



საქართველოს ეროვნული ბანკი  
National Bank of Georgia



საპარტეზილოს მრეწველობის სარეგულაციო ფონდი



**FIRILDAQÇILIQ  
SXEMLƏRİ VƏ**



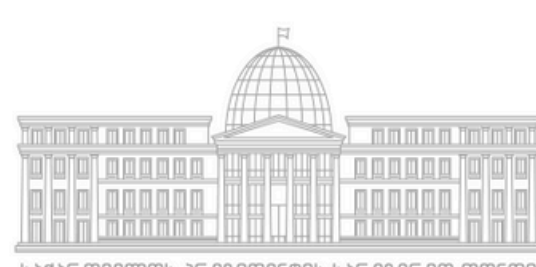
**MALİYYƏ  
TƏHLÜKƏSİZLİYİ**



ფინანსი



საქართველოს ეროვნული ბანკი  
National Bank of Georgia



საპარტეზილოს მრეწველობის სარეგულაციო ფონდი





Yəqin ki, fırıldaqçılıq sxemləri barədə eşitmisiniz ki, hansılar səbəbindən insanlar maddi baxımdan ziyanə düşürlər. Həmin broşürənin məqsədi Sizi maliyyə fırıldaqçılığının ən yayılmış formaları və fırıldaqçılığın qarşısını almaqda Sizə kömək edəcək təcrübi məsləhətlər barədə məlumat ilə tanış etməkdir.

## İNTERNET FIRILDAQÇILIĞI

Bu günkü vəziyyətdə, ondan irəli gələrək ki, əhalinin böyük hissəsi fəal olaraq internetdən istifadə edir, məhz internet istifadəçiləri fırıldaqçılıq üçün ən asan əlçatan olan hədəfdirlər. İnternetin fəal yayılması və istifadə edilməsi və eləcə də texnoloji inkişaf fırıldaqçılıq baxımından yeni növ riskləri yaratmışdır.

İnternet fırıldaqçılığının ən yayılmış formalarından biri fişinqdir. Fişinq (phishing) termini ingilis sözü - fishing-dən irəli gəlir ki, bu da balıq ovu deməkdir.

Fişinq çərçivəsində, fırıldaqçılar tərəfindən şəxsi faydanı əldə etmək məqsədilə internet istifadəçiləri barədə, şəxsi nömrə, internet bankın parolu, kartın və ya bank hesabının nömrəsi, kartın arxa tərəfində

yazılmış 3-rəqəmli (məsələn: VISA və ya Mastercard tipli kartlarda) və ya 4-rəqəmli (məsələn: American Express tipli kartlarda) təhlükəsizlik kodu kimi, məlumatlar və digər məxfi məlumatlar əldə edilir. Həmin məlumatların ələ keçirilməsi yolu ilə fırıldaqçılar Sizin icazəniz olmadan müxtəlif sanksiyalaşdırılmamış əməliyyatları həyata keçirə (məsələn, Sizin adınızdan kredit götürə) və Sizin məbləğinizi mənimseyə bilərlər.

Fişinq, bir qayda olaraq, elektron məktubları (e-mail) göndərməklə həyata keçirilir.

Bu cür məktub, ilk baxışdan, bank, sığorta şirkəti, ödəmə xidmətinin provayderi və potensial qurbanın münasibəti ola biləcəyi digər təşkilat kimi etibarlı mənbədən alınmış bildirişə bənzəyir.

