Part of the ProCredit Group

ProCredit Bank
ПроКредит Банк

Рекомендації щодо безпечної роботи з системою Електронного банкінгу в мережі Інтернет

В своїй діяльності АТ “ПроКредит Банк” прагне забезпечити прозорість операцій клієнтів та конфіденційність інформації. Пропонуючи послуги клієнтам, ми постійно працюємо над підвищенням якості обслуговування, надійності та безпечності використання системи Електронного банкінгу.

Проте, Інтернет та електронна пошта можуть бути використані шахраями з метою отримання конфіденційної інформації для подальшого використання її в шахрайських цілях і тому ми рекомендуємо Вам завжди дотримуватись декількох простих правил, направлених на забезпечення безпечної роботи з системою Електронного банкінгу.

Основні застережні заходи:

Вхід в систему Електроного банкінгу АТ “ПроКредит Банк”:

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. Не відповідайте на листи з проханням вислати Вашу особисту або фінансову інформацію та не переходьте по вказаних посиланнях, оскільки всі листи з запитом конфіденційної інформації є шахрайськими. Якщо виникли питання, зв’яжіться з Контакт-Центром АТ "ПроКредит Банк" за телефонами 044 590 10 00 або 0 800 50 09 90 (всі дзвінки зі стаціонарних телефонів на території України безкоштовні).

Безпечне зберігання паролей:

Нікому не надавайте свій логін, пароль та інші конфіденційні дані. АТ "ПроКредит Банк" та співробітники правоохоронних органів ніколи не надсилають запити на отримання конфіденційної інформації клієнтів через електронну пошту, не здійснюють розсилку листів з проханням вислати конфіденційну інформацію, логін чи пароль, не розсилають, засобами електронної пошти, програмне забезпечення для встановлення на Ваші комп'ютери.

Безпека грошей:

Не звертайте уваги на “щирі” електронні листи, в яких описуються методи заробітку в Інтернеті. Привабливі пропозиції про легкий заробіток – це шахрайство, яке має на меті отримання конфіденційної інформації про Ваші рахунки.

Комп'ютер для роботи з системою Електронного банкінгу:

Використовуйте ліцензійні копії операційної системи та програмного забезпечення на комп’ютерах, які використовуються для роботи з системою Електронного банкінгу. Застосовуйте на робочому місці спеціалізовані програмні засоби безпеки: персональні фаєрволи, анти-шпигунське та анти-вірусне програмне забезпечення і т.п. з максимально можливими налаштуваннями безпеки. Уникайте використання системи Електронного банкінгу з комп’ютерів в громадських місцях (інтернет-кафе, бібліотеках та зонах Free Wi-Fi), а також з інших комп’ютерів, налаштування яких знаходиться поза межами Вашого контролю.

Додаткові застережні заходи:

1. Пам'ятайте Ваш пароль та іншу конфіденційну інформацію **напам'ять**. Радимо усі повідомлення, які містять персональну інформацію, таку як паролі, знищити. Ми рекомендуємо відключити функцію «автозаповнення».

2. Не використовуйте однакові паролі для системи Електронного банкінгу та інших програм.

3. При зміні паролю новий пароль повинен бути довжиною не менше 8 символів та складатись з набору маленьких і великих літер, цифр та спеціальних символів.

4. Ніколи не надавайте логін, пароль та інші конфіденційні дані стороннім особам (а також членам сім'ї та друзям).

5. АТ "ПроКредит Банк" ніколи не запитує паролі клієнтів, котрі телефонують до Контакт-Центру.

6. Завжди використовуйте посилання «Увійти» на офіційному веб-сайті АТ "ПроКредит Банк", щоб отримати доступ до Інтернет-банкінгу в браузері, і завжди виходьте з Інтернет-банкінгу, натиснувши кнопку «Вийти».

7. Ввійшовши до системи Електронного банкінгу, не залишайте комп'ютер без нагляду.

8. Обмежте доступ персоналу, який не має відношення до роботи з системою Електронного банкінгу, до комп'ютерів, які використовуються для роботи з ним.

9. Залежно від Вашого інтернет-браузера рядок стану може бути частково або повністю зелений. Натиснувши на символ «Замок», ви можете перевірити, який орган видав сертифікат. Якщо «Замок» відкритий або якщо сертифікат не був виданий **АТ "ПроКредит Банк"**, не робіть ніяких операцій та негайно зверніться до банку.

