РАДАБАНК

# Рекомендації щодо кібербезпеки та запобігання шахрайству

Зараз популярна тенденція відмовлятись від готівки на користь платіжних карток, тому що це дійсно зручно й досить безпечно, якщо дотримуватись певних правил та уникати небезпечних ситуацій. Клієнтам Банку важливо знати про способи шахрайства з платіжними картами, що допоможе не стати жертвою зловмисників.

Фішинг (за допомогою листів), смішинг (СМС) та вішинг (телефоном) — найпоширеніші атаки на клієнтів банків. Це прийоми так званої соцінженерії.

*«Це з банку»: фішинг*

Фішинг — це електронні листи від шахраїв, які хитрощами вивідують особисті, фінансові чи пов'язані з безпекою дані.

Як улаштований прийом

Надходить лист:

· подібний до справжніх електронних листів з банку: з логотипом, звичним оформленням і стилем;

· з формулюваннями, що спонукають діяти, наприклад: «Брак негайної відповіді загрожує штрафом!»;

· у листі просять завантажити додаток чи перейти за посиланням.

Кіберзлочинці покладаються на зайнятість жертв: на перший погляд фальшиві листи схожі на справжні. Внаслідок цього, адресат сприймає написане всерйоз і діє згідно із задумом зловмисника.

Як діяти

· Оновлювати програмні засоби, зокрема, браузер, антивірус, операційну систему.

· Особливо пильнувати, якщо «з банку» вимагають таємну інформацію (скажімо, ваш пароль до системи клієнт-банк). Справжній банк спілкується лише захищеним каналом, наприклад, коли ви ввійшли до системи «Клієнт-Банк».

· Ретельно перевіряти, чи немає в листі розбіжностей або чогось безглуздого. Наприклад, нуль замість літери «О». Навести курсор на адресу відправника й подивитися, яка справжня адреса з'явиться. За можливості, порівняти адресу з попередніми справжніми листами з банку. Перевіряти, чи немає помилок у правописі.

· Не відповідати на підозрілі листи, натомість пересилати їх до банку, вводячи його адресу вручну.

· В жодному разі не клацати на посиланнях і додатках, вводити адреси в браузері вручну.

· Обережно з мобільними пристроями! Спробу фішингу може бути важче виявити на телефоні чи планшеті. Навести мишку на підозріле посилання не

можна, на меншому екрані важче помітити навіть очевидні помилки. Якщо лист фальшивий, повідомте банк, — про прийоми шахрайства мають знати всі. У разі будь-чого сумнівного зв'язуватися з банком.

*«Це з банку»: вішинг*

Вішинг (від слів «Voice» у значенні «голосовий зв'язок», і «фішинг»): шахрай телефонує й переконує жертву повідомити особисті, фінансові чи пов'язані з безпекою дані або переказати гроші.

Як діяти

· Пильнувати в разі дзвінків, не ініційованих вами.

· Спитати, з якого номера телефонують, і сказати, що ви перетелефонуєте. Для перевірки дізнатися номер названої організації (на її веб-сайті або через пошукову систему) й зателефонувати за цим номером.

· Не використовувати номер, повідомлений людиною, яка телефонувала.

· Шахраї можуть знайти ваші дані в Інтернет (зокрема, в соціальних мережах). Наявність цих даних — ще не доказ, що телефонує не шахрай.

· Не переказуйте нікому гроші на вимогу телефоном. Працівники банків цього ніколи не просять.

· Якщо дзвінок видався шахрайським, повідомити в банк.

*«Це з банку»: СМС*

Смішинг (від слів «СМС» та «фішинг»): шахраї надсилають текстові повідомлення, щоб вивідати особисті, фінансові чи пов'язані з безпекою дані. Шахрай удає довірену особу — співробітника банку, оператора зв'язку, підприємство комунальних послуг.

Як улаштований прийом

Надходить СМС з вимогою (здебільшого, нагальною) перейти за посиланням чи перетелефонувати на певний номер, щоб «перевірити» або «відновити» рахунок. Посилання веде на фальшивий сайт, а з номера відповідає шахрай, що видає себе за співробітника компанії. Шахраї намагаються вивідати будь-які відомості, що допоможуть вкрасти у вас гроші.

