Безпека роботи з системою Клієнт-банк

1. Найбільш поширені в наш час загрози:

Встановлення на комп'ютер шкідливих програм – вірусних і троянських програм, здатних вкрасти пароль і секретний ключ електронно-цифрового підпису.
Розсилка листів від імені банку з проханнями перейти на вказану інтернет-адресу, вказати шлях і пароль до свого ключа електронно-цифрового підпису, або вислати персональні дані для їх перевірки чи поновлення в базах даних банку, тощо.

2. Засоби захисту реалізовані в системі клієнт-банк

Шифрування даних - для забезпечення конфіденційності інформації.
Електронний цифровий підпис під електронними документами – підписуючи документ, Ви будете певні, що Ваш документ переданий до банку саме в тому вигляді, в якому Ви його створили.
IP-фільтрація - для забезпечення доступу до системи клієнт-банк тільки з комп'ютерів, які використовуєте Ви.
Оперативне сповіщення за допомогою безкоштовних SMS-повідомлень або електронних листів про події, такі, як вхід до системи або проведення платежів – для того, щоб Ви завжди були в курсі всіх подій і мали можливість реагувати на них.
Одноразові паролі - для додаткового контролю при вході до системи клієнт-банк

3. Засоби захисту робочої станції

Електронні листи - ніколи не відкривайте листи від відправників, які Вам не знайомі, тим більше, якщо до листа включені будь-які файли. Не відповідайте на такі листи і не відправляйте свою персональну інформацію. Пам'ятайте, таким способом шахраї часто намагаються отримати Ваші персональні дані, такі як паролі, логіни, номери пластикових карток і рахунків та ін.
Операційна система - використовуйте тільки ліцензійне програмне забезпечення, проводьте регулярні оновлення, як правило, вони завжди доступні на сайті розробника. По можливості, налаштуйте автоматичне оновлення. Це важливо, тому що в оновленнях містяться нові елементи для забезпечення безпеки Вашого комп'ютера.
Антивірусне програмне забезпечення - завжди використовуйте та оновлюйте на Вашому комп'ютері антивірусне програмне забезпечення. Ми, зі свого боку, рекомендуємо використовувати тільки офіційні продукти

Бажано проводити сканування комп'ютера такими програмами раз на день, але обов'язково не рідше ніж раз на тиждень.
Мережевий екран (firewall) на Вашому комп'ютері - це захист від небажаного доступу з Інтернету. За допомогою такого доступу шахраї можуть встановлювати вірусні, троянські та інші шкідливі програми на Ваш комп'ютер.

4. Правила роботи з системою клієнт-банк

Персональна відповідальність - ніколи не передавайте іншим особам персональну інформацію, таку як ключі та паролі, або токени.
Закінчуючи роботу, завжди виходьте із системи клієнт-банк для того, щоб ніхто
інший не міг скористатися нею для доступу до Ваших даних.
Пароль - намагайтеся використовувати складні для вгадування комбінації. Не використовуйте дати народження, прості комбінації цифр і паролі, які Ви використовуєте для входу на будь-який інший сайт або в іншу програму, тощо.
Підозра компрометації – якщо Ви підозрюєте, що Ваші персональні дані скомпрометовані, або Ви помітили щось незвичайне в роботі системи клієнт-банк, негайно зв'яжіться з Контакт-центром банку