# Методи шахрайства у мережі Інтернет

Іванна Сабадаш
*Кафедра СКІД*
*Національний університет "Львівська політехніка"*
*Львів, Україна*
*ivanna.t.sabadash@lpnu.ua*

Нестор Думанський
*Кафедра СКІД*
*Національний університет "Львівська політехніка"*
*Львів, Україна*
*nestor.o.dumanskyi@lpnu.ua*

***Abstract. The activity of scammers was analyzed: methods and means of attracting users to visit illegal websites and provide their personal, compromising or financial information.***

**Ключові слова: шахрайство, веб-сайт, інформатизація, фішинг.**

Глобальна інформатизація уможливила здійснення швидких платежів через мережу Інтернет, покупки, навчання та роботу в режимі онлайн. Кожного дня у світі створюється близько мільйона веб-сайтів. Серед них, близько 25% мають на меті обдурити користувачів для отримання їхніх грошей або особистих даних (номерів банківських карток, логіни та паролі облікових записів, особисту компрометуючу інформацію для подальшого шантажу).

За даними Української єдиної міжбанківської асоціації (ЄМА) з усіх шахрайських дій, 65% припадає на використання Інтернет та соціальної інженерії. Використовуючи різноманітні психологічні прийоми, шахраї та аферисти виманюють персональні дані або схиляють користувачів до оплати фейкових пропозицій.

## ШАХРАЙСТВО В ІНТЕРНЕТІ

У випадку банкоматного шахрайства, банки іноді компенсують збитки, якщо їх можна підтвердити фактами. Але у соціальній інженерії підстав для компенсації немає, адже клієнт сам добровільно розкриває персональну інформацію або перераховує гроші. Деякі ініціативні банки можуть блокувати або вимагати додаткове підтвердження переказу коштів на рахунки, які мають підозрілий статус. Але, якщо клієнт таки підтвердив і здійснив операцію, повернути гроші буде досить складно. Зараз повернення можливе лише за умови визнання факту вчинення злочину судом.

Саме тому доцільно правильно ідентифікувати чи здійснення фінансових операцій не відбувається за шахрайською схемою. Основні схеми роботи шахрайських сайтів поділяються на копіювання/клонування офіційних сайтів та створення сайтів з коротким терміном існування (рис.1).

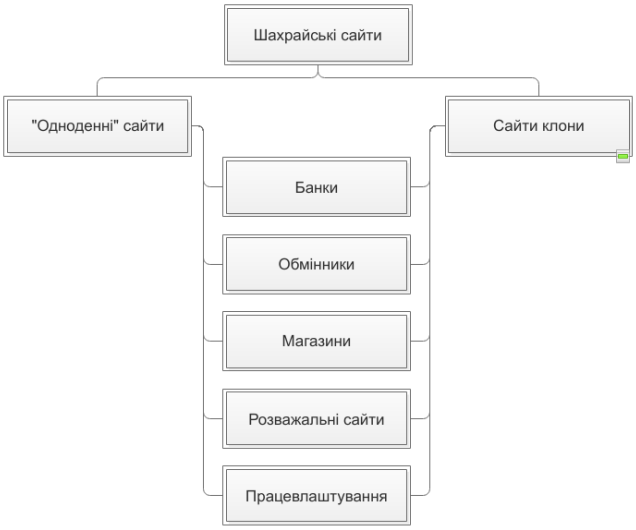


Рис.1. Основні напрямки роботи шахрайських сайтів

Для заманювання клієнтів на свої ресурси шахраї застосовують усі можливі засоби. До них належать і різноманітні розсилки (пошта, СМС, соціальні мережі, месенджери...), і реклама в різних системах та на сайтах, і навіть друковані листівки та реклама на біг-бордах. Варто пам'ятати як саме ви потрапили на певний сайт, адже клікнути на посилання – найлегший шлях, але не завжди найнадійніший.

Середовище Інтернету наповнене сайтами, які пропонують легкий заробіток, дешеві онлайн-курси, неймовірні виграші та інші способи легкого збагачення. За статистикою, близько третини таких сайтів виявляються



Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

шахрайським. Кожні пів хвилини у мережі Інтернет з'являється новий сайт, який призначений для виманювання грошей зі своїх користувачів. Шахрайство полягає у незаконному збагаченні власників сайту, отримання банківських, паспортних чи інших особистих даних.

Основний метод шахрайських схем – обман користувачів на сайтах розіграшів чи лотерей та пропозицій роботи в Інтернеті. За статистикою, яку склали користувачі Інтернету, банки, їхні клієнти та департамент кіберполіції, на них припадає більша частина випадків шахрайства. За ними у рейтингу йдуть фальшиві онлайн-магазини та пропозиції вивчення навчальних матеріалів. Немалу частку серед шахрайських займають ті сайти, які пропонують інвестувати гроші у бізнес, який має принести високі прибутки (криптовалюту, акції та облігації, коштовні матеріали, альтернативне паливо тощо). Сайти, які пропонують заробіток на соцопитуваннях і мають платну реєстрацію в більшості випадків також є обманом. На пострадянському просторі ще однією надзвичайно поширеною схемою шахрайства є пропозиція участі в азартних іграх. Швидкі кредити в Інтернеті пропонують сплатити комісію за надання кредиту, але в результаті не надають ніяких коштів своїм клієнтам, отримуючи їхні гроші і банківські дані. Деякі сайти обіцяють користувачам виплату компенсації за медичні витрати, субсидії, соціальні виплати чи перерахунки податків. Все це робиться заради отримання паспортних та банківських даних для подальшого збагачення шахраїв.

Одним із типів шахрайства в Інтернеті є фішинг. Під неправдивими приводами, придуманими зловмисниками, окремих осіб чи цілі організації змушують розкривати компрометуючу та особисту інформацію. Часто такий метод шахрайства називають «підводним полюванням» або фішинг-атаками. "Data breach and incident response" (DBIR) у своєму звіті опублікував результати досліджень, згідно з якими фішинг був основним вектором атак в 32% випадках всіх витоків даних. Найчастіше це відбувається у формі розсилки електронних листів з пропозиціями підтвердити реєстрацію облікового запису і посиланням на сайт, який повністю копіює дизайн оригінальних ресурсів. Це змушує користувачів самостійно розкривати конфіденційну інформацію. Одним із різновидів фішингу є фармінг. Це дії зловмисників, спрямовані на отримання конфіденційних даних шляхом незначної зміни DNS (Domain Name System) адреси, але інтерфейс сайту залишається незмінним з оригінальним. Це робиться для того, щоб користувач прийняв недостовірний сайт за справжній і без сумнівів ввів особисту інформацію.

Ретельна перевірка сайтів допоможе оминути схеми обману в Інтернеті. Існує декілька методів ідентифікації шахрайських веб-сайтів:

- самостійна перевірка;
- перевірка у базах даних шахрайських сайтів;
- онлайн сервіси перевірки.

## Висновки

Розвиток Інтернет-технологій та інформатизація суспільства відкриває великі можливості та доступність інформації, але з іншого боку вимагає обережності та захисту персональних даних.

З кожним роком можливості шахраїв зростають пропорційно до методів боротьби з ними. Знаючи схеми шахрайства у мережі, можна убезпечити себе від дій зловмисників.

## Література


[1] Шапочка, С. "До питання боротьби з шахрайством, яке вчиняється з використанням можливостей мережі Інтернет." Правова інформатика 3 (2014): 89-95.

[2] Кіпа, О. О. "Правопорушення в мережі Інтернет." Часопис Київського університету права (2010).

[3] Markovets O. Modeling of Citizen Claims Processing by Means of Queuing System/O. Markovets, A. Peleschyshyn// International Journal of Computer Science and Business Informatics (IJCSBI), Vol. 15, No. 1. January 2015. – P. 36-46.

[4] Markovets O., Dumanskyi N. The structure of the system of processing citizens' appeals // Econtechmod. – 2017. – Том 6 № 2. С. 33–38.





Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua