ШЛЯХИ ВИЯВЛЕННЯ І ЗАПОБІГАННЯ ШАХРАЙСТВУ В ІНТЕРНЕТ-ПРОСТОРІ

Навроцький І. С., *першого (бакалаврського) рівня вищої освіти факультету технологій та дизайну,*
Кондель В. М., *кандидат технічних наук, доцент, доцент кафедри професійної освіти, дизайну та безпеки життєдіяльності,*
Полтавський національний педагогічний університет імені В.Г. Короленка,
м. Полтава

Інтернет-простір став невід'ємною складовою нашого життя. За допомогою Інтернету ми можемо швидко та зручно здійснювати покупки, забронювати квитки на подорож, спілкуватися з друзями та родичами, а також здобувати знання. Проте, разом з багатьма корисними можливостями, Інтернет також приховує велику кількість ризиків та небезпек, однією з яких є шахрайство.

Шахрайство в Інтернеті – це злочинна діяльність, яка полягає у шахрайському обмані та шахрайському поводженні з людьми в Інтернеті з метою здобуття фінансової вигоди або іншої користі. Шахраї в Інтернеті використовують різні методи, щоб здійснити свої злочинні дії, включаючи фішинг, фармінг, шахрайські листи тощо.

У цій статті ми розглянемо шляхи виявлення та запобігання шахрайству в Інтернеті. Наша мета – допомогти студентам та викладачам розуміти проблему шахрайства в Інтернеті, виявляти підозрілі дії в Інтернеті та вживати дієві заходи для захисту від шахраїв.

Дослідження показують, що шахраї в Інтернеті стають все більш винахідливими та складними для відслідковування. Згідно з дослідженням, проведеним компанією Norton, у 2020 році тільки в США було виявлено понад 5,7 мільйонів випадків онлайн-шахрайства. Це призвело до збитків в розмірі більше ніж 3,3 мільярда доларів [1, 2, 3].

Згідно з даними Державної служби статистики України, за період з січня по вересень 2021 року було зареєстровано 2,5 тисячі випадків шахрайства в Інтернеті.

Крім того, у 2019 році Національна поліція України провела дослідження стосовно онлайн-шахрайства. Згідно з результатами цього дослідження, у 2018 році було зареєстровано близько 6 тисяч випадків шахрайства в Інтернеті, що на 16% більше, ніж у 2017 році. Найпоширенішим видом шахрайства в Інтернеті в Україні було шахрайство з використанням банківських карток та електронних грошей.

В Україні також проводяться дослідження стосовно випадків онлайн-шахрайства та розробки методів їх виявлення. Наприклад, у 2019 році проведено дослідження «Інформаційна безпека України», яке включало аналіз випадків онлайн-шахрайства та розробку рекомендацій щодо захисту від них.

Також існують окремі наукові роботи на тему виявлення шахрайства в Інтернеті в Україні. Наприклад, у 2017 році науковці з Національного університету «Львівська політехніка» розробили методику виявлення шахрайства в електронних комунікаціях на основі аналізу мовленнєвих характеристик повідомлень [4].

Такі дослідження та розробки допомагають поліпшити захист користувачів від шахрайства в Інтернеті в Україні та сприяють розвитку вітчизняної науки в галузі кібербезпеки.

Одним з найпоширеніших методів шахрайства в Інтернеті є фішинг. Фішинг – це спосіб шахраїв отримати чутливу інформацію від користувачів, таку як паролі, номери кредитних карток та інші особисті дані. Це робиться шляхом надсилання користувачам листів, що містять посилання на фальшиві веб-сайти, які дуже схожі на легітимні веб-сайти. Коли користувачі вводять свої особисті дані на таких веб-сайтах, шахраї можуть використовувати ці дані для злочинних цілей [3].

Іншим методом шахрайства в Інтернеті є фармінг. Фармінг – це спосіб шахраїв отримувати особисті дані користувачів, використовуючи фальшиві веб-сайти або комп’ютерні програми, які приховано встановлюються на комп'ютер користувача. Шахраї можуть використовувати отримані таким шляхом дані для здійснення різних злочинних дій, таких як крадіжка особистої інформації або шахрайські фінансові операції.

Інші методи шахрайства в Інтернеті включають шахрайські повідомлення (скам), які надсилаються користувачам електронної пошти, месенджерів або соціальних мереж і містять вимогу переказати гроші або надати особисті дані. Також можуть використовуватись такі методи, як соціальний інжиніринг, коли шахраї намагаються отримати доступ до чутливої інформації, використовуючи психологічний тиск на потенційну жертву або використовуючи розумні техніки обману.

Дослідження також показують, що багато людей не відчувають загрози шахрайства в Інтернеті, тому що вони не розуміють ризики, пов’язані з використанням Інтернету та соціальних мереж. На жаль, це може призвести до серйозних наслідків, які можуть включати фінансові збитки, втрату особистої інформації, викрадення ідентичності та інші.

