Ольга Смагло
к.е.н., доцент, доцент кафедри фінансів, банківської справи та страхування,
Вінницький навчально-науковий інститут економіки
Західноукраїнського національного університету, м. Вінниця

ОСОБЛИВОСТІ ПРОТИДІЇ ФІШИНГУ ЯК РІЗНОВИД ФІНАНСОВИХ ТЕХНОЛОГІЙ

Кількість людей, які зайняті віддаленою роботою, стрімко зростає, як і кількість потенційних цифрових загроз. Одним із найнебезпечніших і найпоширеніших видів інтернет-шахрайства є фішинг.

Фішинг – це вид кіберзлочинності, заснований на шахрайстві. Під час фішингової атаки кіберзлочинець зв'язується зі своєю цільовою особою (зазвичай електронною поштою) і намагається змусити її зробити щось, що може поставити під загрозу її дані. Користувача можуть заохотити поділитися своїми обліковими даними та фінансовою інформацією або встановити зловмисне програмне забезпечення, яке дозволить зловмиснику отримати доступ до його комп'ютера.

Традиційно фішингові атаки використовувалися для атаки на сотні чи навіть тисячі людей одночасно. Сьогодні ці атаки стають все більш цілеспрямованими; замість того, щоб надсилати загальну електронну пошту багатьом користувачам, зловмисник вивчатиме свою ціль, перш ніж надсилати їй повідомлення, а потім прикидатиметься кимось, кого ціль знає, щоб завоювати їх довіру. Через це атаки є набагато переконливішими та їх важко помітити – ціль, швидше за все, поділиться конфіденційною інформацією. Ці цільові фішингові атаки відомі як «фішинг».

Окрім традиційного фішингу та цілеспрямованих фішингових атак, є ще кілька типів фішингових атак:

- Китобійний промисел – це різновид фішингу, націленого на високопоставлених членів організації, наприклад керівників, які, ймовірно, мають привілейований доступ до критично важливих корпоративних систем або цінних даних;
- Вішинг, скорочення від «голосовий фішинг», – це фішингова атака, яка здійснюється за допомогою телефонного дзвінка, а не електронною поштою. Ці атаки часто створюють високе відчуття терміновості, оскільки зловмисник спілкується з користувачем у режимі реального часу і може використовувати це, щоб збільшити тиск;
- SMiShing або «SMS-фішинг» доставляється за допомогою текстового повідомлення. Ці атаки часто стверджуються, що вони походять від довіреної організації, наприклад банку чи компанії, що займається доставкою електронної пошти, а не від конкретної особи;
- Фішингові веб-сайти виглядають як звичайні веб-сторінки (зазвичай сторінки входу або оплати), але вони збирають дані користувачів і надсилають їх безпосередньо зловмиснику. Часто користувачі відкривають фішингові

сторінки за посиланнями, надісланими у фішингових електронних листах, але іноді вони можуть натрапити на них під час перегляду, якщо зловмиснику вдалося приховати шкідливу сторінку на законному веб-сайті.

Фішинг (phishing) – це один з найпопулярніших видів кіберзлочинів. Основна мета шахраїв – добровільно отримати доступ до вашої конфіденційної інформації. Фішинг є одним із найбільш поширених та небезпечних видів кіберзлочинів. Його цілі та завдання можуть змінюватись в залежності від конкретної ситуації та намірів зловмисників. Його особливість у тому, що жертва шахрайства надає свої дані добровільно. Фішингові атаки відбуваються за стандартною схемою: зловмисники закидають наживку – це може бути лист, повідомлення, посилання на сайт. А потім намагаються упіймати на неї довірливих користувачів. Сучасні кіберзлочинці вдосконалюють свої методи, використовують психологічні маніпуляції та інноваційні технології для того, щоб заволодіти вашими грошима.

Фішинг (у перекладі з англійської «риболовля») – це вид шахрайства в Інтернеті, що дає змогу шахраям виманити персональні дані та незаконно заволодіти вашими коштами. В основі цього виду шахрайства лежать методи соціальної інженерії. Іншими словами, своїми діями шахрай прагне викликати довіру в жертви, щоб та надала йому необхідну інформацію.

Специфікою фішингу є те, що жертва шахрайства надає свої конфіденційні дані добровільно. Для цього зловмисники оперують такими інструментами, як фішингові сайти, e-mail розсилка, фішингові landing page, спливаючі вікна, таргетована реклама. Користувач отримує пропозицію зареєструватися для отримання будь-якої вигоди або підтвердити свої персональні дані нібито для банківських або комерційних установ, клієнтом яких він є. Як правило, шахраї маскуються під відомі компанії, додатки соціальних мереж, сервіси електронної пошти. Електронна адреса відправника дійсно схожа на адресу знайомої користувачеві компанії. Наприклад, щоб замаскуватися під інтернет-магазин Aliexpress, шахраї шлють листи з адрес, що містять слово Alliexpress або Aliexxpress. Працює та сама схема, яка змушує людей купувати дешеві китайські кросівки таких «всесвітньо відомих брендів», як Pumma або Abibas.

