УДК 004.056

С.А. Думчиков
В.В. Лукічов

СТАТИСТИКА ФІШИНГОВИХ ІНЦИДЕНТІВ В УКРАЇНІ ЗА 2021 РІК

Вінницький національний технічний університет

Анотація
В даній роботі звертається увага на статистику інцидентів, що пов'язані з фішинговим вмістом та ресурсами в Україні станом на 2021 рік.
Ключові слова: Фішинг, Україна, статистика.

Abstract
This work draws attention to the statistics of incidents related to phishing content and resources in Ukraine as of 2021.
Keywords: Phishing, Ukraine, statistics**.**

Вступ

Фішинг – це шахрайська атака, що здійснюється через Інтернет з метою отримання та використання без авторизації конфіденційної інформації користувачів Інтернету, такої як імена користувачів, паролі, дані кредитної картки та дані банківського рахунку. Фішинг – одна з найчастіших форм кіберзлочинності, з якою стикаються користувачі Інтернету і є порушенням принципів кібербезпеки. Деякі спроби фішингу, що широко використовуються, включають використання спуфінгу електронної пошти або обміну миттєвими повідомленнями з метою переконати жертву відвідати підроблені веб-сайти, що призведе до отримання інформації про потерпілого. У звіті Phishlabs про тенденції в області фішингу за третій квартал 2021 року [1] згадується, що об'єм фішингу зріс майже на 32% у порівнянні з 2020 роком, вішингові (голосовий фішинг) інциденти зросли більш ніж вдвічі другий квартал поспіль, загрози соціальних медіа зросли на 82% з січня 2021 року, кількість фішингових повідомлень на Office 365 збільшується 4 квартали підряд, зловмисники покладаються на різні вектори атак: електронну пошту, соціальні мережі, мобільні пристрої та інші. У фішерів також є доступ до безкоштовних SSL-сертифікатів. Майже половина всіх фішингових веб-сайтів в даний час використовує протокол HTTPS, який був одним з основних індикаторів легітимності веб-сайтів [2].

Результати дослідження

За даними опитування, проведеним OLX [3] серед 55 тис. покупців у серпні 2021 року, з 01.01.2020 року по 01.07.2021 року відсоток українців, які звернулися б до правоохоронців через шахрайські дії, впав з 21% до 10%. Водночас 50% стикнулися зі зловмисниками в інтернеті, а 14% втратили кошти через фішинг. Мешканці Київської, Дніпропетровської та Харківської областей найбільше страждають від онлайн-шахраїв. Найчастіше фішинг-атаки відбуваються через популярні месенджери. У період з 01.01.2021 по 01.07.2021 45% з опитаних українців стикалися зі спробами онлайн-шахрайства. В той самий період 2020 року цей показник був 22%. Найчастіше з початку 2021-го атакують жителів великих міст – дві треті випадків. Кіберзлочинці намагаються активніше атакувати жіночу аудиторію, але їх жертвами часто стають і чоловіки (40% чоловіків та 60% жінок). Більше половини шахрайських інцидентів (54%) – продаж вигаданих товарів з передоплатою. На другій позиції (28%) – фішингова атака, коли у месенджерах користувачам надсилали посилання на підробну платіжну форму. На третій позиції (11%) – шахрайство з надсиланням фейкових скріншотів/квитанцій про оплату товару. Після фішингових атак шахраїв у 2021 році під час онлайн-шопінгу 14% жертв втратили свої кошти. Здебільшого (83% випадків) сторонні посилання на шкідливі сайти надходили у месенджери (Telegram, Viber, WhatsApp). 6% жертв отримали фішингове посилання через SMS, через пошту шахраї практично не атакують українців – таких спроб зафіксували лише 2%. У порівнянні зі схожим опитуванням OLX

у 2020 році [4], значно знизилася частка українців, які звернуться до поліції та служби підтримки ресурсу у випадку шахрайства (табл. 1).

Таблиця 1 – Статистика реагування на шахрайські дії

Що ви робите, якщо стикаєтесь із шахрайством в інтернеті? (оберіть декілька варіантів)	2020 рік	2021 рік
Намагаюся розв'язувати свої питання самостійно	35%	41%
Розповідаю близьким	48%	32%
Звертаюся до Служби підтримки онлайн-ресурсу	58%	17%
Звертаюся до Кіберполіції	21%	10%
Не роблю нічого	17%	26%

У період з 01.01.2021 по 01.07.2021 6 тис. осіб із 55 тис. опитаних отримували фішингове посилання від шахраїв. 18% українців, які стикалися із шахрайством у 2021 році, не знають жодного способу захисту своїх платіжних даних. А про методи протидії шахрайству 51% опитаних в цьому році вже дізналися з соцмереж, 31% – від друзів, 18% – з телебачення. Майже 40% українців уже знають, що надіслані посилання від малознайомих людей можуть бути шахрайською атакою, тому не відкривають їх і не обговорюють фінансові питання в месенджерах, якщо співрозмовник поводиться підозріло. 20% перевіряє користувача за номером телефону, 14% – уважно вчитується в зміст сторонніх SMS та email-листів, а 10% – перевіряє посилання сайтів, щоб не потрапити на шахрайський сайт-копію [3].