Fırıldaqçılıq göndərişində bir çox halda vebşəhifənin linki verilir ki, hansının ünvanı, demək olar ki, həqiqi vebşəhifənin ünvanından fərqlənmir. Lakin, saxtalaşdırılmış vebşəhifəyə keçərkən, istifadəçi tərəfindən daxil edilmiş məlumat - adı və soyadı, internet-bankın istifadəçisinin adı və parolu, bank kartının və ya hesabının nömrəsi, təhlükəsizlik kodu və s. - avtomatik olaraq b.a. “fişerin” əlinə keçir. Fırıldaqçılıq elektron məktubuna eləcə də fayl bərkidilə bilər ki,



hansı açıldıqdan sonra Sizin kompüterinizə daxil olmaq mümkün olur. Fişinqin digər yayılmış üsulları da mövcuddur. Bu cür üsullardan biri də sosial şəbəkədə saxta təkliflərin yayılmasıdır. Belə olan halda, sosial şəbəkənin istifadəçisi elə bir reklam və ya təklif ilə qarşılaşa bilər ki, hansının arxasında saxta təşkilat və ya elə bir şəxs (şəxslər qrupu) durur ki, hansıların məqsədi istifadəçinin şəxsi və məxfi məlumatlarını əldə etməkdir. Müvafiq olaraq, sosial şəbəkələrdə alınan təkliflərlə əlaqədar olaraq diqqətli olmalısınız və sosial şəbəkə ilə şəxsi məlumatın paylaşılmasını maksimal olaraq məhdudlaşdırsanız, yaxşı olar.

Fişinq internetsiz də həyata keçirilə bilər. “Smışinq” / smishing - SMS-fişinq - fişinqin növlərindən biridir, hansı ki, qısa mətnli bildirişin göndərilməsi yolu ilə həyata keçirilir, hansında məktubu göndərən olaraq bankın və ya digər təşkilatın adı göstərilir və hansının daxilində fırıldaqçı vebünvana keçid linki vardır. Vişinq / vishing isə telefon fırıldaqçılığının növüdür ki, hansından fırıldaqçılar məxfi məlumatı əldə etmək məqsədilə istifadə edirlər. Məsələn, fırıldaqçılar bankın adından istifadəçi ilə telefonla əlaqə saxlaya və kartın rekvizitləri və PIN-kodun paylaşılmasını xahiş edə bilərlər. Müvafiq olaraq, istifadəçi telefon kommunikasiyası zamanı da ehtiyatlı olmalıdır.

Nəzərə alın ki, fişinq/saxta elektron məktubları bir çox halda “Spam” şəklində gəlir. “Spamminq” / spamming elektron məktubların alandan xəbərsiz və onun istəyi olmadan göndərilmə prosesi adlanır.

Bir qayda olaraq, bənzər məktublar

reklam xarakterlidir, lakin hakerlər “spamminqdən” bir çox halda fırıldaqçılıq sxemləri üçün də istifadə edirlər və potensial qurbana udulmuş mükafatı almaq üçün məbləği köçürmək tələbi, fırıldaqçılıq məqsədilə tanış olmaq tələbi, qeyri-düzgün köçürülmüş məbləği geri qaytarmaq tələbi, dərmanları və ya digər məhsulları satın almaq təklifi və sair kimi müxtəlif məzmunlu bildirişləri göndərirlər. Bu səbəbdən, Sizin istəyiniz olmadan, “Spam” şəklində gələn təkliflərdən ehtiyat edin.

Şəxsi və maliyyə məlumatının oğurlanması fişinq qurbanı olan istifadəçinin qarşılaşa biləcəyi yeganə təhlükə deyildir. Fişinq/saxta veb-səhifədə zərərli və ya casus proqramı da ola bilər.

Beləliklə, əgər Sizin fırıldaqçıların maraqlana biləcəyi bank hesabınız yoxdursa, bu o demək deyildir ki, Siz tamamilə təhlükəsizlikdəsiniz.

Fırıldaqçı Sizin elektron poçtunuzun məlumatlarını oğurlaya bilər ki, ondan digər istifadəçilər arasında “Spam” və virusları yaymaq üçün istifadə etsin.

