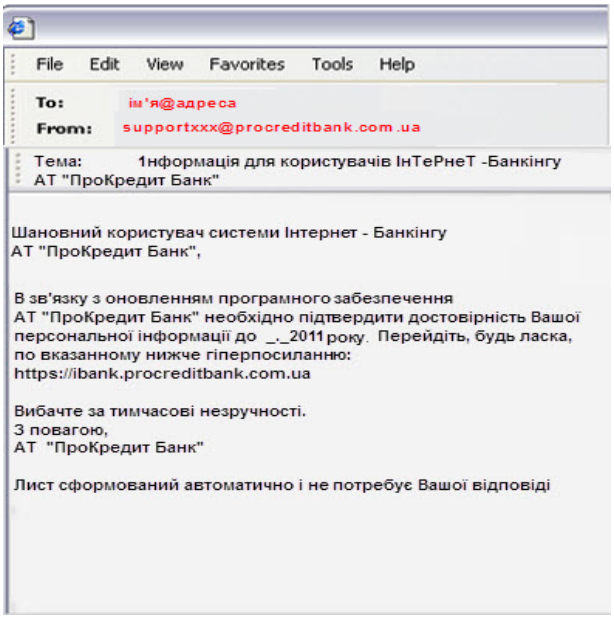
Рекомендації щодо захисту від фішингу

Що таке фішинг?

Фішинг (англ. phishing, від fishing – рибальство) — вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційної інформації користувачів - логінів та паролей.

Це досягається шляхом проведення масових розсилок електронних листів або повідомлень в соціальних мережах від імені відомих організацій, наприклад, від імені банків. У листі, зазвичай, міститься пряме посилання на сайт, який ззовні не відрізняється від справжнього. Після того, як користувач потрапляє на підроблену сторінку, шахраї намагаються різними психологічними прийомами примусити його зазначити свій логін та пароль, який він використовує для отримання доступу до певного сайту. Отримання конфіденційної інформації користувача дає можливість шахраям використовувати облікові записи та банківські рахунки користувачів в своїх цілях.


File Edit View Favorites Tools Help

To: ім'я@адреса

From: supportxxx@procreditbank.com.ua

Тема: 1нформація для користувачів ІнТеРнеТ -Банкінгу АТ "ПроКредит Банк"

Шановний користувач системи Інтернет - Банкінгу АТ "ПроКредит Банк",

В зв'язку з оновленням програмного забезпечення АТ "ПроКредит Банк" необхідно підтвердити достовірність Вашої персональної інформації до _._2011 року. Перейдіть, будь ласка, по вказанному нижче гіперпосиланню:
https://ibank.procreditbank.com.ua

Вибачте за тимчасові незручності.
З повагою,
АТ "ПроКредит Банк"

Лист сформований автоматично і не потребує Вашої відповіді

Рис.1 Зразок фішингового листа

Ознаки фішингових листів:

1. Адреса відправника

Електронна адреса, що відображається в полі "Від:" **НЕ є гарантією** відправки електронного листа через поштову систему АТ “ПроКредит Банк”.
Фішингові повідомлення, зазвичай, мають вигляд електронного листа, який ззовні не відрізняється від оригінального, відправленого з поштової системи АТ “ПроКредит Банк”.
За допомогою шкідливого програмного забезпечення, шахраї можуть підмінити електронну адресу, яка відображається в будь-якому поштовому клієнті.

2. Екстрений характер повідомлення

З метою збільшення кількості відгуків, зловмисники намагаються надати повідомленням екстрений характер, окреслюючи ліміт часу, і викликати необдумані дії користувача.

3. Помилки в темі листа

Як правило, в фішингових листах, в полі "Тема:", використовується різний регістр літер, набір літер та цифр, допускаються граматичні або друкарські помилки (наприклад пОмиЛка, 1нформац1я) для уникнення фільтрів поштових програм.

4. Гіперпосилання на підроблені сайти

Посилання, зазначені в фішингових листах, ззовні схожі на офіційну веб-адресу АТ "ПроКредит Банк" і перенаправляють користувачів на веб-сайти, які імітують зовнішній вигляд легітимного сайту Банку.

Як розпізнати підроблений сайт?

