СЕКЦІЯ 2
АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Фішинг як сучасний вид інтернет-шахрайства з банківськими платіжними картками та заходи з профілактика цього кримінального злочину

Вайда Т.С.
кандидат педагогічних наук, доцент
доцент кафедри спеціальної фізичної та вогневоїпідготовки
Херсонського факультету ОДУВС

Актуальність проблеми. Інтернет-шахрайство з банківськими картками в Україні стає все більш масовим негативним явищем з того часу, відколи громадяни стали активно користуватися цим платіжним інструментом.

Небезпечність піднятої нами проблеми підтверджується не тільки значним збільшенням кількості крадіжок грошей у власників платіжних карток, а й фіксацією правоохоронцями нових схем афер (перехоплювачі клавіатури, спеціально розроблені веб-сайти, поштові повідомлення, складені за всіма правилами соціальної інженерії тощо). З іншого боку, самі громадяни добровільно залишають багато особистої інформації в базах даних супермаркетів, інтернет-магазинів (наприклад, OLX, «Розетка», Leboutique, Work, Parfums, Makeup, тощо) при заповненні анкетних даних (ПІБ, місце та рік народження, моб. телефон і т.д.), котрі зловмисники можуть використати у своїх корисних цілях.

За даними системи «Exchange-Online» та Української міжбанківської асоціації членів платіжних систем (ЕМА) щодо випадків шахрайства з використанням платіжних інструментів, у 2016 році 63 % всіх крадіжок коштів з карт здійснювалось шляхом інтернет-шахрайства. Ще 24 % крадіжок грошей вчинялось через банкомати, 9 % − через системи інтернет-банкінгу і 4 % через POS-термінали (еквайрингова мережа). На думку заступника директора ЕМА О. Данильченко, така тенденція сформувалась за останні два роки − шахраї зосередили свою увагу саме на власниках платіжних карток [1].

Частіше за все паролі і дані платіжних карток в українців виманюють або через спеціально створені сайти (фішинг), або способом особистого спілкування шахраїв з жертвою по телефону (вішинг). У першому випадку злочинці використовують сайти, призначені для переведення грошей з однієї картки на іншу, поповнення рахунку мобільних телефонів і т.п. Як зазначають фахівці ЕМА, перший такий сайт у списку результатів пошукового запиту буде фішинговим з ймовірністю до 98 %. За минулий рік кількість таких ресурсів зросло в 4,5 рази: з 38 одиниць у 2015 році до 174 одиниці у 2016-му. За 1-2 дня фішинговий сайт може зкомпроментувати біля 800-2500 платіжних карт [1].

Стан розробленості проблеми. Визначення умов щодо подальшого удосконалення профілактики шахрайства як кримінального злочину та розробка ефективних шляхів організації боротьби з цим негативним соціально-економічним явищем знайшла своє відображення в наукових дослідженнях багатьох вчених, які розглядували різні аспекти цієї проблеми.

Зокрема, О.В. Смаглюк розглядав комплекс теоретичних і практичних питань, пов'язаних із дослідженням суті, змісту, сутності та юридичної природи кримінально-правової норми про відповідальність за шахрайство (ст. 190 ККУ), поняття обману, зловживання довірою; вченим уточнено склад цього злочину та кваліфіковані його види [2]. О.В. Кравченко досліджувала комплекс правових, кримінологічних та психологічних проблем, пов'язаних з шахрайством як одним із високолатентних і суспільно небезпечних способів злочинної діяльності; вченим дослідником проведено психологічний аналіз загальної схеми шахрайської операції, визначено її основні компоненти, маніпулятивні техніки, прийоми та засоби впливу шахрая на свою жертву; встановлені психологічні особливості мовного впливу шахрая на свою жертву, запропоновані шляхи профілактики шахрайства [3].

