Ми, команда "Яковлєва Law Partner" — адвокати та IT-спеціалісти з більш ніж 20-річним досвідом у сферах права, інформаційних технологій та кібербезпеки. Розуміючи виклики сучасного цифрового світу, ми прагнемо ділитися своїм досвідом та знаннями, щоб допомогти бізнесу та користувачам захистити себе від кіберзагроз. У рамках цього завдання ми розпочинаємо серію статей, присвячених актуальним питанням інформаційної безпеки. Наша мета — зробити складні теми зрозумілими та корисними для всіх, незалежно від рівня технічної підготовки.

Перша стаття цієї серії присвячена фішингу — одному з найпоширеніших методів кіберзлочинності.

Що таке фішинг, чому це небезпечно і як розпізнати загрози?

Фішинг — це одна з найпоширеніших форм кіберзлочинності, яка полягає у спробах зловмисників викрасти особисту або конфіденційну інформацію користувачів. Зазвичай це здійснюється шляхом обману, коли жертва сама, не підозрюючи про небезпеку, передає шахраям доступ до своїх даних. Назва походить від англійського слова “fishing” (“риболовля”), оскільки хакери, подібно до рибалок, закидають “вудку” у вигляді підроблених повідомлень, сайтів або дзвінків, сподіваючись, що хтось “клюне” на їхню пастку.

Чому це небезпечно?

Фішингові атаки можуть завдати серйозної шкоди як окремим людям, так і компаніям:

Фінансові втрати. Зловмисники можуть отримати доступ до банківських рахунків або викрасти кошти через онлайн-платежі.

- **Компрометація даних.** Викрадені дані можуть використовуватися для крадіжки особистості або навіть продажу на чорному ринку.

Порушення роботи бізнесу. У компаніях фішинг часто стає початковим етапом складніших атак, таких як впровадження шкідливого програмного забезпечення (наприклад, програми-шифрувальники).

Репутаційні ризики. Витік конфіденційних даних може призвести до втрати довіри клієнтів і партнерів.

Які бувають види фішингу?

Фішинг постійно розвивається, адаптуючись до нових технологій і звичок користувачів. Нижче описані основні види атак:

1. **Фішинг через електронну пошту** – Найпоширеніший спосіб атак. Зловмисники розсилають електронні листи, які виглядають як офіційні повідомлення від банків, онлайн-магазинів або інших сервісів. У листах зазвичай є посилання на підроблений сайт, що зовні майже ідентичний справжньому. Потрапивши на такий сайт, користувач вводить свої дані, які одразу потрапляють до рук шахраїв.
2. **Фішинг на смартфонах** – У смартфонах використовуються два основні види атак:
    - **SMS-фішинг (“смішинг”):** шахрайські текстові повідомлення, які зазвичай містять посилання на фальшивий сайт або просять передзвонити на вказаний номер.

    - **Дзвінковий фішинг (“vishing”):** шахраї телефонують, представляючись працівниками банків, технічної підтримки або держустанов, і вимагають розкрити конфіденційну інформацію.

3. **Фішинг через соціальні мережі** – У соцмережах шахраї створюють фальшиві профілі компаній чи відомих осіб і надсилають повідомлення з вигідними “пропозиціями” або проханнями підтвердити ваш акаунт через посилання. Ціль — отримати ваші дані або доступ до профілю.
4. **Фішинг через “розумні” пристрої** – Сучасний дім наповнений пристроями, підключеними до Інтернету: телевізори, колонки, пилососи. Зловмисники можуть використати підроблені повідомлення про “оновлення” або навіть взяти контроль над пристроєм для збору ваших даних.
5. **Фішинг у месенджерах** – Шахраї активно використовують месенджери для розсилання підроблених повідомлень. Це можуть бути фальшиві посилання або файли, які містять шкідливе програмне забезпечення.

Як розпізнати фішинг?

Щоб захиститися від фішингових атак, слід бути уважним і обережним. Ось кілька порад:

1. **Перевіряйте відправника.** Уважно аналізуйте адресу електронної пошти чи номер телефону. Часто шахраї використовують схожі, але не автентичні домени (наприклад, замість “bank.com” “bank-security.com”).
2. **Не переходьте за підозрілими посиланнями.** Наведіть курсор на посилання, щоб перевірити, куди воно веде. Справжній сайт банку або сервісу завжди має офіційний домен.
3. **Будьте обережними з вкладеннями.** Ніколи не відкривайте файли, якщо вони надходять від невідомих відправників. Вони можуть містити віруси або шпигунське ПЗ.
4. **Звертайте увагу на мову.** Часто фішингові повідомлення містять граматичні помилки, погано структурований текст або зайвий наголос на терміновість дій (“Ваш рахунок буде заблоковано через 24 години!”).
5. **Не повідомляйте особисту інформацію.** Ніколи не розкривайте свої паролі, PIN-коди або інші конфіденційні дані через електронну пошту, телефон або месенджери.

Поради для захисту

- Використовуйте двофакторну автентифікацію (2FA) для всіх важливих акаунтів.
- Регулярно оновлюйте програмне забезпечення на своїх пристроях.
- Встановіть надійний антивірус та антифішингові розширення для браузера.
- Зберігайте резервні копії важливих даних.
- Постійно підвищуйте свою кібергігієну та навчайте цьому своїх близьких.

Фішинг — це невидима загроза, яка може торкнутися кожного. Але знання про те, як працюють ці атаки та як себе захистити, значно знижує ризик стати жертвою. У наступних статтях ми детальніше розглянемо реальні приклади фішингових атак та способи їх уникнення.