УДК 004.056

І. О. Бондаренко
Д. О. Пінчук
А. Р. Магденко

ФІШИНГ ТА СОЦІАЛЬНА ІНЖЕНЕРІЯ: МЕТОДИ МАНІПУЛЯЦІЇ ТА ПРОТИДІЇ

Вінницький національний технічний університет

Анотація

У тезах розглянуто основні види фішингових атак та методи соціальної інженерії, а також їх психологічні аспекти. Проаналізовано сучасні тенденції у використанні цих атак, їхні наслідки та ефективні методи протидії. Особлива увага приділяється технічним, освітнім та організаційним заходам захисту, а також ролі штучного інтелекту у виявленні та запобіганні фішинговим загрозам.

Ключові слова: фішинг, соціальна інженерія, кібербезпека, маніпуляція, захист інформації, фішингові атаки, багатофакторна автентифікація, машинне навчання, штучний інтелект, кіберзагрози.

Abstract

The theses consider the main types of phishing attacks and social engineering methods, as well as their psychological aspects. Modern trends in the use of these attacks, their consequences and effective methods of counteraction are analyzed. Special attention is paid to technical, educational and organizational protection measures, as well as the role of artificial intelligence in detecting and preventing phishing threats.

Keywords: phishing, social engineering, cybersecurity, manipulation, information protection, phishing attacks, multi-factor authentication, machine learning, artificial intelligence, cyber threats

Вступ

Фішинг та соціальна інженерія є одними з найпоширеніших методів кіберзлочинців для отримання несанкціонованого доступу до конфіденційної інформації. Ці методи базуються на маніпуляції людською психологією, використовуючи довіру, страх або цікавість жертв. Розуміння механізмів цих атак та розробка ефективних заходів протидії є критично важливими для забезпечення кібербезпеки.

Результати дослідження

Протягом останніх двох десятиліть інтернет став невід'ємною частиною нашого повсякденного життя. Ми регулярно користуємося цифровими платіжними системами, здійснюємо оплату комунальних послуг через інтернет-банкінг та підтримуємо як професійне, так і особисте спілкування в мережі.

Нехтування базовими правилами безпеки може призвести до того, що ваші приватні дані опиняться в руках шахраїв. Особливо небезпечним є фішинг – різновид інтернет-шахрайства, спрямований на незаконне отримання доступу до конфіденційної інформації користувачів.

Шахраї розробляють спеціальні схеми, які спонукають користувачів добровільно розкривати свої персональні дані: телефонні номери, банківські реквізити, паролі до електронної пошти та акаунтів у соціальних мережах. Для цього вони пропонують привабливі послуги чи можливості. Наприклад, користувачам Instagram обіцяють показати, хто переглядав їхній профіль (функція, яку насправді не пропонує сама платформа), а покупцям інтернет-магазинів – неймовірно вигідні знижки на товари.

Статистика свідчить, що 96% фішингових атак здійснюється через електронну пошту, 3% – через шкідливі вебсайти, і лише 1% – телефоном. За даними досліджень Symantec, у 2020 році серед 4200 електронних листів щонайменше один був фішинговим [1].

У 2024 році кількість кібератак на Україну зросла на 69,8%, досягнувши 4315 інцидентів, у порівнянні з 2023 роком, коли було зафіксовано 2541 кіберінцидентів. Наразі спостерігається стійка тенденція до зростання кібератак передусім на критично важливу інфраструктуру України, зазначає урядова команда реагування на комп’ютерні надзвичайні події CERT-UA [2]. Зростання рівню фішингових атак зображено на рисунку 1.

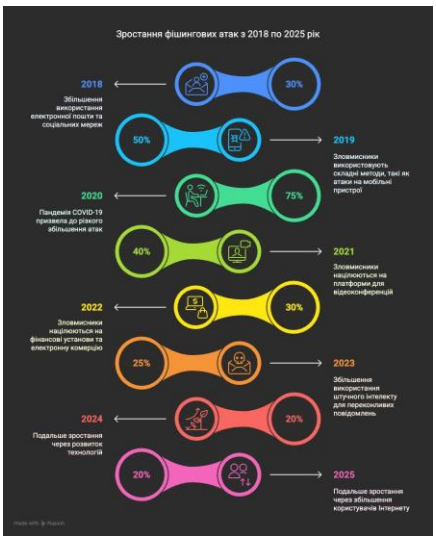

Рисунок 1 – Зображення схеми зростання фішингу

Фішинг має на меті викрадення конфіденційної інформації, такої як паролі та дані кредитних карток, за допомогою обманних електронних листів. Однак існують і більш спеціалізовані форми цієї загрози.

Фішинг можна поділити на декілька видів [3]:

– Цільовий фішинг (spear phishing) – це більш просунутий варіант фішингу, спрямований на конкретні організації чи особи.