В.Р. Мойсик здійснив кримінально-правову характеристику шахрайства з фінансовими ресурсами (ст. 222 КК України), приділивши увагу детальному розкриттю змісту елементів і ознак складів цього злочину; вченим вперше комплексно розглянуто питання кваліфікації шахрайства з фінансовими ресурсами за чинним ККУ [4]. А.А. Патик комплексно досліджував сучасні проблеми взаємодії слідчих та оперативно-розшукових підрозділів як умови забезпечення розкриття та розслідування майнових злочинів [5]. Р.М. Крикливий досліджував проблеми підтримання державного обвинувачення у справах про шахрайство [6]. Ю.Л. Шуляк провела комплексний порівняльно-правовий

аналіз питань теоретичного та прикладного характеру щодо кримінальної відповідальності за шахрайство [7].

Разом з тим, таким аспектам піднятої нами актуальної для сучасного суспільства проблеми, як попередження інтернет-злочинності, припинення та притягнення до відповідальності осіб, які здійснюють шахрайство з платіжними картками вченими приділялось недостатньо уваги. Вимагає додаткового розгляду питання щодо підвищення дієвості профілактики вказаного злочину в контексті зростання рівня банківського сервісу, котрим (платіжними картами) активно користуються громадянами для зручності та мобільності розрахунків. Це дозволяє конкретизувати мету нашого дослідження та визначити пріоритетність вирішуваних завдань у цій роботі.

Метою роботи є розгляд фішингу як найбільш поширеного методу інтернет-шахрайства, завдяки котрому правопорушниками для заволодіння коштами власників банківських платіжних карт використовуються їх реквізити, а також надання громадянам рекомендацій для потенційного уникнення таких життєвих ситуацій.

Пропоноване дослідження проведено у відповідності до тематичного плану науково-дослідної роботи Одеського державного університету внутрішніх справ із проблеми «Пріоритетні напрямки розвитку та реформування правоохоронних органів в умовах розгортання демократичних процесів у державі» (державний реєстраційний № 0116U006773).

Результати дослідження. Розглянемо особливості фішингу як одного з видів шахрайств, котрі застосовуються злочинцями для крадіжки коштів з платіжних банківських карт.

Фішинг (підробні сайти) – назва цього прийому шахраїв походить від англ. fishing (рибалка, лов на живця) [8]. Як свідчить практика, це досить розповсюджена технологія інтернет-шахрайства, котра полягає у крадіжці приватної конфіденційної інформації (паролів доступу, даних банківських карт та ін.) шляхом введення в оману їх користувачів-власників. Тільки за останні роки число веб-сайтів, котрі призначені для крадіжки персональних даних, збільшилось в десятки разів (дані звіту робочої групи APWG (Anti-Phishing Work GroupPhishing Activity Trends Report 2nd Half) [1].

Технологія інтернет-шахрайства завдяки розповсюдженої в інтернет-мережі значної кількості підроблених веб-сайтів полягає в наступному: 1) імітація «один до одного» представництва крупних чи дрібніших банків та інших фінансових кредитних організацій (доменні імена, фірмовий стиль цих сайтів, їх зміст тощо) часто важко відрізнити від оригіналу, тобто є майже дзеркальним відображенням справжніх веб-сайтів банківських установ; 2) мета подібних «ресурсів» – отримати конфіденційну фінансову інформацію від відвідувачів сайту, для чого використовуються свідомо помилкові банківські реквізити та інша контактна інформація.

Схема фішингу проста: завдяки спамерським розсиланням або поштовим вірусам потенційним жертвам в надії на їх наївність направляються листи начебто від імені легальних організацій, в котрих їх просять зайти на фальшивий сайт та підтвердити паролі, PIN-коди та іншу приватну інформацію, котра згодом буде використана злочинцями для крадіжки грошей з розрахункового рахунку жертви чи в інших злочинах. Причому всі дії жертва виконує абсолютно добровільно, не розуміючи що відбувається насправді. Для досягнення цієї мети злочинці використовують технології соціальної інженерії, нейролінгвістичного програмування, психології.

