

Ми, команда "Яковлева 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.

Фішинг на телефоні: як захистити себе від мобільних шахраїв

Сучасні смартфони — це не просто засіб зв'язку, а й міні-комп'ютери, які зберігають безліч важливих даних: контакти, банківські рахунки, паролі, фотографії, повідомлення тощо. Однак цей комфортний інструмент став привабливою ціллю для кіберзлочинців. Однією з найбільш поширених загроз є фішинг, який на телефонах має свої унікальні форми. У цій статті ми розглянемо, як працює фішинг на мобільних пристроях, чому він небезпечний і як захиститися від нього.

Як фішинг працює на смартфонах?

Фішинг на телефонах відрізняється від класичних атак через електронну пошту, хоча використовує схожі принципи. Основні види атак включають:

1. **Смішинг (SMS-фішинг):** Зловмисники надсилають шахрайські текстові повідомлення, які зазвичай містять посилання на фальшивий сайт або прохання передзвонити на вказаний номер. Наприклад, повідомлення може виглядати так: "Ваш банківський рахунок заблоковано. Перейдіть за посиланням для розблокування".
2. **Вішинг (Voice Phishing):** Шахраї телефонують, представляючись співробітниками банку, технічної підтримки або держустанов. Вони намагаються отримати конфіденційну інформацію: паролі, PIN-коди, дані картки тощо. Часто їхні розмови побудовані на залякуванні або створенні відчуття терміновості.
3. **Фішинг через месенджери:** Популярні месенджери, такі як WhatsApp, Telegram або Viber, використовуються для розсилки повідомлень зі шкідливими посиланнями. Наприклад, вам можуть надіслати пропозицію виграти приз або отримати знижку, що потребує переходу за підозрілим лінком.
4. **Фальшиві мобільні додатки:** Зловмисники створюють підроблені програми, які виглядають як офіційні додатки банків, магазинів чи інших сервісів. Користувач, завантаживши такий додаток, вводить свої дані, які миттєво передаються шахраям.
5. **Фішингові оголошення:** Під час перегляду сайтів на смартфоні можуть з'являтися рекламні оголошення, які перенаправляють на фальшиві сторінки. Вони часто видають себе за технічну підтримку або оновлення для вашого пристрою.

Чому фішинг на телефоні особливо небезпечний?

Мобільні пристрої мають кілька характеристик, які роблять фішинг на них ефективним:

1. **Малий екран:** Через невеликий розмір екрана користувачам складніше помітити підозрілу URL-адресу або інші дрібні деталі, які видають шахраїв.
2. **Обмежений контроль:** Мобільні браузері і додатки часто приховують повну URL-адресу, що ускладнює перевірку справжності сайту.

3. **Швидкість дій:** Користувачі смартфонів зазвичай діють швидше, не завжди звертаючи увагу на деталі.
4. **Особиста інформація:** Смартфони зазвичай містять більше конфіденційних даних, ніж комп'ютери, включаючи доступ до месенджерів, фото та додатків із фінансовими акаунтами.

Як розпізнати фішинг на телефоні?

1. **Неочікувані повідомлення:** Якщо ви отримали SMS або повідомлення в месенджері з інформацією про виграш, блокування рахунку чи іншу термінову ситуацію, будьте уважні. Справжні організації рідко спілкуються таким чином.
2. **Підозрілі посилання:** Навіть якщо посилання виглядає офіційно, його потрібно перевірити. Довгі або незрозумілі адреси — це ознака фішингу.
3. **Нестандартний номер чи відправник:** SMS від банків зазвичай надходять із коротких номерів або офіційних імен. Якщо повідомлення надійшло з невідомого номеру, це може бути шахрайство.
4. **Використання терміновості:** Повідомлення, яке змушує вас негайно діяти ("Ваш рахунок буде закрито через 24 години!"), майже завжди є шахрайським.
5. **Запити конфіденційної інформації:** Банки та інші сервіси ніколи не запитують ваші паролі чи PIN-коди через SMS, дзвінки або месенджери.

Як захиститися від фішингу на телефоні?

1. **Не переходьте за підозрілими посиланнями:** Якщо ви отримали повідомлення з посиланням, перевірте його в офіційному додатку чи на сайті організації.
2. **Перевіряйте відправника:** Уважно аналізуйте номер телефону або ім'я відправника. Якщо є сумніви, краще звернутися до організації напряму.
3. **Не встановлюйте додатки з невідомих джерел:** Завантажуйте програми тільки з офіційних магазинів (Google Play, App Store).
4. **Використовуйте антивірус:** Встановіть надійний антивірус для мобільних пристроїв. Деякі з них мають функції захисту від фішингу.
5. **Регулярно оновлюйте ПЗ:** Оновлення операційної системи та додатків містять виправлення для відомих вразливостей.
6. **Увімкніть двофакторну автентифікацію (2FA):** Використовуйте 2FA для своїх акаунтів. Навіть якщо шахраї отримають ваш пароль, їм буде важко отримати доступ до акаунта без додаткового коду.
7. **Блокуйте підозрілі номери:** Якщо ви отримали підозрілий дзвінок або SMS, заблокуйте номер.
8. **Навчайтеся кібергігієні:** Розкажіть своїм близьким про методи фішингу, щоб вони також могли захиститися.

Що робити, якщо ви стали жертвою фішингу?

1. **Негайно змініть паролі:** Якщо ви ввели свої дані на підозрілому сайті, одразу змініть паролі від акаунтів.

2. **Повідомте свій банк:** Якщо ви надали дані банківської картки, негайно зв'яжіться з банком і заблокуйте картку.
3. **Зверніться до технічної підтримки:** Якщо зломисники отримали доступ до ваших акаунтів, зверніться до служби підтримки відповідного сервісу.
4. **Перевірте пристрій на наявність вірусів:** Запустіть сканування антивірусною програмою, щоб переконатися у відсутності шкідливого ПЗ.

Ми детально проконсультуємо вас та допоможемо налагодити вам інформаційну безпеку - ВАШ ЗАХИСТ "під ключ" **“Яковлева Law Partner”**
Офіційний партнер адвокатського об'єднання «ДАНКО» – це не просто адвокатська фірма, але і справжня команда професіоналів з більш ніж 20-річним досвідом у сфері права. Наші юристи не просто вирішують ваші юридичні питання – вони знають, як забезпечити успішний результат. Наша команда присвячена захисту ваших інтересів та наданню вам відчуття впевненості в будь-якій ситуації. Обираючи **“Яковлева Law Partner”**

+ 380963369987 yakovlieva.advokat@lawpartner.com.ua