– Вейлінг (whaling) – це цілеспрямована форма фішингу, яка націлена на керівників вищої ланки в компаніях.

Різниця між фішингом і вейлінгом пов’язана з рівнем персоналізації. У той час як фішингові атаки не персоналізовані та можуть бути відтворені для мільйонів користувачів, вейлінг атаки спрямовані на одну особу, як правило, на керівників найвищого рівня. Мета вейлінг атаки – змусити особу розкрити особисту або корпоративну інформацію [4]. Цей тип атаки вимагає значного обсягу досліджень щодо цієї особи, що зазвичай робиться шляхом перегляду її активності в соціальних мережах та іншої публічної поведінки. Це поглиблене дослідження призводить до більш складного охоплення та більшої ймовірності успіху. Успішний вейлінг, як правило, призводить до значно більших фінансових та репутаційних втрат для організації через високий статус та доступ цілей до критично важливих ресурсів. Обидва типи атак становлять серйозну загрозу для безпеки організацій та вимагають підвищеної пильності та відповідних заходів захисту [5].

Хоча спочатку вейлінг атаки вимагають більшого планування та зусиль, вони часто приносять величезні прибутки, оскільки цілі мають доступ до цінних даних або фінансових ресурсів, необхідних для здійснення атаки програм-вимагачів.

– SMS-фішинг, смішинг (smishing) поєднує в собі «SMS» і «фішинг», Аналогічно до фішингових електронних листів, зловмисники розсилають SMS-повідомлення з подібними сценаріями та посиланнями на шкідливі вебсайти або проханнями перетелефонувати на шахрайські номери з метою виманювання конфіденційної інформації у жертви.

SMS-фішинг атаки стали популярними серед злочинців, оскільки люди проводять більше часу за мобільними пристроями. Хоча користувачі стали вправнішими у виявленні фішингу електронної пошти, багато людей набагато менше усвідомлюють ризики, пов’язані з текстовими повідомленнями.

SMS-фішинг атака вимагає невеликих зусиль від загрозливих учасників і часто здійснюється шляхом простого придбання підробленого номера та встановлення шкідливого посилання.

– Голосовий фішинг, вішинг (vishing) складається з комбінації слів «voice» та «фішинг». У цьому типі атак використовуються телефонні дзвінки для отримання конфіденційних даних цілі [3].

– Соціальна інженерія (social engineering) – це вид шахрайства, який представляє собою комплекс шахрайських технік, спрямованих на отримання доступу до приватних даних через психологічний вплив. Шахраї активно використовують емоційні тригери – страх, цікавість або довіру – для маніпулювання свідомістю людини. Типові приклади соціальної інженерії включають підроблені повідомлення від імені відомих компаній, запити на підтвердження персональних даних або пропозиції перейти за підозрілими посиланнями [6].

Фішингові та соціально-інженерні атаки залишаються одними з найефективніших засобів кіберзлочинців для отримання несанкціонованого доступу до конфіденційної інформації. Протидія цим атакам вимагає як технологічних засобів, так і постійного підвищення обізнаності користувачів. На рисунку 2 наведено загальні методи захисту від фішингових атак.

Рисунок 2 – Методи захисту

Одним із ключових методів протидії, за даними CISA, є підвищення обізнаності серед співробітників: "Організації повинні навчати працівників розпізнавати підозрілі електронні листи та повідомлення, особливо ті, що містять несподівані вкладення або посилання, термінові прохання чи прохання надати персональні дані". З цією метою рекомендується проводити регулярні симуляції фішингових атак, щоб допомогти працівникам виявляти загрози у реальному часі [7].

Попри великий та доступний обсяг інформації, щодо методів протидії фішингу, атаки не є рідкістю в наш час. Яскравим прикладом є випадок з компаніями Google та Facebook, які, за даними BlueVoyant, стали жертвами фішингової афери на суму понад 100 мільйонів доларів. У період з 2013 по 2015 роки зловмисник на ім’я Евалдас Римасаускас створив фальшиву компанію і надсилав фішингові листи від імені відомого виробника комп’ютерного обладнання. У листах містилися сфабриковані рахунки, контракти та офіційні листи. Через переконливість цих документів обидві компанії переказали на рахунки шахрая значні суми грошей. Як наслідок, Римасаускас був заарештований і засуджений у США, але сам факт шахрайства підкреслює вразливість навіть технологічних гігантів перед класичним фішингом [8].

Ще один резонансний інцидент стався з компанією Pepco Group у 2024 році. Шахраї за допомогою фішингової атаки спрямованої на угорське відділення компанії змусили співробітників здійснити переказ коштів на суму близько 15,5 мільйонів євро. Атака була дуже добре спланована: зловмисники використовували фальшиві електронні листи, які виглядали як офіційна внутрішня корпоративна комунікація. Незважаючи на наявність систем контролю, внаслідок людського фактору гроші були переведені на рахунок шахраїв, що призвело до серйозних фінансових втрат для компанії [9].

