdır. Hətta bəzi hallarda tanıdığımız şəxslərin adından da WhatsApp və digər sosial şəbəkələrdə mesajlar göndərilir. “Uşağım xəstədir”, “atam xəstədir”, “bu məbləğdə pula ehtiyacım var” kimi müraciətlər edilir.

Şəxsi təcrübəmdə də bu cür hallar olub. Tanıdığım şəxsin adından eyniməzmunlu mesajlar həmin vaxtda bir neçə adama göndərilib. Sonradan məlum olub ki, o şəxsin hesabı ələ keçirilib və onun dost siyahısındakı insanlardan pul istənilib. Belə vəziyyətlə qarşılaşdıqda mütləq şübhəli adından mesaj göndərilən şəxslə əlaqə saxlanılmalı və məlumat dəqiqləşdirilməlidir.

yaradır və həmin kart vasitəsilə törədilən qanunsuz əməliyyatlara görə cinayət məsuliyyəti riski formalaşır. Eyni zamanda, belə bir vəziyyət maliyyə təhlükəsizliyi ilə yanaşı, həm də hüquqi təhlükəsizlik məsələsi kimi diqqət çəkir.

Müasir kiber cinayətkarlığın geniş yayılmasının əsas səbəblərindən biri də sosial mühəndislik amili ilə bağlıdır. Bu metod təkə texniki zəifliklərlə yanaşı, insan

psixologiyasını da hədəfə alır. Təcili təhlükə hissi yaratmaq, yüksək qazanc vədi vermək, dövlət qurumu və ya bank əməkdaşı kimi təqdim olunmaq, sosial şəbəkə vasitəsilə emosional manipulyasiya kimi amillər istifadəçinin müdafiə mexanizmlərini zəiflətməyə yönəlidir.

O.Hacıyevin sözlərinə görə, respublikada kiber cinayətkarlığın geniş yayılması daha çox saxta bank zəngləri və SMS-lər, fişinq linkləri vasitəsilə kart məlumatlarının toplanması, sosial şəbəkələrdə investisiya və kriptovalyuta adı altında dələduzluq, “kartınızı təsdiqləyin” və ya “hesabınız bloklanacaq” tipli mesajlara əsaslanır. Bu hücumların qarşısının alınması isə birbaşa maarifləndirmə səviyyəsindən asılı olur.

## Kibertəhlükəsizlik və özünüqoruma fəndləri

Bu gün kiber cinayətkarlıq artıq fərdi səviyyədə maddi zərər problemindən çox, makroiqtisadi və milli təhlükəsizlik məsələsi kimi qiymətləndirilir. Ekspertlər bildirirlər ki, əgər vətəndaşların bank sisteminə etimadı zəifləyərsə, nağdsız ödənişlərin artım tempi, eləcə də rəqəmsal bankçılığın inkişafı ləngiyə, kölgə iqtisadiyyatının riskləri isə güclənə bilər. Bütün bunlar yekunda xarici investorların risk qiymətləndirmələrinin aşağı düşməsi ilə nəticələnər.

Rəqəmsal iqtisadiyyatın inkişafı üçün əsas şərtlərdən biri etibarlı kibertəhlükəsizlik ekosistemidir. Bu ekosistem yalnız texniki həllərlə deyil, həm də hüquqi mexanizmlər, institusional koordinasiya və ictimai maarifləndirmə ilə formalaşır. Azərbaycan Baş Prokurorluğunun və Kapital Bankın yazının əvvəlində diqqətə çatdırılan çağırışları da maarifləndirmənin artıq prioritet istiqamətə çevrildiyini göstərir. Sosial videoçarxlar, vizual kampaniyalar, real hadisələr əsasında hazırlanan ictimai mesajlar isə səmərəli təsir vasitəsi kimi kibertəhlükəsizliklə mübarizədə maarifləndirmə baxımından önəmli rol oynayır.