Фішинг класифікується на три види: поштовий, онлайновий і комбінований. Спочатку злочинцями використовувався лише поштовий − по e-mail відправлялись листи з пропозиціями до власника карти вислати (підтвердити) певні її дані. При онлайновому фішингу копіюються визначені сайти (частіше за все − інтернет-магазинів), використовуючи подібні доменні імена і аналогічний дизайн. А далі реалізується проста схема – жертва, яка потрапила на такий сайт, вирішує придбати товар (на такому сайті покупців приваблюють низькими цінами на товари, а всі підозри відкидаються через довіру до популярного справжнього бренду на сайті-фальшивці). Замовляючи товар, покупець реєструється, вводить номер та інші дані своєї платіжної картки. Такі прийоми застосовуються досить давно, хоча вони поступово втрачають свою ефективність через підвищення комп'ютерної грамотності населення та досвіду окремих громадян, набутого на власних помилках.

Третій вид фішингу – комбінований. Суть його полягає у створенні підробного сайту певної організації, на котрий заманюються потенційні жертви. Тут шахраї пропонують користувачам (з врахуванням знань психології) провести деякі операції самостійно.

Багаточисельні попередження, котрі практично щоденно з'являються в інтернет-мережі, роблять подібні методи шахрайства достатньо відомими. Тому тепер шахраї стали частіше використовувати key-loggers – спеціальні програми, котрі відслідковують натискання клавіш і відсилають отриману інформацію по завчасно визначеним адресам. Фішинг-атаки актуальні не тільки для дальнього зарубіжжя, перша їх спроба на території СНГ була зареєстрована ще в 2004 році.

Розглянемо особливості деяких видів фішингу.

Перший спосіб: для збирання карткових реквізитів про банківські картки користувачів створюються спеціальні (фішингові) сайти, які збирають цю інформацію під виглядом надання неіснуючих послуг. У 90 % випадків − це послуги з переказу коштів із картки на картку та поповнення мобільного рахунку. Нерідко фішингові веб-ресурси маскуються під сайти організацій, яким довірять користувачі, наприклад «Приват24», portmone.com, ukrposhta.com − фішингові сайти схожі на справжні не лише із дизайном, але й подібні електронною адресою.

Також шахраї намагаються обирати популярні інтернет-ресурси, доменні імена котрих тільки на одну-дві букви відрізняються від розкручених порталів, котрі продають товари або надають послуги. На цих сайтах клієнтам пропонується ввести реквізити платіжної карти для оплати будь-якої послуги. Але фактично послуга не надається, а виконується тільки збір даних про платіжні карти клієнтів для їх наступного використання (В. Довганич, начальник управління інформаційної безпеки ПУМБ) [9]. Наприклад, у серпні 2017 року в мережі інтернет був запущений фішинговый сайт − клон популярного сервісу «Приват24». Метою його створення було виманювати у клієнтів популярного державного банку їх паролі доступу в інтернет-банкінг з номерами телефонів (Асоціація ЕМА) [10]. Адреса підробного сайту (http://pb24corp.at.ua) несуттєво відрізнялася від оригінального (privat24.ua).

Враховуючи зростання поінформованості користувачів банківських та інтернет послуг про кібершахрайство, злочинці в свою чергу стають ще більш винахідливими. Наприклад, адресний рядок деяких шахрайських веб-ресурсів починається з https, що говорить про «захищене з'єднання». Відсутність «s» в адресі (http, а не https − уточнено нами) − одна з ознак фішингового сайту, так як легітимні ресурси завжди встановлюють безпечне інтернет-з'єднання. Однак деякі шахраї навчились створювати сайти з https, тим самим підвищуючи для користувача ризик потрапити в їх пастку. Тому відсутність «s» − ознака шахрайського сайту апріорі, але й присутність «s» в електронній адресі − це ще не ознака легітимного сайту. Про цю різницю важливо пам'ятати, − відзначають спеціалісти ЕМА [1].