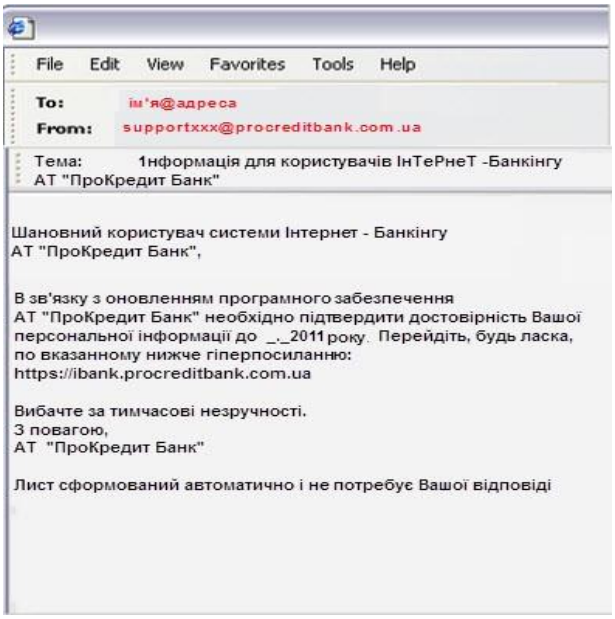
10. Якщо **Ви помітили** підозрілі зміни в роботі або в інтерфейсі системи Електронного банкінгу АТ "ПроКредит Банк", підозрілі електронні листи або сумнівні транзакції, фішингові вебсайти або отримали відомості подібного змісту, **виявили** несанкціонований доступ (спробу доступу) або зміну інформації в системі дистанційного обслуговування, **негайно зв'яжіться** з Контакт-Центром банку за телефонами 044 590 10 00 або 0 800 50 09 90 (*всі дзвінки зі стаціонарних телефонів на території України безкоштовні)* або надішліть нам листа електронною поштою за адресою ukr.cc@procredit-group.com

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 у 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

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”. У більшості випадків злочинці не знають Вашого імені і тому будуть використовувати анонімну форму адреси, наприклад «Шановний клієнте».

2. Екстрений характер повідомлення

З метою збільшення кількості відгуків, зловмисники намагаються надати повідомленням екстрений характер, окреслюючи ліміт часу, та 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.

Рекомендації щодо захисту від фармінгу

Що таке фармінг?

Фармінг відноситься до практики заміни IP-адреси певної домашньої сторінки шахрайською IP-адресою. Користувач автоматично перенаправляється на підроблений сайт, навіть не підозрюючи про це.

Як розпізнати підроблений сайт?

1. **Адреса веб-сайту**

Приклад адресного рядка

Більшість методів фармінгу зводиться до маскування підроблених посилань на фармінгові 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 запитують конфіденційну інформацію. При цьому справжній сайт банку буде відображатись у фоновому режимі. Таким чином, вся, зазначена Вами, інформація в підробленому спливаючому вікні буде доступна шахраям.

Як захиститися від фішингових та фармінгових 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 шахрайським 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 інформації є шахрайськими.

2. Якщо Ви отримали сумнівний електронний лист від імені АТ "ПроКредит Банк", повідомте про це Контакт-Центр банку за телефонами 044 590 10 00 або 0 800 50 09 90 (в*сі дзвінки зі стаціонарних телефонів на*

території України безкоштовні), або перешліть сумнівний лист з коментарями на електронну адресу: ukr.cc@procredit-group.com

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

4. При передачі персональної інформації завжди перевіряйте та використовуйте шифроване з'єднання. При використанні безпечного з'єднання адреса сайту завжди розпочинається з "https://", а не з http://. Крім того, переконайтеся, що доменне ім'я в URL-адресі завантаженої сторінки написано вірно і не перенаправлено на доменне ім'я з трохи іншим написанням, можливо, з додатковими буквами або з перестановкою букв. Негайно завершіть сеанс, якщо вони недійсні або в браузері відображається повідомлення про помилку.

5. При розкритті конфіденційної інформації переконайтеся, що Ви перебуваєте на зашифрованій домашній сторінці (на що вказує символ «Замок» в рядку стану). Натиснувши на символ «Замок», Ви зможете переглянути сертифікат безпеки сторінки. Ім'я домену, вказане в сертифікаті, має збігатися з ім'ям домашньої сторінки, на яку Ви щойно отримали доступ.

6. Зв'язуйтесь з Контакт-Центром 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 надішліть нам листа електронною поштою за адресою ukr.cc@procredit-group.com , коли ситуація здається Вам підозрілою.

7. Ознайомтесь з довідником банків, що містить інформацію про банки та їх відокремлені підрозділи, який розміщено на сторінці офіційного Інтернет-представництва Національного банку України за посиланням https://bank.gov.ua/supervision/institutions.