УДК 004.056.5

Вікторія ПЯНКОВСЬКА, Інна ЯРОВА

Національний університет «Одеська політехніка»

СУЧАСНІ МЕТОДИ ТЕЛЕФОННОГО ТА ОНЛАЙН-ШАХРАЙСТВА В УКРАЇНІ: МЕТОДІ ПРОТИДІЇ ТА РОЗКРИТТЯ ЗЛОЧИНІВ

Вступ. В епоху цифрових технологій методи соціальної інженерії стають все більш витонченими, а в умовах повномасштабного вторгнення в Україні ця проблема набула особливої гостроти. Зловмисники майстерно адаптують свої схеми під актуальні потреби громадян, спекулюючи на темах евакуації, благодійних зборів та державних виплат. Масштаби загрози підтверджує статистика НБУ: хоча кількість шахрайських операцій у 2024 році дещо зменшилась, загальна сума збитків зросла на 37 % і сягнула 1,1 млрд грн, а середня сума однієї незаконної операції досягла значення 4247 грн [1]. Причому 83 % шахрайських операцій відбулися в мережі Інтернет, що робить кіберпростір основним полем діяльності для злочинців. Ключовою причиною злочинів залишається соціальна інженерія – 84 % збитків сталися через те, що люди самі розголошували свої дані .

Мета: Проведення аналізу поширених та новітніх схем шахрайства в кіберпросторі, розгляд методів протидії з боку правоохоронних органів та надання практичних порад для захисту громадян.

1. Найпоширеніші схеми шахрайства

Спираючись на Конвенцію Ради Європи про кіберзлочини, використання методів соціальної інженерії в кіберпросторі можна кваліфікувати як шахрайство, що пов'язане з використанням цифрових технологій, спрямоване на порушення конфіденційності персональних даних з їх подальшим незаконним використанням, вчинене зовнішнім порушником. Поширеними методами онлайн-шахрайства є фішинг і вішинг, причому вішінг може реалізовуватися як в кіберпросторі з використанням соцмереж та поштових сервісів, так і у вигляді телефонного шахрайства.

Використовуючи фішинг, злочинці створюють фейкові сайти, що копіюють сайти банків, поштових служб, або державні портали (наприклад, «Дія») з метою збору логінів, паролів та даних карток. Новим способом фішингу є створення та поширення фейкового контенту, в якому під виглядом благодійних фондів або державних організацій пропонується надання допомоги малозабезпеченим верствам населення, в тому числі внутрішнім переселенцям [2]. На підконтрольному зловмисникам сайті жертва має ввести свої персональні дані та дані банківської картки.

Також поширеним є шахрайство в інтернет-торгівлі: продаж неіснуючих товарів за передоплатою або надсилання фішингових посилань на «безпечну оплату».

В умовах обмеженого офлайн-спілкування актуальною проблемою є фішінг в соцмережах: злам акаунтів для розсилки повідомлень з проханням позичити гроші та створення фейкових сторінок для псевдоблагодійних зборів.

Вішинг – маніпуляція з використанням онлайн-листування або телефонного дзвінка з метою отримання конфіденційних даних. Основні сценарії вішингу:

– «лист або дзвінок з банку»: під приводом підозрілої активності на рахунку злочинець отримує від жертви CVV-код, паролі з SMS та іншу банківську інформацію;

– «Ви виграли приз»: повідомляючи про виграш, злочинець просить сплатити неіснуючий «податок» або «комісію» для отримання призу;

– «дзвінок від мобільного оператора»: вішинг з використанням телефону, коли під виглядом «покращення зв'язку» жертву просять набрати комбінацію, яка встановлює переадресацію SMS, надаючи доступ до онлайн-банкінгу;

– «родич у біді»: створюючи емоційний шок телефонним повідомленням про ДТП чи затримання родича, зловмисник вимагає перерахувати гроші для «вирішення питання» онлайн-банкінгом.

2. Новітні загрози: Deepfake та атаки на eSIM

Прогрес створює нові вектори атак, залучаючи новітні цифрові технології, які складно розпізнати звичайному користувачу.

Аудіо-дипфейки (Deepfake): злочинець використовує штучний інтелект для клонування голосу. На основі оригінальних зразків голосу злочинець може згенерувати аудіоповідомлення або зателефонувати від лиця знайомої людини: родича, друга чи керівника. Метою цього є отримання термінового переказу грошей або одноразових кодів доступу [3]. Атаки на віртуальні SIM-карти (eSIM): зловмисники отримують контроль над eSIM жертви через підроблені запити до оператора, таким чином перехоплюючи SMS-повідомлення з кодами підтвердження для входу в додатки онлайн-банкінгу [3].