Əgər yekunlaşdırsa, Siz şəxsi məlumatınızı mütləq ehtiyatla qorumalısınız. Maksimal olaraq şəxsi/pasport nömrəsini, eləcə də bank kartının və hesabın məlumatlarını, o cümlədən, kartın nömrəsini, PIN-kodunu, kartın etibarlılıq müddəti və kartın arxa tərəfində yazılan 3- və ya 4-rəqəmli təhlükəsizlik kodunu paylaşmaqdan çəkinin. Əgər Siz həqiqətən xidmət bankınız ilə söhbət etdiyinizə əmin deyilsinizsə - bu el-poçt, SMS, telefon və ya sosial şəbəkələrlə ola bilər - mütləq rəsmi telefon nömrəsi vasitəsilə bank ilə əlaqə saxlayın və vəziyyəti araşdırmağı xahiş edin. Unutmayın ki, fişinq/fırıldaqçılıq hücumlarının uğuru əsasən istifadəçilərin məlumatsızlığı və diqqətsizliyindən asılıdır!

İnternet fırıldaqçılığının qarşısını almaq məqsədilə internetlə “şopping” həvəskarları maaşınızın köçürüldüyü və ya böyük miqdarda məbləği yerləşdirdiyiniz əsas kartınızdan istifadə etməsəz, daha yaxşı olar; arzu olunur ki, müxtəlif əşyaları və xidməti onlayn-məkanda satın almaq üçün ayrıca hesabınız və kartınız olsun ki, hansında internet-satınalmaları yerinə yetirmək üçün lazım olan məbləği dəqiq miqdarda saxlayacaqsınız. Bununla yanaşı, təhlükəsizliyin əlavə, lakin qeyri-mükəmməl mexanizmi internet tranzaksiyalarının qorunmuş veb-səhifələrdə həyata keçirilməsidir ki, hansılarda veb-səhifənin ünvanı http:// ilə deyil, https:// və ya shttp:// ilə başlayır. Veb-səhifənin qorunmuş olduğunu eləcə də bağlı yaşıl kilid rəmzi göstərir, hansı ki, veb-səhifə xanasında

görünür və hansına tıklayaraq veb-səhifənin etibarlılığı və təhlükəsizliyini təsdiq edən sertifikatı görə bilərsiniz.

Əlavə olaraq, arzu olunur ki, internet ödəmə 3D təhlükəsizlik texnologiyasına malik olan veb-səhifədən həyata keçirilsin, Sizin kartınızda isə 3D müdafiə mexanizminin olması yaxşı olar (əgər Sizə xidmət göstərən bankın həmin funksionalı təklif etmək imkanı varsa). Bununla yanaşı, daha yaxşı olardı ki, Sizin mobayl və internet bankınıza daxil olmaq üçün mürəkkəb paroldan istifadə edəsiniz və ikisəviyyəli avtorizasiya funksiyasını aktivləşdirəsiniz, hansı ki, parolun göstərilməsi ilə yanaşı, sistemə daxil olmanı təsdiq edən birdəfəlik kodun SMS, el-poçt və ya xüsusi cihaz – token (birdəfəlik istifadə edilən kodu generasiya edən b.a. “dicipas”) ilə alınması və sistemə daxil edilməsi kimi əlavə təhlükəsizlik vasitələrindən istifadə edilməsini nəzərdə tutur. İkisəviyyəli avtorizasiyadan istifadə edilmə internetbank və ya mobaylbank ilə tranzaksiyaların həyata keçirilməsi zamanı da məqsədəuyğundur, həmin halda da hər bir tranzaksiyanı həyata keçirmək üçün SMS, el-poçt və ya token ilə unikal kodu alacaqsınız. Parola gəldikdə isə, arzu olunur ki, o, ən azı səkkiz rəmzdən ibarət olsun və tərkibində böyük, eləcə də kiçik hərflər, rəqəmlər və digər rəmlər (məsələn, nöqtə, defis, nida işarəsi) olsun. Kartın rekvizitlərini, internetbank istifadəçisinin adı və parolunu kompüterdə, mobil telefonda və digər elektron cihazlarda



saxlamayın. İctimai WiFi-dən (naqilsiz internetdən) istifadə edərkən internetbankdan istifadə etməyin və sistemə kartın məlumatlarını daxil etməyin.

