Рекомендації щодо безпечного використання системи дистанційного банківського обслуговування OTP Smart

Для запобігання доступу сторонніх осіб до конфіденційної інформації клієнта в системі дистанційного банківського обслуговування **OTP Smart**, а також перегляду передачі або модифікації даних використовується багаторівнева архітектура системи безпеки, що включає у себе:

- обов’язкову авторизацію та автентифікацію користувачів;
- протоколювання усіх дій користувачів в системі;
- обмін даними лише за стандартизованими інтерфейсами;
- захист каналу передачі даних на основі TLS 1.2;
- контроль прав доступу користувача до об’єктів системи.

Кожен користувач системи дистанційного банківського обслуговування OTP Smart є гарантом і складовою частиною системи безпеки та повинен дотримуватись наступних правил:

- Не розголошуйте свій логін і паролі третім особам;
- Користуйтеся кнопкою «Вихід» для завершення сеансу роботи з системою;
- Виконуйте вимоги щодо забезпечення інформаційної безпеки системи дистанційного банківського обслуговування OTP Smart, що викладені у Публічному договорі, під час роботи з системою.

Не розголошуйте свій логін і пароль третім особам

Система дистанційного банківського обслуговування OTP Smart ідентифікує користувача за логіном і паролем на вхід у систему. Щоб уникнути несанкціонованого доступу до вашої конфіденційної інформації, не розголошуйте свої реквізити на вхід у систему третім особам. Кожному новому користувачу банк видає:

- логін – ім'я користувача;
- пароль – пароль на вхід у систему.

В цілях безпеки при першому вході обов’язково необхідно змінити пароль на вхід у систему.

Система дистанційного банківського обслуговування OTP Smart фіксує всі спроби зміни і підбору пароля на вхід у систему.

Використовуйте кнопку «Вихід» після закінчення сеансу роботи з системою.
Відволікання від комп'ютера при виконаному вході в систему без завершення сеансу роботи з програмою може спровокувати іншу особу скористатися ситуацією.

Використовуйте автентифікацію одноразовим паролем задля уникнення несанкціонованого доступу до вашої конфіденційної інформації та використання її у шахрайських цілях.
Працівники банку ніколи не запитують ваші паролі!

Банк не рекомендує користувачеві працювати з системою дистанційного банківського обслуговування OTP Smart:

- в інтернет-кафе та інших подібних місцях, де немає гарантії того, що за діями користувача не стежить стороння людина;
- у місцях, де встановлені пристрої відеоспостереження, за допомогою яких можна отримати інформацію про пароль користувача;
- якщо немає упевненості в безпеці встановленого програмного забезпечення (наявність вірусів, спеціальних програм, що пересилають паролі користувача третім особам тощо).

Забезпечення безпеки під час роботи через інтернет

Безпека обміну даними під час роботи в мережі інтернет забезпечується на рівні надійної взаємної автентифікації учасників обміну даними.
Зашифрований канал передачі даних, налаштований за найкращими практиками шифрування, не дає змоги зловмиснику перехопити з'єднання та отримати будь-яку інформацію.
Авторизація користувача відбувається за його персональним логіном та паролем, користувачам при цьому рекомендується встановити власні логіни та паролі для користування системою.
Додатково рекомендується налаштувати підтвердження входу до системи та платежів в межах рахунків користувача за допомогою одноразового пароля, який може надсилатися через смс/пуш-повідомлення або генеруватися за допомогою апаратного токена.

В разі виявлення здійснення несанкціонованого доступу до облікового запису в систему дистанційного банківського обслуговування, компрометацію мобільного застосунку або його злам негайно зверніться до довідкового центру за телефоном +38 044 490 05 00 (цілодобово, вартість дзвінків згідно з тарифами Вашого оператора).

Пам'ятайте! АТ «ОТП БАНК» ніколи не здійснює дзвінки та розсилку електронних листів з проханням надати конфіденційну інформацію про логіни, паролі або інші конфіденційні дані.