MÜASİR DÖVRDƏ GENİŞ YAYILMIŞ BİR KİBER HÜCUM HAQQINDA

QULİYEV N.Ə.
BDU, dosent, fizika-riyaziyyat elmləri namizədi

Müasir dünyada onlayn fəaliyyət formasına keçid formalaşmaqdadır. Xüsusəndə onlayn fəaliyyət formasına geniş miqyaslı keçidi koronovirus pandemiyası dövrü sürətləndirmişdir və bunu alternativsiz bir vasitəyə çevirmişdir. Bu gün dünyada maliyyə dövriyəsinin böyük hissəsi onlayn şəkildə və ya ödəniş kartları vasitəsilə həyata keçirilir. Onlayın fəaliyyətin, bunula bərabər istifadə olunun onlayın ödənişlərin, plastik kartların geniş istifadə olunması da bu sahədə bir çox özünə məxsus təhlükələri də meydana gətirir. Bu məqalə məhz bu tipli təhlükələr və onlarla mübarizə ilə bağlıdır. Bu baxımdan bu məqalənin çap edilməsi çox aktualdır.

***Açar sözlər**: Kiber hücum, fişinq hüçüm, fişer, fişinq hücumlarının növləri, anti- fişinq*

Müasir dövrdə bütün dünyada əksəriyyət fəaliyyət formalarının onlayn fəaliyyət sisteminə keçidi başlamışdır. Bu keçid xüsusəndə koronovirus pandemiyası dövründə daha da sürətlənmişdir. Həmçinin koronovirus pandemiyası dövründə əksəriyyət fəaliyyət formalarında onlayın fəaliyyət forması alternativsiz fəaliyyət formasına çevrilmişdir. Onu da qeyd edək ki, bütün bəşəriyyətin ən əsas fəaliyyət formalarından biri də ticari münasibətlər sistemidir. Müasir koronovirus pandemiyası dövründə də ticari münasibətlərin onlayn forması ən əsas ticarət formasına çevrilmişdir. Onlayn ticarətin əsas amillərindən biri də ödəmə kartlarının geniş istifadəsidir. Onlayın fəaliyyətin, bunula bərabər istifadə olunun onlayın ödənişlərin, plastik kartların geniş istifadə olunmasıda bu sahədə bir çox özünə məxsus təhlükələri də meydana gətirir.

Onu da qeyd edək ki, müasir dövrdə informasiya texnologiyaları, kompüter texnikaları və ümumiyyətlə texniki tərəqqi nə qədər inkişaf etsə də, cinayətkarlar, fırıldaqçılar bunu öz xeyrinə çevirmək üçün daha mürəkkəb və ixtiraçı cəhdlər edirlər. Belə cəhdləri cinayətkarlar əsasəndə daha çox onlayın alış- verişdə və ödəmə kartlarında həyata keçirməyə cəhd edirlər. Aydındır ki, son dövrlər nağd pulların daha çox plastik ödəmə kartları ilə dövr etməsi müşahidə edilməkdədir. Xüsusində koronovirus pandemiyası müddətində bu keçid daha da sürətlənmişdir və post koronovirus dövründə də bu ənənənin dava da genişlənəcəyi gözlənilir. Ciblərimizdəki nağd pul təchizatı nə qədər aktiv şəkildə, plastik ödəmə kartları ilə əvəzlənirsə, onları sındırmağın yolları da bir o qədər çox tapılır.

Bu baxımdan cinayətkarların, fırıldaqçıların bank kartlarından istifadə etmək üçün hansı üsullardan istifadə etməsini bilmək hər kəs üçün çox fayda-

lıdır və müasir dövrümüzün ən aktual məsələlərindən biridir. Bu üsulları, qaydaları bilməklə istifadəçilər cinayətkarların, fırıldaqçıların asan qurbanı olmaya bilərlər. Bank kartlarına hücum edənlərin ən sevimli üsullarından biri də fişinq hücumlarıdır.

