Тэма

Беражыце вашы грошы

Што рабіць, каб не патрапіць на «вуду» інтэрнэт-злачынцаў?

Высокія тэхналогіі, якія з кожным годам усё больш пранікаюць у наша жыццё, прыцягваюць і ўвагу злачынцаў. Сёлета за пяць месяцаў у гэтай сферы ўжо зафіксавана больш за тры тысячы парушэнняў закону. Прыкладна траціна з іх прыходзіцца на крадзяжы грошай з банкаўскіх плацежных картак. Падрабязней пра гэта расказалі спецыялісты ўпраўлення «К» Міністэрства ўнутраных спраў.

Зламыснікі часцей за ўсё выкарыстоўваюць два метады. Першы з іх — гэта так званая сацыяльная інжынерыя. «Нацягнуўшы» на сябе маску вашага знаёмага (для чаго нярэдка могуць узломвацца і акаўнты ў сацыяльных сетках), у нейкі момант да вас у асабістыя паведамленні «стукаецца» зламыснік. Ён можа прыкінуцца, напрыклад, супрацоўнікам банкаўскай установы або пакупніком тавару, якому трэба перавесці грошы. Размова можа пачацца здалёк, але ў выніку перапіска звядзецца да таго, што ў вас папросяць звесткі з вашай пластыкавай карткі. Мэта пры гэтым будзе заяўлена высакародная — напрыклад, аддаць грошы, якія чалавек цяпер просіць пазычыць.

Памятайце: нягледзячы на тое што ў Беларусі дзейнічае прынцып «нулявой адказнасці», банк мае права адмовіць вам у вяртанні грашовых сродкаў, калі вы самі перадалі зламысніку ўсе доступы да вашага рахунку. Таму гэта якраз той выпадак, калі ваша бяспека перш за ўсё ў вашых руках.

— У выпадку калі вам пішуць з нагоды набыцця нейкага тавару, нядобразычлівы суразмоўца прапануе перавесці перадаплату за тавар на банкаўскую плацежную картку. Маўляў, зараз ён знаходзіцца за мяжой і так яму зручней. Прычым якраз тут ён кажа праўду: як правіла, зламыснікі, якія праварочваюць такія справы, знаходзяцца па-за тэрыторыяй Беларусі. Далей яны просяць паведаміць нумар плацежнай карткі і тэрмін яе дзеяння. І вось гэта павінна стаць «чырвонай лініяй», за якую заходзіць нельга.

У ведамстве, аднак, канстатуюць, што ў абсалютнай большасці выпадкаў уладальнікі картак самі лёгка перадаюць іх рэквізіты сваім суразмоўцам. Больш за тое, яны нават паведамляюць змест SMS, якія прыходзяць ад банка на іх мабільныя тэлефоны, і іншую канфідэнцыяльную інфармацыю, якую мусіць ведаць выключна ўладальнік карткі. Яна прызначана для таго, каб спісваць грошы з рахунку. Гэта, напрыклад, трохзначны CVV-код, што размешчаны на адваротным баку пластыкавай карткі, сеансавыя паролі, код аўтарызацыі, пароль 3D-Secure. Ці пашпартныя звесткі.

— Другі распаўсюджаны метад выманьвання даных — фішынг. У перакладзе з англійскай мовы гэты тэрмін азначае «рыбалка». Вось толькі на кручок прасунуты «рыбак» падчэплівае занадта даверлівага чалавека. А ў такім выпадку метады фішынгу і сацыяльнай інжынерыі нярэдка камбінуюцца.

...У канцы мінулага года жыхарка Маладзечна вырашыла прадаць праз адну з гандлёвых пляцовак у сеціве тэлевізар. На сувязь з ёй у месенджары выйшаў адзін з меркаваных пакупнікоў. Ён пажадаў унесці колькі грошай у якасці перадаплаты, для гэтага папрасіў перадаць рэквізіты плацежнай карткі. Здавалася б, трывіяльная рэч для тых, хто нешта купляе праз інтэрнэт.

І вось цяпер пачынаецца самае цікавае. Праз колькі часу пакупнік зноў выходзіць на сувязь з гаспадыняй тэлевізара і паведамляе ёй пра тое, што, маўляў, транзакцыя з нейкай прычыны не прайшла. Пасля ён прапанаваў удакладніць, чаму гэта адбылося, непасрэдна ў банку. І даслаў ёй спасылку на сайт фінансавай установы.

Тут бы задацца пытаннем: чаму невядомы суразмоўца дасылае нейкія спасылкі, калі сайт банка адкрываецца па першым жа выніку запыту ў любым пошукавіку? Вось і аказалася, што пакупнік адправіў жанчыну на падроблены сайт. Мэта гэтай электроннай пляцоўкі ў адным: «выцягнуць» усе рэквізіты, неабходныя для правядзення аперацый на рахунку. Так у адзін момант небарака засталася без 20 тысяч долараў і 13 з паловай тысяч еўра.

