Рекомендації щодо безпечної роботи з Електронним банкінгом

АТ «ПроКредит Банк» iBank2UA в мережі Інтернет

1. Щоб увійти на Web-сторінку системи Електронного банкінгу АТ «ПроКредит Банк» використовуйте лише адресу **https://ibank.procreditbank.com.ua**

2. Уникайте використання системи Електронного банкінгу iBank2UA з комп'ютерів в громадських місцях (інтернет-кафе, бібліотеках та зонах Free Wi-Fi), а також з інших комп'ютерів, налаштування яких знаходиться поза Вашим контролем.

3. Не відповідайте на листи з проханням вислати секретний ключ електронно-цифрового підпису (ЕЦП), пароль та інші Ваші конфіденційні дані. Подібні листи створюють зловмисники, банк ніколи не надсилає запит на отримання у клієнтів конфіденційної інформації через електронну пошту, не здійснює розсилку електронних листів з проханнями вислати секретний ключ ЕЦП і пароль, не розсилає дистрибутиви програмного забезпечення для встановлення на Ваші комп'ютери.

4. Під час роботи з електронною поштою та сервісами обміну миттєвими повідомленнями (ICQ, Skype, Mail.Ru-Агент і т.п.) звертайте особливу увагу на відправника повідомлення. Що б не було написано в тексті повідомлення, якщо відправник Вам невідомий – відкривати прикріплені файли або посилання не рекомендується.

5. Не встановлюйте і не зберігайте підозрілі файли, отримані з сумнівних джерел, завантажені з невідомих Web-сайтів, надіслані електронною поштою або отримані на форумах. Рекомендуємо такі файли негайно видаляти. У випадку необхідності завантаження файлу, обов'язково перевірте його за допомогою антивірусу.

6. Відмовтесь від відвідування сайтів сумнівного змісту (сайти еротичного змісту, сайти піратського програмного забезпечення, хакерські сайти і т.п.). Зазвичай, такі сайти містять шкідливі програми, які завантажуються і запускаються під час входу на них.

7. Використовуйте ліцензійні копії операційної системи та програмного забезпечення на комп'ютерах, які використовуються для роботи з iBank2UA.

8. 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 над файлами (таких як зчитування та запис), поштовими базами та аналіз трафіку.

9. Застосовуйте на робочому місці спеціалізовані програмні засоби безпеки: персональні фаєрволи, анти-шпигунське програмне забезпечення і т.п. з максимально можливими налаштуваннями безпеки.

10. Використовуйте OTP-Токен (One-Time Password Token) – пристрій, що використовується для генерування одноразових паролів, та проведення додаткової ідентифікації Клієнта в системі Електронного банкінгу.

11. Використовуйте сервіс «IP-фільтрації» - механізм обмеження доступу до системи Електронного банкінгу за «IP-адресами» комп'ютерів, з яких здійснюється підключення до системи Електронного банкінгу.

ProCredit Bank

Правила використання ключа ЕЦП і пароля доступу до ключа

1. Використовуйте для зберігання файлів з секретними ключами ЕЦП окремі носії: CD/DVD, USB флеш-накопичувачі, захищені носії типу Token.

2. Від'єднуйте носії з ключами ЕЦП, якщо вони не використовуються для роботи з Електронним банкінгом iBank2UA.

3. Зберігайте носії з ключами ЕЦП в сейфі або столі, що зачиняється на ключ.

4. Обмежте або унеможливте доступ персоналу, який не має відношення до роботи з Електронним банкінгом, до комп'ютерів, які використовуються для роботи з iBank2UA.

5. Обмежте обслуговування комп'ютерів, які використовуються для роботи з iBank2UA, нелояльними співробітниками або сторонніми особами та забезпечте контроль над виконанням таких дій.

6. Замініть ключ ЕЦП у разі звільнення відповідального співробітника, який мав доступ до секретного ключа ЕЦП.

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

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

9. При виявленні незвичної поведінки програмного забезпечення iBank2UA чи будь-яких змін в інтерфейсі програми - зателефонуйте до банку та з'ясуйте, чи не пов'язані такі зміни з оновленням програмного забезпечення. Якщо ні - заблокуйте ключі ЕЦП.

10. Контролюйте стан Ваших розрахункових рахунків щонайменше 1-2 рази на день, навіть якщо Ви не здійснюєте платіжні операції в системі.

Звертаємо Вашу увагу, що АТ «ПроКредит Банк» не має доступу до Ваших секретних ключів і можливості підписання платіжних документів електронно-цифровим підписом від імені Вашої організації. У банку зберігається відкритий ключ Вашого ЕЦП, який використовується виключно для перевірки ЕЦП на підписаних Вашим секретним ключем електронних платіжних документах.

Банк не несе відповідальності за збереження секретних ключів ЕЦП, які знаходяться у Вас, і можливі фінансові втрати у випадку виконання фальшивих платіжних документів, адже Ви - єдиний власник ЕЦП.