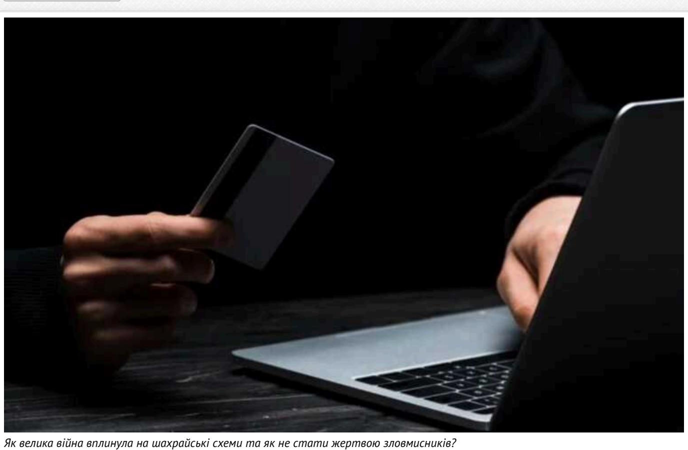
Як велика війна вплинула на шахрайські схеми та як не стати жертвою зловмисників?

Читать на русском



Як велика війна вплинула на шахрайські схеми та як не стати жертвою зловмисників?

Війна аніскільки не заважає шахраям виманювати гроші в українців та вигадувати для цього нові схеми. Навпаки – воєнні часи дозволили їм урізноманітнити свої інструменти. Хоча банки вдосконалюють свої системи безпеки, вони не можуть захистити людей від їх довірливості.

Напередодні в Україні почала набирати обертів нова схема: пропозиція легкого заробітку в інтернеті за "лайки" в соцмережах. Шахраї навіть оплачують перші "завдання", втираючись у довіру своїх жертв, однак потім виманюють у них набагато більші суми. Зловмисники пристосувалися до війни та використовують проти людей їхні тривожність та фінансову безграмотність, а також скрутне становище в економіцізая видання "Економічна правда".

Як виманюють гроші: основні схеми

"Основними типами шахрайства в Україні залишаються фішинг та соціальна інженерія, зважаючи на вразливість населення у зв'язку із ситуацією в країні. Їх частка становить майже 80% від усіх видів шахрайства, які ми фіксуємо в інтернет-просторі", – повідомили ЕП в пресслужбі Приватбанку.

Фішинг – це спосіб виманити в людини дані банківської картки за допомогою інтернет-ресурів. Для цього шахраї створюють копії сайтів банків, інтернет-магазинів чи платіжних систем. Проводячи на таких сайтах оплату, жертва вносить туди свої банківські дані, після чого шахраї отримують доступ до її банківського рахунку.

Шахраї можуть створити не лише копію відомого сайту, а й новий сайт. Часто таким чином створюють інтернет-магазини техніки та гаджетів з привабливими цінами.

"Клієнт проводить оплати на сайті як звичайний платіж в інтернеті, вводячи дані картки та підтверджуючи платіж. Часто після успішного списання коштів жертва певний час не розуміє, що відбулося шахрайство, оскільки впевнена, що це платіж за товар і вона його скоро отримає", – пояснює голова правління "Універсал банку" Ірина Старомінська.

Ще один варіант фішингу пов'язаний з використанням служб доставки – "Нової пошти", DHC, "Укрпошти". Жертвам може прийти повідомлення про доставку посилки і необхідність сплатити за неї кошти. Для проведення розрахунків шахраї пропонують перейти за посиланням на фішинговий сайт, який імітує сайт служби доставки.

Соціальний інжиніринг – це складніші схеми: зловмисники намагаються зробити так, аби жертва добровільно переказала їм кошти або назвала конфіденційну банківську інформацію, нічого при цьому не запідозривши. Для цього шахраї можуть втертися в довіру до цієї людини, зокрема видавши себе за знайомого чи родича жертви.

Інколи зловмисники можуть зламати акаунт людини в соцмережах та отримати доступ до її листування. Проаналізувавши діалоги, шахраї обирають близьких та друзів жертви, які можуть погодитися без зайвих запитань надіслати гроші "для вирішення термінової проблеми". Це можуть бути проблеми із здоров'ям або затримання правоохоронцями, тоді злочинці просять гроші нібито на хабар.

Поширеними є випадки, коли шахраї телефонують жертві та представляються працівниками служби безпеки банку або представниками державного органу, якому особа може довіряти. Для більшої переконливості для таких схем зловмисники завчасно отримують певну інформацію про свою жертву, зокрема її повне ім'я.

"Шахраї можуть представитися працівниками безпеки банку чи НБУ. Після цього клієнт повідомляє їм реквізити платіжної картки, пароль до дистанційного банківського обслуговування, otp-паролі, надіслані клієнту з використанням технологій 3D Secure, що дозволяє переказувати кошти на рахунки в інших банках", – відзначають у Нацбанку.

Зловмисники часто намагаються грати на почутті страху. Вони представляються представниками банку і лякають жертв тим, що до їх рахунків отримали доступ шахраї або що кошти будуть заблоковані через підозрілу фінансову активність. Іноді зловмисники гратють на позитивних емоціях, наприклад, обіцяють захмарні виграші.

"Сценарій майже однаковий для всіх: стороння особа надає клієнту сумнівну схему, за якою начебто клієнт стовідсотково отримає виграш. Клієнт переказує кошти цій особі, як правило, не один раз, адже шахраї пояснюють, що так більше шансів виграти", – пояснює Старомінська.

Банки навчилися реагувати на більшість таких схем. Зокрема, для доступу до банківського застосунку або проведення операції банки можуть зателефонувати клієнту або надіслати йому додатковий код-підтвердження.

Також банки налаштували свої системи так, аби виявляти підозрілу фінансову поведінку. Такі підозрілі операції можуть блокуватися, а разом з ними – і рахунки шахраїв. Це дозволяє банкам відбивати більшість "атак" і навіть повертати жертвам кошти. Наприклад, антифрод-система Приватбанку дозволяє попереджувати 90% спроб несанкціонованих платежів. Такі ж показники ефективності мають аналогічні системи і в інших великих українських банках.

"Алгоритми антифрод-системи здійснюють скоринг кожної операції. Якщо модель виявляє нетипову поведінку для клієнта, антифрод-система залежно від типу аномальної операції може тимчасово заблокувати транзакцію для додаткової її верифікації через дзвінок клієнту або заблокувати доступ до онлайн-банку чи картки клієнта, щоб унеможливити здійснення з ними шахрайства поза межами онлайн-банкінгу", – каже начальник управління менеджменту інформаційної безпеки "Райффайзен банку" Олексій Скиба.

Однак розвиваються не лише системи безпеки банків, а й шахрайські схеми. Вони пристосовуються і до умов війни.

Як пристосовуються шахрайські схеми

Після початку великої війни обсяги шахрайства різко скоротилися, кажуть представники великих банків. "У 2022 році було значне зменшення числа випадків шахрайства. Це пояснюється тим, що з початку війни старі схеми втратили актуальність з точки зору легенд та внутрішніх процесів у шахрайських центрах", – відзначає пресслужба "А-банку".

Зловмисникам знадобився час, щоб виявити, як можна використати війну для отримання неправомірних доходів. Як наслідок, у 2023 році банки фіксують суттєвий приріст шахрайських операцій.

"З початку 2023 року спостерігається зростання випадків соцінжинерії та фішингу відносно до аналогічного періоду 2022 року орієнтовно на 20%. Цьому сприяє довірливість населення, що опинилося в складних життєвих умовах. Злочинці легко до цього адаптуються, підлаштовуючи схеми до умов сьогодення", – додають у Приватбанку.

Зростання кількості випадків шахрайства у 2023 році фіксує і Національний банк. Зокрема, там виявили збільшення числа звернень українців, які скаржилися на такі схеми.

Мета шахраїв – зробити так, аби людина їм довірилася та погодилася переказати гроші. Зловмисники підлаштовують свої схеми до актуальних подій та роблять їх правдоподібними.

Так, після початку великої війни стала поширеною схема з нібито зарахуванням коштів від держави, Червоного хреста чи ООН. Жертви довіряли шахраям, адже різні грошові допомоги справді виплачувалися людям, наприклад, на деокупованих територіях.

"Обман полягає в тому, що для отримання виплати вимагається її ініціювання через особистий кабінет онлайн-банкінгу банку. Клієнт, перейшовши на фішинговий сайт за посиланням у повідомленні, вводить логін та пароль на фішинговому сайті, шахраї паралельно отримують ці дані та вводять їх на легітимному сайті онлайн-банкінгу.

Якщо введені шахраями дані коректні, то банк відправляє смс на фінансовий номер клієнта для додаткового підтвердження входу. Клієнт вводить код підтвердження на фішинговому сайті, шахраї перехоплюють цей пароль, вводять на дійсному сайті й отримують доступ до онлайн-банкінгу", – пояснив Скиба.

Також поширеними стали фейкові збори на допомогу армії. Часто їх проводять від імені відомих волонтерів, зокрема створюючи їхні фейкові сторінки в соцмережах. У Нацбанку серед шахрайських схем воєнного часу виділили фейкові збори на допомогу переселенцям, малозабезпеченим і навіть плату нібито за евакуаційні перевезення (шахраї отримують передоплату за евакуацію з небезпечних районів, а потім зникають).

