УДК 519.6

ВИЯВЛЕННЯ ШКІДЛИВИХ РЕСУРСІВ У СОЦІАЛЬНІЙ МЕРЕЖІ TELEGRAM ТА ПРАВИЛА БЕЗПЕЧНОЇ ПОВЕДІНКИ ОНЛАЙН

Наталія Чернящук, Юлія Камєнєва

DETECTION OF MALICIOUS RESOURCES IN THE TELEGRAM SOCIAL NETWORK AND RULES FOR SAFE ONLINE BEHAVIOR

Nataliia Cherniashchuk, Yulia Kameneva

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *This summary highlights the risks of fraudulent activity in Telegram, including phishing, identity theft, and deepfake video scams. It emphasizes the importance of digital literacy, two-factor authentication, and awareness of emerging cyber threats.*

Telegram є однією з найпопулярніших платформ обміну повідомленнями у світі, з понад 800 мільйонами активних користувачів щомісяця. Високий рівень довіри до платформи, зручність і псевдоанонімність роблять її привабливою не тільки для звичайних користувачів, але й для шахраїв та кіберзлочинців. Серед найпоширеніших загроз – міжособистісне шахрайство, фішинг, соціальна інженерія, а також використання Telegram як інструменту координації злочинної діяльності.

На тлі стрімкого зростання цифрової комунікації, платформи обміну повідомленнями, зокрема Telegram, стають не лише інструментом повсякденного спілкування, а й зоною підвищеного ризику для користувачів. Шахрайські схеми, фішинг, клонування акаунтів та використання deepfake-технологій стають дедалі поширенішими. Telegram при цьому часто використовується не тільки для особистих або корпоративних цілей, а й як канал для координації незаконних дій. Саме тому тема безпечної поведінки в месенджерах є вкрай актуальною, особливо в умовах кібергігієни, гібридної війни та зростання соціального інжинірингу.

Метою дослідження є виявлення сучасних шахрайських схем у соціальній мережі Telegram, аналіз їх механізмів та розробка рекомендацій щодо безпечної поведінки користувачів у мережі. Завдання дослідження: проаналізувати типові приклади шахрайства в Telegram на основі реальних кейсів; оцінити методи, які використовують кіберзлочинці для компрометації акаунтів і викрадення даних; визначити інструменти та сервіси, що використовуються для автоматизації атак; сформувати перелік практичних заходів цифрової безпеки, що можуть зменшити ризики для користувачів.

Однією з розповсюджених схем є так звана «Проголосуй, будь ласка». Жертві приходить повідомлення від нібито знайомої особи з проханням проголосувати за учасника конкурсу, зазвичай із прикріпленим посиланням або QR-кодом. Після переходу за цим посиланням користувача просять ввести персональні дані, включно з номером телефону. Після підтвердження через SMS-код шахраї отримують доступ до акаунта та використовують його для подальшого поширення шахрайства серед контактів.

Інша небезпечна схема – клонування профілю. Використовуючи спеціалізовані сервіси, зловмисники можуть визначити номер телефону жертви, створити фейковий акаунт із такими ж ім’ям, фото та біографією. Після цього вони звертаються до знайомих жертви з проханням позичити гроші, створюючи ілюзію реального прохання. Завдяки функціям Telegram щодо

деанонімізації, шахраї можуть відстежити активність користувача, використати отриману інформацію і налаштувати атаку персонально.

Значну небезпеку становлять шахрайства з використанням відеоповідомлень («кружечків»), які нібито надсилає сама жертва. За допомогою відеомонтажу або навіть технологій deepfake шахраї створюють фальшиві звернення, у яких користувач просить переказати гроші. Далі ці відео надсилаються знайомим або родичам, які довіряють людині, зображеній у повідомленні. Часто наслідком стає втрата коштів та контроль над акаунтом.

Ще однією новітньою формою обману є розсилка провокаційних або образливих повідомлень із захоплених акаунтів. Ціль – змусити отримувача перейти до профілю зловмисника, де в шапці зазначене посилання. Перехід за ним відкриває шлях до зараження пристрою або компрометації інших акаунтів, включно з Instagram чи поштою. Це фішингові атаки, спрямовані на викрадення даних через психологічний тиск і зацікавлення.

Окрему загрозу становлять дії, пов’язані з реальними злочинами, координованими через Telegram. Наприклад, в Україні були зафіксовані випадки поширення закликів до диверсій через наклейки з QR-кодами, які вели на проросійські ресурси. У Львові правоохоронці запобігли спробі теракту, який організували молоді особи на замовлення російських спецслужб. Виконавці отримали інструкції саме через Telegram.

Для запобігання подібним загрозам критично важливо дотримуватись правил цифрової гігієни: встановити двофакторну автентифікацію, не відкривати незнайомі посилання, регулярно змінювати паролі, обмежувати доступ до вашого акаунта через налаштування приватності. У випадку підозри на злам – негайно звертатись до Кіберполіції України, заблокувати банківську картку, повідомити оператора зв’язку та переглянути список активних сесій у Telegram.

Дослідження показало, що Telegram є одним із ключових каналів розповсюдження кіберзлочинності у форматі соціальної інженерії. Найнебезпечнішими проявами є персоналізовані атаки з використанням фейкових акаунтів, відеоповідомлень, посилань на фішингові ресурси, а також контент, який має ознаки ворожої пропаганди або диверсійної діяльності. Надзвичайно важливо формувати навички цифрової гігієни серед користувачів, своєчасно впроваджувати налаштування конфіденційності та перевіряти всі підозрілі дії. Підвищення обізнаності та грамотності у сфері кібербезпеки є запорукою безпечного користування соціальними мережами в умовах сучасних загроз.

Бібліографія

1. Кіберполіція України. Портал звернень громадян URL: https://ticket.cyberpolice.gov.ua/. Дата звернення: 25.04.2025.
2. Національний банк України. Сторінка про кіберзагрози та шахрайство URL: https://bank.gov.ua/. Дата звернення: 25.04.2025.
3. CheckMyLink. Онлайн-сервіс перевірки посилань URL: https://checkmylink.com/. Дата звернення: 25.04.2025.
4. Україна. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III (в редакції станом на 2025 рік) URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text . Дата звернення: 25.04.2025.