УДК 004.056.5

Н.В. Соловйов
Н.Р. Кондратенко

ФІШИНГ ЯК СОЦІАЛЬНЕ ЯВИЩЕ: ВПЛИВ ПАНДЕМІЙ ТА ВОЄННИХ КОНФЛІКТІВ НА ЗРОСТАННЯ АТАК

Вінницький національний технічний університет

Анотація. *У роботі досліджено фішинг як соціальне явище, що посилюється під час пандемій і воєн. Розглянуто вплив COVID-19 і війни в Україні на активність, роль психологічних маніпуляцій і засоби протидії, зокрема ШІ та кіберграмотність*.

Ключові слова: фішинг, кібератаки, соціально-психологічні маніпуляції, пандемія COVID-19, воєнні конфлікти, штучний інтелект, кіберграмотність.

Abstract. *The paper explores phishing as a social phenomenon intensified by pandemics and war. It analyzes the impact of COVID-19 and the war in Ukraine, the role of psychological manipulation, and countermeasures such as AI and cyber literacy.*

Keywords: phishing, cyberattacks, socio-psychological manipulation, COVID-19 pandemic, military conflicts, artificial intelligence, cyber literacy.

Вступ

Фішинг як інструмент соціальної інженерії дедалі більше виходить за межі технічного виміру та постає як соціальне явище, що використовує людські вразливості, зокрема страх, довіру та когнітивні упередження. У періоди глобальних криз (пандемій і воєн), кіберзлочинці особливо активно експлуатують ці чинники.

Метою дослідження є вивчення впливу глобальних соціальних криз на активізацію фішингових атак, а також оцінка ефективності сучасних підходів до протидії цим загрозам. Особливу увагу приділено аналізу соціально-психологічних факторів, що сприяють успіху фішингу, та можливостям їх нейтралізації через поєднання технічних рішень із підвищенням кіберграмотності населення.

Результати дослідження

Пандемія COVID-19 стала ключовим каталізатором для зростання фішингових атак, створюючи ідеальні умови для соціальних маніпуляцій. У 2020 році кількість фішингових кампаній, пов’язаних із тематикою пандемії, зросла на 600% порівняно з попередніми роками [1]. Часто обіцяли доступ до вакцин або фінансову допомогу, підштовхуючи жертв до швидких дій без перевірки джерел. Таймери та обмежені терміни були типовими елементами таких атак.

Віддалена робота зробила компанії вразливішими: слабкий контроль IT-інфраструктури та відсутність підготовки працівників до кіберзагроз підвищили успішність атак [4]. Фішингові листи, що імітували внутрішні корпоративні повідомлення, часто використовувалися для отримання облікових даних працівників. Організації, які не проводили регулярних тренінгів із кібербезпеки, мали на 30% вищий ризик компрометації даних [4].

Воєнні конфлікти, зокрема війна в Україні, створили унікальний контекст для фішингових атак, де соціально-психологічні маніпуляції відігравали ключову роль. З початку повномасштабного вторгнення у 2022 році кількість фішингових атак у країні зросла на 40%, що пояснюється інформаційним хаосом і високим рівнем емоційної напруги [2]. Кіберзлочинці використовували теми гуманітарної допомоги, зборів на підтримку армії та фальшивих новин для обману громадян і організацій. Наприклад, один із задокументованих випадків стосувався фальшивого сайту, який імітував платформу для збору коштів на дрони для Збройних сил України. Такі кампанії часто апелювали до патріотичних почуттів, використовуючи національну символіку, що підвищувало їхній успіх на 25% порівняно зі стандартними атаками [2].

Особливістю воєнного контексту є швидка адаптація зловмисників до новинного порядку денного. Фішингові кампанії з’являлися протягом кількох годин після резонансних подій, таких як обстріли чи гуманітарні ініціативи. Локалізована мова і символіка, як показали дослідження викликали особливу довіру в перші місяці конфлікту

[2].

Демографічні дані показують, що молоді користувачі (18-25 років) частіше ставали жертвами через брак досвіду, а старші (50+) – через надмірну довіру до «офіційно виглядаючих» повідомлень [3]. Кризи призводили до «інформаційного перевантаження», коли люди ігнорували перевірку доменів чи джерел. У пандемію 60% жертв не перевіряли посилання через стрес, у війну – через потік новин і тривожність [3].

