**Памятка по безопасности при работе в Мобильном приложении Банка**

Сервис Банка представляет собой Мобильное приложение Банка, позволяющий Пользователям осуществлять взаимодействие с Банком в рамках заключенных договоров банковского обслуживания и/или договора электронных денег, а также без заключения таковых, включая обмен информацией и совершение отдельных операций через интернет или специальное приложение мобильного устройства (смартфона, планшета и т.п.), а также систему электронных платежей, позволяющую Пользователям мобильных устройств производить оплату услуг, осуществлять денежные переводы между физическими лицами через сервисы Банка и совершать покупки в интернете.

**Ознакомьтесь пожалуйста с основными правилами безопасности:**

- ✓ никому не передавайте и не сообщайте одноразовый пароль 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/ Системы ДБО 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 логин, пароль, 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 Пользователя;
- ✓ 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 паролем, 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;
- ✓ подключите услугу «SMS-информирование», 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 номеру 595 (бесплатный звонок по РК) или на электронный адрес security@freedombank.kz.