ДОСЛІДЖЕННЯ СУЧАСНИХ ПІДХОДІВ ДО ЗАХИСТУ ВІД ОНЛАЙН-ШАХРАЙСТВ ТА МАНІПУЛЯЦІЙ У ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ

Богдан БЕНЧАК, Ольга ЛУНГОЛ

Цифровий світ створює нові можливості для комунікації, бізнесу, навчання та доступу до інформації. Водночас із розвитком технологій зростає кількість випадків онлайн-шахрайств, що стає серйозною загрозою для користувачів. Зловмисники застосовують різні методи для отримання конфіденційної інформації, фінансових даних та незаконного доступу до персональних акаунтів. Тому, метою даного дослідження є аналіз сучасних видів онлайн-шахрайства та маніпуляцій й систематизація відповідних ефективних способів протидії цифровим загрозам.

Для дослідження видів онлайн-шахрайства, які є популярними на території України в наш час, ми проаналізувати матеріали офіційних сайтів Кіберполіції НПУ [1] та Державної служби спеціального зв’язку та захисту інформації України [2]. Значного поширення набули онлайн-шахрайства, пов’язані із відстеженням публічних повідомлень людей, які шукають інформацію про своїх близьких, що перебувають у неволі. Видаючи себе за волонтерів, журналістів, представників державних установ або навіть за осіб, пов’язаних із країною-агресором, шахраї пропонують організувати телефонний дзвінок, надати відомості про місцеперебування рідних чи сприяти їхньому звільненню. Під приводом надання допомоги зловмисники намагаються отримати конфіденційну інформацію: особисті дані військовослужбовців (ПІБ, підрозділ, звання, статус тощо), банківські реквізити, а також вимагають фото документів та інші особисті відомості. Щоб уникнути таких маніпуляцій та захистити себе від подібних шахраїв рекомендуємо дотримуватися наступних заходів безпеки:

- перед тим як передати будь-яку інформацію або виконати запит, перевірте, чи справді особа представляє ту чи іншу організацію. Це можна зробити через офіційні сайти, гарячі лінії або особисті контакти;

- уникайте спілкування з особами, які не можуть підтвердити свою особу офіційними документами або відповідними посвідченнями;

- переконуйтесь у справжності телефонних номерів та електронних адрес: шахраї часто використовують підроблені контакти, тому варто перевіряти їх через офіційні канали;

- ніколи не розголошуйте інформацію про військовослужбовців, їхні підрозділи, місце перебування чи статус. Не передавайте банківські реквізити, PIN-коди, фото документів та інші особисті дані;

- будьте обережні з фото- та відеоматеріалами, оскільки навіть звичайні фото можуть містити метадані (геолокацію, дату, час тощо);

- для спілкування використовуйте захищені месенджери (Signal, Telegram з таймером самознищення повідомлень), шифрування та VPN;

- встановлюйте оновлення для операційної системи та додатків, щоб усувати вразливості;

- використовуйте двофакторну автентифікацію (2FA);

- будьте уважні до підозрілих посилань, оскільки шахраї можуть надсилати фішингові листи або посилання, що ведуть на підроблені сайти.

Частково перетинається з поняттями онлайн-шахрайства та маніпуляцій у віртуальному середовищі кібернасильство, хоча не є їхньою складовою в класичному розумінні. Якщо онлайн-шахрайство – це здебільшого злочин, спрямований на отримання фінансової або особистої вигоди шляхом обману. Наприклад, фішинг, крадіжка особистих даних, підробка акаунтів, шахрайські збори коштів тощо. Натомість кібернасильство (кібербулінг, харасмент, сексторшен тощо) має на меті психологічний або емоційний вплив на жертву, а не прямий матеріальний зиск. Однак, у певних випадках ці явища можуть перетинатися, таких як сексторшен (сексуальний шантаж, зловмисники виманюють у жертви інтимні фото та шантажують їх, вимагаючи гроші або певні дії) та шахрайство з емоційним тиском.

В той же час кібернасильство можна вважати однією з форм маніпуляції у віртуальному середовищі, оскільки воно базується на впливі на емоції жертви (такі, як погрози, залякування, образи, шантаж тощо); використовує неправдиву інформацію або психологічний тиск (наприклад, створення фейкових акаунтів

для дискредитації людини); часто спрямоване на підрив репутації або соціального статусу особи.

Отже, кібернасильство не є класичним онлайн-шахрайством, але може включати шахрайські елементи, проте його можна віднести до маніпуляцій у віртуальному середовищі, оскільки воно передбачає психологічний та емоційний тиск на жертву. До основних підходів запобігання та боротьби з кібернасильством відносимо: правове регулювання та покарання, розробку освітніх програм з підвищення цифрової грамотності, технологічний захист та кібергігієну; психологічну підтримку жертв кібернасильства та активну громадська протидію у вигляді кампаній проти кібернасильства, флешмоби, ініціативи з підтримки постраждалих тощо.

До сучасних видів маніпуляцій у віртуальному середовищі також можна віднести:

- кібербулінг, оскільки використовує страх, залякування та образи для психологічного контролю;
- бодішеймінг – маніпулює почуттям невпевненості людини, змушуючи її відповідати нав’язаним стандартам;
- деднеймінг, оскільки навмисно підриває особисту ідентичність людини, створюючи психологічний дискомфорт;
- флеймінг – провокує агресію та ворожнечу, змушуючи людину реагувати емоційно;
- тролінг, викликаючи негативні емоції або провокуючи конфлікти для впливу на поведінку жертви;
- аутинг – порушує конфіденційність людини, піддаючи її соціальному осуду або дискримінації.

До основних рекомендацій відносимо: ігнорування провокацій; максимальне не розголошення персональної інформацію в мережі; використання налаштувань приватності на цифрових платформах; використання функції блокування й скарг у соціальних мережах для припинення кібербулінгу та мови

ворожнечі; розвиток цифрової грамотності та дотримання правил кібергігієни [1 – 3].

Онлайн-шахрайства та маніпуляції у віртуальному середовищі є серйозною загрозою, проте завдяки дотриманню базових правил кібербезпеки можна значно зменшити ризики. Критичне мислення, обережність із персональними даними та використання сучасних засобів цифрового захисту є ключовими інструментами у протидії зловмисникам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Рекомендації. *Кіберполіція НПУ*: URL: https://cyberpolice.gov.ua/articles/ (дата звернення: 29.01.2025).

2. Рекомендації. *Державна служба спеціального зв'язку та захисту інформації України*: URL: https://cip.gov.ua/ua/faqs (дата звернення: 29.01.2025).

3. Лунгол О.М. Роль кібергігієни у безпеці та розвитку українського суспільства. *Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів*: мат. VII Всеукр. науково-практ. конф., м. Одеса, 30 квітня 2024 р. Одеса: ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Центр соціально-політичних досліджень «Politicus», 2024. С. 268-270.

БЕЗПЕКА В МЕРЕЖІ: ЯК УНИКНУТИ ПАСТОК ОНЛАЙН-СПІЛКУВАННЯ

Олена ГОРОБЕЦЬ

У сучасному світі, де технології розвиваються з неймовірною швидкістю, онлайн-спілкування стало невід'ємною частиною нашого життя. Від соціальних мереж до відеоконференцій інтернет забезпечує нам безліч можливостей для взаємодії з людьми з різних куточків планети. Для багатьох людей набагато легше комунікувати онлайн, адже такий формат дозволяє уникнути безпосередньої взаємодії і почуватися більш комфортно. За умови безпечного