Рекомендації щодо безпечної роботи з e-Banking АТ “ПроКредит Банк” iBank2UA в мережі Інтернет

У 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 безпеки використання системи e-Banking (iBank2UA).

Проте Інтернет та електронна пошта можуть бути використані шахраями з метою отримання конфіденційної інформації для подальшого використання її в шахрайських цілях. Тому ми рекомендуємо вам завжди дотримуватись декількох простих правил, спрямованих на забезпечення безпечної роботи з системою e-Banking (iBank2UA).

1. Вхід до системи e-Banking (iBank2UA) АТ “ПроКредит Банк” здійснюйте лише з офіційної сторінки банку за посиланням: https://ibank.procreditbank.com.ua/web/
2. Уникайте використання системи e-Banking (iBank2UA) на комп’ютерах у громадських місцях (інтернет-кафе, бібліотеках, зонах Free Wi-Fi), а також на інших комп’ютерах, налаштування яких знаходяться поза вашим контролем.
3. Не відповідайте на листи з проханням вислати особистий ключ ЕП, пароль та інші ваші конфіденційні дані. Подібні листи створюють зловмисники. Банк ніколи не надсилає запитів на отримання конфіденційної інформації через електронну пошту, не здійснює розсилку листів з проханнями вислати особистий ключ ЕП і пароль, не розсилає дистрибутиви програмного забезпечення для встановлення на ваші комп’ютери.
4. Не встановлюйте і не зберігайте підозрілі файли, отримані з сумнівних джерел, завантажені з невідомих вебсайтів, надіслані електронною поштою або отримані на форумах. Рекомендуємо такі файли негайно видаляти. У випадку необхідності завантаження файлу, обов’язково перевірте його за допомогою антивірусу.
5. Відмовтесь від відвідування сайтів сумнівного змісту (сайти еротичного змісту, сайти піратського програмного забезпечення, хакерські сайти тощо). Зазвичай такі сайти містять шкідливі програми, які завантажуються і запускаються під час входу на них.
6. Використовуйте ліцензійні копії операційної системи та програмного забезпечення на комп’ютерах, які використовуються для роботи з e-Banking (iBank2UA).
7. Використовуйте на робочому місці ліцензійні засоби антивірусного захисту відомих виробників. Антивірус повинен бути налаштований на регулярне автоматичне оновлення антивірусних баз, регулярне сканування всіх локальних дисків і постійний моніторинг операцій з файлами (таких як зчитування та запис), поштовими базами та аналіз трафіку.
8. Застосовуйте на робочому місці спеціалізовані програмні засоби безпеки: персональні фаєрволи, антишпигунське програмне забезпечення тощо з максимально можливими налаштуваннями безпеки.
9. Використовуйте SMS-повідомлення для входу в e-Banking (iBank2UA) та ініціювання дистанційних платіжних операцій з метою забезпечення посиленої автентифікації та підвищення рівня безпеки обслуговування в e-Banking (iBank2UA).
10. Використовуйте сервіс “IP-фільтрації” – механізм обмеження доступу до системи e-Banking (iBank2UA) за “IP-адресами” комп’ютерів, з яких здійснюється підключення до системи e-Banking (iBank2UA).

1. Правила використання особистого ключа ЕП і пароля доступу до нього

1. Використовуйте для зберігання файлів з секретними ключами ЕП окремі захищені носії типу Token (Кристал, Алмаз).
2. Від’єднуйте від комп’ютера носії з особистими ключами ЕП, якщо вони не використовуються для роботи з e-Banking (iBank2UA).
3. Зберігайте носії з особистими ключами ЕП у сейфі або столі, що зачиняється на ключ.
4. Обмежте або унеможливіть доступ персоналу, який не має відношення до роботи з e-Banking (iBank2UA), до комп’ютерів, які використовуються для роботи з e-Banking (iBank2UA).
5. Обмежте обслуговування комп’ютерів, які використовуються для роботи з e-Banking (iBank2UA), нелояльними співробітниками або сторонніми особами та забезпечте контроль над виконанням таких дій.

