Варта адзначыць, што ў апошні час пачасціліся выпадкі супрацьпраўных дзеянняў у сферы інфармацыйных тэхналогій, а менавіта крадзяжоў з БПК і рахункаў фізічных і юрыдычных асоб, прыклады падобных фактаў прыведзены далей.

1. Зламыснік пасля несанкцыянаванага доступу да старонак карыстальнікаў у сацыяльных сетках рассылае карыстальнікам, якія знаходзяцца ў раздзеле «Сябры», паведамленні з просьбай аб аказанні дапамогі ў перакладзе грашовых сродкаў пад рознымі падставамі: «Прывітанне, ці не мог ты пазычыць мне грошы, аддам праз пару дзён», «Прывітанне, пакладзі, калі ласка, 10 рублёў на тэлефон, я аддам», «Прывітанне, можна я перавяду табе на карту свае грошы, а то ў мяне скончыўся тэрмін дзеяння карты (ці не атрымліваецца перавесці на сваю)». Далей уваходзіць у давер да неабыякавых карыстальнікаў і, нібыта для пераводу ім грашовых сродкаў, просіць паведаміць рэквізіты БПК і коды з смс-паведамленняў. Карыстальнік, уведзены ў зман адносна асобы, якая ажыццявіла паказаную рассылку, і не здагадваючыся аб злачыннасці намераў, паведамляе яму названыя звесткі, з прычыны чаго зламыснік атрымлівае доступ да грашовых сродкаў карыстальніка і здзяйсняе іх крадзеж.

Правёўшы несанкцыянаваную аперацыю па перакладзе грашовых сродкаў, зламыснік часта паведамляе карыстачу, што па тэхнічных прычынах не можа ажыццявіць аперацыю і просіць паўтарыць названыя дзеянні з якой-небудзь іншай картай (сваякоў ці знаёмых).

2. На гандлёвых пляцоўках «Куфар», «Барахолка» і іншых правапарушальнік знаходзіць аб'яву, размешчанае карыстальнікам аб продажы якой-небудзь маёмасці, пасля чаго ў розных мэссэнджарах піша дадзенаму карыстачу аб тым, што хацеў бы набыць яго маёмасць, названую ў аб'яве, аднак па розных прычынах не мае магчымасці за ім прыехаць. Ён прапануе вырабіць аплату шляхам пераводу грашовых сродкаў на БПК карыстальніка і, пасля таго як карыстальнік згаджаецца, высылае ў яго адрас спасылку з фішынгавай старонкай сайта якой-небудзь банкаўскай установы (старонка можа быць візуальна падобная са старонкай інтэрнэт-банкінгу і адрозніваецца толькі сімвалам у адрасным радку даменнага імя сайта). Пераходзячы па паказанай спасылцы, карыстальнік не заўважае, што знаходзіцца не на дзеючай старонцы інтэрнэт-банкінгу пэўнага банка.

У акне, якое адкрылася на паказаным сайце карыстачу, як правіла, прапануецца ўвесці свой лагін і пароль ад інтэрнэт-банкінгу альбо пашпартныя даныя, а таксама коды з смс-паведамленняў. Увёўшы паказаную інфармацыю карыстачу, як правіла, паведамляецца пра памылку або адсутнасці плацяжу. У гэты час усю уведзеную інфармацыю бачыць зламыснік і ўводзіць на сапраўдным сайце банка, атрымліваючы тым самым доступ да грашовых сродкаў карыстальніка і здзяйсняючы іх

крадзеж. Правёўшы несанкцыянаваную аперацыю па перакладзе грашовых сродкаў, правапарушальнік нярэдка паведамляе карыстачу, што па тэхнічных прычынах не можа ажыццявіць аперацыю, і просіць паўтарыць названыя дзеянні з якой-небудзь іншай картай (сваякоў ці знаёмых).

3. На гандлёвых пляцоўках «Куфар», «Барахолка» і іншых зламыснік размяшчае аб'яву аб продажы якой-небудзь маёмасці, якая карыстаецца попытам, і выстаўляе цану, як правіла, ніжэй рыначнай. Карыстальнікі, якія ўбачылі аб'яву, пішуць асобе, якая яго размясціла, і ў ходзе перапіскі зламыснік паведамляе, што не мае магчымасці сустрэцца для перадачы названай ў аб'яве маёмасці і прапануе скарыстацца паслугамі «Дастаўка Куфар», «Белпошта (ЕМС)», «кур'ерская служба (СДЭК)» і т. д. Пры згодзе пакупніка зламыснік высылае ў адрас карыстальніка спасылку з фішынгавай старонкай сайта якой-небудзь дастаўкі, дзе прапануецца ўвесці рэквізіты банкаўскай карты для аплаты тавару, паслуг курьера, пашпартныя даныя, нумар мабільнага тэлефона, а таксама коды з смс-паведамленняў. Пасля ўводу гэтай інфармацыі карыстачу звычайна паведамляецца пра памылку небудзь сайт перастае загружацца (завісае). У гэты час усю ўведзеную інфармацыю бачыць зламыснік і ўводзіць яе на сапраўдным сайце банка, атрымліваючы доступ да грашовых сродкаў карыстальніка і здзяйсняючы іх крадзеж. Правёўшы несанкцыянаваную аперацыю па перакладзе грашовых сродкаў, зламыснік паведамляе карыстачу, што па тэхнічных прычынах не можа ажыццявіць аперацыю і просіць паўтарыць названыя дзеянні з якой-небудзь іншай картай (сваякоў ці знаёмых).

4. На мабільны тэлефон фізічнай асобы паступае ўваходны званок ад зламысніка. Як правіла, дадзеным спосабам зламыснік карыстаецца сэрвісам па падмену нумара тэлефона і паказвае абаненцкі нумар, які належыць якому-небудзь банку або падобны з ім. Далей ён прадстаўляецца супрацоўнікам банка (можа назваць карыстальніка па імені і па бацьку, а таксама назваць частку нумара банкаўскай карты або інфармацыю аб нядаўна зробленых аплатах). Зламыснік паведамляе аб падазроных аперацыях па пераводзе буйных сум грашовых сродкаў на карт-рахункі замежных банкаў. Калі карыстальнік паведамляе, што ніякіх аперацый ён не рабіў, зламыснік паведамляе, што названыя аперацыі неабходна заблакіраваць, у сувязі з чым просіць карыстальніка паведаміць асобныя рэквізіты БПК або пашпартныя даныя, і паведамляе, што ў адрас карыстальніка высылае смс-паведамленні з кодамі, якія неабходна назваць пасля гукавога сігналу. У гэты час усю атрыманую інфармацыю зламыснік уводзіць на сапраўдным сайце банка, атрымлівае доступ да грашовых сродкаў карыстальніка і здзяйсняе іх крадзеж.

5. На мабільны тэлефон фізічнай асобы паступае ўваходны званок ад зламысніка. Як правіла, пры дадзеным спосабе махлярства зламыснік карыстаецца сэрвісам па падмену нумара тэлефона і паказвае абаненцкі

нумар, які належыць якому-небудзь банку або падобны з ім. Далей ён прадстаўляецца супрацоўнікам праваахоўных органаў (міліцыянерам, следчым) (можа назваць карыстальніка па імені і па бацьку, а таксама назваць частку нумара банкаўскай карты або інфармацыю аб нядаўна зробленых аплатах). Зламыснік паведамляе аб тым, што на імя пацярпелага ад неўстаноўленага супрацоўніка банка ўзяты крэдыт, і з мэтай устанаўлення дадзенага супрацоўніка банка, у цяперашні час праводзіцца спецаперацыя і пацярпеламу неабходна прыняць у ёй удзел, а менавіта – узяць крэдыт на сваё імя (у адным або некалькіх банках). Пасля атрымання крэдыту просіць прадаставіць звесткі аб карце, або самастойна пералічыць грашовыя сродкі на паказаны ім рахунак з мэтай анулявання крэдыту. У наступным прапануе накіравацца ў іншы банк, або проста спыняе зносіны з пацярпелым. У далейшым пацярпелы пазнае, што на яго імя аформлены крэдыт (або крэдыты), а грашовыя сродкі выкрадзеныя неўсталяванай асобай.

6. На мабільны тэлефон фізічнай асобы (як правіла пажылым сваякам) паступае ўваходны званок ад зламысніка. Як правіла, дадзеным спосабам зламыснік карыстаецца сэрвісам па падмену нумара тэлефона і паказвае абаненцкі нумар, які належыць якому-небудзь банку. Далей ён прадстаўляецца супрацоўнікам праваахоўных органаў (міліцыянерам, следчым) і паведамляе, што сваяк пацярпелага трапіў у ДТЗ і знаходзіцца без памяці (або часам даюць пагутарыць па тэлефоне нібыта з дачкой, сынам, мужам і да т.п., якія ў ходзе размовы просяць дапамагчы) і сваяк вінаваты ў дадзеным ДТЗ і для «вырашэння» пытання просяць перадаць праз курьера канверт з грашовымі сродкамі. Пасля чаго прыязджае кур'ер і забірае дадзеныя грашовыя сродкі.

Уся запытаная злачынцам паказаная ў вышэй пазначаных сітуацыях інфармацыя вядома супрацоўнікам банка, якія не ўсталёўваюць яе ў ходзе тэлефоннай размовы.

Для таго каб засцерагчы сябе і свае грашовыя сродкі ад падобных спосабаў крадзяжу, неабходна:

не выдаваць лагіны, нумары тэлефонаў, паролі, пін-коды, рэквізіты разліковых рахункаў, сакрэтныя CVC/CW-коды, даныя датычна апошніх плацяжоў і тэрміну дзеяння пластыкавых карт трэцім асобам;

у ходзе выкарыстання карты падключыць і выкарыстоўваць тэхналогію «3D Secure». На сапраўдны момант – гэта самая сучасная тэхналогія забеспячэння бяспекі плацяжоў па картках ў сетцы Інтэрнэт. Дазваляе адназначна ідэнтыфікаваць сапраўднасць трымальніка карты, які ажыццяўляе аперацыю, і максімальна знізіць рызыку махлярства па карце. Пры выкарыстанні гэтай тэхналогіі трымальнік банкаўскай карты пацвярджае кожную аперацыю па сваёй карце спецыяльным аднаразовым

паролем, які ён атрымлівае ў выглядзе SMS-паведамлення на свой мабільны тэлефон;

выключыць перадачу староннім асобам атрыманыя ў SMS-паведамленнях часовыя паролі для пацверджання аперацый, а таксама сваіх банкаўскіх карт, якім бы там ні было спосабам;

уводзіць сакрэтныя даныя толькі на сайтах, абароненых сертыфікатамі бяспекі і механізмамі шыфравання. Даменныя імёны гэтых рэсурсаў у адрасным радку кожнага браўзэра пачынаюцца з https://;

выконваюць рэгулярны маніторынг выкананых аперацый, выкарыстоўваючы раздзел з гісторыяй плацяжоў;

не адмаўляцца ад дадатковага ўзроўню бяспекі (сістэмы шматузроўневай аўтэнтыфікацыі);

падабраць складаны пароль, выкарыстоўваючы набор лічбаў, загалоўных і малых літар, які будзе зразумелы толькі ўладальніку акаўнта. Мяняць пароль кожныя 2-4 тыдня, калі карыстаецеся чужымі кампутарамі для ўваходу ў сістэму інтэрнэт-банкінгу;

не ўжываць аўтаматычнае запамінанне пароляў у браўзэры, калі да персанальнага кампутара адкрыты доступ староннім асобам або для ўваходу на сайт выкарыстоўваецца кампутар агульнага доступу;

у ходзе выкарыстання інтэрнэт-банкінгу ўсталёўваць антывірусную абарону, своечасова абнаўляючы базы даных вірусаў і шпіёнскіх утыліт;

уваход у асабісты кабінет на сайце інтэрнэт-банкінгу прывязаць да MAC або IP-адрасу. Гэта дзеянне забяспечыць максімальны ўзровень бяспекі;

у выпадку просьбаў узяць крэдыт, самастойна звярнуцца ў банкаўскую ўстанова (або асабіста, або па абаненцкім нумарах, названых на афіцыйным сайце з гарадскога тэлефона) з мэтай удакладнення ці маецца на яго імя крэдыт. Не паддавацца на ўгаворы ўзяць на сябе якія-небудзь грашовыя абавязацельствы;

не ўдзельнічаць у «спецаперацыях па тэлефоне» (у выпадку правядзення спецаперацыі, супрацоўнікі міліцыі звяртаюцца асабіста, з прадстаўленнем службовага пасведчання і з абавязковым прадстаўленнем адпаведных дакументаў асобе, з якой ён знаёміцца і падпісвае). Супрацоўнікі міліцыі ніколі не праводзяць «спецаперацыях па тэлефоне» і не адпраўляюць фатаграфію свайго службовага пасведчання ў месенджарах;

не паддавацца на ўгаворы невядомых асоб, якія прадстаўляюцца супрацоўнікамі праваахоўных органаў, на перадачу ім грашовых сродкаў. Супрацоўнікі праваахоўных органаў Рэспублікі Беларусь ніколі «не вырашаюць» пытанні аб неўзбуджэнні крымінальнай справы шляхам перадачы ім грашовых сродкаў ці іншых паслуг. Адным з прыярытэтных напрамкаў дзейнасці праваахоўных органаў Рэспублікі Беларусь з'яўляецца

барацьба з карупцыяй, пры паступленні аналагічных званкоў, або прапаноў ад супрацоўнікаў аб дачы ім хабару, неадкладна спыняць дыялог з дадзенымі асобамі (незалежна ад таго размова была па тэлефоне, або асабіста) і паведамляць у службу «102», або па гарачай ананімнай лініі ў МУС.

У выпадку выяўлення згубленай кім-небудзь БПК не варта выкладваць яе фатаграфію ў сетцы Інтэрнэт з мэтай пошуку ўладальніка. Інфармацыі, якая маецца на малюнку БПК, дастаткова для здзяйснення аперацый з выкарыстаннем гэтых дадзеных без ведама ўладальніка банкаўскай карты, чым і карыстаюцца зламыснікі.