Виявлені фішингові вебсайти або отримані відомості подібного змісту

Фішинговий сайт - це шахрайський вебресурс, що здійснює крадіжку реквізитів платіжних карт під виглядом надання послуг (це може бути, наприклад, поповнення мобільного рахунку або переказ коштів з картки на картку), або клон вебресурсу організації. За статистикою понад 90 % фішингових сайтів надають саме вдавані послуги поповнення мобільних рахунків і переказу коштів з картки на картку.

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. Зловмисниками можуть також застосовуватись голосовий фішинг, фішингові СМС-повідомлення та фішинг в соціальних мережах, але по принципу дії вони дуже схожі.

Суть використання схеми з фішинговими вебсайтами – збір конфіденційної інформації. 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. 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 передтим як вводити свої дані на вебсайті потрібно звернути увагу на:

- неправильне доменне ім'я – як правило, шахраї реєструють схожі домени;
- 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;
- граматичні, орфографічні і дизайнерські помилки.

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 (тобто клієнт-банк). Таким чином отримавши електронне повідомлення на свою пошту з проханням чи пропозицією перейти за посиланням та здійснити передачу своїх облікових даних чи здійснити операцію з

платіжною карткою – можете бути впевненими, що це на 99,99% несанкціонована шахрайська розсилка.

Завжди здійснюйте візуальну перевірку доменного імені сайту для впевненості, що це офіційна, а не фішингова сторінка зловмисників. На даний час АКЦІОНЕРНЕ ТОВАРИСТВО «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ» має наступні офіційні вебсайти:

https://www.bisbank.com.ua/ - офіційний вебсайт Банку;

https://www.bisbank.com.ua/banking/ - офіційний вебсайт Банку для доступу до системи дистанційного обслуговування **«bis24».**

Наголошуємо, що АКЦІОНЕРНЕ ТОВАРИСТВО «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ» ні за яких обставин не здійснює телефонні дзвінки своїм діючим та потенційним клієнтам з метою отримання будь-якої конфіденційної інформації. Отримання конфіденційної інформації можливе лише у разі особистої присутності клієнта у приміщеннях Банку (в Головному офісі чи відділеннях Банку) та з використанням офіційних систем дистанційного обслуговування рахунків Банку).