Для ефективної протидії фішингу потрібне поєднання технічних рішень і освіти. Алгоритми ШІ досягають 95% точності у виявленні класичних фішингових схем, але стикаються з труднощами при нових, адаптивних атаках [1]. Вони здатні виявити незвичні домени або мовні конструкції, однак потребують постійного оновлення.

Кіберграмотність критично важлива. Освітні ініціативи, як-от українська кампанія «Обережно, фішинг!» у 2023 році охопила понад 2 мільйони людей і знизили кількість атак на 15% [2]. Короткі інформаційні кампанії через соціальні мережі чи SMS виявилися особливо ефективними в умовах воєнного часу. Наприклад, розсилка попереджень про фальшиві благодійні сайти зменшила кількість жертв на 10% у перші тижні після запуску [2].

Технічні рішення, такі як двофакторна автентифікація (2FA) і фільтри спаму, відіграють важливу роль, але їхня ефективність обмежена без належної освіти користувачів. Дослідження показало, що 40% жертв фішингу під час пандемії використовували двофакторну автентифікацію, але передавали дані через фальшиві форми, що імітували офіційні портали [4].

Висновки

Дослідження показало, що фішинг як соціальне явище тісно пов’язаний із кризовими контекстами, зокрема пандемією COVID-19 та воєнними конфліктами. Саме такі обставини створюють сприятливі умови для маніпуляцій, коли емоційний стан, інформаційне перевантаження та зниження критичності мислення значно підвищують вразливість користувачів. Зловмисники активно адаптують фішингові стратегії до актуального інформаційного середовища, використовуючи локалізовані повідомлення, символіку та мовні особливості.

Успішність фішингових атак залежить не лише від технічної складності, а й від психологічних і соціокультурних чинників. Тому ефективна протидія має бути комплексною: поєднувати сучасні технічні засоби (ШІ, 2FA, фільтрацію) з систематичним підвищенням кіберграмотності населення та швидким інформаційним реагуванням на нові загрози. Особливої актуальності це набуває в умовах криз, коли ціна інформаційної безпеки зростає багаторазово.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Al-Qahtani A. F. The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19 [Електронний ресурс] / Ali F. Al-Qahtani, Stefano Cresci // IET Information Security. – 2022. – С. 324–325. – Режим доступу: https://doi.org/10.1049/ise2.12073 (дата звернення: 05.05.2025).
2. Fyshchuk I. Managing cyberattacks in wartime: The case of Ukraine [Електронний ресурс] / Iryna Fyshchuk, Mette Strange Noesgaard, Jeppe Agger Nielsen // Public Administration Review. – 2024. – С. 619–627. – Режим доступу: https://doi.org/10.1111/puar.13895 (дата звернення: 05.05.2025).
3. Montañez R. Human Cognition Through the Lens of Social Engineering Cyberattacks [Електронний ресурс] / Rosana Montañez, Edward Golob, Shouhuai Xu // Frontiers in Psychology. – 2020. – Т. 11. – Режим доступу: https://doi.org/10.3389/fpsyg.2020.01755 (дата звернення: 05.05.2025).
4. Reddy Vaka P. Phishing attacks or COVID-19 and Remote Work Security [Електронний ресурс] / Pavan Reddy Vaka // Turkish Journal of Computer and Mathematics Education (TURCOMAT). – 2020. – Т. 11, № 3. – С. 3044–3052. – Режим доступу: https://doi.org/10.61841/turcomat.v11i3.14958 (дата звернення: 05.05.2025).

Соловйов Назарій Валерійович – студент 2 курсу групи 2БС-23б, факультет інформаційної технологій та комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: nazarsolovioff@gmail.com.

Кондратенко Наталія Романівна – к.т.н., проф., професор кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: kondratenko.natalia@vntu.edu.ua

Soloviov Nazarii Valeriiovych – second-year student of group 2BS-23b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: nazarsolovioff@gmail.com

Kondratenko Nataliia Romanivna – Phd in Technical Sciences, Professor, Department of Information Security, Vinnytsia National Technical University, Vinnytsia, email: kondratenko.natalia@vntu.edu.ua