Овсієнко І. В.,
здобувач вищої освіти обліково-фінансового факультету
Науковий керівник – **Мікуляк К.А.,**
асистент кафедри фінансів, банківської справи та страхування,
Миколаївський національний аграрний університет, м. Миколаїв

ОНЛАЙН-ШАХРАЙСТВО ТА ФІШИНГ: ЗАГРОЗИ Й ЕФЕКТИВНІ СПОСОБИ ПРОТИДІЇ

Інтернет-фішинг – одна з найпоширеніших форм онлайн-шахрайства, при якій зловмисники створюють фейкові листи або сайти від імені банків, соцмереж чи інших організацій, щоб викрасти паролі чи дані кредитних карток [1]. Шахраї також можуть імітувати державні установи чи благодійні організації, щоб обдурити довірливих людей [2]. Для убезпечення сімейного бюджету важливо розуміти типові схеми: наприклад, фальшиві інтернет-магазини пропонують «вигідні» покупки з передоплатою, а потім зникають із грошима. Інколи шахраї телефонують, видаючи себе за працівників банку чи поліції, і змушують жертв терміново переказувати кошти. Проте, як свідчить практика, вміти розпізнавати підозрілі сигнали можна: у фішингових повідомленнях часто містяться граматичні помилки, підозрілі посилання і невластиві організаціям формулювання [1]. За даними експертів, зловмисники у 2023 р. почастішали та вдаються до соціальної інженерії навіть в месенджерах – наприклад, видаючи себе за родичів, що нібито потрапили в біду, аби виманити гроші.

Щоб не піддаватися паніці, перш за все варто не поспішати з рішеннями. Кіберексперти радять «зупинитися і подумати» перед тим, як надсилати кому-небудь гроші або повідомляти персональні дані. Інформація про можливу проблему може бути неправдивою, тому відразу необхідно звертатися за підтвердженням через офіційні канали. Відомо що шахраї часто створюють відчуття терміновості, тому, щоб уникнути маніпуляцій, слід завжди перевіряти джерело інформації та не довіряти заявам «це потрібно зробити прямо зараз» [2]. Кіберполіція закликає користуватися лише офіційними сайтами урядових або відомих організацій [2] і не повідомляти незнайомцям конфіденційну інформацію (номери телефонів, паролі, дані карток тощо) [2, 3].

Перевірка адрес і змісту повідомлень – ще один важливий захід захисту. Перед тим як ввести якісь дані, необхідно звернути увагу на URL сайту – він має точно відповідати офіційному (правильно писатися, містити протокол «https» і значок замка) [1]. Навіть ці показники не завжди гарантують безпеку, але їхня відсутність одразу викликає підозри. У фішингових листах адреса електронної пошти чи домен зазвичай містить одну-дві змінені букви. Також у тексті може міститися прохання терміново оновити облікові дані або підтвердити транзакцію [1]. Не слід переходити за невідомими посиланнями та

завантажувати вкладення з підозрілих листів, навіть якщо лист виглядає офіційно, реквізити можуть вести на підроблений сайт або містити шкідливе ПЗ.

Часто атаки починаються з телефонного дзвінка чи SMS. У таких випадках експерти радять одразу «класти слухавку» і самостійно телефонувати в установу за офіційним номером. На сучасних смартфонах є вбудовані фільтри спаму та блокування анонімних дзвінків, тож виникає необхідність увімкнути ці функції й не відповідати незнайомим номерам. Не менш важливим є захист облікових записів. Важливо використовувати надійні, унікальні паролі для кожного сервісу [3]. Не варто повторно застосовувати один пароль для електронної пошти та онлайн-банкінгу. Рекомендується зберігати складні паролі в спеціальних менеджерах. До того ж обов'язковою є активація двофакторної автентифікації (2FA) там, де це пропонує сервіс [1, 3]. Двофакторна автентифікація додає другий шар безпеки: окрім пароля, необхідним є введення коду з SMS або з додатка, що робить доступ до рахунків особи надзвичайно складним для шахрая навіть у разі викрадення пароля [1].

Захист комп'ютера та смартфона – це ще один рівень безпеки, слід постійно оновлювати операційну систему, браузери й усі програми на пристроях [1], адже розробники регулярно виправляють уразливості, тому кожне оновлення допомагає запобігти атакам. Необхідно використовувати ліцензоване антивірусне програмне забезпечення та брандмауер [1, 3], а кіберполіція радить уникати підключення до невідомих або незахищених мереж Wi-Fi, особливо під час банківських операцій. Якщо необхідно користуватися загальнодоступним інтернетом (наприклад у кафе чи аеропорту), краще скористатися VPN або мобільним інтернетом, який є захищеним каналом.

Загальні рекомендації правоохоронців та фахівців такі: користувачам не слід повідомляти своїх банківських даних і паролів [2, 3], не слід вірити «занадто вигідним» пропозиціям – як зазначають експерти, якщо щось здається надто хорошим, щоб бути правдою, швидше за все, це оманливий хід шахраїв [3], зберігати пильність при будь-якій взаємодії в інтернеті: необхідно постійно перевіряти повідомлення, навіть начебто від знайомих, і не відкривати сумнівного контенту. Крім того, слід навчити цього членів родини: підвищення обізнаності про шахрайські схеми серед друзів і родичів значно знижує ризики потрапити на гачок аферистів [1, 4].

Отже, захист від онлайн-шахрайства вимагає системного та усвідомленого підходу. Поєднання знань про найпоширеніші фішингові схеми з технічними методами безпеки – регулярними оновленнями програм, використанням надійних паролів, двофакторної автентифікації та антивірусного захисту – суттєво зменшує ризик потрапити на шахрайські хитрощі. Постійна пильність, перевірка інформації з офіційних джерел і відмова від взаємодії з підозрілими контактами є ключовими умовами збереження особистих даних та

фінансових ресурсів. Дотримання цих рекомендацій дозволяє забезпечити надійний захист особистого і сімейного бюджету в цифровому середовищі.

Список використаних джерел:

1. Що таке фішинг та як від нього захиститися. Whitepay. URL: https://whitepay.com/uk/news/shho-take-fishing-ta-yak-vid-nogo-zahistitisya.
2. Інтернет-шахрайство: в МВС розповіли про методи протидії. Міністерство внутрішніх справ України. URL: https://mvs.gov.ua/news/internet-saxraistvo-v-mvs-rozpovili-pro-metodi-protidiyi.
3. Як розпізнати та захистити себе від онлайн-шахрайства. Європейська Бізнес Асоціація (EBA). URL: https://eba.com.ua/yak-rozpiznaty-ta-zahystyty-sebe-vid-onlajn-shahrajstva/.
4. Як не стати жертвою онлайн-шахраїв: кіберполіція розповіла про найпоширеніші схеми. URL: https://porady.org.ua/internet-shakhraystvo.