6. Замініть особистий ключ ЕП у разі звільнення відповідального співробітника, який мав доступ до нього.

7. У разі виникнення будь-яких підозр на компрометацію (копіювання, втрату) особистих ключів ЕП або компрометацію середовища виконання (наявність шкідливих програм у комп'ютері) – обов'язково зателефонуйте в банк і заблокуйте особистий ключ ЕП.

8. У разі крадіжки особистого ключа ЕП, зміна пароля доступу до нього не захищає від використання його зловмисниками. З метою дотримання безпеки ваших платежів необхідно згенерувати новий особистий ключ ЕП.

9. У випадку втрати мобільного пристрою та/або номера мобільного телефону, на який надходять SMS-повідомлення, повідомте про це банк будь-яким способом та змініть номер мобільного телефону, подавши до банку заяву про зміну номера телефону.

10. При виявленні незвичної поведінки програмного забезпечення e-Banking (iBank2UA) чи будь-яких змін в інтерфейсі програми зателефонуйте до банку та з'ясуйте, чи не пов'язані ці зміни з оновленням програмного забезпечення. Якщо ні – негайно заблокуйте доступ до системи електронного банкінгу.

11. Контролюйте стан ваших розрахункових рахунків щонайменше 1–2 рази на день, навіть якщо ви не здійснюєте платіжних операцій у системі.

Звертаємо вашу увагу, що АТ «ПроКредит Банк» не має доступу до ваших особистих ключів ЕП і не може підписувати платіжні документи електронним підписом (ЕП) від імені вашої організації. У банку зберігається лише відкритий ключ вашого ЕП, який використовується виключно для перевірки підпису на електронних платіжних документах.

Банк не несе відповідальності за збереження ваших особистих ключів ЕП, які знаходяться у вас, а також за можливі фінансові втрати у випадку виконання фальшивих платіжних документів, оскільки ви є єдиним власником особистого ключа ЕП.

Рекомендації щодо захисту від фішингу

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

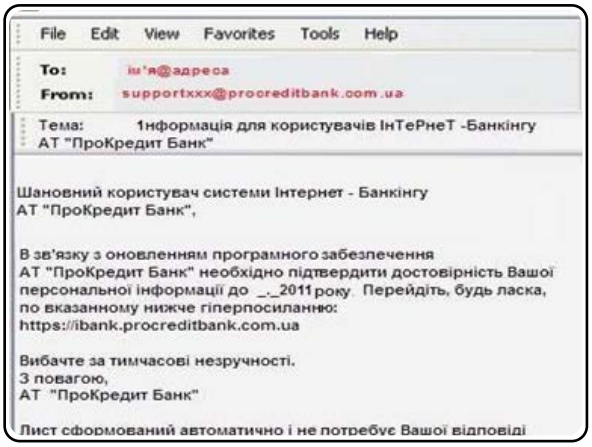
Це досягається шляхом масових розсилок електронних листів або повідомлень у соціальних мережах від імені відомих організацій, наприклад банків. У листі зазвичай міститься пряме посилання на сайт, який зовні не відрізняється від справжнього. Після переходу на підроблену сторінку шахраї застосовують різні психологічні прийоми, щоб змусити користувача ввести свій логін і пароль.

Отримавши конфіденційну інформацію, зловмисники можуть використовувати облікові записи та банківські рахунки жертви у власних цілях.

1. Адреса відправника

Електронна адреса, що відображається в полі "Від:", не є гарантією того, що електронний лист був надісланий через поштову систему АТ "ПроКредит Банк".

Фішингові повідомлення зазвичай мають вигляд електронного листа, який зовні не відрізняється від оригінального, відправленого з поштової системи АТ "ПроКредит Банк".
У більшості випадків злочинці не знають вашого імені, тому використовують анонімне звернення, наприклад: "Шановний клієнте".


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

2. Екстрений характер повідомлення

Щоб збільшити кількість відгуків, зловмисники намагаються надати повідомленням термінового характеру, обмежуючи час для дій та провокуючи користувачів на необдумані вчинки.

3. Помилки в темі листа

Як правило, у фішингових листах у полі "Тема:" використовується змішаний регістр літер, комбінація літер і цифр, а також можуть міститися граматичні або друкарські помилки (наприклад: *пОмиЛка, 1нформац1я*) для обходу фільтрів поштових програм.

Рекомендації щодо захисту від фармінгу

Фармінг – це шахрайська практика, що передбачає підміну IP-адреси офіційного вебсайту на шахрайську. У результаті користувач автоматично перенаправляється на підроблений сайт, не підозрюючи про це.

1. Адреса відправника

Адреса веб-сайту
Більшість методів фармінгу зводиться до маскування підроблених посилань на шахрайські сайти під посилання реальних організацій. Зловмисники часто використовують адреси з друкарськими помилками або субдомени, щоб ввести користувачів в оману.

Насправді веб-адреса (URL) таких сайтів складається з випадкового набору цифр і літер, а їхній вміст є підробленим. Водночас частина інформації та некритичні посилання можуть залишатися оригінальними, щоб підвищити довіру користувача.

Рис.2 Приклад адресного рядка

2. Спливаючі вікна

Шахраї можуть використовувати шкідливе програмне забезпечення для створення та розміщення підроблених спливаючих вікон на легітимних сайтах. Такі вікна запитують конфіденційну інформацію, тоді як справжній сайт банку продовжує відображатися у фоновому режимі.

У результаті вся введена вами інформація в підробленому спливаючому вікні стає доступною шахраям.

Як захиститися від фішингових та фармінгових атак?

АТ “ПроКредит Банк” ніколи не надсилає запити на отримання конфіденційної інформації від клієнтів через електронну пошту, не здійснює розсилку листів із проханням надати конфіденційну інформацію, логін чи пароль, а також не надсилає програмне забезпечення для встановлення на ваші комп’ютери.

Дотримання наведених нижче правил допоможе вам успішно протистояти шахрайським атакам:

1. Ніколи не передавайте логін, пароль та інші конфіденційні дані стороннім особам. Не відповідайте на листи з проханням надіслати вашу особисту або фінансову інформацію та не переходьте за вказаними у них посиланнями. Усі такі запити є шахрайськими.

2. Якщо ви отримали підозрілий електронний лист від імені АТ “ПроКредит Банк”, негайно повідомте про це Контакт-центр за телефонами: 044 590 10 00; 0 800 50 09 90 (безкоштовно зі стаціонарних телефонів в Україні); 0990 (короткий номер для дзвінків у застосунку Rakuten Viber) або перешліть лист із коментарем на електронну адресу: ukr.cc@procredit-group.com

3. Використовуйте найновішу версію браузера. Такі браузери, як Microsoft Edge, Firefox, Google Chrome, Opera, регулярно оновлюються та містять вбудовані механізми захисту від фішингу.

4. Перед передачею персональних даних переконайтеся, що використовуєте захищене з’єднання. Безпечні сайти мають адресу, що починається з “https://”, а не “http://”. Також перевіряйте доменне ім’я в URL-адресі, щоб уникнути підміни (наприклад, додаткові або переставлені літери). Якщо браузер повідомляє про помилку або сертифікат є недійсним – негайно завершіть сеанс.

5. Перед введенням конфіденційної інформації переконайтеся, що перебуваєте на захищеній сторінці. На це вказує значок замка в адресному рядку. Натиснувши на нього, ви зможете переглянути сертифікат безпеки. Доменне ім’я в сертифікаті має збігатися з адресою сайту, на який ви зайшли.

6. Якщо у вас виникають підозри щодо безпеки, зв’яжіться з Контакт-центром: 044 590 10 00; 0 800 50 09 90 (безкоштовно зі стаціонарних телефонів в Україні); 0990 (короткий номер для дзвінків у застосунку Rakuten Viber) Або напишіть нам на ukr.cc@procredit-group.com

Будьте уважні та дбайте про безпеку своїх даних!