Також шахраї змінюють реквізити на потрібні на сторінках волонтерських організацій, котрі займаються наданням допомоги важкохворим людям, воїнам АТО тощо. Тому перед перерахуванням грошей для допомоги громадянам необхідно спочатку телефоном уточнити номер рахунку цієї організації (фізичної особи).

Другий спосіб фішингу − створення тимчасових сайтів з розміщеною на них інформацією про певні товари чи послуги, котрі продаються, як правило, за суттєво заниженими цінами. При встановленні зв'язку за вказаним на сайті телефоном продавець пропонує провести попередню оплату (перерахувати завдаток) за товар, котрий за ціною є значно дешевшим за аналогічні моделі в магазинах. Після перерахування коштів сайт видаляється, зв'язок із продавцем припиняється [10].

Надамо деякі рекомендації власникам платіжних карт щодо мінімізації можливостей та уникнення заподіяння шкоди їх фінансовим ресурсам внаслідок вчинення даного виду інтернет-шахрайства.

1. Особам, які стали жертвами шахраїв, фахівці Національної поліції та банківські працівники радять оперативно звертатися за допомогою до кіберполіції.

2. Завжди потрібно звертати увагу на URL (адрес) сайту, на котрому громадяни роблять придбання товарів. Оплачувати можна тільки на тих сторінках сайтів, котрі використовують захищене з'єднання – протокол https (значить secured). При оформленні (відкритті) нової платіжної картки в банку, поцікавтесь, чи підтримує вона захист 3-D Secure (банк пов'язує користування платіжної картки з номером мобільного телефону клієнта). В інтернет-мережі рекомендується розраховуватися тільки такими банківськими картками. Причому спеціалісти рекомендують оплачувати товар тільки на сайтах, котрі також підтримують протокол 3-D Secure. Зрозуміти це легко: користувачеві не вдасться навіть ввести номер платіжної картки і оплатити сайту за придбання товару. Спочатку портал відправить на номер мобільного телефону клієнта вказаного банку sms-повідомлення із спеціальним кодом, і тільки після того як користувач його введе, здійсниться проплата грошей (Є. Міщенко, спеціаліст сектору безпеки управління платіжних карт «Банку Нацкредит») [9]. 3-D Secure – це підстраховка на будь-який випадок користування грошима при оплаті через інтернет. Якщо після такого списання грошей шахраї якимось способом все ж таки вкрадуть кошти у клієнта банку, їх зобов'язана компенсувати власнику банківська установа.

3. Використовувати тільки перевірений веб-сервіс, до послуг котрого користувач звертається не вперше. С. Березюк, працівник підрозділів протидії злочинам в сфері електронної комерції кіберполіції рекомендує перед тим як скористатися сайтом, перевірити інформацію про нього: вивчити відгуки користувачів, чорний список ЕМА, форуми, де потерпілі обмінюються інформацією про шахрайські ресурси [1], тобто, перевірити репутацію сервісу в інтернеті. Якщо користувач не знайшов інформації про компанію, котра надає послуги, немає про неї відзивів користувачі − мова йде про шахрайський ресурс. Нерідко можна виявити негативні відзиви тих користувачів, хто вже став жертвою шахрайського

ресурсу. Не полінуйтесь затратити декілька хвилин і переконатися, що у обраного вами сервісу є позитивна репутація, історія та «стаж роботи».

4. Зверніть увагу на домен реєстрації сайту (це повинен бути домен.ua, котрий можна зареєструвати тільки при наявності торгової марки). Якщо український сервіс зареєстрований не на домені.ua, то потрібно, на думку Р. Федоровської, керівника EMA Academy, одразу ж шукати інший. Справа в тому, що шахраям невигідно використовувати цей домен − тільки його реєстрація займає 1,5 роки, при цьому ще треба мати обов'язково торгову марку [1].

