Памятка по безопасности при работе на сайте системы дистанционного банковского обслуживания и в мобильном приложении Банка

Сервисы Банка представляют собой мобильное приложение и сайт Банка https://mykassa.kz, позволяющие пользователям осуществлять взаимодействие с Банком в рамках заключенных договоров банковского обслуживания и/или договора электронных денежных средств, 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;
- ✓ никому не сообщайте и не передавайте реквизиты платежной карточки, а также данные CVC/CVC2-кода/пароля 3D Secure;
- ✓ избегайте подключений к сайту https://mykassa.kz по баннерным ссылкам или по ссылкам, содержащимся в электронной почте. Проверяйте, что соединение с веб-сайтом защищено шифрованием (наличие префикса https), а также доменное имя веб-сайта (имя мошеннического веб-сайта может отличаться всего на один символ) – https://mykassa.kz. Рекомендуем ввести этот адрес веб-сайта самостоятельно и добавить его в закладки браузера;
- ✓ 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 сообщения о принятых и непринятых Банком операциях, а также немедленно информируйте Банк о случаях несанкционированного зачисления (перечисления) денег;
- ✓ в случае утери/кражи мобильного телефона, на который Банк отправляет SMS - сообщения с подтверждающим одноразовым паролем, или неожиданного прекращения работы SIM-карты Вам следует как можно быстрее обратиться к своему оператору мобильной связи и заблокировать SIM-карту, а также проинформировать об этом Банк;
- ✓ подключите услугу «SMS-информирование», установите лимиты на карточные операции в сети Интернет;
- ✓ всегда выходите с веб-сайта https://mykassa.kz через ссылку «Выход», в этом случае Ваш сеанс будет прекращен безопасно и корректно;
- ✓ избегайте мест с публичными точками доступа в Интернет (таких как интернет-кафе и игровые клубы) для использования веб-сайта https://mykassa.kz, так как Вы не можете быть уверены, что на компьютерах данных заведений не стоят программы-шпионы, способные сохранить ваши конфиденциальные идентификационные и персональные данные;
- ✓ используйте для работы на веб-сайте https://mykassa.kz только проверенные и надежные компьютеры;
- ✓ своевременно устанавливайте обновления операционной системы своего компьютера, рекомендуемые компанией-производителем;
- ✓ используйте лицензионное антивирусное программное обеспечение и следите за его регулярным обновлением;

- ✓ регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ;
- ✓ 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 веб-сайта https://mykassa.kz или мобильного приложения Вам необходимо незамедлительно обратиться в Контакт-центр по номеру 595 (бесплатный звонок по РК) или на электронный адрес security@bankffin.kz.