Kiber cinayətkarlıqla mübarizə təkə hüquq-mühafizə orqanlarının və ya bankların məsuliyyəti deyil. Bu, eyni zamanda, dövlət -bank -cəmiyyət əməkdaşlığı modelini tələb edir. Dövlətin üzərinə hüquqi bazanı gücləndirmək, kiberinsidentlərə operativ reaksiya mexanizmlərini inkişaf etdirmək və kibertəhlükəsizlik mərkəzlərinin fəaliyyətini genişləndirmək kimi vəzifələr düşür.

Bank sektorunun qarşısında süni intellekt əsaslı fırıldaqçılıq aşkarlama sistemlərinin tətbiqinin gerçəkləşdirilməsi, risklərin təhlili mexanizmlərini təkmilləşdirməsi və müştəri məlumatlandırma kampaniyalarının həyata keçirilməsi əsas məqsədlər sırasında durur. Vətəndaş isə bu məsələdə rəqəmsal davranış mədəniyyətini formalaşdırmalı, şəxsi məlumatların qorunmasını şəxsi məsuliyyət kimi qəbul etməlidir.

Beləliklə, Azərbaycanda kiber cinayətkarlıq risklərinin artması rəqəmsal transformasiyanın qaçılmaz nəticəsidir. Lakin bu risklər idarəolunandır. Əsas məsələ balansın düzgün qurulmasıdır. Başqa sözlə, texnoloji inkişaf davam etməli, lakin təhlükəsizlik arxitekturası paralel şəkildə gücləndirilməlidir. Azərbaycan Baş Prokurorluğunun vətəndaşlara ünvanladığı rəsmi xəbərdarlıq və eyni tarixdə ölkənin aparıcı maliyyə institutlarından biri olan Kapital Bankın müştərilərinə müraciəti isə cəmiyyətə açıq mesajdır.

Bu mesaj hazırda kibertəhlükəsizliyin ictimai məsuliyyət olduğunu diqqətə çatdırır. Bank kartını qorumaq, şəxsi məlumatı paylaşmamaq, şübhəli mesajlara reaksiya verməmək kimi məsələlər isə sadə davranış qaydaları kimi görünərsə də, əslində, milli iqtisadi təhlükəsizliyin əsas elementləridir. Bu baxımdan rəqəmsal gələcəyin təhlükəsizliyi hər bir vətəndaşın bu gün atdığı addımlardan asılıdır.

**Vaqif BAYRAMOV**  
XQ

Azərbaycan Baş Prokurorluğunun fevralın 18-də vətəndaşlara ünvanladığı rəsmi xəbərdarlıq və eyni tarixdə ölkənin aparıcı maliyyə qurumlarından olan Kapital Bankın müştərilərinə müraciəti respublikada kiber cinayətkarlıq risklərinin yeni mərhələyə keçdiyini diqqətə çatdıran ciddi signal oldu. Bu müraciətlər təsadüfi xarakter daşımır, əksinə, rəqəmsal transformasiyanın sürətləndiyi, elektron xidmətlərin genişləndiyi və maliyyə əməliyyatlarının böyük hissəsinin onlayn müstəviyə keçdiyi bir dövrdə təhlükələrin də paralel şəkildə artdığını nümayiş etdirir.

İnformasiya-kommunikasiya texnologiyalarının inkişafı dövlət idarəçiliyində səmərəliyin artırılması, biznes mühitinin liberallaşdırılması, vətəndaş məmnunluğunun yüksəldilməsi baxımından mühüm rol oynasa da, bu proses, eyni zamanda, yeni risk arxitekturası formalaşdırır. Rəqəmsal mühitdə təhlükə fiziki məkanla məhdudlaşmır, sərhəd tanımır və çox zaman anonim xarakter daşıyır. Bu isə kiber cinayətkarlığı ən mürəkkəb və dinamik təhdidlərdən birinə çevirir. Eyni zamanda, müasir dövrdə informasiya-kommunikasiya texnologiyalarının sürətli inkişafı cəmiyyətin bütün sahələrinə müsbət təsir göstərsə də, paralel olaraq kiberdələduzluq risklərini də artırır.