5. Перевірити дату і термін реєстрації сайту (для цього існує безплатний сервіс **whois**). Якщо сервіс зареєстрований недавно і терміном всього на рік − він шахрайський. Також в EMA радять перевіряти незнайомі ресурси на сайті цієї організації: на порталі Асоціації існує два списки платіжних веб-сервісів, один з яких − чорний список шахрайських сайтів.

6. Спілкуватися з працівниками банку за номером мобільного телефону, який починається на 0800… або вказаний на платіжній картці (банкоматі).

Висновки. На основі проведеного аналізу спеціальної літератури, рекомендацій фахівців та сучасних інтернет-публікацій з піднятої проблеми можемо зробити наступні узагальнення щодо удосконалення способів боротьби з випадками шахрайства з використанням викрадених реквізитів платіжних карт:

- потрібно завжди бути уважними при користуванні інтернет-банкінгом. Власникові доцільно підключитися до SMS-банкінгу і отримувати повідомлення про всі операції з готівковими коштами, які зберігаються на картці;
- зберігайте окремо платіжну картку та її PIN-код;
- не розраховуйтесь в інтернеті зарплатною карткою. Замовте у банку до неї спеціальний (другий) пластик для транзакцій і перераховуйте на нього невеликі суми для здійснення платежів в інтернет-мережі; перераховувати на неї гроші тільки тоді, коли збираєтесь робити покупки, причому невеликі суми. В цьому випадку навіть при успішній інтернет-атаці шахраїв збиток виявиться не надто великим;
- не залишайте в інтернеті номер телефону, котрий зв'язаний з платіжною карткою. В ідеалі потрібно мати окремий телефон для здійснення операцій по банківській картці, котрий знає тільки власник;
- не надавайте реквізити картки (номер картки, її термін дії, пін-код, CVV-код (три чи чотири цифри на зворотному боці картки), в тому числі по телефону, третім особам – ні працівникам торгівлі, ні навіть банку, котрий випустив пластикову платіжну картку (працівник банку ніколи не буде телефонувати, щоб уточнити особисті дані користувача банківських послуг); не рідше раз в місяць змінюйте (наприклад, через банкомат) свій PIN-код;
- ніколи не давайте свою картку в руки стороннім особам. Якщо даєте картку в магазині або інших суб'єктах господарювання для проведення розрахунку, − не випускайте її з виду;
- встановіть ліміт на платежі у торговій мережі та в інтернеті (обмежте можливий масштаб крадіжок);
- перепишіть у блокнот код безпеки для розрахунків в інтернеті (CVV2/CVC2 код) і заклейте його на картці папером, щоб його не змогли переписати сторонні особи під час розрахунку карткою;
- повністю заблокуйте проведення платежів по платіжній картці в інтернеті. Деякі банки сьогодні забороняють (блокують) оплату VIP-картками в інтернеті (Gold, Platinum, Premium);
- замовте банку послугу щодо випуску картки не з магнітною смугою, а з чіпом (вони коштують на 30-50 грн дорожче, але зате набагато безпечні при користуванні). До цього часу у світі не було зареєстровано жодного випадку взлому або підробки чіпу;
- з метою мінімізації випадків нападу на карткові рахунки під час покупок в інтернеті та для надійного захисту коштів клієнтів багато банків пропонують активувати послугу 3D-Secure, котра гарантує здійснення покупок тільки власником картки. Таким сервісом вже користуються біля 95 % суб'єктів торгівлі в інтернет-мережі (Є. Демянов, директор департаменту продуктів і маркетингу для роздрібних клієнтів «Райффайзен Банка Аваль»);
- щоб вбезпечити клієнтів банку, фінансова установа також може встановити користувачам незначний ліміт по платежам в інтернеті. Якщо клієнт й стане жертвою карткових шахраїв, то вони не зможуть викрасти більше, ніж на 100 грн. Коли ж людині дійсно потрібно буде оплатити більш вартісний товар в інтернет-мережі, власнику карти достатньо тільки зателефонувати в call-центр і збільшити ліміт (А. Шаперенков, заступник голови правління, директор банку VAB Банк) [9].