Як діяти

· Якщо надійшло несподіване СМС, не відкривати посилання, додатки, графіку, спершу перевірити відправника. Номер можна пошукати в Інтернет (якщо то був шахрай, хтось міг про це вже написати) або порівняти зі справжнім номером компанії, представника якої вдає шахрай.

· Зберігати спокій. Не квапитися, перевірити все до пуття, перш ніж реагувати.

· Не відповідати на СМС, де вимагають реквізити платіжної картки, пароль до системи «Клієнт-Банк» чи особисті дані, що стосуються безпеки.

· Якщо ви відповіли на СМС, надали банківські реквізити, а згодом запідозрили, що це смішинг, слід негайно сповістити банк.

«Доброго дня, шановний клієнт, ваша картка буде заблокована банком у зв'язку…»

Але середньостатистичний «шановний клієнт» чув про такі шахрайські фокуси і вже із підозрою ставиться до подібних дзвінків. Тому, зрозумівши, що клієнт вчиться, шахраї почали працювати більш хитро і тонко.

Сама схема принципово не змінилася, змінилися лише деякі технічні параметри, але сам «злам мозку клієнта», як і раніше, відбувається через вухо.

Крім того, якщо раніше типовою жертвою таких «розводів» були люди похилого віку, то зараз ситуація змінилася. Вік і стать тепер не мають значення та не впливають на здатність протидіяти оновленим шахрайським схемам.

Вашій увазі декілька найпоширеніших сьогодні шахрайських схем, що, як і раніше, кінцевою метою мають заволодіння вашими грошима.

*IVR (система голосових меню)*

Пересічний громадянин, як ми і писали у вступі, вже вчений і ляканий. Свідомо і підсвідомо боїться вже він виказувати різні секретні дані телефоном. Та шахраї і цей факт використовують на свою користь, підкріплюючи ці побоювання: «Нікому не кажіть СМС-код, який вам зараз прийде» – попереджають злочинці свою майбутню жертву. Після чого просять переключитися на IVR (інтерактивне голосове меню), який залізним робо-голосом просить ввести цей секретний СМС-код у тоновому режимі після сигналу… І легко зчитують (підслуховують) набрані цифри.

А код цей, як ви вже здогадалися, це код підтвердження про виведення коштів з рахунку або про вхід у Інтернет-банк жертви.

*Віддалений доступ (Remote desktop)*

Шахрай, назвавшись співробітником служби безпеки банку, повідомляє «шановного клієнта»-жертву, що його (клієнта) смартфон чи комп'ютер заражений жахливим вірусом, а дбайливий банк терміново хоче допомогти його позбутися. Для цього жертві надають посилання для завантаження програми, яка наче допоможе співробітникам банку «вилікувати» заражений пристрій, за яким наляканий «клієнт» завантажить програму віддаленого доступу.

Сама по собі ця програма не є шкідливою, але надає вона шахраєві повний доступ до смартфону (комп'ютеру). Це може бути TeamViewer, AnyDesk, RemotePC або якась інша схожа програма.

Після встановлення такої програми злочинцям ще потрібен код доступу, який відображається в цій програмі. Якщо назвати ще й цей код, то шахрай, в залежності від ОС і виробника смартфону жертви, отримає:

Android (наприклад, Samsung) — повний віддалений доступ до смартфону жертви. Шахрай здійснює платежі зі смартфону жертви, оскільки коди підтвердження операцій надходять на нього ж.

Apple iOS і деякі смартфони на Android (наприклад, Nexus) — шахрай отримає дозвіл на перегляд екрана. Шахрай керує діями клієнта («Натисніть тут, а тепер тут»). В результаті клієнт сам перераховує кошти шахраям.

*«Безпечний рахунок»*

Знову-таки зі «служби безпеки банку» телефонують жертві і повідомляють, що її рахунок у небезпеці (от-от буде заблоковано, або якісь злодії почали виводити кошти) і пропонують жертві не гаяти дорогоцінних секунд, а переказати усі кошти на «безпечний рахунок».

Звісно, що «безпечний рахунок», це рахунок шахрая. Але у такій ситуації наляканий «клієнт», як правило, робить переказ не думаючи.

