Пам’ятка інформаційної безпеки
під час використання клієнтом систем дистанційного обслуговування та здійсненні платежів електронними засобами

Рекомендації щодо безпечного використання систем дистанційного обслуговування банку та уникнення випадків підвищеного ризику збитків для користувачів електронних платіжних засобів.

З метою недопущення будь-яких шахрайських дій щодо Клієнтів під час користування системами дистанційного банківського обслуговування та/або використання Клієнтами електронних платіжних засобів, АТ «АЙБОКС БАНК» (далі - Банк) здійснює низку організаційних, адміністративних та технологічних заходів.
Водночас, для підтримання високого рівня інформаційної безпеки при використанні системи Клієнт-Банку, здійсненні інтернет платежів та розрахунків з використанням платіжних карток, клієнтам рекомендується наступне.

При розрахунках карткою, клієнт має здійснювати це особисто, не передавати картку іншим особам з метою уникнення компрометації платіжних реквізитів картки. Тримати картку таким чином, щоб уникнути розголошення кодів CVV2.

Перед користуванням банкоматом звертати увагу на отвір для прийому карток/коштів, на клавіатуру і зовнішній вигляд банкомату. У випадку виявлення сторонніх або підозрілих предметів, не вставляти карток, не вносити коштів і взагалі не здійснювати операцій.

При введенні ПІН-коду в банкоматах обов’язково приховувати натискання на клавіатуру з метою унеможливлення їх імовірного зчитування сторонніми особами, що можуть знаходитись поруч або спостерігати за допомогою відео.

Клієнти зобов’язані тримати в таємниці власні персональні дані, CVV2-код, терміни дії картки. Банк не зв’язується з клієнтами для отримання будь-яких його даних. За необхідності зв’язатись з Банком клієнт зобов’язаний використовувати номер телефону, що вказаний на офіційній інтернет-сторінці Банку.

Клієнти мають розуміти, що внесення платіжних реквізитів банківських карток на сумнівних інтернет-сайтах, або через незахищене з’єднання з інтернет-сайтом, або з використанням ненадійного комп’ютера, на якому приховано встановлене зловмисне ПЗ, може призвести до компрометації платіжних реквізитів картки і, як наслідок, заволодіння зловмисниками коштами клієнта.

У випадку втрати платіжних карток або компрометації їх платіжних реквізитів клієнт зобов’язаний негайно звернутись до банку для блокування його картки та перевипуску нової.

При дистанційному обслуговуванні системою Клієнт-банк та при використанні електронних платіжних засобів, для забезпечення безпеки інформації та захисту від імовірного шахрайства, клієнт зобов’язаний зберігати в таємниці та в недоступних третім особам місцях використовувані в платіжних засобах відповідні реквізити (терміни дії та CVV2-коди карток, логіни, паролі, секретні ключі, паролі на секретні ключі, власні персональні дані, кодові слова тощо).

Для убезпечення клієнтів від імовірних шахрайських дій сторонніх осіб, Банк рекомендує для здійснення фінансових операцій використовувати апаратне забезпечення (комп’ютер)

що задовольняє наступним вимогам:

- На комп'ютері використовується лише необхідне для роботи інтернет Банкінгу програмне забезпечення (ПЗ);
- До комп'ютера не допускаються сторонні особи, в тому числі шляхом встановлення паролю, блокування робочого екрану комп'ютера під час його простою, вимикання на час, коли він не використовується;
- Комп'ютер не використовується для відвідування Інтернет-сторінок і на нього не завантажуються з інтернету сторонні документи або програмне забезпечення;
- Встановлене виключно ліцензійне ПЗ;
- Використовується антивірусне ПЗ з автоматичним щоденним оновленням вірусних баз та сигнатур шкідливого ПЗ;
- В автоматичному режимі встановлюються оновлення системи та програмного забезпечення;
- На робочих/персональних комп'ютерах, з яких здійснюється запуск банківських/фінансових додатків працюють штатні та додаткові засоби безпеки («брандмауери», «файрволи»);

З метою мінімізації ризиків безпеки інформації, Банк рекомендує клієнтам:

- Не використовувати загальнодоступні (публічні) точки доступу до Інтернет для використання при дистанційному банківському обслуговуванні;
- Не залишати комп'ютер (або інший мобільний пристрій) без нагляду.
- Не використовувати сторонні комп'ютери (пристрої) для зв'язку з Банком.
- Дотримуватись вимог керівництва користувача використовуваного ПЗ, що розміщене на сайті банку;
- Уважно контролювати дані, що вносяться або містяться в системі дистанційного обслуговування;
- Використовувати надійні паролі з довжиною не менше восьми символів;
- Надійно зберігати в недоступних іншим особам місцях особисті ключі та носії ключової інформації. Зберігати сертифікати на зовнішніх носіях, окремо від комп'ютера та окремо від логіну і пароля.
- Не довіряти стороннім користувачам користуватись Вашим сертифікатом.
- Користуватись кнопкою «Вихід» для завершення роботи з системою.
- Від'єднати носій інформації одразу після завершення сеансу роботи.