Активно здійснюється профілактика шахрайств з платіжними картками й правоохоронцями підрозділів кіберполіції Національної поліції − вся інформація про нові схеми шахрайств публікується на відомчому та регіональних сайтах.

Отже, чим більша кількість власників платіжних карток будуть знати існуючі способи шахрайства з цим банківським інструментом, тим даний вид злочину матиме мінімальну можливість для реалізації або зникне зовсім.

Література:

1. Карточные мошенники научились по-новому воровать деньги у украинцев [Електронний ресурс]. – Режим доступу: .

2. Смаглюк О.В. Шахрайство за Кримінальним кодексом України 2001 року : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право» / О.В. Смаглюк. – Київ, 2004. – 19 с.

3. Кравченко О.В. Психологічні особливості шахрайства: автореф. дис. на здобуття наук. ступеня канд. психол. наук : спец. 19.00.06 «Юридична психологія» / О.В. Кравченко. – Харків, 2005. – 21 с.

4. Мойсик В.Р. Проблеми кримінальної відповідальності за шахрайство з фінансовими ресурсами: автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право» / В.Р. Мойсик. – Київ, 2002. – 17 с.

5. Патик А.А. Взаємодія слідчих та оперативно-розшукових підрозділів при розкритті та розслідуванні майнових злочинів : автореф. дис. на здобуття наук. ступеня канд. юрид. наук **:** спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» / А.А. Патик. – К., 2011. – 18 с.

6. Крикливий Р.М. Підтримання державного обвинувачення у справах про шахрайство**:** автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.10 «Судоустрій; прокуратура та адвокатура» / Р.М. Крикливий. – Одеса, 2011. – 20 с.

7. Шуляк Ю.Л. Кримінальна відповідальність за шахрайство: порівняльно-правове дослідження: автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право» / Ю.Л. Шуляк. – Київ, 2011. – 22 с.

8. Мюллер В.К. Англо-русский словарь: 53 000 слов /Владимир Карлович Мюллер. – 21-е изд., испр. – М.: Рус. яз., 1987. – С. 655.

9. Лысенко Е. Шесть приёмов против карточных мошенников в Украине / Елена Лысенко [Електронний ресурс]. – Режим доступу: http://vesti.ua/poleznoe/23667-kak-ukraincam-uberech-bankovskie-karty-ot-moshennikov. – Название с экрана.

10. Появился клон Приват24, выуживающий пароли [Електронний ресурс]. – Режим доступу: https://newsyou.info/poyavilsya-klon-privat24-vyuzhivayushhij-paroli

Забезпечення доступу до інформації в умовах надзвичайних (типових та нетипових) адміністративно-правових режимів

Веселов М.Ю.
кандидат юридичних наук, доцент
доцент кафедри кримінально-правових дисциплін КФ
Національного університету «Одеська юридична академія»

Інформаційний простір, постійно розширюючись і відіграючи дедалі важливішу роль у житті людей, формує новий життєвий простір у вигляді цілісного поля, усередині якого індивіди взаємодіють між собою. Специфіка його полягає в розірваності двох рівнів буття: реального й віртуального, що зумовлює нові норми й ситуації існування. Набуваючи глобального характеру, інформаційні технології сприяють розширенню комунікацій і формуванню єдиного комунікативного простору, у рамках якого формуються свої особливі закони та норми поведінки й світосприйняття [1, с. 10-11]. О. П. Дурбас відзначає, що поняття «інформаційний простір» поєднує два терміни: «простір» та «інформація» [2, с. 224]. У свою чергу Л. П. Коваленко до основних елементів «інформаційної сфери» відносить а) інформацію, в тому числі інформаційні ресурси (документи, банки й бази даних, архіви, бібліотеки, музейні фонди тощо) й б) інформаційну інфраструктуру (організаційні структури, що забезпечують збирання, оброблення, зберігання, розповсюдження, пошуки й передачу інформації, а також гарантують