Зловмисники не лише адаптують легенди, а й присовуються до систем безпеки банків. Наприклад, якщо банк запровадив тимчасові обмеження до рахунку клієнта-жертви, то шахраї можуть проводити платіж не одразу, а через деякий час, коли такі обмеження припинять діяти.

Інвестиції та робота в інтернеті

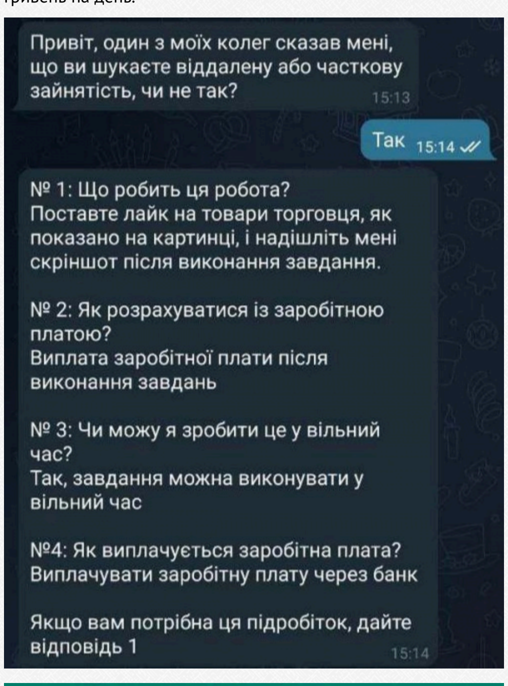
Мабуть, найскладнішими схемами з виманювання грошей є обіцянки заробітків за допомогою інвестицій або виконання простої роботи в інтернеті, наприклад, ставити "лайки" в інтернет-магазинах або соцмережах.

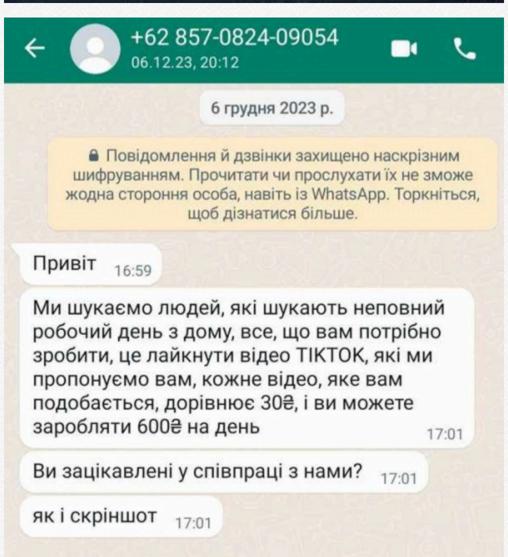
Для таких схем зловмисники створюють спеціальну інфраструктуру, наприклад, сайт з "особистим кабінетом" інвестора-жертви, наймають юристів, менторів та брокерів, організовують курси, де "вчать інвестуванню". Такі проєкти відстежує Національна комісія з цінних паперів та фондового ринку і публікує перелік сумнівних ресурсів.

Суть схеми полягає в тому, що шахраї пропонують людині варіанти дуже вигідного вкладання коштів, обіцяючи захмарну прибутковість. Довірившись зловмисникам, жертва отримує доступ до "свого електронного кабінету" і певний час бачить, як зростає її рахунок. Зловмисники зацікавлені в тому, аби виманити в людини якомога більше коштів, а жертва, спостерігаючи за "ростом" свого капіталу, наївно вірить у ці обіцянки.

Проблеми починаються тоді, коли людина хоче забрати гроші. Навіть тоді шахраї намагаються виманити кошти нібито для оплати комісій чи податків. Коли ошукана особа відмовляється платити, злочинці обривають з нею всі контакти.

Друга схема називається "робота в інтернеті". Останнім часом вона набула особливої популярності. Зловмисники розсилають людям повідомлення з пропозиціями дистанційного працевлаштування. Суть роботи – ставити "лайки" в соцмережах або позитивні оцінки товарам в інтернет-магазинах. Сума винагороди – кілька сотень гривень на день.





Перший "заробіток" зловмисники дійсно виплачують. Таким чином вони завойовують довіру та переходять до другої частини схеми. Жертву просять внести кошти нібито для купівлі товару з метою його перепродажу.

"Кошти, які клієнт переказує, ідуть на картки таких самих жертв. Ті переказують їх наступним жертвам. При спробах вивести кошти клієнта вмовляють зробити наступні платежі, пояснюючи це комісіями та податками. Коли людина відмовляється платити, чат блокують і з нею більше не контактують", – пояснює Старомінська.

