РАДАБАНК

Повідомлення про виявлені фішингові вебсайти або отримані відомості подібного змісту

Фішинг – це певна схема, застосування якої змушує користувачів передавати певну конфіденційну інформацію для послідуючого використання такої інформації у зловмисних цілях. До такої інформації відносяться: логіни та паролі, номера, термін дії та інші реквізити платіжних карток, адреса електронної пошти та номера фінансових телефонів, відповіді на секретні питання, тощо. Схема як правило працює у двох напрямках – використання несанкціонованих розсилок електронних листів (СПАМу) та переадресування користувачів на зловмисні (підробні) вебсайти які ззовні або по імені дуже схожі на офіційні вебсайти певних організацій.

Тобто при виконанні певних дій зі сторони користувача операції (як то відправка інформації з певних форм чи здійснення транзакції по платіжній картці) фактично не виконуються, а введена користувачем інформація – направляється злочинцям для використання у зловмисних цілях. Як приклад, отримавши по схемі фішинга інформацію про номер платіжної картки, термін дії, імені та прізвище власника платіжної карти, CVV-коду – зловмисники використовують цю інформацію для здійснення несанкціонованих списань грошових коштів з таких платіжних карт. Більше 90 % фішингових сайтів надають неіснуючі послуги з поповнення мобільного рахунку та переказу коштів з картки на картку.

З більш розширеною та детальною інформацією про фішинг можна ознайомитись на офіційному вебсайті провідного розробника програмних продуктів для захисту від зловмисного коду – компанії ESET: https://eset.ua/ua/support/entsiklopediya_ugroz/fishing.

Для боротьби з фішингом Українська міжбанківська асоціація членів платіжних систем ЕМА, яка за підтримки Державного департаменту США реалізує в Україні Національну програму сприяння безпеці електронних платежів і карткових розрахунків Safe Card, створила та регулярно оновлює список виявлених фішингових сайтів. Ознайомитися з переліком сайтів, які становлять небезпеку, може кожен інтернет-користувач на офіційному ресурсі ЕМА.

- «Чорний список сайтів»: https://www.ema.com.ua/citizens/blacklist/;
- перевірені платіжні сервіси: https://www.ema.com.ua/citizens/whitelist/;
- посилання на офіційні сторінки учасників Української міжбанківської асоціації членів платіжних систем ЕМА (банки, платіжні системи): https://www.ema.com.ua/about/members/

Щоб зберегти свої персональні дані (конфіденційну інформацію) та грошові кошти в безпеці перед тим як вводити свої дані на вебсайті потрібно звернути увагу на:

2.1. Неправильне доменне ім'я – як правило, шахраї реєструють схожі домени. Наприклад, замість «radabank.com.ua» можна побачити «rada.bank.com.ua» або «radbank.com.ua». Також сайт може розташовуватися на піддомені, наприклад, «radabank.site.ua» тощо.

2.2. Відсутність SSL сертифікату – пошукові системи використовують шифрування SSL для передачі даних користувачів. При використанні цієї технології адреса сайту починається на «https: //». Якщо вебсайт починається на «http: //», це привід засумніватися в оригінальності сторінки. Шахраям не важко отримати дійсний SSL сертифікат для підробленого сайту – його можна отримати безкоштовно за допомогою спеціальних сервісів.

2.3. Граматичні, орфографічні і дизайнерські помилки – розпізнати шахраїв можна за наявністю граматичних і орфографічних помилок в тексті вебсайтів. Насторожити повинні неправильні назви організації, велика кількість помилок.

2.4. Різниця структур сторінок з оригінальним сайтом і підозрілі платіжні форми – потрібно звертати увагу на наявність посилань на сторінці. Якщо при натисканні на них ви переходите на сторінку з помилкою або на сторінки, які не схожі на оригінальний вебсайт, отже, ви потрапили на фішинговий сайт. Просто закрийте вкладку і не вводьте персональні дані в платіжні форми.

2.5. Старий дизайн – ознакою фішингової форми може стати той факт, що вона розміщена на тлі застарілого дизайну вебсайту.

2.6. Розділ вебсайту «Контакти» – слід перевіряти розділ «Контакти», щоб переконатись, що фізична адреса вказана правильна, а не вигадана. Наприклад, авіакомпанія не може перебувати в промисловій зоні, а банківська установа в покинутому офісі на околиці міста. При роботі з електронною поштою все набагато простіше – жодна банківська установа не буде розсилати електронні повідомлення як своїм діючим так і потенційним клієнтам, в яких буде міститись посилання на якісь вебсайти для здійснення фінансових операцій. Всі фінансові операції, окрім розрахунків з використанням особистих кабінетів інтернет-магазинів, чи сервісів замовлення квитків, здійснюються виключно через системи дистанційного обслуговування рахунків.

Для унеможливлення потрапляння клієнтів банків на фішингові вебсайти Національний банк України на своєму офіційному Інтернет-представництві розмістив офіційний перевірений перелік вебсайтів банків України. Перейшовши за даним посиланням можна легко перевірити автентичність доменного імені та належність вебсайту конкретній банківській установі: https://bank.gov.ua/supervision/institutions