УДК 004.056:316.77

Т.А. Присяжнюк

ФІШИНГ ЯК МЕТОД СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Вінницький національний технічний університет

Анотація

У тезах розглянуто фішинг як метод соціальної інженерії. Фішинг є одним із найпоширеніших методів соціальної інженерії, який використовується кіберзлочинцями для викрадення конфіденційної інформації, таких як логіни, паролі, банківські дані тощо. У роботі досліджуються основні механізми фішингових атак, їх різновиди та психологічні прийоми, на яких вони базуються. Також аналізуються сучасні методи захисту від фішингу, включаючи технічні рішення та підвищення обізнаності користувачів. Дослідження підкреслює важливість комплексного підходу до протидії фішингу, що поєднує технологічні засоби та освітні ініціативи.

Ключові слова: фішинг, соціальна інженерія, кіберзлочинці, механізми атак, методи захисту.

Abstract:

The thesis examines phishing as a method of social engineering. Phishing is one of the most widespread methods of social engineering, which is used by cybercriminals to steal confidential information, such as logins, passwords, banking data, etc. The work investigates the main mechanisms of phishing attacks, their varieties, and the psychological techniques on which they are based. Modern methods of protection against phishing are also analyzed, including technical solutions and raising user awareness. The research emphasizes the importance of a comprehensive approach to countering phishing that combines technological tools and educational initiatives.

Key words: phishing, social engineering, cybercriminals, attack mechanisms, methods of protection.

Вступ

У сучасних умовах цифровізації та активного використання гаджетів, актуальною є проблема фішингу. Цей вид соціальної інженерії ґрунтується на маніпуляції людською психікою, а не на технічних вразливостях систем, що робить його особливо складним для виявлення та профілактики. Фішинг-атаки постійно вдосконалюються: якщо раніше це були масові безособові розсилки, то зараз злочинці створюють індивідуальні сценарії, використовуючи сучасні технології, зокрема штучний інтелект. Вони вражають і приватних осіб, і компанії, призводячи до серйозних наслідків – втрати коштів, витоку даних або навіть повного доступу зловмисників до конфіденційної інформації. У цьому контексті постає необхідність як теоретичного осмислення проблеми, так і пошуку ефективних шляхів її вирішення.

Результати дослідження

Інтернет міцно пустив коріння майже в кожну сферу життя сучасної людини. Сучасне суспільство активно користується електронними платіжними сервісами, сплачує комунальні послуги через інтернет-банкінг, веде ділову та особисту електронну переписку. Ця повсякденна практика вимагає постійного введення персональних даних, що створює потенційні джерела кіберзагроз. Як тільки інтернет став доступним великій кількості людей, шахраї почали використовувати його як засіб для викрадення грошей, особистої інформації тощо.

Попри впроваджені найпотужніші системи кіберзахисту, ризик того, що зловмисники одержать доступ до конфіденційної інформації, все одно існує. Вся справа – у людському факторі. Часто шахраї навіть не намагаються скористатися системними вразливостями – їхні дії націлені на людей, їхні слабкості, емоції, розгубленість та неуважність. У цьому й полягає суть соціальної інженерії: маніпулюючи особливостями людської психіки, хакери одержують бажану інформацію.

Фішинг як метод соціальної інженерії має низку різновидів, кожен із яких відрізняється специфікою реалізації та цільовою аудиторією. Класичний електронний фішинг використовує листи для

викрадення даних. Більш цілеспрямований spear phishing атакує конкретних осіб чи організації, а вейлінг спеціалізується на топ-менеджерах. Для масових атак застосовують смішинг (SMS) [1] та вішинг (телефонні дзвінки) [2], які експлуатують довіру через інші канали зв'язку. Такі методи працюють через маніпуляції в соціальній інженерії, експлуатуючи слабкості людей.

Окремо варто виділити тактику бейлінг [3], яка ґрунтується на створенні штучної стресової ситуації з елементом терміновості, що спонукає жертву до негайних дій без належного аналізу. Претендування на особу передбачає імітацію довірених осіб (колег, фінансових установ чи знайомих), що дозволяє зловмисникам експлуатувати соціальну довіру для отримання конфіденційної інформації або контролю над фінансовими операціями.

