

УДК 332.012+004.056

**Тетяна Олексіївна ФРОЛОВА,**

*курсант 2 курсу групи Ф4-201 факультету № 4 (кіберполіції)*

*Харківського національного університету внутрішніх справ;*

**Денис Олександрович ГРИЩЕНКО,**

*старший викладач кафедри кібербезпеки факультету № 4 (кіберполіції)*

*Харківського національного університету внутрішніх справ*

## **ФІШИНГ ЯК СУЧАСНА ЗАГРОЗА ВТРАТИ ГРОШЕЙ З БАНКІВСЬКОГО РАХУНКУ**

З часом світ розвивається, стає більш прогресивним та досконалим. Люди вже звикли до мобільного зв'язку, Інтернету, сучасних засобів спілкування. В нашій країні зараз також відбувається багато реформ, і ми все частіше чуємо про те, що, наприклад, багато адміністративних, банківських, розрахункових та інших послуг можна отримати онлайн не виходячи з дому. Але з розвитком цивілізації розвивається і злочинність. І сьогодні все частішають випадки скоєння злочинів у всесвітній мережі Інтернет. Розглянемо новий різновид шахрайства, який з'явився у ХХІ сторіччі – фішинг.

**Фішинг** – один з видів соціальної інженерії. Найчастіше його суть полягає у створенні підробленого вебсайту банку чи іншої установи з метою «витягнути» у користувача конференційної інформації (наприклад, логін/пароль від акаунта), що дає можливість зловмиснику, наприклад, перевести чи зняти всі гроші з банківського рахунку жертви. Частіше за все, фішинг розрахований на неуважних користувачів, які не звертають уваги на незвичні назви сайтів, на орфографічні помилки в тексті, зовнішній вигляд знайомих ресурсів та нехтують основним правилами сучасної кібербезпеки.

У 2017 році в Україні зменшилась кількість фішингових сайтів на 38%. Та вважати це перемогою неможна, бо статистика показує, що лише 66% українців знають, що ризиковано використовувати нові, невідомі веб-сервіси для поповнення мобільного телефону або здійснення грошових переказів на картку [1].

На сьогодні існує дуже велика кількість різних типів фішингових сайтів. Але постійно з'являються нові види фішингових сайтів, наприклад:

### **1. Заробіток на участі в опитуванні**

Користувач бачить під оголошеннями про купівлю-продаж на певному популярному сайті коментар з пропозицією заробити на участі в опитуваннях – користувачам пропонують пройти невелике опитування і, наприклад, одночасно взяти участь в розіграші випадкової суми (до 5000 доларів США). Винагороду за участь у опитування пропонують перевести на банківську картку користувача. Однак замість виграву, наївних клієнтів очікує обман і крадіжка грошей з їх банківських рахунків.

## 2. Онлай-кредитування

Сьогодні дуже активно рекламуються сайти для отримання «онлайн кредитів» де для отримання грошової позики потрібно пройти верифікацію платіжної картки клієнта. Шахраї за допомогою підrobних сайтів такого типу отримують доступ до даних справжньої платіжної картки потерплх.

## 3. Дешеві квитки

На таких сайтах «продають» неіснуючі квитки, наприклад, на авіа чи залізничний транспорт, футбольний матч, концерт тощо.

Клієнтів на такі сайти заманюють привабливими пропозиціями – низькими цінами, більшими знижками. Мета такого веб-ресурсу, як й інших фішингових «сервісів» – переконати потенційного покупця розкрити секретні реквізити своєї банківської картки. З цією метою на фішинговому «квитковий» ресурсі розміщується звичайна платіжна форма, нібито для замовлення квитка онлайн. Заповнюючи форму, користувач вказує конфіденційні реквізити своєї картки, які потрібні, щоб підтвердити оплату, що здійснюються в Інтернет.

Такі сайти або крадуть секретні дані карти (і згодом шахраї використовують їх, щоб здійснювати грошові перекази з картки жертви на свої рахунки), або на них встановлена спеціальна програма, яка миттєво перенаправляє операцію на легітимний сервіс платежів (в результаті, з картки клієнта знімає вартість квитка, але в процесі «покупки» відбувається підміна реквізитів отримувача коштів на номер карти шахрая). Деякі сайти-підrobки сервісів з продажу квитків навіть видають квитки ... Користувач може їх роздрукувати, однак на ділі вони виявляються несправжніми.

## 4. Вербування «дропів»

Дроп або «грошовий мул» – це людина, яка погодилась, щоб його банківська карта стала «транзитної» для вкрадених шахраями грошей. Дроп переводить незаконно отримані грошові кошти між різними рахунками. Такий ланцюжок грошових переказів потрібний для того, щоб заплутати сліди кіберзлочинців і ускладнити роботу слідства.

Дропи допомагають злочинцям «відмивати» нелегально отримані гроші. Наприклад, гроші, здобуті шляхом здійснення кіберзлочинів в сфері електронної комерції і платіжних операцій (фішинг, вішинг, смішинг).

Дропи також можуть бути залучені до схем відмивання грошей, здобутих іншими злочинними шляхами: торгівлею наркотиками, торгівлею людьми та ін.

Оголошення про вербування дропом можуть бути замасковані під пропозиції про роботу від реальних компаній. Створюються цілі підrobлені сайти, схожі на офіційні веб-ресурси реально існуючих компаній.

