



0 (800) 500-178

(дзвінок в межах України безкоштовно)



www.iboxbank.online



АТ "АЙБОКС БАНК": 03150, Київ, вул. Ділова, 9а

IBOX BANK

Рекомендації

АТ «АЙБОКС БАНК» щодо виявлення фішингових веб-сайтів та уникнення випадків підвищеного ризику збитків для користувача електронного платіжного засобу

Дотримання рекомендацій дасть змогу забезпечити держателям платіжних карток надійне їх зберігання, нерозголошення реквізитів платіжної картки, ПІН та інших даних, а також зменшить можливі ризики під час здійснення операцій з використанням платіжної картки в банкоматах, безготівкові оплати товарів і послуг.

Загальні рекомендації

1. Ніколи не розголошуйте ПІН стороннім особам.
2. Ніколи не передавайте платіжну картку для використання іншим особам.
3. Не розголошуйте та не повідомляйте персональні дані або інформацію про платіжну картку (у тому числі ПІН) на вимогу будь-яких сторонніх осіб, у тому числі й працівникам банку. У разі виникнення такої ситуації зателефонуйте до банку-емітента, який видав платіжну картку, і повідомте про цей факт.
4. У разі розкриття ПІНу, персональних даних, втрати платіжної картки , існує ризик здійснення незаконних дій з коштами на Вашому рахунку з боку третіх осіб. У разі втрати платіжної картки держатель повинен негайно повідомити про це Банк.

Рекомендації щодо здійснення безготівкових операцій

1. Розрахунки з використанням платіжної картки мають використовуватися тільки у присутності держателя картки. Це забезпечить зниження ризику неправомірного отримання персональних даних, зазначених на даній картці.
2. Під час використання платіжної картки для оплати товарів або послуг продавець/касир може вимагати від держателя платіжної картки надати паспорт, підписати квитанцію або ввести ПІН. Перед набором ПІНу слід переконатися, що треті особи не зможуть його побачити.
3. Якщо під час спроби здійснити оплату товарів або послуг з використанням платіжної картки не вдалося здійснити успішно операцію, то необхідно зберігати один примірник виданої терміналом квитанції для перевірки відсутності зазначеної операції у виписці про рух коштів за рахунком.

Закриття карткового рахунку

1. Поточні та карткові рахунки закриваються на підставі заяви клієнта, якщо інше не передбачено договором.
2. Під час закриття карткового рахунку (після виконання зобов'язань або в разі розірвання чи закінчення терміну дії договору) банк зобов'язаний видати залишок коштів у разі його наявності).

Фішинг –це певна схема, застосування якої змушує користувачів передавати конфіденційну інформацію шахраям для послідууючого використання такої інформації у зловмисних цілях.

До такої конфіденційної інформації відносяться:

- номер, термін дії, CVV2/CVC2, ПІН платіжної картки;
- одноразові цифрові паролі;
- адреса електронної пошти;
- номер телефону;
- картковий пароль (кодове слово), відповіді на секретні питання тощо.

Схема як правило працює у двох напрямках –використання несанкціонованих розсилок електронних листів (СПАМу) або переадресування користувачів на зловмисні (підробні) веб-сайти які ззовні або по імені дуже схожі на офіційні веб-сайти певних організацій. Зловмисники можуть також застосовувати голосовий фішинг, фішингові СМС–повідомлення, фішинг в соціальних мережах тощо. Як приклад, отримавши по схемі фішинга інформацію про номер платіжної картки, термін дії, імені та прізвище держателя платіжної карти, CVV/CVC2-коду, одноразового цифрового паролю–зловмисники можуть використати конфіденційну інформацію для здійснення несанкціонованих списань грошових коштів з даної платіжної карти. Держатель платіжної картки дізнається про несанкціоновані операції вже по факту їх здійснення, отримуючи інформацію про рух коштів за допомогою SMS-інформування

З метою забезпечення високого рівня безпеки інформації та унеможливлення доступу до конфіденційної інформації сторонніх осіб при роботі з веб-сайтом АТ« АЙБОКС БАНК» (далі –Банк) для клієнтів Банку пропонуємо використовувати рекомендації наведені нижче:

- 1) Користуватись лише офіційним веб-сайтом Банку за посиланням <https://iboxbank.online>
- 2) Ніколи не здійснювати введення конфіденційної інформації у разі якщо Вас було переадресовано на невідомий веб-сайт з незрозумілим доменним іменем.

УВАГА! АТ «АЙБОКС БАНК» ні при яких обставинах не здійснює телефонні дзвінки своїм діючим та потенційним клієнтам для отримання будь-якої конфіденційної інформації.

Посилання на сторінку офіційного Інтернет-представництва Національного банку, на якій розміщено перелік власних веб-сайтів банків

З метою унеможливлення потрапляння клієнтів банків на фішингові веб-сайти Національний банк України на своєму офіційному Інтернет-представництві розмістив офіційний перевірений перелік веб-сайтів банків України. Перевірити автентичність доменного імені та належність веб-сайту конкретній банківській установ і клієнти банків можуть перейшовши заданим посиланням [ПОСИЛАННЯМ](#)