Знаковим прикладом є і атака на бельгійський банк Crelan. У 2016 році за допомогою фішингового листа, надісланого від імені генерального директора, шахраї змогли переконати співробітників переказати близько 75 мільйонів євро на підставні рахунки. У цьому випадку зловмисники використали техніку "business email compromise" (BEC), коли підробляються електронні адреси високопоставлених осіб компанії для ініціювання фальшивих фінансових транзакцій [10].

Ці приклади демонструють, що навіть найбільш обережні організації можуть стати жертвами фішингових атак, якщо не впроваджуються багаторівневі засоби перевірки транзакцій і відсутня культура цифрової обачності.

Висновки

Фішинг та соціальна інженерія залишаються серйозними загрозами в сучасному цифровому світі. Поєднання технічних, освітніх та організаційних заходів є ключем до ефективної протидії цим атакам. Постійне підвищення обізнаності користувачів та впровадження новітніх технологій можуть значно знизити ризики, пов'язані з фішингом та соціальною інженерією.

Важливо розуміти, що кіберзлочинці постійно вдосконалюють свої методи, адаптуючись до нових захисних механізмів. Тому захист від таких загроз має бути динамічним процесом, а не одноразовим

заходом. Організації повинні регулярно проводити навчання персоналу, симулювати фішингові атаки для підвищення пильності працівників та впроваджувати багаторівневі системи захисту.

Особливо вразливими до атак соціальної інженерії є нові користувачі цифрових технологій, люди похилого віку та особи, які не мають достатньої обізнаності щодо кібербезпеки. Тому важливо проводити широкомасштабні освітні кампанії, спрямовані на різні верстви населення.

У кінцевому підсумку, людський фактор залишається найслабшою ланкою в системі кібербезпеки. Навіть найдосконаліші технічні засоби захисту можуть виявитися неефективними, якщо користувач добровільно надає свої дані під впливом психологічних маніпуляцій. Саме тому формування культури кібербезпеки та критичного мислення має стати пріоритетом для суспільства в епоху цифрової трансформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке фішинг і фішингова атака. URL: https://hostiq.ua/blog/ukr/internet-phishing/ (дата звернення: 22.03.2025)
2. У 2024 році кількість кібератак на Україну зросла на 70%. *Інститут масової інформації*. URL: https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931 (дата звернення: 29.04.2025).
3. Види соціальної інженерії - CoreWin. *CoreWin*. URL: https://corewin.ua/blog/social-engineering-types/ (дата звернення: 26.03.2025).
4. Robinson S., Lutkevich B., Clark C. What is a whaling attack (whaling phishing)? | Definition from TechTarget. *Search Security*. URL: https://www.techtarget.com/searchsecurity/definition/whaling (date of access: 01.04.2025).
5. B. Lenaerts-Bergmans. 10 Types of Social Engineering Attacks | CrowdStrike. *CrowdStrike: We Stop Breaches with AI-native Cybersecurity*. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/ (дата звернення: 04.04.2025)
6. Соціальна інженерія: що це та як уберегтися від шахрайства. ZEN.COM. URL: https://www.zen.com/uk/blog/personal-finance-uk/social-engineering-how-to-protect-yourself-from-fraud/ (дата звернення: 10.04.2025)
7. Avoiding Social Engineering and Phishing Attacks. CISA. URL: https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks (дата звернення: 29.04.2025)
8. Devastating Phishing Attack Examples and Prevention Tips. BlueVoyant. URL: https://www.bluevoyant.com/knowledge-center/8-devastating-phishing-attack-examples-and-prevention-tips (дата звернення: 29.04.2025)
9. The 5 Biggest Phishing Attacks of 2024. Memcyco. URL: https://www.memcyco.com/the-5-biggest-phishing-attacks-of-2024 (дата звернення: 29.04.2025)
10. The Top 5 Phishing Scams of All Times. Check Point Software. URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/the-top-5-phishing-scams-of-all-times (дата звернення: 29.04.2025)

Пінчук Дар'я Олександрівна **–** студентка групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: dashapinchukschool@gmail.com

Магденко Анастасія Романівна **–** студентка групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: anastasiiamahdenko@gmail.com

Науковий керівник: ***Бондаренко Ірина Олексіївна*** **–** асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Pinchuk Daria O. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: dashapinchukschool@gmail.com

Mahdenko Anastasiia R. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: anastasiiamahdenko@gmail.com

Supervisor*:* ***Bondarenko Iryna O.*** **–** assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua