УДК 336.719

В. А. Янковська

КІБЕРШАХРАЙСТВО

Харківський інститут ПрАТ «ВНЗ «МАУП»

Анотація. *У статті досліджено проблему кібершахрайства та шляхи боротьби з незаконним заволодінням коштів***.**

Ключові слова: кібершахрайство; банк; платіжна карта.

CYBER FRAUD

Abstract. *The article examines the problem of cyber fraud and ways to combat the misappropriation of funds*.

Key words: cyber fraud; bank; payment card.

Пандемія COVID-19 змусила більшість підприємств і організацій у всьому світи перейти на віддалену роботу. Ця тенденція дала можливість шахраям розвивати більш витончені засоби махінацій, змушувати людей надавати доступ до конфіденційної інформації.

Розглянемо найбільш популярні види шахрайства, які все частіше мають місце і в Україні. Взагалі, шахрайство це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою та вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки [1].

Існує багато ознак класифікацій шахрайства, але найбільшого поширення в останній час став такий вид, як шахрайство у мережі Інтернет. До них відносять:

1) шахрайство з телефоном та Інтернетом: а) вішинг - (vishing) - voice fishing - вивудження за допомогою голосу; б) смішинг -SMiShing - похідна від «SMS» + «фішинг» - вивудження через SMS-повідомлення;

2) шахрайство з банкоматом: а) скіминг - (skimming) - не дайте чужій ложці зняти ваші вершки; б) траппінг - (card trapping) - не роби з себе маріонетку; в) фантом - (phantom) - визнач за зовнішнім виглядом, чи є зміст; г) шаттер - (cash trapping) - дочекайся запитаного; д) шиммінг -(shimming) - не допустіть прихованого посередництва;

3) шахрайство з платіжними картками: а) трешинг -(trashing) - все своє носи з собою; б) фармінг - (farming) - не культивуй на своїй ділянці рослину-паразит; в) фішинг - (fishing)– не попадись на гачок [2].

Отже, зупинимося на такому поширеному на сьогодні виді шахрайства як фішинг (англ. від fishing — риболовля) — вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів. Шахраї намагаються змусити користувачів самостійно розкрити конфіденційні дані — наприклад, надсилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів [3].

Способів фішингу безліч. Найпоширеніші з них наступні:

- направлення листа електронною поштою з повідомленням про виграш у лотерею та прохання надіслати реквізити картки для зарахування грошового призу;

- направлення листа начебто від банку з проханням надіслати реквізити картки для її підтвердження/розблокування та ін.;

- використання шахрайських Інтернет-сайтів (Інтернет-магазинів);

- використання вікон, що спливають та не мають стосунку до сайту, через який здійснюється операція;

- перенаправлення на шахрайські сайти за допомогою модифікації посилань;

- телефонні дзвінки начебто з банку, комунальних підприємств, контролюючих або правоохоронних органів з проханням підтвердити реквізити картки у зв’язку з підозрою шахрайських операцій, наявності уявної заборгованості, уточнення щодо платежів та ін.;

- крадіжка даних з комп'ютера за допомогою шкідливого програмного забезпечення (віруси, програми віддаленого доступу та ін.) [4].

Так, за даними дослідження Atlas VPN Google було виявлено у 2020 році рекордну кількість фішингових сайтів – 2,11 млн., що на 25% більше, ніж у попередньому році, коли було виявлено всього 1,69 млн. шкідливих доменів [5].

Тенденцію щодо кількості фішингових сайтів за останні 10 років можна проаналізувати за допомогою таблиці 1.

Таблиця 1 – Кількість фішингових сайтів, виявлених Google у 2010-2020 роках [6]

Рік	Кількість виявлених фішингових сайтів, млн.	Рік	Кількість виявлених фішингових сайтів,млн.
2010	0,11	2016	0,57
2011	0,07	2017	0,70
2012	0,10	2018	1,18
2013	0,14	2010	1,69
2014	0,12	2020	2,11
2015	0,27		

Отже, найбільше зростання спостерігається за останні 5 років, з 2016 року кількість таких сайтів зросла на 27%.

В Україні ситуація не набагато краща, аніж у світі. Як повідомляється на сайті НБУ, на 1 мільйон гривень видаткових операцій з картами у 2019 році припало 42 гривні незаконних або сумнівних операцій, а в середньому на одну незаконну операцію у 2019 році припадало близько 2100 гривень. Найбільша кількість незаконних дій з платіжними картами у 2019 році припало на операції в мережі Інтернет - 41,4 тисячі випадків або 58% від загальної кількості, але у порівнянні з 2018 роком цей показник знизився майже вдвічі. Для незаконних дій з картами шахраї найчастіше використовували метод соціальної інженерії, вводячи громадян в оману і з'ясовуючи персональні дані. кількість операцій з використанням платіжних карт в Україні у 2019 році у порівнянні з попереднім роком зросла на 29% - до 5 мільярдів штук, а обсяг цих операцій - на 24%, до 3,6 трильйона гривень [7].