Sizin elektron cihazlarınızı – o cümlədən, smartfonları, planşetləri və leqtopları – haker hücumlarından qorumaq üçün Sizə proqram təminatını vaxtında yeniləməyi və ona əmin olmağı məsləhət görürük ki, antivirus proqramlarının ən yeni versiyalarından istifadə edərsiniz.

Və sonunda, bu və ya digər veb saytın həqiqiliyini və mənsəyini müəyyən etmək üçün bir çox veb saytın bizə təklif etdiyi WHOIS xidmətindən (protokolundan) istifadə edə bilərsiniz. Bunun üçün şübhəli vebünvanın (domenin) adını göstərməyiniz kifayətdir, WHOIS isə ictimai məlumat bazalarında qeyd edilən vebünvan haqqında, onun qeydiyyat və ehtibarlılıq müddəti, domenin hazırkı sahibi və sair kimi, məlumatı axtarib Sizə çatdıracaqdır. Bu isə Sizə veb sahifənin həqiqiliyini müəyyən etməkdə kömək edəcəkdir. Məsələn, əgər bilirsiniz ki, Sizin üçün tanış olan şirkətin veb sahifəsi uzun müddət mövcuddur, şübhəli veb sahifənin qeydiyyat tarixi isə nisbətən yenidir – ehtimal olaraq, Siz fırıldaqçılıq ilə qarşılaşmısınız.

## **BANK ÖDƏMƏ KARTINDAN, BANKOMATDAN VƏ POS-TERMINALDAN İSTİFADƏ ETMƏKLƏ FIRILDAQÇILIQ**

Əgər diqqətli olmazsanız, fırıldaqçılar Sizin ödəmə kartınızın məlumatlarını bankomatdan və ya POS-terminaldan istifadə etdiyiniz zaman da mənimseyə bilərlər.

Bankomatdan istifadə edərkən ehtiyatlı olun: yol verməyin ki, başqa insan həddindən artıq Sizin yaxınlığınızda dursun və hansı kodu yığdığınızı görsün; bankomatın klaviaturasından istifadə edərkən onun üstünü örtün, bankomatı yaxşıca baxışdan keçirin və əmin olun ki, bankomatın üzərində və ya onun ətraf ərazisində banka məxsus olmayan və kartınızın məlumatları qeyd edə bilən kamera və ya cihaz quraşdırılmamışdır. Və sonunda, diqqət yetirin ki, kartınız və pulunuz bankomatda qalmasın.

(1. Məsələn, [www.whois.net](http://www.whois.net), [www.whois.com](http://www.whois.com), və s.)

İstifadəçilər öz kartını bir çox halda diqqətsiz qoyurlar ki, bu da fırıldaqçılar üçün əlverişlidir. Kartı və maliyyə sənədlərini işdə

masanın üzərində və ya universitetdə, mağında və ya başqa insan üçün əlçatan olduğu ictimai toplaşma yerlərində qoymayın. PİN-kodu kartınızın üzərinə yazmayın və kartı vərəqə yazılmış PİN-kod ilə birlikdə pul qabına qoymayın. Bununla yanaşı, artıq söhbət etdiyimiz kimi, kartın məlumatlarını – nömrəsi, etibarlılıq müddəti, təhlükəsizlik kodunu – telefon və ya el-poçt vasitəsilə göndərməyin və həmin məlumatları dostlarınız və hətta ailə üzvləriniz ilə paylaşmayın.

Maliyyə fırıldaqçılığının diqqətəlayiq formalarından biri olan skiminq barədə də söhbət etməyimiz əhəmiyyətliidir. Skiminq zamanı bankomatda və ya POS-terminalda xüsusi cihaz – skimmer quraşdırılır ki, hansının məqsədi kartın məlumatlarını (PİN-kod, kartın nömrəsi, etibarlılıq müddəti, təhlükəsizlik kodu) oğurlamaqdan ibarətdir, hansılardan fırıldaqçı məbləği mənimsəmək üçün istifadə edir.