Тому важливо, щоб користувачі знали про потенційні загрози та заходи, які можна вжити для запобігання шахрайству в Інтернеті. Далі ми розглянемо деякі з цих заходів.

Заходи для запобігання шахрайству в Інтернеті:

1. Будьте обережні з особистою інформацією: Ніколи не розголошуйте свої паролі, номери кредитних карток або інші особисті дані в Інтернеті, якщо необхідно, забезпечте додатковий рівень захисту, використовуючи двофакторну автентифікацію.

2. Будьте уважні зі спамом та фішингом: Ніколи не відкривайте посилання, які вам незнайомі або підозрілі, не завантажуйте файли з незнайомих джерел. Будьте уважні при відповіді на листи від незнайомих

відправників та при заповненні форм на сайтах, перевіряйте адресу сайту, щоб переконатися, що це дійсно сайт, на якому ви зазвичай реєструвалися.

3. Встановлюйте антивірус та оновлюйте його регулярно: Встановлення антивірусного програмного забезпечення є обов'язковим для захисту вашого комп'ютера від вірусів, троянів та інших шкідливих програм. Оновлюйте свій антивірус та операційну систему регулярно, щоб забезпечити їх ефективну роботу.

4. Використовуйте безпечні паролі: Паролі повинні бути складними та унікальними для кожного облікового запису. Використовуйте різні паролі для різних сайтів. Якщо ви маєте проблеми з запам'ятовуванням паролів, скористайтеся менеджером паролів.

5. Будьте уважні зі своїми соціальними мережами: Не діліться особистою інформацією з незнайомими людьми та не діліться приватними даними відкрито на вашій стіні. Дотримуйтеся налаштувань приватності та не приймайте запити на дружбу від незнайомих людей. Не діліться своїми особистими даними, наприклад, номерами телефонів, адресами електронної пошти та домашніми адресами.

6. Купуйте та завантажуйте програмне забезпечення з надійних джерел: Завжди перевіряйте джерело програмного забезпечення, яке ви купуєте або завантажуєте, перевірте відгуки користувачів та рейтинги. Використовуйте лише надійні і популярні маркети програмного забезпечення.

7. Захищайте свої файли: Робіть резервні копії важливих файлів та зберігайте їх в безпечному місці, такому як зовнішній жорсткий диск або хмарне сховище. Шифруйте свої файли та зберігайте їх в безпечному місці.

8. Використовуйте безпечні платіжні системи: Використовуйте платіжні системи з надійним захистом, такі як PayPal, Apple Pay, Google Wallet тощо. Ніколи не використовуйте публічні Wi-Fi-мережі для виконання фінансових операцій.

9. Навчайтеся розпізнавати шахрайство: Навчіться розпізнавати ознаки шахрайства в Інтернеті, такі як підозрілі електронні листи, спам, фішинг та інші. Знайомтеся зі списками найпоширеніших шахрайських схем та ніколи не підписуйтеся на підозрілі або невідомі сервіси.

10. Повідомляйте про шахрайство: Якщо ви стали жертвою шахрайства в Інтернеті або помітили підозрілу діяльність, повідомте про це відповідні служби та організації, наприклад, вашого банку або локальної поліції. Якщо ви маєте інформацію про шахрайство, також повідомте про це служби безпеки Інтернету або локальну поліцію. Це допоможе не тільки захистити вас, але і захистити інших користувачів від потенційних загроз.

Дослідження різних методів виявлення шахрайства в Інтернеті допомагає покращити ефективність заходів по запобіганню шахрайства. Існує два основних методи виявлення шахрайства в Інтернеті, які широко використовуються, це аналіз поведінки користувача та машинне навчання.

Аналіз поведінки користувача полягає у вивченні звичок та дій користувача в Інтернеті. Цей метод базується на зборі та аналізі великої

кількості даних про користувачів та їх поведінку в мережі. Наприклад, можна відстежувати, які сторінки відвідує користувач, які запити він вводить у пошукові системи, з яких пристроїв він заходить на сайт тощо. Ці дані можуть бути використані для виявлення шахрайських дій, наприклад, якщо користувач раптом змінив свої звички та почав вводити запити на незвичайні товари, це може свідчити про те, що його облапошують.

Інший метод – машинне навчання – полягає у використанні алгоритмів машинного навчання для виявлення шахрайства. Цей метод використовується для аналізу великої кількості даних, щоб знайти шаблони та ознаки шахрайства. Наприклад, можна створити модель машинного навчання, яка буде визначати, чи є певний сайт або транзакція шахрайською на основі ряду факторів, таких як тип пристрою, IP-адреса, країна походження тощо.