Fişinq (ingilis dilində Phishing "balıqçılıq" sözündən götürülmüşdür), məqsədi istifadəçilərin gizli məlumatlarına, məsələn, loqin və parollarına giriş əldə etmək olan İnternet dələduzluğunun, saxtakarlığının bir növüdür. Fişinq hücumları İnternetdə çox geniş yayılmış kiber hücum növlərindən biridir. Fişinq hücumları adətən məşhur brendlərin, markaların adından elektron poçtların kütləvi göndərilməsi ilə baş verir, habelə müxtəlif xidmətlər içərisində, məsələn, bankların adından və ya sosial şəbəkələrin daxilindəki şəxsi mesajlar göndərməklə nail olunur. Göndərilən məktubda tez-tez əsl saytdan görkəmcə fərqlənməyən saxta bir sayta və ya redriktorlu sayata (URL yönləndirməsi istiqamətləndirilməsi (İngilis sözü olan URL redirection sözündən götürülmüşdür)- World Wide Web-də veb səhifəni bir neçə URL-lər altında əldə etmək üçün istifadə olunan bir texnikadır) birbaşa istinad yerləşir. Hər hansı bir istifadəçi belə saxta səhifəyə daxil olduqdan sonra, fırıldaqçılar (fişinq hücumunu təşkil edənlər) müxtəlif psixoloji fəndlərlə istifadəçini həmin saxta səhifədə öz login və parolunu daxil etməyə təhrik edir, hansı ki bunları istifadəçi müəyyən bir sayta daxil olmaq üçün istifadə edir. Bu login və parollar isə fırıldaqçılara həmin istifadəçilərin hesablarına və bank hesablarına daxil olmağa imkan verir.

Fişinq, digər tərəfdən şəbəkə təhlükəsizliyinin əsaslarını bilməyən istifadəçilərə əsaslanan sosial mühəndislik növlərindən biridir. Şəbəkə təhlükəsizliyinin əsaslarını təşkil edən faktlardan biri də ondan ibarətdir ki, adətən onlayın fəaliyyət göstərən xidmətlər öz qeydiyyat verilənlərinizi, məsələn, parol və s.-ni göstərməyinizi tələb edən elektron məktublar göndərmir.

Fişinq hücumlarını təşkil edən şəxslərə fişerlər də deyilir. Bu gün fişerlərin hədəfi bankların və elektron ödəmə sistemlərinin müştəriləridir. Fişerlər hələ kifayyət qədər İT savadlılığı olan ABŞ- da meydan oxuyurlar. ABŞ-da Daxili Gəlirlər Xidməti (ingilis dilində *Internal Revenue Service*) (ABŞ-ın vergi xidmətidir Amerika Birləşmiş Ştatları Federal Hökumətinin vergi toplayan və vergi qanunlarına əməl edilməsinə nəzarət edən dövlət orqanıdır) adı ilə maskalanaraq, gizlənərək fişerlər vergi ödəyiciləri haqqında kifayyət qədər verilənləri, məlumatları toplamışdılar. Burada fişerlərin hücum taktikasıda dəyişmişdir. Əgər ilk məktublar təsadüfən onlara lazım olan bankın və ya xidmətin müştərilərinə çatacaqları ümidi ilə göndərilirdisə, indi fişerlər zərər çəkmiş şəxsin hansı xidmətlərdən istifadə etdiyini müəyyən edə bilir və məqsədli poçt göndərmələrini tətbiq edir. Son fişinq hücumlarının bir hissəsi birbaşa şirkətlərdə rəhbər vəzifələrdə çalışan rəhbərlərə və şirkətlərdə yüksək vəzifələr tutan digər insanlara yönəldirilmişdir.