1. Адреса веб-сайту

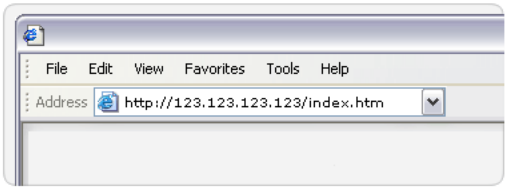


Рис.2 Приклад адресного рядка

Більшість методів фішингу зводиться до маскування підроблених посилань на фішингові сайти під посилання реальних організацій. Шахраї часто використовують адресу з друкарськими помилками або субдомени.

В дійсності, адреса сайту (URL) складається з набору цифр та літер і вміст сайту є підробленим. Але частина інформації та некритичні посилання можуть бути оригінальними.

2. Спливаючі вікна

Користуючись різним шкідливим програмним забезпеченням, шахраї мають змогу створювати та розміщувати підроблені спливаючі вікна на основі легітимного сайту, котрі запитую конфіденційну інформацію. При цьому справжній сайт банку буде відображуватись в фоновому режимі. Таким чином, вся, зазначена Вами, інформація в підробленому спливаючому вікні буде доступна шахраям.

Як захиститися від фішингових атак?

АТ "ПроКредит Банк" ніколи не надсилає запит на отримання у клієнтів конфіденційної інформації через електронну пошту, не здійснює розсилку листів з проханням вислати конфіденційну інформацію, логін чи пароль, не розсилає, засобами електронної пошти, програмне забезпечення для встановлення на Ваші комп'ютери.

Виконання перерахованих нижче правил дозволить Вам успішно протистояти фішинговим атакам:

1. **Ніколи не надавайте логін, пароль та інші конфіденційні дані стороннім особам.** Не відповідайте на листи з проханням вислати Вашу особисту або фінансову інформацію та не переходьте по вказаних посиланнях, оскільки **всі листи, з запитом конфіденційної інформацію є шахрайськими.**

2. **Якщо Ви отримали сумнівний електронний лист від імені АТ "ПроКредит Банк",** повідомте про це Контакт-Центр АТ "ПроКредит Банк" за телефонами 044 590 10 00 або 0 800 50 09 90 *(всі дзвінки зі стаціонарних телефонів на території України безкоштовні)*, або перешліть сумнівний лист з коментарями на електронну адресу: **probanking@procreditbank.com.ua**.

3. Для входу на Web-сторінку Електронного Банкінгу АТ "ПроКредит Банк" використовуйте лише адресу **https://probanking.procreditbank.com.ua/,** введену **ВРУЧНУ** в адресний рядок Вашого браузеру або користуйтесь власними закладками.

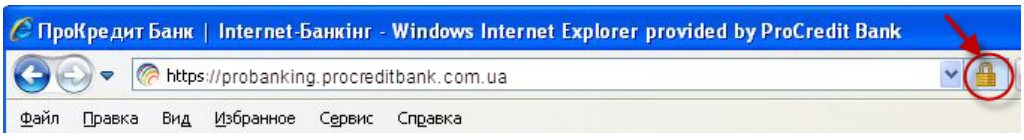
4. Використовуйте останню версію браузера. Такі браузери як Internet Explorer, FireFox, Google Chrome, Opera систематично оновлюються і мають фільтр захисту від фішингу.

5. Завжди перевіряйте, при передачі персональної інформації, та використовуйте шифроване з'єднання. При використанні безпечного з'єднання адреса сайту завжди розпочинається з **"https://",** а не з **http://**.

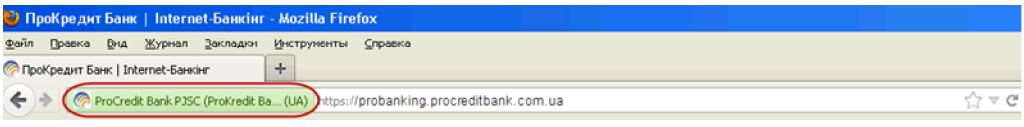
6. Для підтвердження автентичності сайту Електронного банкінгу АТ "ПроКредит Банк", необхідно перевірити цифровий сертифікат безпеки шляхом натискання на символ безпечного з'єднання в Вашому браузері[1], як зазначено на рисунку 3.

Internet Explorer 9

Internet Explorer 8



Firefox 13



Google Chrome 19

Рис. 3. Види символів безпечного з'єднання

[1] Символ безпечного з'єднання індивідуальний для кожного типу браузера.