Організації, до яких можна звернутися за допомогою, зазвичай залежать від типу шахрайства, з яким ви стикаєтеся. Наприклад, якщо вас обманули в Інтернеті під час покупки товарів або послуг, зверніться до організації споживчого захисту. Якщо ви отримали шахрайський електронний лист, зверніться до служби безпеки Інтернету або поштової служби, яку ви використовуєте.

Також в Україні діють органи, які займаються протидією онлайн-шахрайству, зокрема, Національна поліція України та кіберполіція. Вони проводять профілактичну роботу серед населення, надають консультації щодо безпеки в Інтернеті та приймають звернення від громадян щодо випадків онлайн-шахрайства.

Статистика звернень до відповідних органів в Україні може коливатися в залежності від різних факторів, таких як рівень свідомості користувачів та ефективність заходів по боротьбі з шахрайством. Проте, за останні кілька років можна помітити зростання кількості звернень до правоохоронних органів та спеціалізованих служб з приводу онлайн-шахрайства в Україні.

За даними Міністерства внутрішніх справ України, у 2020 році зареєстровано більше 30 тисяч кримінальних правопорушень, пов’язаних з комп’ютерною злочинністю, що на 13,3% більше, ніж у 2019 році. Проте, варто зазначити, що не всі жертви шахрайства звертаються до правоохоронних органів, оскільки бояться втратити гроші, відкрити свої особисті дані, стати об’єктом соціального тиску або репресій з боку злочинців. Тому, важливо забезпечити конфіденційність і захист жертв шахрайства, щоб вони мали достатньо довіри до правоохоронних органів та повідомляли про злочини.

Також, в Україні функціонує Національна поліція, яка спеціалізується на боротьбі з кіберзлочинами та має відповідні підрозділи, наприклад, кіберполіцію. Ці органи ведуть роботу з виявлення та розслідування випадків шахрайства в Інтернеті та забезпечують захист прав інтернет-користувачів.

Також існують громадські організації та ініціативи, які працюють у напрямку просвіти та підвищення свідомості користувачів щодо безпеки в Інтернеті та шахрайства. Наприклад, такою ініціативою є проект «Захистись від

кіберзлочинів», який започаткований Національною поліцією в співпраці з партнерами.

Дуже важливо повідомляти про будь-яку підозрілу діяльність, навіть якщо ви не стали жертвою шахрайства. Це допоможе попередити інших користувачів про можливі загрози та дозволить службам безпеки Інтернету діяти швидко і ефективно.

Шахрайство в Інтернеті є серйозною проблемою, яка може призвести до великих фінансових втрат та порушення приватності користувачів. Проте, існують деякі методи, які можуть допомогти у попередженні шахрайства та захисті від нього.

Найважливішим кроком є збільшення свідомості користувачів про можливі загрози та ризики шахрайства в Інтернеті. Користувачі повинні бути обізнані з тим, які види шахрайства існують, як їх виявляти та як запобігати їм. Для цього можуть бути проведені спеціальні навчальні курси та семінари, а також здійснюватися роз'яснювальна робота через соціальні мережі та медіа.

Також важливим є застосування заходів безпеки та захисту даних в Інтернеті, таких як встановлення антивірусного програмного забезпечення, зберігання паролів в надійних місцях, та дотримання налаштувань приватності в соціальних мережах та інших сервісах.

Нарешті, важливо повідомляти про будь-яку підозрілу діяльність, яку ви помітили в Інтернеті. Це допоможе не тільки захистити вас, але і інших користувачів від можливих загроз.

Отже, онлайн-шахрайство є проблемою не тільки в світі, але й в Україні, і владні органи проводять заходи для боротьби з цією проблемою.

Усі ці кроки можуть допомогти знизити ризики шахрайства в Інтернеті та забезпечити більш безпечний та захищений Інтернет-простір [5, 6].

Список використаних джерел

1. Federal Trade Commission. (2021). How to Avoid a Scam (Як уникнути шахрайства): веб-сайт. URL : https://www.ftc.gov/office-inspector-general/ftc-imposter-scams (дата звернення : 22.03.2024).

2. National Cyber Security Alliance. (2021). Stay Safe Online: веб-сайт. URL : https://staysafeonline.org/ (дата звернення : 22.03.2024).

3. Norton Life Lock. (2021). What is Phishing? (Що таке фішинг?): веб-сайт. https://us.norton.com/blog/online-scams/what-is-phishing (дата звернення : 22.03.2024).

4. Звіт Національної поліції України про результати роботи у 2021 році. URL : https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit 2021/Zvit_NPU_2021_.pdf (дата звернення : 22.03.2024).

5. Про План реалізації Стратегії кібербезпеки України. URL : https:// zakon.rada.gov.ua/laws/show/n0087525-21#Text (дата звернення : 22.03.2024).

6. Кіберзлочинність та електронні докази = Cybercrime and digital evidence: навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан]; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с.