Буйныя сумы грошай, якія вокамгненна «перацякаюць» у кішэню злачынцы, неаднаразова фігуруюць у падобных справах. У лютым гэтага года невядомы зламыснік займеў рэквізіты да пластыкавай карткі жыхара Мінска і скраў з карт-рахунку больш за 16 тысяч рублёў. Прыблізна такой жа сумы ў эквіваленце пазбавіўся і жыхар Рэчыцы — інтэрнэт-зламыснік «звёў» з яго карткі каля 7 тысяч беларускіх рублёў і 4 тысяч долараў ЗША.

Аднак інтэрнэт-злачынцаў цікавіць любая сума, якая ляжыць на вашым рахунку. Прыклад «наадварот» — калі махляром аказаўся не пакупнік, а прадавец. На адной з інтэрнэт-пляцовак ён размясціў аб'яву пра тое, што прадае дзіцячую каляску. На абвестку ў студзені гэтага года адгукнулася жыхарка сталіцы. Пачалася перапіска, падчас якой візаві пажадаў даведацца пра рэквізіты банкаўскай карткі пакупніцы. Хоць, здавалася б, навошта яму тыя звесткі? Гэта ж ён мусіць атрымаць грошы, а не яна. Але гэтая акалічнасць не насцярожыла жанчыну. Яна і выдала рэквізіты сваёй карткі, пасля чаго зламыснік перавёў з яе рахунку на свой суму прыкладна ў 800 рублёў.

— Схемы інтэрнэт-махлярства могуць быць вельмі разнастайныя. Гэта просьбы аб дабрачыннай фінансавай дапамозе, паведамленне пра выйгрыш у латарэю (у якой вы маглі і не ўдзельнічаць), прапановы дадатковага заробку. Часам яны выходзяць за межы выключна віртуальнай прасторы — вам можа пазваніць чалавек, які прадстаўляецца супрацоўнікам банка.

Спецыялісты ўпраўлення «К» МУС раяць падчас падрыхтоўкі да правядзення плацежных аперацый у інтэрнэце звяртаць увагу на некаторыя моманты. Гэта, папершае, вельмі нізкая цана на прапанаваны тавар, закліканая прыцягнуць да сябе ўвагу. Але зноў жа, нельга сказаць, што кожны, хто хоча штосьці прадаць танней, абавязкова з'яўляецца махляром. А вось спробы любым шляхам атрымаць рэквізіты вашай банкаўскай карткі — ужо трывожны званочак. На многіх інтэрнэт-пляцоўках рэалізавана сістэма абароны ад віртуальнага махлярства: напрыклад, пакуль вы не пацвердзіце, што атрымалі тавар, грошы будуць заблакіраваны на транзітным рахунку. Злодзеі гэта ведаюць і таму імкнуцца працягнуць гутарку ў інтэрнэт-месенджары або праз электронную пошту. А пераход на любыя дасланыя вашым суразмоўцам спасылкі з высокай доляй імавернасці цягне за сабой пераадрасацыю на падроблены сайт.

«Схемы інтэрнэт-махлярства могуць быць вельмі разнастайныя. Гэта просьбы аб дабрачыннай фінансавай дапамозе, паведамленне пра выйгрыш у латарэю (у якой вы маглі і не ўдзельнічаць), прапановы дадатковага заробку. Часам яны выходзяць за межы выключна віртуальнай прасторы — вам можа пазваніць чалавек, які прадстаўляецца супрацоўнікам банка».

— Лепш за ўсё аформіць асобную картку для пакупак анлайн і на выпадак выезду за мяжу. Пераводзіць туды грошы найлепш незадоўга да здзяйснення меркаванай транзакцыі. Што да картак, якія выкарыстоўваюцца ў Беларусі, то не будзе лішнім абмежаваць да іх доступ з іншых краін — такую магчымасць банкі даюць. Логін і пароль да інтэрнэт-банкінгу трэба ўводзіць толькі на ўласных смартфоне і камп'ютары, да якіх не маюць доступ пабочныя асобы. Лепш таксама ўсталяваць ліміт на максімальную суму грашовай аперацыі. Вельмі пажадана ўключыць двухфактарную аўтэнтыфікацыю і SMS-апавяшчэнне.

А што рабіць, калі невядомы тэлефануе і прадстаўляецца супрацоўнікам банка? Трэба ведаць, што банкаўскія супрацоўнікі не будуць запытваць у вас па тэлефоне асабісты нумар, пашпартныя звесткі і рэквізіты саміх картак. Але калі вы сутыкнуліся з такой сітуацыяй, то ператалефануйце ў банк на нумар, указаны на афіцыйным сайце фінансавай установы.

І памятайце: нягледзячы на тое што ў Беларусі дзейнічае прынцып «нулявой адказнасці», банк мае права адмовіць вам у вяртанні грашовых сродкаў, калі вы самі перадалі зламысніку ўсе доступы да вашага рахунку. Таму гэта якраз той выпадак, калі ваша бяспека перш за ўсё ў вашых руках.