Шахраї вигадують «поважні» причини, за якими їм потрібно переводити гроші з одного рахунку на інший. Найпоширеніша причина – ухилення від податків. Дропів вербують від імені якоїсь

компанії, якій, нібито, потрібно мінімізувати податкові виплати (і для цього слід переводити частину доходу через рахунки фізичних осіб).

Пропозиція про роботу може надійти і у вигляді листа на електронну пошту.

Щоб не стати жертвою кібершахраїв, які використовують у своїй злочинній діяльності фішингові вебсайти та електронні листи, необхідно.

1) звертати увагу на незвичні назви сайтів, на орфографічні помилки в тексті;

2) звертати увагу на адресата електронного листа: якщо він пропонує роботу від імені компанії, але при цьому в адресі відправника листа не вказано домен компанії, а вказана веб-служба, наприклад, Gmail, Yahoo, Windows Live Hotmail тощо.

Якщо ви вважаєте, що ви стали жертвою фішингу, виконайте наступні дії:

1) змініть свої паролі;

2) зверніться до свого банку, щоб повідомити про те, що ви, можливо, стали жертвою шахрайства.

3) запустіть повне сканування системи на виявлення вірусів на вашому пристрої;

4) проскануйте ваш пристрій за допомогою спеціалізованого програмного забезпечення, наприклад, Norton Power Eraser. Це може допомогти виявити більш складні загрози, ніж традиційна антивірусна програма.

З огляду на вище сказане, можна зробити висновок про те, що сучасний злочинний світ також стає більш прогресивним, і використовує великі можливості Інтернету для реалізації своїх злочинних намірів. З метою запобігання можливим фінансовим збиткам та мінімізації ризику стати жертвою фішингу необхідно, бути більш уважним з сайтами, якими ви користуєтесь. Користуючись новим сайтом, будьте обережні, бо невідомо, яку шкоду він вам може нанести. Дотримуйтесь порад, щодо того як не стати жертвою шахрайства. Якщо кожен з нас буде більш пильніше, злочинцям стане набагато важче зашкодити нам.

### **Список бібліографічних посилань**

1. Скачко Є. Топ-5 новин в сфері шахрайства з платіжними інструментами // Pingvin.Pro. 03.02.2017. URL: <https://pingvin.pro/gadgets/article-gadget/top-5-novyn-v-sferi-shahrajstva-z-platizhnyy-instrumentamy-6.html> (дата звернення: 30.10.2018).

2. Соціальна інженерія або маніпуляції свідомістю // Zillya антивірус. 12.05.2015. URL: <https://zillya.ua/sotsialna-inzheneriya-abo-manipulyatsi-svidomisty> (дата звернення: 30.10.2018).

3. Ногалес К. Социальная инженерия // 4 Brain. 12.12.2017. URL: <https://4brain.ru/blog/soциальная-инженерия/> (дата звернення: 30.10.2018).

4. Соціальна інженерія: виклики та перспективи боротьби в українському контексті : есе з права ІТ // Українське право. 01.11.2017 09:03. URL:

[http://ukrainepravo.com/legal\\_publications/essay-on-it-law/it\\_law\\_demchuk\\_Social\\_engineering\\_perspectives\\_of\\_the\\_struggle\\_in\\_ukrain/](http://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_demchuk_Social_engineering_perspectives_of_the_struggle_in_ukrain/) (дата звернення: 30.10.2018).

5. Фишинг в Украине: итоги первого полугодия 2017 года // PaySpace magazin. 05.07.2017 12:00. URL: <https://psm7.com/news/fishing-v-ukraine-itogi-pervogo-polugodiya-2017-goda.html> (дата звернення: 30.10.2018).

Одержано 02.11.2018

УДК 343.988

**Наталія Юрїївна ЦВІРКУН,**

*кандидат юридичних наук,*

*викладач кафедри кримінального права і кримінології*

*факультету №1 (слідства)*

*Харківського національного університету внутрішніх справ;*

*ORCID: <https://orcid.org/0000-0001-9195-3349>*

## **ВІКТИМОЛОГІЧНА ПРОФІЛАКТИКА ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ ТОРГІВЛЕЮ ЛЮДЬМИ**

Віктимологічну профілактику, можна визначити як систему взаємопов'язаних, організаційно забезпечених державних, громадських й індивідуальних заходів, спрямованих на виявлення та усунення або нейтралізацію чинників, які формують особисту чи масову можливість стати жертвою злочину.

Залежно від цілей і завдань, віктимологічна профілактика має три рівні: загальносоціальний, спеціальний та індивідуальний.

**Загальносоціальний рівень** включає заходи, пов'язані з вирішенням соціально-економічних і культурно-виховних завдань, спрямованих на усунення чи нейтралізацію факторів, що сприяють процесу віктимізації людей.

**Спеціальний рівень** – це здійснення державними органами, громадськими об'єднаннями й окремими громадянами заходів, які мають своєю спеціальною метою попередження злочинів шляхом недопущення реалізації віктимних властивостей окремих груп осіб (підлітків, людей похилого віку, представників окремих професій тощо).

**Індивідуальний рівень** охоплює профілактичні заходи стосовно осіб, які, враховуючи їх поведінку або сукупність особистісних характеристик, можуть із великою ймовірністю стати жертвами злочинів. Такі заходи спрямовані на підвищення захисних реакцій, а також забезпечення особистої, майнової та іншої безпеки цих громадян [1].

Об'єктом віктимологічної профілактики є: фактори, що формують індивідуальну чи масову віктимність; обставини віктимної ситуації та процес віктимізації.

Систему суб'єктів віктимологічної профілактики становлять: