ПРОБЛЕМА ОНЛАЙН-МАХІНАЦІЙ

Єрмоленко Д. В., студ. (гр. КВ-73, ФПМ КПІ ім. Ігоря Сікорського);
Соколовський Б. М., студ. (гр. КВ-73, ФПМ КПІ ім. Ігоря Сікорського);
Полукаров Ю. О., к.т.н., доц. (каф. ОППЦБ КПІ ім. Ігоря Сікорського);

Анотація. Статтю присвячено дослідженню проблеми онлайн-махінацій та рекомендаціям, як від них уберегтись.

Ключові слова: онлайн-махінації, Інтернет, онлайн-банкінг, фішинг, онлайн-шахраї, хакери, соціальна-мережа, кіберзлочин, соціальна інженерія, захист інформації.

Abstract. The paper is devoted to study problem of online-schemes and how to prevent them.

Keywords: online-scheme, Internet, online-banking, fishing, online-swindlers, hackers, social network, cybercryme, social engineering, information security.

Вступ. У наш цифровий час, коли велика кількість людей має доступ до високошвидкісного Інтернету з персональних комп'ютерів, ноутбуків, планшетів, смартфонів та навіть зі смарт-телевізорів, питання безпеки персональних даних та банківських рахунків при користуванні різноманітними інтернет-послугами чи просто телефоном стоїть досить гостро, бо існує велика кількість онлайн-шахраїв. Вони з кожним роком використовують все більш досконалі методи махінацій, на які потрапляють навіть досвідчені користувачі. За статистикою 2019 року в українців через різноманітні онлайн-махінації було викрадено понад 361 мільйон гривень [1]. Тому наразі надзвичайно важливо зараз знати про найрозповсюджені онлайн-махінації та як не наразитись на них.

Аналіз стану питання. Серед онлайн-махінацій можна виділити такі основні види: фішинг, телефонні дзвінки, розважальна махінація, махінація з онлайн-працевлаштуванням. Усі перелічені махінації мають за собою такі цілі: або отримати від жертви напряму гроші або отримати персональні дані разом із реквізитами картки, щоб вже потім отримати доступ до банківського рахунку та вивести з нього кошти. В більшості випадках використовується психологічний вплив на жертву через використання соціальної-інженерії.

Мета роботи: описати найбільш поширені онлайн-махінації та рекомендації, як вберегтися від них.

Методики, матеріали і результати досліджень. Розпочнемо з розбору фішингу. Фішинг (з англ. - рибалка) являє собою схему, у якій хакери створюють фальшивий сайт, який виглядає ідентично оригінальному сайту, з якого робилася копія. Найчастіше всього копіюють офіційні сайти банків, фінансових сервісів або торговельних майданчиків. Посилання на сайт-підробку розповсюджують найчастіше всього через використання спам розсилки на електронні почтові скриньки. Особливістю електронних листів, що є частиною схеми фішингу, наступна: вони зазвичай виглядають як офіційні листи від довіреного джерела з посиланням на сайт-пастку та запитом щодо оновлення інформації про акаунт. Після переходу на фішинговий сайт

користувач бачить сайт, якому він може довіряти та вводить конфіденційну інформацію на ньому. Для того, щоб не потрапити у дану махінацію потрібно дотримуватись таких порад:

- якщо в листі при наведені на посилання у браузері знизу чи зліва показується інше посилання, то з великою ймовірністю ви маєте справу зі шахрайською схемою;
- не довіряйте листу, який містить багато граматичних чи орфографічних помилок чи який має терміновий чи погрозливий тон;
- використовуйте найсвіжішу версію вашого браузера, оскільки сучасні браузери мають антифішингові засоби;
- якщо у посиланні домен сайту починається з http://, а не з https:// - то сайт, як мінімум є небезпечним, а як максимум – є фішинговим.
- якщо в адресному рядку на всіх сторінках сайту однакові адреси, то точно маємо справу із сайтом-підробкою.
- взагалі перевіряйте те, чи є посилання у листі дійсно на офіційний сайт. Для цього у пошуковій мережі (наприклад Google) треба зробити запит "офіційний сайт банку/компанії тощо", потім перейти на офіційний сайт та порівняти адрес з адресного рядка браузера із тим, що в листі. Але й тут потрібно бути дуже обережним тому, що досвідчені хакери можуть зробити так, що адрес «сайту-фальшивки» виглядає ідентичним до офіційного. Це досягається, зокрема, використанням ідентичних на вигляд чи практично подібних символів (наприклад немає ніякої візуальної різниці між "с" латиницею та "с" кирилицею).