Якщо людина відмовляється переказувати кошти, то їй пропонують стати "фінансовим помічником": на її рахунок переказують гроші та надсилають перелік рахунків та суми для "виплати зарплат".

Банкам складно протидіяти таким схемам, оскільки зловмисники майже не використовують власні банківські рахунки, а розраховуються з жертвами з рахунків таких самих жертв.

Лише клієнти monobank в листопаді втратили на таких схемах близько 65 млн грн. Жертвами шахраїв стали 3 тис клієнтів. Кількість жертв та суми збитків могли бути набагато більшими, каже співзасновник проєкту Олег Гороховський. За його словами, банку вдалося запобігти 70% випадків фейкового заробітку в інтернеті.

Як не стати жертвою шахраїв

Рекомендації щодо того, як не потрапити на гачок шахраїв, прості та давно відомі, проте банки не припиняють на них наголошувати.

Перше і найголовніше – ніколи не розголошувати банківські дані, передусім CVV-код, логіни та паролі до банківських застосунків, PIN-код від банківської картки та одноразові паролі, які надсилає банк для підтвердження операції. Ні працівники банку, ні представники НБУ, СБУ чи ООН ніколи не телефонують клієнтам, аби запитати конфіденційну банківську інформацію.

"Працівники банку ніколи не будуть вас запитувати про ці дані. Якщо ви отримуєте дзвінок або електронний лист, у якому просять надати цю інформацію, сміливо припиніть комунікацію", – говорить Скиба.

Щоб не попастися на фішинг, слід уважно вивчати сайти, з яких планується здійснення оплати. Будь-які відмінності в URL-адресі можуть свідчити про підробку. Інколи справжній сайт відрізняється від підробки одним символом.

"Якщо необхідно перейти на сайт компанії, адресу якого ви отримали в посиланні, введіть у пошуковій системі назву необхідного сайту і лише тоді переходьте на вебресурс", – рекомендують у Нацбанку. Регулятор також рекомендує налаштувати багатофакторну автентифікацію для входу до своїх акаунтів у соцмережах та в електронну пошту.

Протидіяти соцінжинірингу можна лише шляхом критичного оцінювання інформації. Якщо людина отримала повідомлення від члена сім'ї чи близького знайомого з проханням про допомогу, слід зв'язатися з ними альтернативними каналами та впевнитися, що їх акаунти або номери телефонів не зламані.

"Донатити" потрібно лише перевіреним організаціям та волонтерам. Якщо якийсь збір роблять від імені відомої людини, варто перевірити, чи згадує ця людина про нього у своїх соцмережах.

Обіцянки швидких заробітків потрібно сприймати максимально критично. Якщо хтось пропонує інвестувати в цінні папери, криптовалюту чи інші інструменти, обіцяючи захмарні відсотки, не варто поспіхом переказувати гроші. Щонайменше, слід перевірити брокера чи ресурс, куди пропонують інвестувати: пошукати інформацію про них та перевірити, чи нема їх у переліку шахрайських схем, який створила НКЦПФР.

"Завжди пам'ятайте: якби ці "фінансисти" знайшли схему простого примноження коштів, вони б самі вклали туди всі свої гроші, а не шукали б вас і не сиділи б на відсотках від вашого "портфеля". Це працює завжди. Той, хто знайшов "золоту гору", ніколи не розповість про неї незнайомцям", – додає Старомінська.

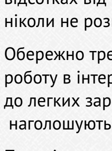
Обережно треба ставитися і до заробітків в інтернеті. "Не вкладайте власні гроші за роботу в інтернеті – у більшості випадків це пропозиції від шахраїв. Будьте уважними до легких заробітків; не сплачуйте жодних послуг, щоб оформитися на роботу", – наголошують в НБУ.

Пильність та критичне мислення – найкращі вартові особистих коштів.

Автор: Ярослав Вінокуров

Джерело: Економічна правда

Теги: Гороховский Олег, А-банк, Райффайзенбанк, Райффайзен банк Аваль, Скиба Алексей, DHC, Укрпошта, Укрпочта, Нова Пошта, Новая почта, фішинг сайти, фишинговые сайты, Приватбанк, Война, Війна, Шахраї, Мошенники, Мошенничество, Шахрайство



Марія Войтенко
ОГЛЯДАЧ НОВИН

15 січня 2024 г., 15:15 · Переглядів: 2885 · Коментарі: 0

Роздрукувати | Надіслати товаришу

Коментарі:

comments powered by Disqus

2013-2026 © АНТИКОР — національний антикорупційний портал
Реклама на сайті • Наші партнери
Політика конфіденційності
Використання матеріалів сайту дозволено лише за наявності активного гіперпосилання на джерело. Усі права на тексти, зображення, фотографії та відеоматеріали належать їх авторам.