Dünyada daha çox istifadəşiyə malik olan Sosial şəbəkələr də fişerlər üçün böyük maraq doğurur. Fişerlər sosial şəbəkələrdən istifadəçilərin şəxsi məlumatlarını toplamaq üçün istifadə edirlər. 2006-cı ildə bir kompüter qurdu (Şəbəkə qurdu, lokal və qlobal (İnternet) kompüter şəbəkələri vasitəsi ilə müstəqil yayılan bir zərərli proqram növüdür) MySpace sosial şəbəkəsində qeydiyyat məlumatlarını oğurlamağa yönəlmiş fişinq saytlarına bir çox linklər, istinadlar yerləşdirmişdir. 2008-ci ilin may ayında ilk belə qurd məşhur rus dilli İnternet mühitinin sosial şəbəkəsi sayılan VKontakte-də yayılmışdır. Mütəxəssislərin fikrincə, sosial şəbəkələrə edilən fişinq hücumlarının 70% -dən çoxu müvəffəqiyyətli olmuşdur.

Ümumiyyətlə, İnternetdə fişinq sürətlə inkişaf edir, lakin onun vurduğu ziyanın qiymətləndirmələri çox dəyişir: Gartner şirkətinə görə, 2004-cü ildə fişerlərin qurbanları 2.4 milyard dollar itirmişdilər, 2006-cı ildə dəymiş ziyan 2.8 milyard dollara çatmışdır, 2007-ci ildə isə dəymiş ziyan 3,2 milyard dollara çatmışdır. Təkcə ABŞ-da 2004-cü ildə 3,5 milyon insan fişinq qurbanı olmudur, 2008-ci ildə isəABŞ-da fişimq qurbanlarının sayı 5 milyona yüksəlmişdir. Nəzərə alsaq ki, dunyada ABŞ dövləti İT texnologiyalarının vətənidir, onda digər dünya dövlətlərində, o cümlədən də ölkəmizdə fişinq hücumları ilə vəziyyətin daha acınacaqlı olduğunu təssəvür etmək çətin deyil.

Fişinq hücumlarının növləri haqqında

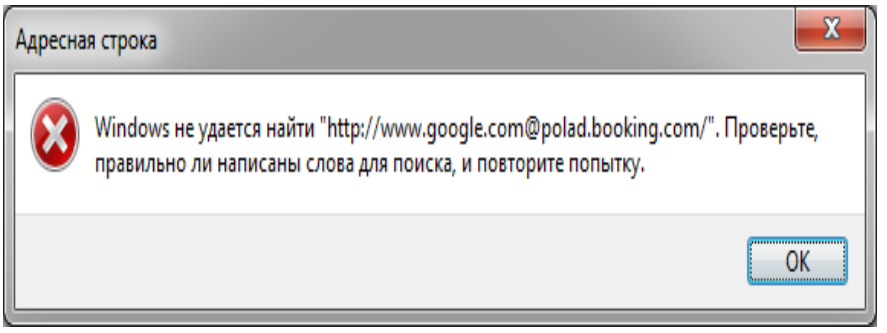
Müasir dövrdə ən çox istifadə olunan kiber hücum növlərindən saylan fişinq hücumlarının da özünə məxsus hücum texnikası vardır. Bu məqalədə bəzi fişinq hücum texnikaları ilə və onlara uyğun mübarizə üsulları ilə tanış olaq. Müasir dövrdə daha çox istifadə olunan və geniş yayılmış fişinq texnikaları əsasən aşağıdakılardan ibarətdir.

Fişinq hücumlarında veb- istinadların istifadəsi

Fişinq hücümlarının, metodlarının bəziləri veb- istinadlar vasitəsilə həyata keçirilir. Bu baxımdan fişinq metodlarının əksəriyyəti, müəyyən həqiqi təşkilatların istinadları altında konkret fişinq saytlarına saxta istinadları gizlətməyə gətirilir. Bu məqsədlə dolaşıq, səhf yazılmış ünvanlar və ya subdomenlər (Subdomen daha yüksək səviyyəli domenin bir hissəsidir) tez-tez fırıldaqçılar tərəfindən istifadə olunur.

