Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Кіберзлочини в сфері інтернет шахрайства: фішинг та способи його уникнення

Фаркаш К.В.
студентка 3 курсу,
факультету №4 ОДУВС ,
Науковий керівник: Косаревська О.В.
кандидат педегогічних наук, доцент
доцент кафедри кібербезпеки та інформаційного забезпечення ОДУВС

В XXI столітті Інтернет відіграє дуже важливу роль у житі суспільства, оскільки він забезпечує цілодобовий доступ до величезної кількості інформації, швидку передачу даних, можливість проведення банківських, торгових, біржових операцій, переказ коштів і багато іншого.

Інтернет полегшує нам життя, але це стрімке полегшення не могло пройти без наслідків. Мається на увазі появлення нового виду злочину, зазначеного у Розділі VI ККУ «Злочини проти власності», ч. 3 ст. 190 – шахрайство, вчинене шляхом незаконних операцій з використанням електронної техніки. Одним із різновидів соціальної інженерії є «фішинг», який спирається на необізнаність користувачів в основах мережевої безпеки .

Фішинг (англ. Phishing) – це вид шахрайства, метою якого є отримання конфіденційної інформації довірливих чи неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів тощо.[3]

Огляд сучасної наукової думки, стосовно проблем інформаційної безпеки, якою опікуються такі науковці, як: Безмалий В.Ф., Бурячок В.Л., Пятіркова Ж., Семко В.В., Толюпа С.В. та інш., дає підстави окреслити основні форми прояву фішингу у вигляді посилань фішингових листів та створення фішингових сайтів.

Шахраї використовують усілякі способи, які найчастіше змушують користувачів самостійно розкрити конфіденційні дані – наприклад: пошук роботи в інтернеті. Шахраї в об’яві ставлять високу заробітну плату, чим заманюють інтерес людини. Потім вони висилають електронний лист, з проханням повідомити свої облікові данні, пароль, PIN-код та інше. Треба запам’ятати один факт, що жодний сервіс не розсилають листів в яких треба зазначити конфіденційні данні.

Фішинговий лист - це лист, який застосовується для поширення посилань на фішингові сайти. Подібні листи — цілком офіційні, але при цьому в них містяться обов’язкові посилання на сайти-підробки, таким чином користувач вносить свої дані і піддається шахрайству.[4]

На сучасному етапі спеціалісти визначають коло певних ознак, що допомагають виявити листи-підробки.

- Відсутність цифрового підпису. Лист має посилання для скачування, які можуть містити вірус, і всілякі вкладення з виконавчими файлами.
- Наявність безлічі знаків оклику, що обумовлене спливом терміну вказаного в листі.
- В тексті міститься велика кількість орфографічних помилок.
- Зазначення адреси відправника із сумлінним посиланням, яке неодноразово дублюється.
- Пропонування надати свої особисті дані: паролі, номери та ПІН-коди карток, а також перевести гроші в якості запоруки дотримання домовленості.[4]

Прикладом фішингового сайту, як шахрайського веб-ресурсу є наявне виманювання реквізитів платіжних карток під виглядом надання неіснуючих послуг (наприклад: поповнення мобільного рахунку, переказів з картки на картку) або створення веб-ресурсу організації, якій користувач довіряє (клон Приват 24), що має на меті збір реквізитів платіжних карток для подальшої крадіжки грошових коштів з рахунків власників платіжних карток.

Як доводить практика, більш як у 90% випадків на фішингових сайтах пропонуються неіснуючі послуги з поповнення мобільного рахунку та переказу коштів з картки на картку.[3]

При цьому комп’ютерні шахраї використовують психологічні прийоми створюючи свій злочинний сайт на експлуатації людських мотивів, а саме: допитливість, бажання отримати вигоду, заробити та інш.

Типовими закликами фішингових сайтів є:

- «Дізнайтеся, чи є ваша картка у базі даних хакерів! Введіть дані, щоб перевірити.»;
- «При поповненні рахунку від 20 грн., Ви, гарантовано отримуєте 10 % від суми поповнення.»;
- «Акція! Поповнення рахунку, а також перекази з карти на карту будь-якого банку України без комісії.».

Таким чином метою фішинг шахрая є отримання вашого логіна і пароля, реквізитів платіжної картки з метою подальшого їх використання у власних інтересах, а саме для крадіжки грошей, які зберігаються на рахунку в банку.[3]

На нашу думку, актуальною є класифікація ознак Безмалого В.Ф., за якими можливо перевірити «умовні пастки» для користувачів та шляхи їх уникнення:

- «Відсутність репутації - небезпечність карткової операції.» Необхідно обов'язково перевірити існуючі відгуки про сайт в інтернеті. У випадку наявності негативних відгуків та відсутності інформації про сервіс в мережі інтернет, слід вважати ресурс ненадійним.

- «Перший не означає легітимний.» Фішингові сайти активно просуваються в інтернеті їх творцями-шахраями, найчастіше вони розміщуються вище за легітимні ресурси. Отже, особливу увагу слід приділити розміщенню ресурсу на сторінці пошукової видачі.

- «Неточний контент - обдурений клієнт.» Наявність будь-яких неточностей (наприклад: лічильника, показники якого не змінюються, помилок та інших хибів) свідчить про оману користувача.

- «Безграмотний контент - не просто незручний момент.» Взагалі шахраї не переймаються граматичною, стилістичною, синтаксичною правильністю викладання текстового змісту контенту.

- «Одна адреса.» Часта зміна адреси сайта при перезавантаженні сторінки свідчить про наявність фішингової пастки.

- «Будьте раціональними.» Під час вибору сайту необхідно опиратись на здоровий глузд, а не казкові акційні обіцянки.[5]

Таким чином , узагальнюючи вище зазначене ми з'ясували, що фішинг, як різновид комп'ютерного шахрайства залежить напряму від розвитку нових технологій та спрямований на зазіхання щодо економічної безпеки громадян.

Основними супутниками протиправних дій у комп'ютерному шахрайстві є низький рівень інформаційної культури громадян, їх власна неуважність, психологічні негативні якості (наприклад: як прагнення до швидкого збагачення за рахунок хибних шахрайських пропозицій, акцій тощо). Запорукою протидії фішингу є додержання користувачами інтернету наступних порад:

Стосовно оформлення паролів:

- необхідно уникати зазначення в паролі ім'я, прізвища та дати народження;
- паролі не слід зберігати в текстовому файлі на робочому столі ПК;
- слід використовувати неоднакові паролі для різних сайтів.

Не слід надавати особисті персональні дані (номер картки, пін-код, ІНН тощо.) шляхом телефонного зв'язку на вимогу бутім-то «співробітника банку"»; «страхового агента», «представника благодійного фонду» та інш.

Література:

1. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. – Режим доступу: http: www.rada.gov.ua

2. Кримінальний кодекс України: Відомості Верховної Ради України (ВВР). Закон від 05.04.2001 №2341-III (Редакція станом на 03.09.2017). Режим доступу: http: www.rada.gov.ua

3. Що таке фішинг? [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Фішинг.

4. Фішинговий лист. [Електронний ресурс] – Режим доступу до ресурсу: http://poradu24.com/tehnika/shho-take-fishing-i-yaka-vid-nogo-zaxist-chitati-tut.html.

5. Безмалий В.Ф. Фішинг (Phishing), Вішинг (vishing), Фармінг – шахрайство в Інтернеті [Електронний ресурс] / В.Ф. Безмалий. – Режим доступу до ресурсу: http://vse-prosto.весьтоп.рф/fishing-phishing-vishing-vishingfarming.html.