Рекомендації клієнтам Полікомбанку
щодо виявлення фішингових вебсайтів

Фішинг – вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів – логінів і паролів. Це спонукання користувача ввести свої ідентифікаційні та аутентифікаційні дані (логін, пароль) або іншу персональну інформацію шляхом запевнення користувачів щодо достовірності та справжності фальшивих (спеціально створених для цього) мережевих ресурсів, таких як пошта, веб-сайти, сторінки авторизації у соціальних мережах тощо.

Найбільш цікавими для шахраїв та кіберзлочинців є логіни і паролі від мережевих гаманців, номери та коди банківських карт, а також паролі від акаунтів соціальних мереж і блогів. Викрадені дані, зазвичай, використовуються для викрадення коштів з банківських рахунків або продаються в Інтернеті.

Як працює фішинг

Фішингові атаки зазвичай здійснюються через електронні листи, оголошення або сайти, схожі на ті, які ви відвідуєте. Наприклад, ви можете отримати електронний лист, схожий на лист із банку, з проханням підтвердити номер банківського рахунку.

Фішинговий сайт – веб ресурс, який виманює реквізити платіжних карток під виглядом надання неіснуючих послуг. Більшість фішингових сайтів надають неіснуючі послуги з поповнення мобільного рахунку, банкінгу та переказу коштів з картки на картку. Часто фішингові сайти копіюють оригінальні сторінки відомих сервісів, банків.

Фішингове повідомлення – лист електронної пошти, SMS, або інше повідомлення, яке виглядає як повідомлення від надійної організації, призначене для викрадення персональних даних користувачів. Зазвичай повідомлення містить гіперпосилання, яке переадресовує користувачів на зловмисні (підробні) веб-сайти, які за виглядом або по імені дуже схожі на офіційні веб-сайти організацій, або вкладений файл, який може містити шкідливий код, або посилання.

Як розпізнати фішинг?

Основні ознаки шахрайського електронного листа:

- тривожний характер повідомлення, наприклад, інформують, що ваші рахунки заблоковано, а кошти – в небезпеці;
- обіцяють "легкі" гроші (виграш, надзвичайно велика знижка на товар тощо);
- спонукають адресата виконати терміново та швидко вказівки з листа;

- у листі просять завантажити певний додаток чи перейти за посиланням;

- помилки в тексті листа та в темі повідомлення.

Якщо поштова програма у адресі відправника відображає поштову адресу нібито від банку (у полі "Від:"), наприклад pcb@policombank.com, це не гарантує, що лист дійсно надійшов від Полікомбанку. Фішингові повідомлення, зазвичай, мають вигляд електронного листа, який ззовні не відрізняється від справжнього листа від банку. Шахраї можуть підмінити електронну адресу, яка відображається в будь-якій поштовій програмі. Фактична адреса шахрая може бути виявлена при перегляді повного тексту листа.

В електронній пошті використовується загальна практика фішингу: надсилання запиту користувачам щодо оновлення інформації про акаунт. Проте, коли ви наводите мишею на посилання, перехід на справжній веб-сайт компанії не відбувається. Замість цього відбувається перехід на фішинговий сайт.

Інформація, яку можуть запитувати фішингові сайти

- Імена користувача та паролі
- Номери соціального страхування
- Номери банківських рахунків
- PIN-коди (особисті ідентифікаційні номери)
- Номери кредитних карток
- Дівоче прізвище матері
- Ваш день народження

Основні ознаки фішингових сайтів

Будьте уважні, якщо:

1. На сайті, який пропонує користувачу ввести конфіденційні дані, відсутнє безпечне з'єднання (домен сторінки захищеного сайту має починатися з починається *з https://* а не з *http://,* та в адресній стрічці браузера відображається символ безпечного з'єднання - замка з замкнутою дужкою). Але ознака захищеного з'єднання не є гарантією безпечності сайту. Зараз все більше фішингових сайтів налаштовані на використання протоколу захищеної передачі даних HTTPS. Використання сайтом HTTPS створює хибне відчуття безпеки, адже багато хто вважає, що замок або «зелена позначка» поряд з адресою сайту свідчить про його надійність. Тому потрібно зазвичай переконатись, що домен сайту дійсно належить певній оргацізації.
2. Сайт зареєстрований на підозрілому домені, створений на конструкторі сайтів, в адресному рядку відображається однакова адреса для всіх сторінок.
3. Наявність нульових комісій та інших неймовірних пропозицій. Якщо лист занадто добрий, щоб бути правдою, він, напевно, є фішинговим.