3. Протидія шахрайству в кіберпросторі з боку правоохоронних органів

Ключову роль у боротьбі з кіберзлочинністю відіграє Департамент кіберполіції, який застосовує комплексний підхід. Основні напрямки його діяльності:

– відстеження фінансових транзакцій: аналіз руху коштів через ланцюжки «транзитних» карток для виявлення організаторів злочину;

– блокування шахрайських ресурсів: у співпраці з банками, операторами мобільного зв'язку та інтернет-провайдерами відбувається оперативне блокування фішингових сайтів, номерів телефонів та рахунків;

– ліквідація колл-центрів: правоохоронці регулярно викривають організовані «офіси», облаштовані комп'ютерною технікою та телекомунікаційним обладнанням;

– активна протидія злочинним групам в соцмережах, які ошукують громадян під приводом надання грошової допомоги переселенцям;

– міжнародне співробітництво: взаємодія з Європолом та Інтерполом є важливою, оскільки кіберзлочинність часто має транснаціональний характер.

4. Як захистити себе: практичні поради для користувачів

Ефективним засобом профілактики кіберзлочинності є підвищення обізнаності громадян щодо можливих дій злочинців і способів протидії. Головною

рекомендацією є порада зберігати спокій і критичне мислення при отриманні неочікуваних листів, повідомлень або дзвінків, адже емоції заважають раціональним діям.

Для пересічного користувача мережі можна запропонувати наступні «золоті правила» інформаційної безпеки:

– нікому не повідомляйте конфіденційні дані: CVV-код, термін дії картки, паролі з SMS та PIN-код: справжні співробітники банків їх ніколи не питають;

– перевіряйте інформацію: отримавши тривожний дзвінок, покладіть слухавку та самостійно зателефонуйте до установи (банку, поліції) за офіційним номером;

– будьте уважні до посилань: не переходьте за підозрілими посиланнями з SMS, месенджерів чи електронної пошти, завжди перевіряйте URL-адресу сайту на наявність помилок та чи захищений він (протокол https);

– використовуйте надійний захист: створюйте складні, унікальні паролі для різних акаунтів та обов'язково вмикайте двофакторну автентифікацію;

– окремий фінансовий номер телефону: використовуйте для онлайн-банкінгу номер телефону, який ви не використовуєте для соцмереж та інших сайтів.

Якщо Ви стали жертвою кібершахрайства:

– негайно заблокуйте картку через онлайн-додаток банку або дзвінком на гарячу лінію банку;

– повідомте банк про несанкціоноване списання коштів;

– подайте заяву до Департаменту кіберполіції (онлайн через сайт) та до найближчого відділення Національної поліції України.

Висновки. Шахрайство з використанням цифрових технологій в Україні постійно еволюціонує, використовуючи для маніпуляцій соціальну інженерію та новітні технології, як-от штучний інтелект. Злочинці активно експлуатують актуальні для суспільства теми, що робить їхні атаки більш переконливими. В цих умовах головним інструментом протидії є високий рівень цифрової грамотності громадян. Розуміння механізмів обману, критичне мислення та дотримання базових правил безпеки дозволяють вчасно розпізнати загрозу. Тому підвищення власної пильності та обізнаності є ключовим для ефективного захисту від шахраїв в кіберпросторі.

Перелік використаних джерел.

1. Національний банк України: офіційний сайт. Кількість випадків шахрайства з картками знизилася, збитки за ними – зросли. [Електронний ресурс]. - Режим доступу: https://bank.gov.ua/ua/news/all/kilkist-vipadkiv-shahraystva-z-kartkami-znizilasya-zbitki-za-nimi--zrosli

2. Національна поліція України: офіційний вебпортал. [Електронний ресурс]. - Режим доступу: https://npu.gov.ua/news/dopomoha-z-sizo-kiberpolitsiia-prypynyla-diialnist-shakhraiskoho-uhrupovannia

3. Офіційний сайт Кіберполіції України. Афери з діпфейками: кіберполіція застерігає від шахраїв. [Електронний ресурс]. - Режим доступу: https://cyberpolice.gov.ua/article/afery-z-dipfejkamy-kiberpolicziya-zasterigaye-vid-shaxrayiv-7638/