Махінації через телефонні дзвінки являють собою схему у якій зловмисники намагаються витягнути конфіденційну інформацію або переведення коштів на рахунок через використання методик соціальної інженерії [2]. Можна виділити 2 сценарії: дзвінок від "родича" чи "знайомого" та дзвінок від представника банку. У першому сценарії відбувається дзвінок з невідомого номеру, після чого голосом родича або знайомого зловмисник повідомляє жертві про те, що нібито хтось з його близьких "втрапив у халепу" і потрібні терміново гроші" або щось подібне. Це також може бути здійснено не через дзвінок, а через sms-повідомлення. Як можна зрозуміти, такий сценарій зазвичай застосовують на літніх людях, тому родичам потрібно попереджати їх про подібну аферу. Другий сценарій врази цікавіший, бо на нього "клюють" навіть вельми обачливі люди. У цьому сценарії зловмисник представляється як "представник банку" та просить для певної операції конфіденційні дані. У такому разі слід відразу зупиняти розмову, бо треба запам'ятати назавжди, що **ніколи** не можна передавати банківську конфіденційну інформацію пов'язану з вашою карткою. Працівники банку не мають права запитувати дану інформацію. Єдина річ, яку можна називати – це номер банківської картки.

Наступний тип махінацій - це махінації з працевлаштуванням [3]. Частіше всього махінації з працевлаштуванням зустрічаються при влаштуванні на віддалену роботу. Це дуже актуальна тема на сьогоднішній день, адже багато людей у всьому світі обирають саме варіант віддаленої роботи. Розглянемо

декілька схем, якими користуються шахраї та, що робити у подібних ситуаціях. Найпопулярніша схема - це передоплата в якості компенсації за невиконану роботу, якщо таке трапиться. Наприклад, є вакансія рерайтера. Є готовий текст, який потрібно переписати «своїми словами». Людині, яка взялася за цю роботу, роботодавець на початку роботи виплачує деяку суму у якості авансу, наприклад 100-150 грн за текст невеличкого обсягу. Ця сума повинна придати певного стимулу для виконання роботи якісно, а також підтвердити серйозність ваших намірів. Якщо ви справитесь з роботою то ця сума буде повернена вам разом із заробітною платою. Насправді ж, після того, як були відправлені гроші псевдо-роботодавець зникає, або не платить за роботу договірну суму.

Іноді шахраї орендують офіс і навіть запрошують потенційних робітників на співбесіду. В кінці співбесіди говорять, що треба йти до дому і чекати доставку на дім спеціального обладнання, ще просять оплатити доставку. В результаті ніхто нічого не доставляє, шахраї з'їжджають з офісу і відключають усі телефони. Звісно, у вас виникає питання, що роботи, щоб не наразитись на такі вакансії. Якщо ви натикаєтесь на такі ситуації, слід уникати таких вакансій, навіть, якщо вам обіцяють дуже велику заробітну плату. Якщо ви все ж таки хочете ризикнути, вам слід пошукати перевірені вакансії та людей, які працюють і вже отримали заробітну плату.

Наступна схема - це служби (сфери послуг), які шукають роботу. Останнім часом стали з'являтися спеціальні служби по пошуку роботи: агентства, рекрутингові фірми та комерційні служби зайнятості. Ці служби обіцяють вас працевлаштувати. Виникне питання - де саме ці служби будуть шукати роботу? Такі служби часто запевнюють, що працюють з відомими компаніями та мають у своїй базі вакансії, яких ніде більше немає. Існує також торгівля вакансіями: наприклад, роботодавець заключає угоду зі співробітником службою по найму на роботу і наймає на роботу людину, яка звернулася на цю ж службу. Для отримання вакансії від цієї служби, треба заплатити від 500 гривень до 2 тисяч гривень. Якщо ви сплатите отримання роботи, вам ніхто не надасть гарантій, що у майбутньому вас не звільнять з будь-якої причини. Що роботи, щоб не потрапляти на такі служби? По-перше, нормальні служби з пошуку праці не беруть грошову суму за пошук праці, а по-друге, дані службі беруть відсоток заробітної плати робітника після влаштування на роботу. По-третє, завжди ретельно перевіряйте інформацію щодо роботодавця.