Özünüzü skiminqdən qorumaq məqsədilə, bankomatdan istifadə edərkən – xüsusilə, xaricə səyahət etdiyiniz zaman - əmin olun ki, o, işıqlandırılmış yerdə yerləşir (gecə saatlarında isə daha yaxşı olar ki, mühafizə olunan mühitdə (məsələn, bankın 24-saatlıq özünəxidmət servis mərkəzlərində) mövcud olan bankomatlardan

istifadə edəsiniz), üzərində zədələnmələr görünmür və bilavasitə olaraq bankomatın üzərində şübhəli cihazlar quraşdırılmamışdır. Məsələn, əgər bankomatın klaviaturasının üzərinə, hansı vasitəsilə istifadəçi öz kartının PİN-kodunu daxil edir, hər hansı bir cihaz və ya şəffaf rezin/plastmass qışa yapışdırılmışdırsa, ödəmə kartını bankomata yerləşdirməyin və həmin bankomatda PİN-kodu yığmayın. Bununla yanaşı, bankomatdan istifadə etməzdən öncə əmin olun ki, onun ekranında bankın rəsmi yazısı yerləşdirilmişdir.

Əgər bankomatdan istifadə edilmənin təhlükəsiz olduğuna əmin deyilsinizsə, o zaman daha yaxşı olar ki, ondan istifadə etməkdən çəkinəsiniz, problemin mövcud olması barədə isə dərhal banka məlumat verin.

POS-terminaldan istifadə etdiyiniz zaman da təhlükəsizlik tədbirlərinə əməl etməlisiniz: əmin olun ki, onun üzərində zədələnmələr görünmür. Bununla yanaşı, tranzaksiyanın Sizin iştirakınızla aparılmasını tələb edin və heç vaxt kartı xidmət göstərən işçi heyətinə verməyin (o cümlədən, benzindoldurma stansiyalarında, restoranlarda və başqa yerlərdə), çünki həmin zaman kartınızın məlumatlarının oğurlanma riski yaranır.



Nəzərə alın ki, məlumatlar yalnız xüsusi cihazlarla deyil, eləcə də çox asanlıqla, şəklini çəkməklə və ya məlumatları köçürməklə də oğurlana bilər. Bu səbəbdən, yol verməyin ki, kartınız Sizin görmə arealınızdan kənara çıxsın. Özünüzü maliyyə fırıldaqçılığından qorumaq məqsədilə bankın SMS-xidmətindən istifadə edilmə yaxşı ideyadır ki, bu da Sizə kartınızla həyata keçirilmiş əməliyyatlar barədə məlumatı ani olaraq mobil telefonunuza almaq imkanını verir. Bununla yanaşı, kart ilə həyata keçirilmiş əməliyyatlara nəzarət etməyin yaxşı vasitəsi mütəmadi olaraq bank çıxarışının yoxlanılmasıdır.

Bu yol ilə Siz, ola bilsin, Sizin yerinə yetirmədiyiniz şübhəli tranzaksiyaları asanlıqla görəcəksiniz. Ödəmə kartı itirildiyi və ya oğurlandığı halda, dərhal Sizə kartı verən maliyyə təşkilatı ilə əlaqə saxlayın və kartın blokladılmasını tələb edin. Bir çox halda kartı internet və mobayl bank ilə də blokladıra bilərsiniz. Əgər kartı blokladırmazsanız, kartınızı oğurlayan və ya tapan fırıldaqçılar ani olaraq fırıldaqçılıq əməliyyatlarını həyata keçirə bilərlər.

