Вікторія Лихопій, старший викладач
Олена Дмитрук, магістрант
Полтавська державна аграрна академія

ФІШИНГ ЯК ВИД ШАХРАЙСТВА З ПЛАТІЖНИМИ КАРТКАМИ

За останні роки активно розвивається використання банками та іншими фінансово-кредитними установами можливостей Інтернет, що вплинуло на збільшення кількості безготівкових платежів. Це призвело також до зростання кіберзлочинності та шахрайств з банківськими картками. Фішинг став одним із лідерів у рейтингу шахрайства з платіжними інструментами в Україні.

Фішинг – це вид шахрайства, який застосовується з метою отримання у власника платіжної картки інформації про реквізити картки шляхом використання підроблених сайтів, введення в оману та інше. Реквізити платіжної картки, на які полюють шахраї, що займаються фішингом:

1. Номер картки.

2. Дата випуску/завершення дії картки.

3. Код CVV2 (тризначне число на звороті платіжної картки, служить кодом підтвердження операцій, що здійснюються в мережі Інтернет або за допомогою телефону).

4. Написання прізвища та імені клієнта латиною.

5. ПІН-код [2].

Фішинг – це схема, за якою хакери змушують користувачів передавати конфіденційну інформацію, наприклад, паролі та номери соціального страхування. Зазвичай вона передбачає надсилання користувачеві повідомлення, яке ніби походить із вартого довіри джерела, наприклад із банку (це наживка). У повідомленні міститься посилання на шахрайський web-сайт, що видається за варте довіри джерело (це пастка). Користувач спокійно вводить інформацію, яка цікавить хакерів, вважаючи, що перебуває на безпечному сайті [1].

Способів фішингу безліч. Найпоширеніші з них представимо в табл. 1.

Таблиця 1

Найпоширеніші способи фішингу та методи їх реалізації

Спосіб фішингу	Метод шахрайських дій
Використання шахрайських Інтернет-сайтів чи Інтернет-магазинів	Створення копії оригінальних Інтернет-сайтів компаній або інші сайти, на яких зазвичай пропонується придбати якусь річ за дуже вигідною (акційною) ціною за допомогою платіжної картки.
Направлення шахрайських листів	В тексті листа міститься прохання надіслати реквізити картки для її підтвердження чи розблокування або повідомлення про виграш у лотерею для зарахування грошового призу.
Використання шкідливого програмного забезпечення (віруси, програми віддаленого доступу та ін.)	Крадіжка даних з персонального комп'ютера клієнта.
Телефонні дзвінки з посиланням на банк, контролюючі або правоохоронні органи	Прохання підтвердити реквізити картки у зв'язку з підозрою шахрайських операцій, наявності неіснуючої заборгованості, уточнення щодо платежів.
Створення модифікації посилань	Перенаправлення клієнта на шахрайські сайти.

Щоб не стати жертвою шахраїв, необхідно навчитися розпізнавати сайти-фішери. Для них характерні такі особливості:

– інтерфейс сайту імітує веб-сервіс для поповнення мобільного, скачування електронних книг або здійснення грошового переказу;

– сервіс пропонує вигідні умови: поповнення без комісій, великі знижки, акції і додаткові послуги;

– адміністратор сайту пропонує заповнити стандартну платіжну форму, в якій має бути вказано номер і конфіденційні дані карти;

– після введення банківських даних на фішинговому сайті з'являється повідомлення, що операція не може бути проведена з технічних причин [3].

Таким чином, визначимо основні превентивні заходи для власників платіжних карток з метою захисту від фішингових атак:

– при введенні інформації з банківської картки для оплати в мережі Інтернет необхідно переконатися в тому, що використовується захищене з'єднання;

– за жодних обставин не слід повідомляти реквізити платіжної картки

іншим особам. Виняток становлять випадки проведення оплати товарів чи послуг за допомогою засобів мобільного зв'язку, але в цьому випадку клієнт має бути повністю впевненим в конфіденційності та надійності здійснюваної операції;

– слід перевіряти оригінальність Інтернет-сторінок та Інтернет-магазинів та не користуватись послугами підозрілих і маловідомих компаній;

– використання ліцензійного програмного забезпечення та вчасне його оновлення (Інтернет-браузера, операційної системи, антивірусного програмного забезпечення підвищує захист від хакерських атак та шахрайських дій;

– для переходу за допомогою посилання, що прийшло на електронну адресу, варто вводити його в адресне поле браузера самостійно та перевіряти правильність написання адреси сайту компанії;

– варто пам'ятати, що банк ніколи не надсилає листів з проханням чи вимогою надіслати номер картки та іншу інформацію щодо неї;

– не слід зазначати реквізити картки (номер, CVV2-код та інші дані) ні в яких формах, окрім випадків оплати товарів у мережі Інтернет на провірених сайтах;

– ні в якому разі не слід допускати копіювання реквізитів платіжної картки.

Література:

1. Онищенко Ю. М. Протидія злочинам, що вчиняються за допомогою методів соціальної інженерії в Інтернеті / Ю. М. Онищенко, К. Е. Петров, І. В. Кобзєв // Право і безпека. – Вип. 1 (64). – Х. : Нац. ун-т внутр. справ. – 2017. – С. 63 – 68.

2. Офіційний сайт Незалежної асоціації банків України [Електронний ресурс] – Режим доступу : http://anticyber.com.ua/fraud_detail.php?id=20

3. Як захистити кошти на банківській картці [Електронний ресурс] – Режим доступу до ресурсу : https://konkurent.in.ua/news/ukrayina/18323/ak-zahistiti-koshti-na-bankivskij-kartci.html