Боротьбу з різного роду шахрайства більш наполегливо почали в Україні у 2020 році, коли у липні Національний банк України запустив Всеукраїнську інформаційну кампанію з протидії платіжному шахрайству. Мета кампанії – навчити українців основним правилам безпеки безготівкових та online-платежів. До кампанії виявили бажання долучитися понад 50 партнерів-представників соціально відповідального бізнесу найрізноманітніших галузей. Спільними зусиллями Національного банку, Кіберполіції, банків, платіжних систем, мобільних операторів, інтернет-магазинів було проведено безпрецедентну інформаційну кампанію [8].

На законодавчому рівні боротьба із незаконним заволодінням коштів проходить у вигляді прийняття необхідних законодавчих актів. Так, у Верховній Раді України зареєстрований законопроект № 4364 про платіжні послуги [9], що здатний суттєво осучаснити регулювання діяльності українського ринку платежів та переказу коштів. Цей документ базується на сучасних вимогах та враховуватиме норми європейських регуляторних актів, зокрема Другої платіжної директиви (PSD2), Директиви з електронних грошей (EMD). Ухвалення цього законопроекту дозволить адаптувати законодавство України до законодавства ЄС, сформувавши правову основу для інтеграції українського платіжного ринку з європейським. Крім того, це сприятиме модернізації платіжного ринку України та створить підґрунтя для подальшого його розвитку [10].

Незалежна асоціація банків України (НАБУ) реалізує проект «Протидія кіберзлочинності». Сайт проекту – це джерело отримання інформації про: боротьбу з кіберзлочинністю в Україні та світі; основні види та загрози кібершахрайства у фінансовій сфері; превентивні заходи, що допоможуть не стати жертвою кіберзлочинців; правила поведінки у випадку виявлення шахрайських дій тощо [11].

Отже, виходячи в викладеної вище інформації, користувачам банківських послуг слід дотримуватися таких основних правил:

- регулярно навчати працівників сфери банківських послуг, шляхом моделювання випадків з реального життя;

- створювати додатковий рівень захисту за допомогою двофакторної аутентифікації;

- користувачам, перед введення даних уважно перевіряти адреси порталу, який повинен починатися з HTTPS; за жодних обставин не передавати третім особам паролі та реквізити картки; не переходити на сумнівні посилання; не користуватися послугами підозрілих і маловідомих компаній; використовувати лише ліцензійне програмне забезпечення та вчасно його оновлювати; з усіх питань стосовно обслуговування карток звертатися безпосередньо до відділення банку та відповідного фахівця за роз'ясненням.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кримінальний кодекс України, ст.190. URL: https://zakon.rada.gov.ua/laws/show/2341-14/page6#Text (дата звернення: 19.01.2021).

2. Види шахрайства. Антикібер. URL: http://www.anticyber.com.ua/fraud.php (дата звернення: 19.01.2021).

3. Фішинг. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Фішинг (дата звернення: 19.01.2021).

4. Фішинг. Антикібер. URL: http://www.anticyber.com.ua/fraud_detail.php?id=20 (дата звернення: 19.01.2021).

5. A record 2 million phishing sites reported in 2020, highest in a decade. URL: https://atlasvpn.com/blog/a-record-2-million-phishing-sites-reported-in-2020-highest-in-a-decade (дата звернення: 19.01.2021).

6. У 2020 році кількість виявлених фішингових сайтів стало рекордним за 10 років. URL: https://minfin.com.ua/ua/2021/01/14/58552994/ (дата звернення: 19.01.2021).

7. Україна скоротила збитки від шахрайських дій з платіжними картками. URL:https://www.unian.ua/economics/finance/10905314-ukrajina-skorotila-zbitki-vid-shahrayskih-diy-z-platizhnimi-kartkami.html (дата звернення: 19.01.2021).

8. Стартувала інформаційна кампанія Національного банку з протидії платіжному шахрайству. URL: https://bank.gov.ua/ua/news/all/startuvala-informatsiyna-kampaniya-natsionalnogo-banku-z-protidiyi-platijnomu-shahraystvu (дата звернення: 19.01.2021).

9. Проект Закону про платіжні послуги. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70412 (дата звернення: 19.01.2021).

10. Клієнтоорієнтованість та підвищення якості платіжних послуг. URL: https://bank.gov.ua/ua/news/all/kliyentooriyentovanist-ta-pidvischennya-yakosti-platijnih-poslug--u-verhovniy-radi-zareyestrovano-zakonoproyekt-pro-platijni-poslugi (дата звернення: 19.01.2021).

11.Ціль проекту Антикібер. URL: http://www.anticyber.com.ua/aim.php (дата звернення: 19.01.2021).

Янковська Вікторія Анатоліївна, кандидат економічних наук, доцент, доцент кафедри менеджменту, Харківський інститут ПрАТ «ВНЗ «МАУП», Харків, e-mail: vika_yank2020@ukr.net

Yankovska Viktoriia A. - Doctor (Candidate) of Economic Sciences, Docent, Associate Professor of the Department of Management, Kharkiv Institute Interregional Academy of Personnel Management, Kharkiv, e-mail: vika_yank2020@ukr.net