Міліцыянер выратаваў бяздомнага

Здарэнне адбылося ў Гродне 25 мая. Прапаршчык міліцыі Сяргей Піліпчык нёс службу па ахове Генеральнага консульства Польшчы. Раптам ён убачыў, што з аднаго з дамоў, размешчаных непадалёк, ідзе дым. Міліцыянер паведаміў пра ўбачанае ў дзяжурную часць і накіраваўся да месца пажару.

— Дом гэты аказаўся закінутым, — паведамілі ў Дэпартаменце аховы МУС. — Унутры яго Сяргей Піліпчык убачыў разведзенае вогнішча. Побач з ім спаў мужчына. Мяркуючы па знешнім выглядзе, там быў бяздомны. Полымя ўжо дайшло да матраца, на якім ляжаў чалавек, пачынала тлець і яго вопратка. Прапаршчык міліцыі выцягнуў небараку на свежае паветра і неадкладна выклікаў хуткую дапамогу.

Тое, што міліцыянер падаспеў на дапамогу, уратавала бяздомнаму жыццё. Медыкі дыягнаставалі нязначнасць апёкаў, аказалі першую дапамогу. Шпіталізацыя не спатрэбілася.

Зайсці ў музей анлайн

У маі гэтага года ўласны сайт займеў музей Міністэрства ўнутраных спраў. Віртуальная пляцоўка месціцца па адрасе: museum.mia.by.

Цяпер наведаць экспазіцыю аддалена можна ў літаральным сэнсе гэтага слова. Справа ў тым, што на сайце музея рэалізавана магчымасць 3D-тура — вы можаце падарожнічаць па яго залах, седзячы перад экранам манітора. Асабліва гэта важна цяпер, калі з-за распаўсюджвання каранавіруса работа музеяў у нашай краіне часова прыпынена.

Фонд музея складаюць фотакопіі арыгіналаў дакументаў, архіўных фотаздымкаў, здымкі табельнай і канфіскаванай зброі, знакаў адрозненння і ўзнагарод, асабістых рэчаў, рэчавых доказаў, службовай тэхнікі...

Сярод прадстаўленых выяў экспанатаў ёсць і вельмі цікавыя. Напрыклад, у раздзеле «Рэчавыя доказы» ёсць здымак фальшывага савецкага пашпарта, датаванага 1970 годам. Выдадзены ён на імя Луны Артура Аганесавіча. На тое, што пасведчанне асобы падробленае, паказваюць дзве рэчы. Па-першае, яго ўладальнік нібыта нарадзіўся ў горадзе Нікалаеве Хабараўскага краю, а такога населенага пункта ў тым рэгіёне ніколі не было. А па-другое, нацыянальнасць грамадзяніна Луны пазначана як «марсіянін».

А сярод асабістых рэчаў міліцыянераў увагу прыцягвае швейцарскі гадзіннік Paul Moser. Ён быў падораны работніку міліцыі Васілю Лазарэнку ў 1927 годзе з нагоды 10-годдзя ўтварэння праваахоўнага органа. На вечку гадзінніка — дароўны надпіс па-беларуску.

Адпачынак без «прыгод»

Нягледзячы на тое што гэтай вясной прырода мала радавала беларусаў добрым надвор'ем, у месцах адпачынку сёлета зарэгістравана ўжо больш за сто злачынстваў.

— На жаль, адпачынак на беразе вадаёмаў для многіх людзей звязаны з распіццём алкагольных напояў ці піва, што ў зонах адпачынку і на пляжах катэгарычна забаронена, — адзначыў **намеснік начальніка арганізацыйна-аналітычнага ўпраўлення міліцыі грамадскай бяспекі МУС Сяргей ГАРОХАЎ. —** Гэта адміністрацыйнае правапарушэнне, якое цягне за сабой штраф у памеры да васьмі базавых велічынь. І між іншым такія выпадкі складаюць каля траціны ўсіх зарэгістраваных парушэнняў. Але купанне і спіртное несумяшчальныя — гэта адна з самых распаўсюджаных прычын гібелі на вадзе.

Таксама ў месцах адпачынку нярэдкія выпадкі выкрадання веласіпедаў, мабільных тэлефонаў, кашалькоў. Сярод іншых распаўсюджаных парушэнняў — паркоўка, купанне і развядзенне вогнішчаў у забароненых месцах. Напрыклад, аматарам пасмажыць шашлыкі на такой тэрыторыі давядзецца раскашэліцца на 12 базавых велічынь, а «несанкцыянаваным» купальшчыкам — на суму да трох.

— Сумесна з падраздзяленнямі МНС, Таварыства ратавання на водах і прыродаахоўнымі арганізацыямі плануецца праводзіць сістэматычныя рэйды, звяртаючы асаблівую ўвагу на месцы адпачынку, размешчаныя паблізу сталіцы і абласных цэнтраў, бо там канцэнтруецца найбольшая колькасць людзей, — дадаў Сяргей Гарохаў.

Матэрыялы паласы падрыхтаваў Валяр'ян ШКЛЕННІК.