«Банк Восток» рекомендує

Підвищити Ваш рівень надійності та безпеки «Клієнт-Банк/Інтернет-Банк»

Безпека операцій в системі залежить в першу чергу від бажання їх захистити.

З чого складається будь-яка система Клієнт-Банк/Інтернет Банк:

Клієнт **Провайдер** **Сервер Банку**

Програмне забезпечення системи Клієнт-Банк або Інтернет-Банк створено таким чином, що інформація від комп'ютера клієнта до серверу Банку передається в зашифрованому вигляді. Для того, щоб її розшифрувати і зламати, необхідно декілька років підбирати ключ на дуже потужних комп'ютерах. Навіть отримуючи інформацію на обладнанні Інтернетпровайдера, її неможливо застосувати ні для розшифрування, ні для відправки платежів.

Сервер Банку знаходиться під постійним контролем спеціалістів банку, від мережевих атак сервер захищений мережевими фільтрами, від вірусів ліцензійним антивірусним програмним забезпеченням. В Банку розроблені і виконуються процедури безпеки по запобіганню будь-яких несанкціонованих дій в інформаційних системах.

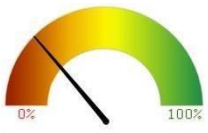
Слабким місцем в цій ланці є комп'ютер Клієнта. На цьому комп'ютері знаходяться всі необхідні інструменти та інформація для ініціалізації платежу. У випадку несанкціонованого проникнення на комп'ютер, зловмисники можуть виконати платіж, який для банку виглядатиме, як нормальний санкціонований платіж.

Ми захистили систему зі сторони банку, та хочемо допомогти захистити Ваше обладнання.

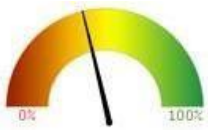
Що робити? Які рішення пропонує Банк?

Технічні рішення, що впроваджені в «Банк Восток»:

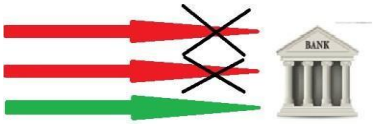
Безпека



1. **SMS інформування.** Вам на мобільний телефон приходить коротке повідомлення про списання з рахунку. Такі повідомлення можна налаштувати для оповіщення будьякого списання, або при списанні платежу більше визначеної суми.



2. **IP-фільтрація.** Наше обладнання може відслідковувати, з якої адреси відбувається підключення до сервера. Якщо це не Ваша звичайна адреса комп'ютера, тоді ми заблокуємо таке підключення. Фільтрацію можна використовувати у випадку, коли Ваш комп'ютер має постійну (статичну) мережеву адресу.



3. **Токен**. Це окремий пристрій зберігання Вашого електронно-цифрового підпису. З цього пристрою неможливо вилучити або підробити Ваш підпис. Без цього пристрою не можливо відправити платежі. Якщо токен не підключений до комп'ютера, то шахраї при не санкціонованому підключені не зможуть виконати операції з системою Клієнт-Банк/Інтернет-Банк.

4. **OTP (one time password)** – це одноразові паролі, які приходять на телефон директору/бухгалтеру для підтвердження операції. Пароль необхідно ввести в систему, щоб відправити платіж.

Скільки поставити перешкод на шляху шахраїв кожен клієнт вирішує самостійно.

Поради і рекомендації:

1) Використовувати ліцензійне антивірусне ПЗ на комп'ютері, де встановлений Клієнт-Банк або Інтернет-Банк. Зробіть налаштування щоденного автоматичного обновлення, і встановить максимальний режим захисту. Це, можливо, перешкодить відображенню деяких мультимедійних і барвистих сайтів, але захистить від зламу.

2) Ми рекомендуємо заблокувати доступ до Інтернету з комп'ютера, якщо це можливо. Дозволити підключення тільки до серверу Банку. Не давати можливість використовувати цей комп'ютер для відвідування соціальних мереж, інтернет магазинів, розважальних сайтів, і для скачування будьяких файлів з Інтернету та USB-накопичувачів.

3) Міняйте паролі не рідше, ніж через 60 днів. Робіть складні паролі, використовуйте великі букви, цифри, непечатні символи і т.п.

Перевірити пароль можна, наприклад, тут https://nordpass.com/secure-password/

4) Зберігайте електронно-цифровий підпис (ЕЦП) на окремому носії (флешкарті, **токені**). Якщо Ви не працюєте з Клієнт-Банком/Інтернет-Банком, витягніть ЕЦП і зберігайте в недоступному для сторонніх місці.

5) Налаштуйте блокування комп'ютера через 10 хвилин простою, щоб при поверненні до роботи необхідно було ввести пароль.

6) Загальний список вимог і рекомендацій Ви можете прочитати в Додатку №1 до Вашого договору користування системою Клієнт-Банк/Інтернет-Банк або на сайті http://bankvostok.com.ua

Наші спеціалісти завжди готові Вам допомогти та надати консультацію для створення максимального рівня захисту Вашого устаткування.

З повагою, «Банк Восток»

Відмова від відповідальності:

ПАТ «Банк Восток» настійливо рекомендує використовувати технічні рішення, запропоновані в даних рекомендаціях, з ціллю підвищення безпеки здійснення розпорядження рахунком (рахунками) в системі Клієнт-Банк/Інтернет-банк, т.я. ПАТ «Банк Восток» не несе відповідальності перед клієнтом за будь-які наслідки (в том числі матеріального характеру), які виникли в зв'язку з виконанням Банком розпоряджень клієнтів, виданих неуповноваженими особами в випадку, коли Банк не зміг встановити факт видачі розпоряджень такими особами.