Anti-Phishing Working Group (APWG) є провідною міжнародною організацією, яка спеціалізується на дослідженні та протидії фішинговим атакам. Заснована як коаліція експертів з кібербезпеки, фінансових установ та правоохоронних органів, APWG систематично збирає, аналізує та публікує дані про глобальні фішингові загрози. У останньому кварталі 2024 року APWG зафіксувала 989 123 фішингові атаки, що демонструє зростання порівняно з попередніми періодами – 877 536 атак у другому кварталі та 932 923 у третьому [4]. Серед основних тенденцій кварталу виділяється активність китайських фішерів, які масово використовували SMS-фішинг, підтримуваний новими злочинними інструментами та популярними доменними іменами.

Ефективна протидія соціальній інженерії вимагає комплексного підходу, що поєднує технологічні, організаційні та освітні компоненти. Підвищення кіберграмотності сприяє розвитку критичного мислення та навичок ідентифікації потенційних загроз. Технічні засоби захисту, такі як багатофакторна аутентифікація, регулярне оновлення програмного забезпечення та шифрування даних, створюють додаткові бар'єри для зловмисників. Ключову роль відіграє організаційна культура безпеки, яка передбачає систематичні тренінги, чіткі протоколи дій та усвідомлення кожним співробітником власної відповідальності за захист інформації.

Висновки

Фішинг як метод соціальної інженерії продовжує залишатись критичною загрозою кібербезпеці, використовуючи складні психологічні механізми маніпуляції. Проведене дослідження демонструє, що сучасні фішингові атаки еволюціонують від примітивних масових розсилок до витончених цільових методів, таких як spear phishing та вейлінг, що значно підвищує їх небезпеку. Основною слабкою ланкою залишається людина, оскільки зловмисники вправно експлуатують емоційні стани, соціальну довіру та когнітивні упередження жертв. Для ефективного протистояння фішингу необхідний комплексний захист, який поєднує технологічні інструменти, постійне навчання персоналу та чіткі організаційні процедури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Чим смішинг відрізняється від фішингу і як від нього захиститися? - HackYourMom [Електронний ресурс] // HackYourMom. – Режим доступу: https://hackyourmom.com/kibervijna/chym-smishyng-vidriznyayetsya-vid-fishyngu-i-yak-vid-nogo-zahystytysya/(дата звернення: 11.06.2025). – Назва з екрана.
2. Вішинг – що це, які особливості вішинга і популярні схеми. ESET. [Електронний ресурс] // ESET. – Режим доступу: https://www.eset.com/ua/support/information/entsyklopediya-zahroz/vishynh/?srsltid=AfmBOorgZRgsBLQx_Q6WD_Luto_G1ydLjFaFqwvzwJByt4zRA8KsuyoF(дата звернення: 11.06.2025). – Назва з екрана.
3. Соціальна інженерія як засіб маніпуляції в інформаційному просторі - Соціальна країна [Електронний ресурс] // Соціальна країна. – Режим доступу: https://welfare.green/socialna-inzheneriya-yak-zasib-manipulyacii-v-informacijjnomu-prostori/(дата звернення: 11.06.2025). – Назва з екрана.
4. APWG | Phishing Activity Trends Reports [Електронний ресурс] // APWG | Unifying The Global Response To Cybercrime. – Режим доступу: https://apwg.org/trendsreports/(дата звернення: 11.06.2025). – Назва з екрана.

Присяжнюк Тетяна Анатоліївна – студентка факультету менеджменту та інформаційної безпеки, Вінницький національний університет, м. Вінниця, електронна пошта: pristaniya25@gmail.com

Науковий керівник: ***Зоря Ірина Сергіївна*** – асистент, магістр з кібербезпеки, Вінницький національний технічний університет, м. Вінниця, електронна пошта: ira.zoria@vntu.edu.ua

Prysiazhniuk Tetiana A. – Department of Information Systems Management and Security, Vinnytsia National Technical University, Vinnytsia, e-mail : pristaniya25@gmail.com

Supervisor: ***Zorya Iryna S.*** – assistant, master in Cybersecurity, Vinnytsia National Technical University, Vinnytsia, e-mail : ira.zoria@vntu.edu.ua