4. Наявність граматичних та синтаксичних помилок у тексті, неактуальна інформація, сумнівний зовнішній вигляд. (але відсутність помилок не є доказом легітимності).
5. Легітимні сайти зазвичай маскують введення паролів та карткових реквізитів (наприклад, зірочками) або використовують віртуальну клавіатуру, фішингові сайти – ні.
6. Після введення даних картки, відбувається збій операції, кошти зняті, але не зараховані.

Як захиститися від фішингу?

Щоб уникнути фішингових атак, звертайте увагу на описані вище ознаки, за допомогою яких можна виявити фішингові повідомлення.

Дотримуйтесь наступних рекомендацій:

1. Завжди перевіряйте доменне ім'я в адресах сайтів та адресах електронної пошти.

   Полікомбанк має офіційно зареєстровані домени:

   policombank.com

   poli.com.ua

   Офіційний веб-сайт Полікомбанку https://www.policombank.com

   Адреса системи Кліент-банк Полікомбанку https://ifobs.policombank.com

   Полікомбанк може використовувать поштові адреси з офіційно зареєстрованих доменних імен, а також адреси:

   policombank@gmail.com

   ifobs@gmail.com

2. Виконуйте перевірку SSL сертифікату для домену і строк його дії. властивості сертифікату можна переглянути натиснувши в браузері на символ безпечного з'єднання (зазвичай значок замка) поряд з адресою сайта.
3. Якщо Ви отримали сумнівного електронного листа від імені Полікомбанку, повідомте про це банк за телефоном контакт центру (0462) 678 000
   (Режим роботи: понеділок – п'ятниця з 09.00 до 12.30 та з 13.30 до 17.00)
   та перешліть сумнівний лист з коментарями на електронну адресу bezpeka@policombank.com.
4. Дізнавайтесь про нові методи фішингу: читайте засоби масової інформації для отримання нової інформації про фішингові атаки, оскільки

кіберзлочинці постійно знаходять нові методи для виманювання даних користувачів.

5. Не надсилайте облікові дані: будьте особливо уважні, коли в електронному листі начебто перевірені організації запитують ваші облікові або інші конфіденційні дані. У разі необхідності перевірте вміст повідомлення, відправника або організацію, яку вони представляють.
6. Не натискайте на підозрілі кнопки та посилання: якщо підозріле повідомлення містить посилання або вкладення, не натискайте та не завантажуйте вміст. Це може призвести до переходу на шкідливий веб-сайт або інфікувати ваш пристрій.
7. Регулярно перевіряйте облікові записи: навіть якщо ви не маєте підозр, що хтось намагається викрасти ваші облікові дані, перевірте банківські та інші облікові записи в Інтернеті на наявність підозрілої активності.

Повідомлення в банк

Негайно проінформуйте банк в разі:

- втрати електронного платіжного засобу;
- несанкціонованого доступу або зміни інформації клієнта в системах дистанційного обслуговування;
- виявлення фішингових вебсайтів або отримання відомостей подібного змісту.

(0462) 678 000
(Режим роботи: понеділок – п’ятниця з 09.00 до 12.30 та з 13.30 до 17.00)

Виявлені фішингові вебсайти

Ознайомитися з переліком сайтів, які становлять небезпеку, можна на офіційному ресурсі ЕМА в розділі BlackList ЕМА:

https://www.ema.com.ua/citizens/blacklist

Гіперпосилання на сторінку офіційного Інтернет-представництва Національного банку, на якій розміщено довідник банків, що містить інформацію про банки та відокремлені підрозділи банків:

https://bank.gov.ua/ua/supervision/institutions