Пам’ятка

щодо поширення кібершахрайства із SMS-повідомленнями та телефонними дзвінками.

ЩО ТАКЕ SMISHING & VISHING?

Сьогодні все частіше шахраї використовують фальшиві SMS та телефонні дзвінки, намагаючись викрасти вашу особисту та фінансову інформацію. Ось як виявити підробку та захистити себе.

Що таке Smishing?

Smishing, або SMS-фішинг - це одна із форм шахрайства - фішингу, яка використовує текстові повідомлення SMS як спосіб отримання особистої інформації. Шахраї знають, що обмін текстовими повідомленнями є поширеною практикою серед фінансових установ, і вони використовуватимуть це як інструмент для крадіжки у вас інформації.

Існує два основних типи застосування:

1. Надсилається текстове повідомлення, яке здається, що воно надійшло з надійного джерела, наприклад вашої банку. Хоча насправді шахраї підробили назву відправника. У тексті попереджається про можливі проблеми з вашим рахунком або платіжними картками та просять надати особисту інформацію для вирішення проблеми. Після передачі цієї інформації вона використовується для здійснення шахрайських покупок, переведення чи зняття ваших грошей.
2. Відправляється текстове повідомлення, яке, знову ж таки, здається, що воно надійшло від надійного джерела. У тексті є вкладення, яке після відкриття завантажує на ваш телефон вірус чи шкідливе програмне забезпечення, щоб шахраї мали доступ до всього, що є на вашому телефоні.

Як правило, справжній текст фінансової установи включатиме конкретну інформацію , таку як:

- назва фінансової установи;
- останні 4 цифри вашої платіжної картки;
- конкретна сума грошей, про яку йдеться;
- ім'я контактної особи банку.

Справжній текст не включатиме:

- запити на інформацію про вашу платіжну картку, таку як номери картки, ваш pin-код, код підтвердження картки або термін дії картки;
- нечіткі посилання на операцію чи працівника банку;
- гіперпосилання на невідомі веб-сайти.

Якщо ви отримаєте текстове повідомлення із таким наповненням, не відповідайте. Банк ніколи не попросить вас надати особисту фінансову інформацію за допомогою текстового повідомлення.

Якщо ви вважаєте, що повідомлення може бути правдивим, зв’яжіться з банком за номером телефону, який є реальним, вказаним на офіційному сайті банку, платіжній картці, в документах, які надавались при видачі картки банком.

Що таке Vishing?

Vishing - ще одна форма фішингу, який шахраї можуть використати, щоб спробувати вкрасти у вас інформацію. Шахраї телефонують клієнту банку по телефону і просять їх увійти на Клієнт-Банк онлайн за допомогою пароля. Шахрай вже викрав ключ доступу і йому потрібний ще тільки пароль доступу. Під виглядом "перевірки" вас як справжнього клієнта банку, запитає пароль. Отримавши пароль, вони негайно увійдуть у ваш рахунок, змінять ваш пароль і виведуть кошти.

Ніколи не повідомляйте особисту інформацію, коди, логіни та паролі по телефону.

Основні поради

1. Не відповідайте на небажані текстові / SMS-повідомлення перед тим, як самостійно підтвердити, що це від банку. Ви можете зробити це, виконавши:
    - Шукайте номер телефону банку (за допомогою документів банку, картки, веб-сайту банку) і встановлюйте контакт безпосередньо з працівниками банку.
    - Не використовуйте номер телефону, який вказаний у тексті (це може бути фальшивий номер).
2. Не натискайте на посилання, вкладення чи зображення, які ви отримуєте в тексті SMS, попередньо не переконавшись, що текст є дійсно від банку.
3. Не поспішайте і зробіть відповідні перевірки, перш ніж відповісти чи щось натиснути.
4. Ніколи не відповідайте на текстові повідомлення, що вимагають PIN-код вашої 4-значної картки, пароль вашого Інтернет-банку або будь-який інший пароль чи особисту інформацію.
5. Якщо ви вважаєте, що таки відповіли на шахрайське текстове повідомлення та вказали свої банківські реквізити, негайно зверніться в банк.