ПАМЯТКА ПО БЕЗОПАСНОСТИ
ПРИ РАБОТЕ В МОБИЛЬНОМ ПРИЛОЖЕНИИ БАНКА

Сервис Банка представляет собой мобильное приложение Банка, позволяющее Клиентам взаимодействовать с Банком в рамках заключенного Договора комплексного банковского обслуживания. Это включает обмен информацией и электронными документами, а также совершение отдельных операций через сеть интернет с использованием мобильного устройства (смартфона, планшета и т. п.).

Кроме того, сервис включает систему электронных платежей, которая позволяет пользователям мобильных устройств оплачивать товары, работы и услуги, осуществлять денежные переводы, а также совершать иные операции, предусмотренные функционалом мобильного приложения.

Ознакомьтесь пожалуйста с основными правилами безопасности:

- ✓ никому не передавайте и не сообщайте одноразовый код из SMS-сообщения, используемый при проведении операций в сети интернет и с использованием сервисов Банка;
- ✓ не используйте номера мобильных телефонов третьих лиц при подключении сервисов Банка;
- ✓ не передавайте права использования Вашим банковским счетом/Платежной карточки/ мобильного приложения третьим лицам, не имеющими на это законные основания (представитель, доверенное лицо);
- ✓ никому не сообщайте и не передавайте реквизиты Платежной карточки, а также данные CVC/CVC2-кода/пароля 3D Secure;
- ✓ ни при каких обстоятельствах не разглашайте свой код из SMS-сообщения никому, включая работников Банка, за исключением случаев самостоятельного обращения в контактный центр Банка для получения консультации или услуги, где требуется предоставление кода из SMS-сообщения. Ответственность за хранение личных конфиденциальных данных и паролей возлагается на Клиента;
- ✓ не переходите по ссылке, полученной посредством SMS-сообщений/мессенджеров, из непроверенных источников;
- ✓ не осуществляйте авторизацию в мобильных приложениях Банка с установкой ПИН-кода или входа по отпечатку пальца на чужом мобильном устройстве;
- ✓ ежедневно анализируйте все уведомления о выполненных и отклоненных Банком операциях, и незамедлительно информируйте Банк о случаях несанкционированных зачислений (перечисления) денег, для минимизации потенциальных убытков;
- ✓ в случае утери/кражи мобильного телефона, на который Банк отправляет SMS - сообщения с одноразовым кодом, или неожиданного прекращения работы SIM-Карты Вам следует срочно обратиться к своему оператору мобильной связи и заблокировать SIM-Карту, а также незамедлительно проинформировать об этом Банк;
- ✓ установите лимиты на карточные операции в сети интернет;
- ✓ своевременно устанавливайте обновления операционной системы мобильного устройства;
- ✓ используйте лицензионное антивирусное программное обеспечение и следите за его регулярным обновлением;
- ✓ регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ;

- ✓ не устанавливайте сторонние приложения по просьбе третьих или малознакомых лиц;
- ✓ Банк владеет всей необходимой информацией и никогда, ни при каких обстоятельствах не осуществляет рассылку электронных сообщений, SMS-сообщений, звонков по телефону с просьбой передать реквизиты платежной карточки, авторизационные данные, ПИН-код к платежной карточке, а также не распространяет по электронной почте программы и их обновления;
- ✓ в случае компрометации данных или обнаружения фактов несанкционированного доступа и проведения с банковских счетов несанкционированных транзакций посредством мобильного приложения Вам необходимо незамедлительно обратиться в Контакт-центр по номерам 4077 (бесплатный звонок по РК), +7-778-099-40-77 или на электронный адрес: SIB@zamanbank.kz.