Загальна інформація щодо системи клієнт-Банк

З метою запобігання доступу сторонніх осіб до конфіденційної інформації клієнта через систему Клієнт-банк, запобігання перехопленню або модифікації даних, Банком використовується багаторівнева архітектура системи безпеки, що включає в себе:

- Обов'язкову авторизацію та автентифікацію користувачів
- Протоколювання дій користувачів в системі
- Обмін даними виключно стандартними інтерфейсами
- Захист каналу передачі даних на основі SSL v3.0
- Цифровий підпис документів з використанням асиметричних алгоритмів
- Контроль прав доступу користувача до об'єктів системи

Весь обмін даними між клієнтським та банківським ПЗ здійснюється в зашифрованому вигляді. Права користувача визначаються режимом роботи, що зазначений в договорі на підключення та обслуговування клієнта системи Клієнт-банк. Користувачу може бути дозволений повний або обмежений доступ до меню системи, до визначених рахунків, до права виконувати певні види операцій, в тому числі перегляд документів без права створення і підпису, створення документів без права підпису, підпис документів без права їх створення.

Для організації не передбачених договором схем організації доступу, клієнт має офіційно звернутись до банку. Банком може стягуватись окрема плата за параметризацію системи відповідно до побажань клієнта.

Кожному користувачу Банк надає Логін – ім'я користувача, пароль – пароль входу в систему, пароль на секретний ключ, первинний сертифікат на носій інформації і таємний ключ.

При користуванні системою Клієнт-банк клієнт має виконувати загальні вимоги забезпечення безпеки інформації, що зазначені вище, а також:

При першому вході в систему з цими реквізитами система Клієнт-банк автоматично ініціює процес створення нового сертифікату та таємного ключа. Також з метою забезпечення безпеки рекомендується змінити пароль входу в систему. Після спливу термінів дії сертифікату і таємного ключа система Клієнт-банк періодично рекомендуватиме користувачу ініціювати процес створення нового сертифікату і таємного ключа.

УВАГА! Після спливу терміну дії первинного сертифікату, система не дозволяє користувачу здійснити його перегенерацію. Тому, наполегливо рекомендуємо здійснювати перегенерацію первинних сертифікатів одразу після їх отримання в Банку.

Система Клієнт-банк фіксує всі спроби зміни та підбору паролю на вхід. Зберігайте Ваш особистий сертифікат і таємний ключ на зовнішньому носії інформації (дискети, накопичувачі, флеш-носії тощо). Зберігання цієї інформації окремо від комп'ютера дозволяє не тільки організувати додатковий захист Вашої конфіденційної інформації, а й забезпечує їх безпеку під час раптового виходу з ладу або інших проблемах з Вашим комп'ютером.

Під час генерації/перегенерації робочого сертифікату і таємного ключа необхідно вказувати шлях збереження на той носій, з якого були прочитані первинні дані. Не зберігайте зовнішній носій інформації разом з Вашими особистим сертифікатом, і таємним ключем разом з логіном та паролем, оскільки у випадку втрати ці дані зможуть несанкціоновано використати треті особи. Не довіряйте стороннім особам користуватись Вашим сертифікатом і таємним ключем для підписання документів Вашим іменем. Однією з функцій системи Клієнт-банк під час підписання документів для відправки в Банк є функція «Підписати від імені…». Ця функція системи дозволяє скоротити час на підготовку документів, однак не довіряйте виконувати цю операцію від вашого імені третім особами – завжди підписуйте документи самостійно (самостійно вводьте Ваш логін та пароль, самостійно підключайте зовнішній носій з Вашим особистим сертифікатом та секретним ключем). Після завершення операції не забувайте вилучити носій секретного сертифікату та ключа. Користуйтесь кнопкою «Вихід» для завершення сеансу роботи з системою. Без правильного завершення сеансу роботи з програмою, ситуацією можуть скористатись треті особи.