Можливий ще й варіант, коли «клієнта» попросять терміново підійти до найближчого банкомата (з функцією cash in) і негайно зняти усі гроші. Якщо клієнту далеко до банкомата, то навіть таксі пропонують оплатити…

Коли готівку знято, – вимагають одразу ж покласти ці кошти на «безпечний рахунок» через той самий банкомат. Якщо «клієнт» починає вагатись та щось підозрювати, його залякують штрафами, пенею, судом та іншими страшними санкціями. Часто цього достатньо, – і жертва сама зробить поповнення рахунку шахраїв знятою перед цим готівкою.

*Операція «Переадресація»*

Нічого не ускладнюючи, замість складної психологічної обробки «клієнта», назвавшись «співробітником банку» чи «служби безпеки банку», шахраї просять набрати на телефоні якусь послідовність символів… Ця послідовність у дійсності є USSD-командою мобільному оператору на ввімкнення переадресації усіх вхідних дзвінків жертви на інший номер. І номер цей, звісно є номером шахраїв, й усі СМС-повідомлення з банківськими паролями та кодами тепер надходитимуть туди.

Крім цього, можуть запитати ще й персональні дані, за допомогою яких потім видаватимуть себе за клієнта під час звернення до коллцентра або для відповіді на дзвінки від справжньої служби безпеки банку.

Захист

• Вірити не можна нікому!

• Покладіть слухавку та самостійно зателефонуйте до банку за номером, що зазначений на звороті вашої картки.

• Не розголошуйте жодних реквізитів вашої картки (за винятком її номера), а також банківські SMS коди та паролі мобільних операторів.

• Ніколи не встановлюйте жодних програм чи застосунків з функціоналом віддаленого доступу на прохання банківських співробітників.

• Не виконуйте USSD-команди на телефонні вимоги банківських співробітників.

• За жодних обставин не переказуйте на прохання банківських співробітників ваші кошти на будь-які інші рахунки та рахунки третіх осіб.

Виходячи з тієї небезпеки, яка нависла над Україною у вигляді глобальної пандемії COVID-19, важливо знати, що це не лише серйозна загроза для нас та наших близьких, але і серйозний виклик для нашої кібербезпеки. Паралельно з

коронавірусом світом поширюється і платіжне шахрайство, що експлуатує тему пандемії. Страх та психічна нестабільність, яка нерідко переходить у паніку, відкрила шахраям нове вікно можливостей. Вірусом і жахаючими новинами створено ідеальне підґрунтя для різного роду шахрайських атак.

Хоча самі ці шахрайські схеми і не є новими (усі вони старі і загальновідомі та лише адаптовані під актуальні корона-новини), але посилення тривоги та страхів, підвищений попит на засоби індивідуального захисту та фармацевтичну продукцію, зайнятість правоохоронних органів у процесі забезпечення громадського порядку, збільшення часу перебування громадян у мережі Інтернет – усі ці фактори, діючи разом, підривають загальний антишахрайський імунітет і критичне мислення громадян. Найпоширеніші схеми «коронашахрайства»:

*Фейковий продаж усього антикоронавірусного*

Дезинфікуючі засоби, ліки, вакцини, тести, медичні маски, рукавички, «антикоронавірусне варення», «дезинфікуючі свічки» тощо. Товари, які рекламуються, можуть бути підробленими або взагалі неіснуючими. Головне – не поспішайте з передоплатою. Робіть її тільки перевіреним продавцям!

*Виявлення коронавіруса «на районі»*

Віруси-крадії маскуються під мобільні додатки, які наче вміють у реальному часі відстежувати спалахи коронавірусу на вашій вулиці, місті, країні. Після встановлення такої програми спалах відбувається у вашому телефоні або комп'ютері. Файли на пристрої блокуються. Далі злочинці вимагають викуп.

*Шахрайскі онлайн-сервіси(курси, розваги, доставка тощо)*

Онлайн-курси з додаткового заробітку в Інтернет, курси з вивчення іноземних мов, підписки на онлайн-кінотеатри та бібліотеки, онлайн-фітнес та тренування, мобільні застосунки для доставки їжі, ліків та алкоголю, онлайн-консультації сімейного лікаря, психо-вірусолога тощо.

*Шкідливі посилання на сайти «відстеження COVID-19»*

Електронною поштою або месенджером від шахраїв надходить інформація про поширення COVID-19 з посиланням на сайт «авторитетної» організації, де є онлайн-карта поширення захворення (наприклад, сайт ВООЗ), а насправді – посилання на фішинговий сайт, який викрадає логіни та паролі.