Остання схема - це «спочатку заплати, а потім працюй» [3]. Наступна схема дуже розповсюджена серед недобросовісних роботодавців. Псевдороботодавці подають вакансію на різні інтернет-ресурси з дуже привабливими умовами. Роботодавець говорить людині, яка хоче влаштуватися на цю вакансію, що людина практично підходить на цю вакансію і відповідає усім вимогам, але для початку потрібно купити спеціальну літературу, або пройти платний тренінг чи курс. Проблема тут у тому, що немає гарантій, що після цього не скажуть, що людина не підходить. Або можуть попросити скористатися послугами псевдокомпанії. Наприклад, хочете працювати у

страховій компанії? Спочатку оформити собі страховку у цій же компанії. Після угоди, можуть вам сказати, що вакансія нібито закрита і взяли іншу людину. Якщо без початкового внеску приступити до роботи неможливо, швидше за все, це обман зі сторони роботодавця. Серйозні компанії можуть безкоштовно видати спеціальну літературу і провести тренінги або курси. А оплата за літературу і курси можуть взяти хіба що у якості відсотку із заробітної плати.

Останній тип махінацій в інтернеті - це купівля різних товарів в інтернет-магазинах [4]. Існують спеціальні інтернет-магазини, в яких люди виставляють товар і продають його, або інтернет-аукціони, де люди виставляють різноманітні речі та проводять аукціон на ці речі. Кожна людина заходить на сторінку товару: дивиться й оцінює товар (виставляє ціну за яку покупець готовий купити товар). Але часто на таких сайтах зустрічаються шахраї, які перед покупкою товарів вимагають гроші авансом, а потім зникають і не відправляють товар або відправляють відвертий брак. Як уникнути таких ситуацій? Перша рекомендація, якщо ви купуєте товар, перш за все, дивіться відгуки на товар або на продавця. Мабуть, цей продавець не вперше продає речі, тому можна подивитись на відгуки попередніх покупців. Якщо відгуки позитивні, - це підвищує шанси купити товар без жодних проблем. Але якщо на товар або на продавця жодного відгуку, то такий товар можна купувати лише на свій страх і ризик. Щодо пошкодженого товару, для уникнення подібних ситуацій товар слід оплачувати виключно накладним платежем у спеціальних службах доставки, наприклад таких як «Нова Пошта». Ви можете отримати товар на пошті, переглянути його і, якщо вас влаштовує якість товару, ви можете спокійно оплачувати його. Однак, цей спосіб має мінус: ви сплачуєте за товар більше ніж було зазначено на сайті магазину, оскільки за послугу накладний платіж відходить деякий відсоток, який потрібно сплатити у будь-якому випадку. Та все ж таки, ви сплачуєте цей відсоток за отримання якісного товару. Остання рекомендація щодо купівлі у інтернет-магазинах: купувати треба товари лише у перевірених інтернет-магазинах, де є якісна онлайн-підтримка. Прикладом таких перевірених інтернет-магазинів є «Amazon», «Ebay», «Rozetka» або навіть «народний» сервіс «Olx».

Висновок. На сьогодні існує багато махінаційних схем не лише в онлайн-просторі, а й у реальному матеріальному світі, за допомогою яких, шахраї хочуть нажитися на довірливих людях. Нажаль ніхто від цього не може бути на 100 % застрахованим. Кожного року шахраї винаходять нові махінаційні схеми або нові методи соціальної інженерії. Але ви можете звести ризик бути ошуканими до мінімуму. Ніколи не “клюйте” на будь-що в інтернеті за надзвичайно малою ціною чи «по дзвінку» від незнайомця. Завжди виконуйте будь-які операції в онлайн-просторі з розумом, щоб це не було: онлайн купівля, онлайн оплата банківською карткою чи онлайн працевлаштування.

Література

1. 13 мошеннических схем, которые позволили украсть у украинцев 362 миллиона. [Електронний ресурс] – режим доступу https://minfin.com.ua/2020/02/14/40729350/

2. Як захистити себе від мобільних афер. [Електронний ресурс] – режим доступу https://chas.cv.ua/politics/53303-oberezhno-shahrajstvo-po-telefonu-yak-zahystyty-sebe-vid-mobilnyh-afer.html

3. Аферы с трудоустройством: пять схем, которые используют работодатели-мошенники [Електронний ресурс] – режим доступу https://www.segodnya.ua/economics/business/afery-s-trudoustroystvom-5-shem-kotorye-ispolzuyut-rabotodateli-moshenniki-1175614.html

4. Осторожно, мошеннический Интернет-магазин! [Електронний ресурс] - режим доступу https://www.ema.com.ua/citizens/cyber-safety-school/beware-fraudulent-online-store/