Не рекомендується користуватись системою Клієнт-банк в громадських місцях та інших місцях, де за діями користувача можуть спостерігати сторонні особи, що може призвести до компрометації логінів, паролів та іншої конфіденційної інформації.

Виявлення фішингових (шахрайських) інтернет сторінок або вішингових ресурсів.

Зловмисниками, з метою заволодіння даними клієнтів або створення враження легітимності інтернет сторінок (в т.ч. для шахрайських SMS-розсилок про виграші, нарахування, різноманітні «блокування» що використовуються для т.зв. «**вішингу**» - телефонного шахрайства), не рідко створюються інтернет-сторінки що мають зовнішню схожість, або навіть ідентичність за зовнішнім виглядом до справжніх сторінок фінансових установ. Часто на цих сторінках розміщуються сфабриковані фото документів (ліцензій, витягів, свідоцтв тощо). З метою перевірки справжності розміщених документів

рекомендуємо використовувати офіційні відкриті реєстри державних органів, наприклад:

https://bank.gov.ua/supervision/institutions

https://bank.gov.ua/supervision/institutions/21570492

https://usr.minjust.gov.ua/content/free-search (для отримання відомостей щодо юридичної особи АТ «АЙБОКС БАНК», ЄДРПОУ 21570492, де містяться офіційні відомості про банк, а також інформація щодо офіційної інтернет-сторінки та електронної пошти).

Оскільки державні органи можуть змінювати розміщення вказаних вище інтернет-сторінок, рекомендуємо також використовувати пошукові системи інтернет (наприклад: https://www.google.com.ua). Зазначаємо, що у витягах, ліцензіях, свідоцтвах та інших офіційних документах вказані виключно юридичні особи, яким ці ліцензії надані офіційними органами. Якщо на «фотокопії» документа за його номером значиться інша фізична або юридична особа, то така «фотокопія» є фіктивною. Розміщення на інтернет сторінці хоча б одного фіктивного документу свідчить про несправжність інтернет-сайту такої компанії в цілому. Відповідно, будь-яке посилання на цей сайт переслідує одну мету – «легітимізація» шахрайського ресурсу або дій шахраїв.

Водночас, за допомогою технології «фішингу» шахраї намагаються заволодіти даними клієнтів для подальшого заволодіння його коштами або отримання несанкціонованих привілеїв від імені клієнта/користувача.

«**Фішинг**» - це тип кібератаки на користувача шляхом надсилання йому засобами комунікації (електронна пошта, мессенджери, соціальні мережі тощо) повідомлення, яке обманним шляхом змушує користувача виконати певні небезпечні дії – відкрити заражений файл або інше вкладення, перейти за посиланням на заражений або підробний сайт, внести в надіслану форму або в на зараженому сайті логін та/або пароль до облікового запису, внести (розкрити) реквізити електронного платіжного засобу користувача, тощо.

Суть атаки на користувача полягає саме в заволодінні його конфіденційною інформацією або конфіденційною інформацією його платіжних засобів. Отримавши таку інформацію, зловмисники прямо або опосередковано використовують її для здійснення несанкціонованих списань грошових коштів з електронних платіжних засобів або рахунків користувача. Зазвичай користувач дізнається про такі несанкціоновані операції вже по факту їх здійснення, отримуючи інформацію про рух коштів за допомогою СМС чи під час перегляду руху коштів в системах Інтернет-банкінгу.

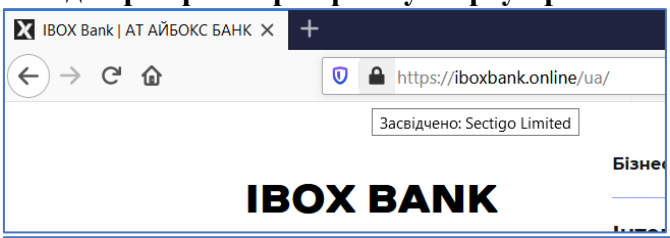
Відповідно, для збереження власних коштів громадяни мають зберігати в таємниці власну конфіденційну інформацію (в т.ч. персональні дані) та вчасно розпізнавати як фішингові сайти, так і випадки телефонного шахрайства.