## SAXTALAŞDIRILMIŞ PULDAN İSTİFADƏ ETMƏKLƏ FIRILDAQÇILIQ

Fırıldaqçılığı saxtalaşdırılmış pul vasitəsilə də həyata keçirmək mümkündür. Bu cür fırıldaqçılıq sxeminin qurbanı isə bizlərdən hər biri ola bilər. Nağd pulu alarkən diqqətli olun, Sizə verilən əsginaza diqqət yetirin və həqiqi pulu saxta puldan fərqləndirən qoruyucu əlamətləri yoxlayın.

Saxtalaşdırılmış əsginazı aşkar etdiyiniz halda mütləq Sizə xidmət göstərən və ya Gürcüstan Milli Bankına və hüquq mühafizə orqanlarına müraciət etməlisiniz. Yenilənmişləri və onun qoruyucu əlamətləri barədə əlavə məlumatı Gürcüstan Milli Bankı tərəfindən xüsusi olaraq bu məqsəd üçün yaradılmış veb sahifədə əldə edə bilərsiniz:  
[www.ganakhlebulilari.ge](http://www.ganakhlebulilari.ge).

## MALİYYƏ PİRAMİDALARI

Müasir dünyada maliyyə fırıldaqçılığının yayılmış formalarından biri b.a. maliyyə piramidasıdır ki, hansı barədə məlumatınızın olması Sizə özünüzü bilmədən şübhəli əqdlərə qoşulmaqdan qorumaqda kömək edəcəkdir.



Maliyyə piramidası elə bir fəaliyyət formasıdır ki, hansı çərçivəsində əhalidən məbləğlər cəlb edilir və əvəzinə, bir qayda olaraq, bazarda mövcud olan faiz dərəcələri ilə müqayisədə olduqca daha yüksək fayda təklif olunur.

Maliyyə piramidası, əksər hallarda, mənfəətli sərmayəni həyata keçirmir və istifadəçiyə vəd edilmiş faydanın ödənilməsinin yeganə mənbəyi yeni və/və ya mövcud olan üzvlərdən əlavə vəsaitlərin cəlb edilməsidir.

Bu cür şirkətin hər hansı bir anda nə qədər uğurlu göründüyünə baxmayaraq, sxemin fəaliyyət göstərməsi üçün yeni üzvlərin və/və ya əlavə məbləğin cəlb edilməsi mütləqdir. Müvafiq olaraq, yeni üzvlərin və/və ya əlavə məbləğin cəlb edilməsi qeyri-mümkün olduğu zaman şirkət üzvlərə qarşı mövcud olan öhdəlikləri artıq ödəyə bilməz və maliyyə piramidası mütləq dağılacaq, onun üzvləri isə sərmayə qoyulmuş pulu itirəcəklər. Maliyyə piramidası və onun tanınma əlamətləri barədə əlavə məlumatı Gürcüstan Milli Bankının hazırladığı bloq-postda əldə edə və aşağıda verilən videoçarxlarda dinləyə bilərsiniz:

Ağlabatan qənaət barədə videoçarx:

<https://www.youtube.com/watch?v=BN8XeByjJl>

Qənaət etdiyiniz məbləği hər hansı bir təşkilata etibar edərkən diqqətli olun – həmin təşkilatın fəaliyyəti və maliyyə vəziyyəti barədə məlumatı ələdə edin və əmin olun ki, fırıldaqçılıq işlərində iştirak etmirsiniz. Unutmayın ki, başqa eyni şəraitdə, vəd edilmiş yüksək fayda yüksək risk ilə də bağlıdır. Və sonunda, heç kər maliyyə fırıldaqçılığından sığortalanmayıbdır. Müvafiq olaraq, tədbirlilik və ehtiyatlılıq, eləcə də öz hüquqları və məsuliyyətləri və maliyyə fırıldaqçılığının ən yayılmış formaları barədə bilik Sizə özünüzü fırıldaqçılıq sxemlərindən qorumaqda və fırıldaqçılıq faktı baş verdiyi halda vaxtında reaksiya verməkdə kömək edəcəkdir.