Məsələn, müəyyən səhflərlə yazılmış http://www.yourbank.example.-com/ ünvanı Your bank adlı bankının ünvanına bənzəyir, amma əslində isə bu ünvan example.com saytının fişinq komponentinə yönləndirir. Bu sahədə başqa bir geniş yayılmış hiylə, xarici görünüşcə düzgün yazılmış istinadı, ünvanı fişinq saytına yönləndirməyi istifadə etməkdir. Məsələn, elə formalaşdırırlar ki, http://ru.wikipedia.org/wiki/Baku istinadı "Baku" məqaləsinə deyil, müəyyən fişinq komponentinə malik olan "York" məqaləsinə daxil olmağa səbəb olacaqdır.

Fişinq sahəsində əvvəllər geniş istifadə olunan aldatma metodlarından biri də, istifadəçi adını və şifrəsini linkə, istinada daxil etmək üçün istifadə olunan "@" simvolu daxil edilmiş linklərin, istinadların istifadə edilməsidir. Məsələn, http://www.google.com@polad.booking.com/ yazılışlı linki, istinadı www.google.com saytına deyil, www.google.com şəklində istifadəçisi adından polad.booking.com səhifəsinə keçidi təmin edir. Bu şəkildə fişinq hücumların qarşısını bəzən brauzerlər səviyyəsində almaq olur. Bu hücumların qarşısını almaq üçün müəyyən brauzerlərə konkret funksiyalar daxil edilmişdir. Belə fəaliyyəti Internet Explorer brauzeri qadağan edir, deaktiv edir. Məsələn, Internet Explorer brauzerində ünvan sətrində http://www.google.com@polad.booking.com/ ünvanını, linkini daxil etdikdə Internet Explorer heç bir səhifəyə keçidi təmin etmir və ekrana aşağıdakı kimi xəbərdarlıq pəncərəsi çıxır (şəkil 1).



Şəkil 1.

Mozilla Firefox və Opera brauzerləri isə belə ünvanlarla qarşılaşanda, bu haqda xəbərdarlıq edir və bu sayta keçidi təsdiqləmək üçün sizin təsdiqinizi təklif edir.

Başqa bir problem brauzerlər tərəfindən Beynəlxalq Domain Adlarını (Internationalized Domain Names (IDN))- milli əlifbaların simvollarını (məsələn, президент.рф) emal edən zaman aşkarlanır: məsələn, rəsmi ünvanla vizual olaraq eyni olan ünvanlar dələduzların saytlarına keçidi təmin edə bilər.

Filtrlərin yoxlanması üsulu

Fişerlər bəzən öz məqsədləri üçün mətn əvəzinə şəkillərdən də istifadə edirlər. Fişerlər tez-tez mətn əvəzinə şəkillərdən istifadə edirlər ki, bu da antifişinq filtrləri ilə saxta e-məktubları aşkarlamağı çətinləşdirir. Lakin mütəxəssislər bu növ fişinqlə necə mübarizə aparmağı da öyrənmişdilər. Beləliklə, poçt proqramlarının filtrləri ünvan kitabında olmayan ünvanlardan göndərilən şəkilləri avtomatik olaraq blok edə bilir. Bundan əlavə, spam və fişinq üçün istifadə olunan eyni növ şəkillərin imzaları ilə şəkilləri müqayisə və emal edə biləcək texnologiyalar da meydana gəlmişdir.

Veb- saytların istifadəsi

Fişinq hücumlarında aldatma qurbanın fişinq saytına baş çəkməsi ilə bitmir. Bəzi fişerlər ünvan sətrini dəyişdirmək üçün JavaScript- dən istifadə edirlər. Buna ya saxta URL ilə bir şəkil ünvan sətrinin üstünə qoymaqla və ya həqiqi ünvan sətrini bağlamaq və saxta URL ilə yenisini açmaqla nail olurlar.