Зловмисники користуються низьким рівнем обізнаності користувачів, зокрема, незнанням елементарних правил мережевої безпеки. Перш за все, організаторів фішинг-атак цікавлять персональні дані, які дають доступ до грошей, тому жертвами фішингу можуть ставати не тільки окремі люди, а й банки, електронні платіжні системи, аукціони. Згідно з даними StationX, у 2023 році спостерігалося близько 5 мільйонів фішингових атак. Це пов'язано з тим, що все більше людей користуються Інтернетом для комунікації, оплати товарів чи послуг.

Однією з основних цілей фішингу є отримання особистих даних користувачів. Зловмисники можуть використовувати фішингові методи, щоб отримати доступ до логіну, паролів, номерів кредитних карток, соціальних страхових номерів та інших важливих особистих даних. Їх можуть

використовувати для скоєння крадіжки особи, шахрайства чи інших злочинних дій. У світі бізнесу фішинг може бути спрямований на отримання конфіденційних даних компанії, таких як бізнес-секрети, плани розробки чи інформація клієнта. Їх можуть продавати конкурентам або іншим сторонам, що може призвести до фінансових втрат та шкоди репутації компанії. Щоб це попередити, великі компанії приділяють все більше уваги захисту конфіденційних даних користувачів. Соціальні мережі та ресурси електронної пошти практикують прив'язку акаунту користувача до IP або мобільного телефона. Інтернет-банкінг також використовує смс-оповіщення. Оскільки електронна комерція поширюється шаленими темпами, торгівля в інтернеті процвітає, соціальні мережі щорічно залучають мільйони нових користувачів, а кримінальне право часто не встигає за розвитком інформаційних технологій. А значить, кількість охочих заробити на людській довірі точно не зменшиться.

Деякі фішинг-атаки можуть бути спрямовані на поширення шкідливих програм, таких як троянські коні, шпигунські агенти або ransomware. Зловмисники можуть використовувати обманні методи, щоб змусити користувачів завантажувати та запускати шкідливі файли, що може призвести до зараження комп'ютерів та крадіжки даних.

Фішинг – це не тільки технічна атака, але й психологічний обман. Зловмисники активно використовують маніпуляції та соціальну інженерію, щоб обдурити користувачів та отримати доступ до їх особистих та фінансових даних. Тому розуміння цілей та завдань фішингу дозволяє бути більш пильними та захищеними у сучасному цифровому світі.

Здатність виявляти та ізолювати шкідливі фішингові повідомлення електронної пошти є великою проблемою як з технічної, так і з управлінської сторони; однак для захисту від фішингових листів буде корисною система обслуговування електронної пошти з вбудованими розширеними функціями безпеки. Як правило, в систему включені функції безпечних вкладень та безпечного посилання. Така система електронної пошти просканує посилання та визначить, безпечна вона чи ні, перш ніж перенаправити користувача на веб-сайт, та заблокує доступ із попередженням для користувача, якщо це відоме шкідливе посилання. Так само функція безпечного вкладення спочатку сканує вкладення в електронному листі, і якщо шкідливість програми підтверджується, вкладення буде замінено з повідомленням для користувача.

Рішення для захисту від фішингу – це категорія програмного забезпечення для кібербезпеки, призначена для запобігання фішинговим атакам. З моменту свого створення фішингові атаки перетворилися на дуже складні та цілеспрямовані, що дозволяє їм уникати традиційних шлюзів безпеки електронної пошти. У відповідь на це постачальники послуг безпеки електронної пошти розробили новий тип рішення, призначеного спеціально для захисту від фішингу та запобігання компрометації бізнес-електронної пошти (BEC): рішення Integrated Cloud Email Security (ICES).

Список використаних джерел:

1. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки*. 2022. № 3. С. 47–59.
2. Вишнівський В. В., Пампуха А. І. Кібербезпека в Україні. *Цифрова трансформація кібербезпеки:* матер. наук.-практ. інт.-конф. (20 квітн. 2022 р., Навчально-науковий інститут захисту інформації Державного університету телекомунікацій). Київ, 2022. С. 31–33.
3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України; Стратегія від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12.
4. Кібератаки можуть прийти через постачальників. Як захиститися? URL: https://delo.ua/telecom/kiberataki-mozut-priiti-cerez-postacalnikiv-yak-zaxistitisya-404662.
5. Кібербезпека бізнесу в умовах нестабільності. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html.
6. Що таке фішинг та як від нього захиститися? URL: https://www.zen.com/uk/blog/personal-finance-uk/what-is-phishing-and-how-to-protect-yourself-from-it/