Багато методів використовують для шахраювання над українцями в інтернеті: пенсіонерів ошукують, наприклад, утричі частіше за інших – через SMS про виграш у лотерею, кожного четвертого підлітка після відкриття фішингового посилання. Мешканці сіл частіше натрапляють на продаж неіснуючого товару по передоплаті, а кияни – на фішингові атаки. Стать, до речі, практично не впливає на вірогідність зустріти шахрая в інтернеті. Такі дані наводить аналітична служба OLX [4], згідно з результатами опитування 25 тис. користувачів інтернету. Місце проживання значно впливає на тип шахрайств. Наприклад, дві треті жителів селищ міського типу та сіл стикаються зі спробами продати їм неіснуючий товар за передоплатою, а от жителі міст у 1,5 раза частіше отримують фішингові посилання. Жителі райцентрів на третину частіше за інших стикаються з підробленими квитанціями про оплату. У селах в цілому менше обізнаних з базовими правилами кібербезпеки. Якщо понад 42% містян не ведуть спілкування за межами платформи, де здійснюють угоду, та не відкривають посилання від незнайомих людей, то серед мешканців сіл – це тільки 33% опитаних. Водночас жителі столиці найбільше потерпають від фішингу (36% від всіх видів онлайн-шахрайств у Києві), а от у Дніпрі, Одесі, Харкові та Львові половина випадків пов'язана з передоплатою неіснуючого товару. Найбільш відповідально до звернень у Кіберполіцію ставляться у Львівській області – кожний 8-ий ошуканий подасть заяву, а найменш – в Одеській – тут звернеться тільки кожний 14-ий. Серед всіх вікових категорій 80% випадків онлайн-шахрайств відбуваються у месенджерах (Viber, Telegram, WhatsApp). Пенсіонерам утричі частіше надсилають шахрайські SMS, у сім раз електронні листи про "виграш в лотерею", "нові умови тарифу" чи "правила карантину". Водночас 57% українців віком від 46 до 65 років натрапили на шахраїв, які просили зробити передоплату за неіснуючий товар. Молодь віком 18-25 років у кожному третьому випадку натрапляє на фішинг, а кожний четвертий неповнолітній втратив гроші після переходу за шкідливим посиланням на сайт підробку відомого бренду. Це пов'язано з тим, що молодь більше за старше покоління проводить час в онлайні, але так само слабо обізнана з базовими правилами кібербезпеки. Молодь більш обізнана з базовими правилами кібербезпеки, однак загальний рівень навичок онлайн-поведінки лишається невисоким(табл. 2).

Таблиця 2 – Статистика 05.10.2021

Правила кібербезпеки	до 18 років	після 65 років
Не відкривають посилання від незнайомців	48%	28%
Не розголошують платіжні дані банківської картки	30%	29%
Звертають увагу на оцінки і відгуки	38%	19%
Не обговорюють угоду поза платформою (у сторонніх месенджерах)	39%	38%
Перевіряють посилання на olx.ua	14%	7$
Перевіряють номер продавця/покупця в базах відгуків	26%	21%

Продовження таблиці 2

Уважно оцінюють текст в SMS чи пошті	22%	14%
Звертають увагу на манеру спілкування (наприклад, чи є психологічний тиск або маніпуляції)	45%	38%

Водночас про кібербезпеку 65% неповнолітніх та 48% пенсіонерів дізнаються з соцмереж, 38% та 23% – від друзів та родичів, а от кожен третій українець віком від 65 років – з освітніх проєктів. Стать практично не впливає на вірогідність натрапити на шахрая. І чоловіки (78%), і жінки (88%) отримують шкідливі посилання від шахраїв у Viber, Telegram чи WhatsApp. Чоловікам удвічі частіше за жінок надходять шахрайські SMS (виграш в лотерею, “ви виграли авто”) – 9% проти 4% від всіх випадків відповідно [5].

Висновки

Згідно представлених даних, менше 50% опитаних респондентів приділяють належну увагу до особистої безпеки. Дана статистика відображає необхідність до підвищення безпеки користувача під час користування інтернет-ресурсами. В даний час запобігання фішингових атак вважається складним завданням в області безпеки систем. Ефективна система виявлення повинна мати можливість виявляти фішингові інформаційні ресурси з невеликою кількістю помилкових спрацьовувань.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. QUARTERLY THREAT TRENDS & INTELLIGENCE REPORT NOVEMBER 2021. URL: https://info.phishlabs.com/hubfs/PhishLabs%20-%20QTTI%20Report%20-%20November%202021.pdf.
2. Patrick Nohe. HTTPS Phishing: 49% of Phishing Websites Now Sport The Green Padlock. URL: https://www.thesslstore.com/blog/https-phishing-green-padlock/.
3. Українці почали вдвічі частіше стикатися з шахраями в інтернеті, найбільше – в месенджерах: результати опитування. URL: https://blog.olx.ua/26779/ukra%d1%97nci-stali-vdvichi-chastishe-stikatisya-z-shaxrayami-v-interneti-najbilshe-v-mesendzherax-rezultati-opituvannya/#.
4. Що знають користувачі про безпеку в інтернеті: результати опитування. URL: https://blog.olx.ua/24800/shho-znayut-koristuvachi-pro-bezpeku-v-interneti-rezultati-opituvannya/.
5. OLX Trust Safe. URL: https://safety.olx.ua/.

Думчиков Станіслав Андрійович – студент групи 1БС-20м, факультет інформаційних технологій та комп’ютерної інженерії, кафедра ЗІ, Вінницький національний технічний університет, м. Вінниця, email: mechanikea@gmail.com.

Лукічов Віталій Володимирович – кандидат технічних наук, старший викладач кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Stanislav Dumchykov – student, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: mechanikea@gmail.com.

Vitaliy Lukichov – PhD (Eng), Senior Lecturer of Information Protection Department, Vinnytsia National Technical University, Vinnytsia.