Təcavüzkar həqiqi bir saytın skriptlərində zəifliklərdən istifadə edə bilər. Bu cür fırıldaqçılıq növü (saytlararası skriptinq kimi tanınır) daha təhlükəlidir, çünki istifadəçi hər şeyin həqiqi göründüyü (veb ünvandan sertifikatlara qədər) rəsmi veb saytın əsl səhifəsində avtorizasiya edir. Bu cür fırıldaqçılıq növü saytlararası skriptinq kimi də tanınır. Xüsusi bacarıqlar olmadan belə fişinq hücumlarını aşkarlamaq çox çətindir. Bu üsul ən böyük debet elektron ödəmə sistemi olan PayPal sisteminə də tətbiq edilmişdir.

Fişinqlik əleyhinə nəzərdə tutulan skanerlərə qarşı mübarizə aparmaq üçün fişerlər Flash texnologiyaya əsaslanan veb saytlardan istifadə etməyə başladılar. Flash texnologiya veb əlavələri və ya multimedialı təqdimatları yaratmaq üçün Adobe Systems şirkətinin multimedia platformasıdır. Bu texnologiyadan reklam plakatları, animasiyalar, oyunlar yaratmaq, habelə veb səhifələrdə video və səs yazıları ifa etmək üçün geniş istifadə olunur. Xarici olaraq, oxşar bir sayt orijinal sayta bənzəyir, ancaq burada mətn multimedia obyektlərində gizlidilir.

Fişinq hücumuna qarşı mübarizə üsulları

Fişinq hücumlarına qarşı mübarizədə müxtəlif üsullar mövcuddur. Bu mübarizə üsullarına, fişinqdən qorunmaq üçün hazırlanmış xüsusi texnologiyalar və qanunvericilik tədbirlər daxildir.

Fişinqlə mübarizə üsullarından biri insanlara fişinqi ayırd etməyi və bununla mübarizə aparmağı öyrətməkdir. Bu baxımdan da bu məqalə çox aktualdır. İnsanlar fişinqlik haqqında müəyyən biliklər əldə etməklə davranışlarını bir az dəyişdirərək fişinq təhlükəsini azalda bilərlər. Beləliklə, hesabın, xüsusəndə bank hesabının "təsdiqlənməsini" xahiş edən bir elektron məktuba cavab olaraq (və ya fişerlərin hər hansı digər adi istəyinə) mütəxəssislər, mesajın orijinallığını yoxlamaq üçün adından mesaj göndərilən şirkətlə əlaqə qurmağı məsləhət görürlər. Bundan əlavə, mütəxəssislər şübhəli mesajda hər hansı bir hiperistinadı istifadə etmək əvəzinə təşkilatın konkret veb ünvanını brauzerin ünvan sətrinə daxil etməyi məsləhət görürlər.

Əsas diqqət ediləsi məsələlərdən biri də ondan ibarətdir ki, təşkilatlardan demək olar ki, daxil olan bütün orijinal mesajlar, fişerlər üçün əlçatmaz olan müəyyən bəzi məlumatların qeydini ehtiva edir. Bəziləri, məsələn, məşhur PayPal ödəmə sistemi, müştərilərinə elektron formada həmişə adları ilə müraciət edir və bu sistemin adından "Hörmətli PayPal müştərisi" ümumi mesajı ilə göndərilən məktublar artıq bir fişinq hücumu cəhdi kimi qiymətləndirilə bilər. Banklardan və kredit təşkilatlarından gələn elektron məktublar özündə çox

vaxt hesab nömrəsinin bir hissəsini də saxlayır. Ancaq son tədqiqatlar insanların hesabın ilk rəqəmlərinin görünüşünü və ya son rəqəmlərin bir-birindən ayırmadığını, ilk rəqəmlərin isə maliyyə təşkilatının bütün müştəriləri üçün eyni ola biləcəyini göstərdi. İnsanlara heç bir xüsusi şəxsi məlumatı olmayan hər hansı bir məktubun şübhəli olduğunu izah edə bilərsiniz. Lakin 2006-cı ilin əvvəlindəki fişinq hücumları oxşar şəxsi məlumatları malik olurdu, buna görə də bu cür məlumatların mövcudluğu da hələ mesajın təhlükəsizliyinə zəmanət vermir. Bundan əlavə, digər başqa bir araşdırmalara görə, şəxsi məlumatların olması, hələ fişinq hücumlarının müvəffəqiyyət dərəcəsini əhəmiyyətli dərəcədə dəyişmədiyini, insanların əksəriyyətinin bu cür təfərrüatlara əhəmiyyət vermədiklərini göstərmişdir.

Fişinq hücumlarına qarşı ən geniş yayılmış mübarizə üsullarından biri də mübarizənin texniki metodlarıdır. Fişinqlə mübarizənin texniki metodları da geniş spektrə malikdir. Bu metodlar əsasən aşağıdakılardan ibarətdir.

Fişinq hücumları haqqında xəbərdarlıq edən brauzerlərin istifadəsi

Fişinq hücumlarından qorunmaq üçün vasitələrdən biri də İnternet- brauzerləri vasitəsilə mübarizədir. Fişinqlərlə mübarizə aparmaq üçün İnternet-brauzerlərində uyğun vasitələrdən istifadə edilir. Bununla bağlı olaraq fişinqlərdən qorunmaq üçün əsas İnternet- brauzerlərinin istehsalçıları istifadəçilərə fırıldaqçılara aid ola biləcək şübhəli sayt açdıqlarını bildirmək üçün eyni metodlardan istifadə etməyə razılıq vermişlər. Belə əsas brauzerlərin son yeni versiyalarında artıq "anti-phishing" adlandırılan bu imkan, xüsusiyyət vardır.

Fişinq hücumlarına qarşı mübarizənin başqa bir istiqaməti, əvvəlcə fişinq saytlarının siyahısını yaratmaq və sonradan onun əsasında müqayisələrin yoxlanılmasıdır. Belə sistemlər Internet Explorer, Mozilla Firefox, Google Chrome, Safari və Opera brauzerlərində mövcuddur. Firefox brauzeri Google şirkətinin antifişinq sistemindən istifadə edir. Opera brauzeri PhishTank və GeoTrust qara siyahılarından istifadə edir. 2006-cı ildə edilən bir müstəqil araşdırmaya görə, Firefox-un Internet Explorer-dən daha çox fişinq saytlarını aşkarlamaqda daha effektiv olduğu aşkar edilmişdir. Buna görədə fişinqlə mübarizəni gücləndirmək üçün daha Firefox brauzerindən istifadə etmək lazımdır.

Avtorizasiya prosedurunun çətinləşdirilməsi

Fişinq hücumlarına qarşı mübarizənin əsas texniki metodlarından biri də istifadəçilərin avtorizasiya prosedurunun çətinləşdirilməsidir. Bir qayda olaraq banklar və maliyyə sistemləri öz istifadəçilərinin avtorizasiyasını loqin və parolla həyata keçirirlər. Fişinqliyin qarşısını almaq üçün isə bu metod o qədər də kifayyət etmir. Ona görədə fişinqliklə mübarizəni gücləndirmək üçün əlavə tədbirlərində görülməsi zərurəti yaranır. Bu tipli əlavə tədbirlərə misal olaraq Amerikanın məşhur maliyyə mərkəzlərindən biri olan Bank of America saytını göstərmək olar. Amerikanın məşhur maliyyə mərkəzlərindən biri olan Bank of America saytı istifadəçilərə onların avtorizasiyası zamanı şəxsi təsviri seçməyi

də təklif edir və istifadəçinin seçdiyi bu şəkli hər parol daxil etmə formasında göstərir. Bu zaman həmin bank xidmətinin istifadəçiləri yalnız seçilmiş təsviri görəndə parol daxil etməlidirlər. Ancaq son bir araşdırma da göstərdi ki, görüntünün olmaması parol daxil edərkən əksər diqqətsiz istifadəçiləri də dayandırmır.

Məhz bu avtorizasiya metodunu Azərbaycanda fəaliyyət göstərən bank sistemləri tətbiq etsə daha faydalı olar və ölkəmizdə onlayn ticarət və ödəmə edənlərin təhlükəsizliyini kifayyət qədər artırmış olarlar. Çünki artıq ölkəmizdə də bu sahədə kiber cinayətkarlıq artmağa başlamışdır. Bunun haqqında 24 aprel 2020 tarixində azərtacın yaydığı məlumatda deyilir. (Bax:https://-azertag.az/xeber/Azerbaycanda_bank_sektoruna_qarsi_kibercinayetler_ toretmekde_teqsirli_bilinen_Bolqaristan_vetendaslari_saxlanilib_VIDEO-1471083). Məlumatda qeyd olunub ki, ölkənin bank sektoruna qarşı kiber cinayətlər törətməkdə təqsirli bilinən Bolqarıstan vətəndaşları saxlanılıb. Belə ki, Daxili İşlər Nazirliyinin Baş Mütəşəkkil Cinayətkarlıqla Mübarizə İdarəsinin əməkdaşları tərəfindən ölkə ərazisində bank sektoruna qarşı kiber cinayətlər törətməkdə təqsirli bilinən Bolqarıstan vətəndaşları Stoychev Marian Nikolov və Mladenov Vladislav Tsvetanov Bakı şəhəri ərazisində saxlanılıblar. "Müəyyən olunub ki, adları çəkilən şəxslər kibercinayətkarlıqda istifadə olunan xüsusi qurğular, eləcə də mikrosxemlər və digər ləvazimatlar vasitəsi ilə paytaxt ərazisində müxtəlif banklara məxsus bankomatlara müdaxilələr ediblər. Bu ilin fevral və mart aylarında ölkəmizə gələn qrup üzvləri əvvəlcədən hazırladıqları plana əsasən bankomat aparatlarına müdaxilələr edərək külli miqdarda pul vəsaitlərini mənimsəməyə cəhd göstəriblər. Onlar bankomat aparatlarının kart oxuyucu hissəsinə xüsusi qurğular yerləşdirərək bu yolla müştərilərə məxsus kartların PİN kodları barədə məlumatları əldə ediblər və kartların qeydiyyatını aparıblar" məlumatda deyilir.

Bu cinayətkarlarında məqsədi ödəmə kartlarının loqin və parollarını oğurlayaraq onlardan istifadə cəhdləri olmuşdur. Azərtacın yaydığı bu məlumat bu məqalənin ölkəmizdə də bu gün ən aktual olan təhlükəsizlik məsələlərindən birinə həsr olnur.

Elektron poçt məlumatlarında fişinqlə mübarizə vasitəsi

Aydındır ki, əksəriyyət fişinq hücumları istifadəçilərə əsasən e-poçt vasitəsilə göndərilir. Bunun üçün e- poçt sistemlərində xüsusi spam filtrlərindən istifadə edirlər. Xüsusi spam filtrləri istifadəçilər tərəfindən qəbul edilən fişinq e-poçtlarının sayını azalda bilir. Bu üsul, fişinq e-poçtlarını təhlil edərkən maşın öyrənməsinə və təbii dil işlənməsinə (Təbii dilin emalı (*Natural Language Processing, NLP*) süni intellekt və riyazi dilçiliyin ümumi istiqamətidir. Bu kompüter analizi və təbii dillərin sintezi problemlərini öyrənir) əsaslanır.

