**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.**

**Як працює фішинг на комп’ютері?**

Фішинг на комп’ютері часто використовує такі підходи:

**Підроблені веб-сайти.**

Зловмисники створюють копії відомих сайтів (банків, онлайн-магазинів, соціальних мереж). Користувач отримує посилання через електронну пошту, месенджери або рекламу, переходить на підроблений сайт і вводить свої дані, які одразу потрапляють до шахраїв.

**Шкідливі вкладення в електронній пошті.**

Електронні листи з вкладеннями, що маскуються під документи (рахунки, контракти), можуть містити шкідливе програмне забезпечення. Після відкриття файлу комп’ютер заражається, і зловмисники отримують доступ до ваших даних.

**Скамерські повідомлення.**

Листи з фальшивими попередженнями ("Ваш акаунт заблоковано!" або "Підтвердьте вашу особу!"). Вони змушують користувача діяти терміново, вводячи паролі чи інші конфіденційні дані.

**Завантаження програм з ненадійних джерел.**

Деякі програми або оновлення, завантажені не з офіційних сайтів, можуть бути замаскованим шкідливим ПЗ. Такі програми відкривають доступ до даних користувача або використовують ПК для незаконної діяльності.

**Фішинг через соцмережі.**

Зловмисники можуть надсилати повідомлення з посиланнями на фальшиві сайти, пропонувати вигідні “акції” або навіть видавати себе за знайомих користувача.

**Приклади фішингових атак на комп’ютері**

**Підроблена електронна пошта.**

Ви отримуєте лист, який виглядає як офіційне повідомлення від банку, з проханням оновити інформацію про акаунт. У тексті міститься посилання, що веде на підроблений сайт.

**Спливаючі вікна (Pop-ups).**

На вашому екрані з’являється повідомлення: "Ваш комп’ютер заражено! Завантажте антивірус”. Завантаживши його, ви встановлюєте шкідливу програму.

**Соціальна інженерія.**

Зловмисники дзвонять або пишуть, видаючи себе за службу підтримки, і вимагають надати доступ до вашого комп’ютера через віддалене підключення.

**Фальшиві оновлення програм.**

На екрані з’являється повідомлення про необхідність оновити програмне забезпечення. Завантаження таких оновлень часто веде до встановлення шкідливих програм.

**Як захиститися від фішингу на комп’ютері?**

**Перевіряйте джерело повідомлення.**

Перед тим як натиснути на посилання або відкрити вкладення, уважно перевіряйте адресу відправника. Офіційні компанії ніколи не використовують поштові домени, які виглядають підозріло.

**Не переходьте за сумнівними посиланнями.**

Якщо ви отримали посилання, наведіть на нього курсор і перевірте, чи домен збігається з офіційним сайтом. Наприклад, замість "bank.ua" це може бути "bcank.ua" (де використано схожий символ "c").

**Використовуйте антивірусне програмне забезпечення.**

Надійний антивірус із функцією захисту від фішингу може блокувати небезпечні сайти та повідомлення.

**Оновлюйте операційну систему та програми.**

Регулярні оновлення закривають вразливості, які можуть використовувати зловмисники для атак.

**Не відкривайте підозрілі вкладення.**

Навіть якщо вкладення виглядає як рахунок чи резюме, переконайтеся, що ви знаєте відправника.

**Використовуйте двофакторну автентифікацію (2FA).**

Вхід у ваші акаунти стає більш захищеним завдяки додатковому коду, який неможливо перехопити через фішингові атаки.

**Навчайте співробітників і близьких кібергігієні.**

Проведіть тренінги, які допоможуть розпізнавати фішинг і уникати його.

**Резервне копіювання даних.**

Регулярно створюйте копії важливих файлів на зовнішніх носіях або у хмарі. Це допоможе швидко відновити інформацію після можливої атаки.

**Що робити, якщо ви стали жертвою фішингу?**

**Змінюйте паролі.**

Якщо ви випадково надали свої облікові дані на підробленому сайті, негайно змініть пароль. Використовуйте унікальний і складний пароль для кожного сервісу.

**Повідомляйте про інцидент.**

Зверніться до служби підтримки компанії, від імені якої було здійснено фішинг. Також повідомте кіберполіцію про спробу шахрайства.

**Перевірте комп’ютер на наявність шкідливого ПЗ.**

Проведіть повне сканування системи за допомогою антивірусу.

**Моніторте фінансові транзакції.**

Якщо ви ввели дані банківської картки, негайно зверніться до банку для блокування картки та моніторингу підозрілих транзакцій.

Ми детально проконсультуємо вас та допоможемо налагодити вам інформаційну безпеку - ВАШ ЗАХИСТ "під ключ" **“Яковлєва 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 “Яковлєва Law Partner”

+ 380963369987 yakovlieva.advokat@lawpartner.com.ua