*Фішингові сайти оплати комунальних послуг*

За час карантину значно зросла кількість громадян, що почали сплачувати комунальні послуги онлайн. Відповідно побільшало і шахрайських (фішингових) сайтів, які «працюють» під виглядом платіжних онлайн-сервісів, а насправді – викрадають гроші або карткові реквізити.

*«Вашого сина відправили на обсервацію з коронавірусом»*

Це адаптація під COVID-19 загальновідомої схеми «Ваш син у відділку». Тепер нічні дзвонарі повідомляють самоізольованим людям, що їхній син,

донька чи онук відправлені на обсервацію. Далі шахраї від імені лікарів пропонують спробувати дорогу сироватку та диктують номер картки, на яку потрібно перерахувати кошти.

*Перевірка даних по кредитам під час карантину*

Шахраї телефонують громадянам від імені банків або мікрофінансових організацій під легендою «Перевірка даних, щоб уникнути штрафів за невчасну сплату кредитів під час карантину». А насправді – виманюють карткові реквізити, банківські SMS-коди та інформацію для віддаленої ідентифікації у банку.

*«Пенсійне посвідченя недійсне» – дзвінки з «ПФУ»*

«Пенсійне посвідчення на час карантину буде недійсним», – кажуть шахраї, телефонуючі і так не на жарт наляканим коронавірусом пенсіонерам. І коли спантеличена жертва «підвисає», пропонують негайно переказати заощадження на нову картку, начебто відкриту на ім'я пенсіонера

*Шахрайство у туристичній індустрії*

Для тих, хто ще до початку пандемії купив путівки, квитки на літак, забронював готель тощо, але не встиг відпочити через спалах коронавірусу та усесвітній карантин і зараз шукає можливість повернути свої гроші – саме для них відкрилася безліч шахрайських сервісів з «повернення коштів».

BEC-атаки: «У нас змінився банківский рахунок»

Шахрай під виглядом постачальника звертається телефоном або електронною поштою до співробітника компанії, який відповідальний за оплату товарів, та повідомляє про зміну банківских реквізитів у зв'язку зі спалахом коронавірусу та надає для оплати свої власні реквізити.

Вербовка мулів. Мулам приготуватися!

Злочинці використовують поточну кризу, вербуючи грошових «мулів» для різних брудних схем з відмивання грошей. Шахраї створили фіктивну організацію Vasty Health Care Foundation і вербують «відмивальників» під прикриттям боротьби з коронавірусом... Схема активно «працює» закордоном, але готуватися потрібно вже і нам.

*«Я знаю твій маленький брудний секрет»*

Sextortion — це онлайн-вимагання, коли шахраї роблять масову розсилку електронною поштою, переконуючи отримувачів листів, що в їхньому розпорядженні є відео-компромат на отримувача. Щоб запис нікуди не потрапив, потрібнозаплатити викуп у біткоїнах. Насправді ж, як водиться, немає ані злому, ні запису. Тепер шахраї змінили погрозу і залякують тим, що інфікують коронавірусом сім'ю жертви, в разі відмови сплатити викуп. Для правдоподібності в тексті листа вказується пароль жертви від електронної

пошти. Поки подібні фішингові листи надсилаються англійською мовою, українські громадяни не поспішають поповнювати біткоїн-гаманець вимагача, але, якщо Nikita напише листа своєю рідною мовою або дасть в листі посилання на онлайн-перекладач, грошова сума на його рахунку може суттєво збільшитись.

ВАЖЛИВО:

- У жодному раз не платіть!
- Перевірте свою адресу через базу відомих зламаних електронних скриньок та паролів www.haveibeenpwned.com. Якщо ваша серед них — змініть паролі до пошти та інших важливих сервісів, якщо пароль у них був однаковий.

*Коронавірус електронною поштою*

Нещодавно кіберзлочинці організували фішингову розсилку від імені Центра громадського здоров'я МОЗ України з «останніми достовірними даними про коронавірус» з прикріпленим документом, що містив зловред, який, завантажуючись на пристрій, надавав зловмисникам віддалений доступ до нього.

ВАЖЛИВО:

- Бути пильними та ні в якому разі не розслаблятися, думаючи, що сайт з онлайн-мапою поширення COVID-19 або посилання на сайт для проведення телеконференції є стовідсотково безпечними.
- Припинити розсилати особисто не перевірені факти від «знайомих» та «друзів». Інакше, замість того, щоб стати Бетменом, що рятує країну від коронавірусу, ви перетворитесь на спільника кіберзлочинців, який збільшує число їхніх жертв.
- Встановіть на свій девайс надійний антивірус.
- Уважно ставтеся до листів з невідомих адрес з підозрілими вкладеннями та посиланнями.
- Якщо під час відкриття файлу, прикріплене до листа, у вас запитується дозвіл на виконання контенту «Enable Content», – особливо пильнуйте!

*«Переможемо коронавірус разом!» – опитування від шейхів*

Шахраї пропонують перемогти коронавірус, пройшовши опитування від арабської фармацевтичної компанії, яка «ударними темпами веде розробку вакцини від SARS-CoV-2».

Все, що потрібно, це зареєструватися на сайті, відповісти на декілька питань та отримати винагороду у розмірі 2000 доларів США. Звідки гроші на опитування? — все просто! Спонсорами виступають найбагатіші люди Сходу. Після того, як ви відповісте на декілька простих питань, накшталт «Чи є у вас температура, кашель або інші симптоми?», вам повідомлять, що 2000 доларів — ваші, але, вам потрібно сплатити податок на отримання коштів у розмірі 5 доларів. Не чекайте на хепіенд! Ви втратите не тільки 5 доларів, але й усі гроші з вашого рахунку.

ВАЖЛИВО:

- Перед тим як брати участь в опитуванні, потрібно перевірити всю інформацію щодо нього: назву компанії та опитування, адресу сайту, відгуки в Інтернет тощо.

- Запам’ятати раз і назавжди: одержувач виграшу особисто не сплачує податків, — вони утримуються з суми винагороди шляхом її зменшення на суму податків.

*Трендові товари з фейковою «OLX-Доставкою»*

На дошці оголошень OLX шахрай виставляє на продаж трендовий товар за низькою ціною. Якщо покупець «клюнув», шахрай переводить спілкування в месенджер. Далі він сам пропонує OLX-доставку, нібито все чесно і безпечно, і скидає посилання на її оформлення. Але проблема у тому, що це посилання веде на фішинговий сайт, який тільки зовні виглядає як сайт OLX. Скориставшись цим посиланням, покупець здійснює оплату прямісінько на карту шахрая. У схемі, яка працює з 2019 року, не змінилося нічого, окрім «наживки» — трендових товарів, що виставляються шахраями на продаж. Якщо раніше це були товари компанії Apple, то у сучасних реаліях трендовими стали захисні маски, антисептики й металошукачі. Чому металошукачі? — тому що городяни кинулися з міст у свої заміські будинки, грибів ще немає, — шукають скарби.

ВАЖЛИВО:

- Не переходити для спілкування в месенджери!
- Шахраїв багато, а OLX-сайт один — OLX.UA(мобільна версія — m.olx.ua).
- Всі угоди з «OLX Доставка» — робіть тількив особистому кабінеті на OLX.UA.

*SMS пенсіонерам про «Вовину тисячу»*

Вже через тиждень після заяви Зеленського про майбутню доплату пенсіонерам 1000 гривень, шахраї почали розсилку SMS-повідомлень від нібито Національного Банку України. Громадянин, який отримав SMS-повідомлення щодо нарахування йому грошей, але не отримав самих грошей, телефонує за довідковими телефонами, що вказані в SMS-повідомленні, шахраї випитують у нього особисті дані та реквізити карти, щоб нібито перевірити, чому сталася помилка і він досі не отримав нарахованої тисячі гривень.

ВАЖЛИВО:

- Подібні SMS — це шахрайство. Національний Банк не нараховує і не виплачує соціальну допомогу.
- У разі отримання подібних SMS та необхідності отримання консультації потрібно перетелефонувати за номером, вказаним на офіційному сайті або на звороті банківської картки(якщо SMS — від банку), а не за номером, вказаним у SMS.
- Нікому, ніколи, за жодних умов не повідомляти телефоном тризначний код зі звороту банківської картки та SMS-паролі, отримані від банків та мобільних операторів.

За матеріалами Української міжбанківської Асоціації членів платіжних систем «ЄМА» https://www.ema.com.ua