Maşın təlimi, öyrətməsi (İngilis *machine learning,* ML) - süni intellekt metodları sinifidir, xarakterik xüsusiyyəti bir problemin birbaşa həlli deyil, bir çox oxşar problemlərin həllərinin tətbiq etmək prosesinin təlimdir. Bu cür me-

todların qurulması üçün riyazi statistika, ədədi metodlar, optimallaşdırma metodları, ehtimal nəzəriyyəsi, qraflar nəzəriyyəsi, rəqəmli formada məlumatlarla işləmək üçün müxtəlif üsullardan istifadə olunur.

Təbii dilin emalı (*Natural Language Processing, NLP*) süni intellekt və riyazi dilçiliyin ümumi istiqamətidir. Bu kompüter analizi və təbii dillərin sintezi problemlərini öyrənir.

Monitorinq xidmətlərinin həyata keçirilməsi

Bəzi şirkətlər antifişinqliklə geniş miqyasda məşgul olmağı özlərinə fəaliyyət forması kimi seçmişdir. Bəzi şirkətlər, fişinq hücumlarına həssas olan banklar və digər təşkilatlara, gecə-gündüz monitorinq, analiz və fişinq saytlarının bağlanmasında kömək təklif edirlər. Fiziki şəxslər bu qruplara kömək edə bilərlər. Belə fəaliyyət formasi ilə məşğul olan misal olaraq PhishTank xidmətini göstərmək olar.

PhishTank– internet istifadəçiləri ilə əməkdaşlıqdan istifadə edərək, fişinqə qarşı yönəlmiş bir xidmətdir. Bu şirkət fişinqin təsdiqlənməsinin özünəməxsus sistemini təklif edir. Bu sistem internet istifadəçilərinin qarşılıqlı fəaliyyətinə əsalanır, belə ki, internet istifadəçilərinin bəziləri fişinq şübhəsi doğuran mənbələrə bağlantıları, linkləri nəşr edirlər, digər istifadəçilər isə bu qaynaqların fişinq olub olmadığına "səs verirlər". Beləliklə də mənbənin doğurdan da fişinq olması aşakarlanır. Bu baxımdan dünyada İnternetdə fişinq mənbələrinin aşkar edilməsində PhishTank ən əsas vasitələrdən biridir. Onu da qeyd edək ki, fişinq hücumlarına qarşı mübarizənin əsas vasitələrindən biri də hüquqi tədbirlərdir.

ОБ ОДНОМ КИБЕРАТАКЕ, КОТОРАЯ ШИРОКО РАСПРОСТРАНЕНА В НАШЕ ВРЕМЯ

ГУЛИЕВ Н.А.

РЕЗЮМЕ

В современном мире происходит переход к онлайн-активности. В частности, широкомасштабный переход к онлайн-активности ускорил период пандемии коронавируса, сделав его без альтернативой. Сегодня большая часть финансового оборота в мире осуществляется онлайн или с помощью платежных карт. Активность в Интернете, а также использование онлайн-платежей, широкое использование пластиковых карт в этой области также создает много неотъемлемых опасностей. В этой статье рассматриваются эти типы угроз и как с ними бороться. В связи с этим публикация этой статьи очень актуальна.

***Ключевые слова**: кибератака, фишинговая атака, фишер, виды фишинг-атак, антифишинг*

ABOUT ONE CYBER ATTACK, WHICH IS WIDESPREAD IN OUR TIME

QULIYEV N.A.

SUMMARY

In the modern world, the transition to online activity is taking shape. In particular, the large-scale transition to online activity has accelerated the period of the coronavirus pandemic, making it without an alternative. Today, most of the financial turnover in the world is carried out online or using payment cards. Online activity, as well as the use of online payments, the widespread use of plastic cards in this area also creates many inherent dangers. This article deals with these types of threats and how to deal with them. In this regard, the publication of this article is very relevant.

Keywords*: cyber attack, phishing attack, phishing, types of phishing attacks, anti-phishing.*