Şəxsi məlumatların oğurlanması, onlayn dələduzluq, fişinq hücumları, kiber zorakılıq və zərərli proqram təminatlarının yayılması həm fərdlər, həm də dövlət və özəl qurumlar üçün ciddi təhlükə yaradır. Bu baxımdan kiber cinayətkarlıqla mübarizə milli təhlükəsizlik, iqtisadi sabitlik və vətəndaşların hüquqlarının qorunması üçün strateji əhəmiyyət daşıyır. Kiber cinayətlərin əsas xüsusiyyətlərindən biri onların çox vaxt istifadəçilərin məlumat-sızlığı və diqqətsizliyi nəticəsində baş verməsidir. Texniki müdafiə mexanizmləri vacib olsa da, insan amili kibertəhlükəsizliyin ən zəif həlqəsi olaraq qalır. Məhz bu səbəbdən kiber cinayətkarlıqla mübarizədə maarifləndirici tədbirlər xüsusi rol oynayır.

## Rəqəmsallaşma və kiber cinayətkarlıq

**Kibertəhlükəsizlik üzrə mütəxəssis Oqtay Hacıyevin** sözlərinə görə, son illər Azərbaycanda bank və dövlət xidmətlərinin, eləcə də elektron ticarətin sürətlə genişlənməsi müşahidə olunur. Onlayn ödəniş sistemləri, mobil bankçılıq, rəqəmsal identifikasiya, məsafədən kredit və kart sifarişi kimi xidmətlər getdikcə vətəndaşların gündəlik həyatının ayrılmaz hissəsinə çevrilir.

Lakin rəqəmsal platformaların genişlənməsi ilə kiberdələduzluğa da yeni şərait yaradılır. Şəxsi məlumatların oğurlanması, fişinq hücumları, saxta sosial media profilləri, zərərli proqram təminatları və sosial mühəndislik üsulları ilə həyata keçirilən aldatma halları artıq global tendensiyanın tərkib hissəsi kimi Azərbaycanda da artım dinamikasına səbəb olur.

Ekspertin fikrincə, kiber cinayətlərin əsas xüsusiyyətlərindən biri onların texniki zəiflikdən daha çox insan amilinə əsaslanmasıdır. Müasir kiber hücumların əksər hissəsi istifadəçinin diqqətsizliyi, məlumatsızlığı və emosional manipulyasiyaya məruz qalması nəticəsində baş verir. Bu baxımdan insan amili kibertəhlükəsizlik zəncirinin ən zəif həlqəsi olaraq qalır. Bu, son dövrlər bank kartlarının ələ keçirilməsi ilə bağlı dələduzluq hallarının artmasında özünü büruzə verir. Dələduz qrupu müxtəlif bəhanələrlə vətəndaşlara bank filiallarından və ya rəqəmsal kanallardan kart əldə etməyi məsləhət bilir, daha sonra isə müəyyən ödəniş qarşılığında həmin kartları və kart məlumatlarını alaraq cinayət əməliyyatlarında istifadə edir.

Belə bir kiberdələduzluq bir neçə ciddi təhlükə yaradır. Bu, özünü daha çox fərdi

məlumatların tam ötürülməsi ilə diqqət çəkir. Belə ki, kartın və ona aid məlumatların üçüncü şəxsə verilməsi, faktiki olaraq, maliyyə identifikatorunun ötürülməsi deməkdir. Bu isə hesaba tam giriş imkanı yaradır. Bundan başqa, qanunsuz yollarla əldə olunan vəsaitlərin izlərinin itirilməsi məqsədilə bu kimi kartların digər şəxslərin istifadəsinə verilməsi dələduza həmin hesabdakı vəsaitdən istədiyi kimi istifadə

etmək hüququ verir. Bu isə istifadəçiye məxsus bütün bank hesablarının təhlükə ilə üzləşməsi və onun son nəticədə maliyyə itkisinə səbəb olması deməkdir.

Kiber cinayətkarlığa qarşı mübarizədə hüquqi məsuliyyət amili mühüm önəm daşıyır. Belə ki, mövcud qanunvericiliyə görə, kart sahibi öz kartı ilə həyata keçirilən əməliyyatlara görə cavabdehdir. Kartın üçüncü şəxsə verilməsi hüquqi öhdəlik