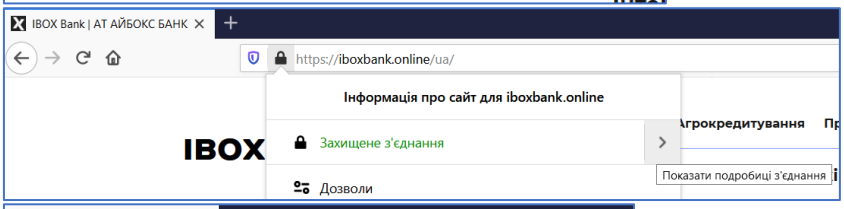
Перед тим, як вводити платіжні реквізити на інтернет-ресурсі користувачам необхідно впевнитись, що:

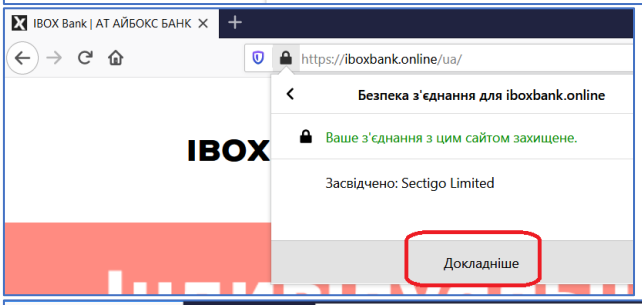
- Введення даних здійснюватиметься на офіційній сторінці Банку, а саме https://iboxbank.online/ і зазначена адреса не містить підмін схожих букв на цифри або інші літери (наприклад, шахраями часто підміняються латинські букви на зовні схожі цифри або кирилічні символи).
- На сайті присутній сертифікат, який використовується для організації захищеного з'єднання Банком. При використанні цієї технології адреса сайту починається з https://
- Сертифікат `*.iboxbank.online` виданий Sectigo RSA Domain Validation Secure Server CA, що належить компанії Sectigo Limited, має серійний номер 00:CF:36:11:3E:92:BD:BA:2A:1D:33:7D:BD:B6:A0:39:72 з терміном дії сертифікату до 16.05.2022.
- На сайті відсутні граматичні, орфографічні, структурні та дизайнерські помилки, розміщені посилання ведуть на внутрішні сторінки, а не містять помилки про відсутність останніх.

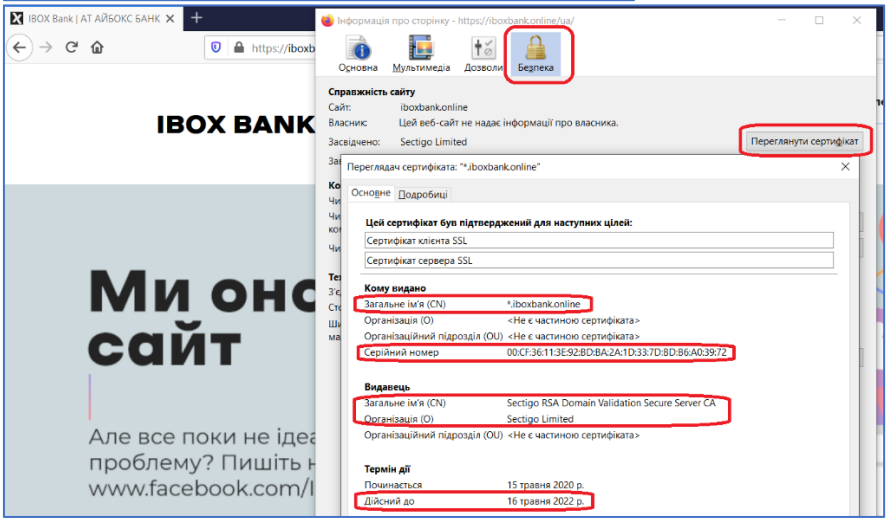
У випадку невідповідності зазначеним вище критеріям, рекомендуємо негайно покинути відвідуваний сайт та повідомити його адресу Банку електронною поштою на bank@iboxbank.online. У випадку отримання фішингових листів, також просимо їх переслати вкладенням до Вашого повідомлення на bank@iboxbank.online

Приклад перевірки сертифікату в браузері FireFox:

1. 

2. 

3. 

4. 

У випадку компрометації Ваших платіжних засобів просимо негайно звертатись до банку для їх вчасного блокування та збереження Ваших коштів. В таких випадках обирайте спосіб зв'язку, який забезпечує терміновість і конфіденційність вирішення Вашого питання.

Зв'язатись з Банком можна наступними каналами зв'язку:
Гаряча лінія: 0 (800) 500-178 (Цілодобово)
Електронна пошта: bank@iboxbank.online

Телеграм-бот: https://t.me/IboxBankOnlineBot
Інстаграм: https://www.instagram.com/iboxbank.online/