Памятка по безопасному использованию интернет- и мобильного банка

Организация процессов информационной безопасности является одним из основополагающих аспектов нашей деятельности. Для безопасности систем мы используем только самые современные информационные технологии, следим за их эффективностью и постоянно совершенствуемся. Программное обеспечение, которое мы вам предлагаем, использует только сертифицированные ФСБ средства защиты информации, а также отвечает всем требованиям Российского законодательства.
Безопасность и защита от несанкционированного доступа к системам ДБО достигается путем применения целого комплекса мероприятий:

- программно-аппаратного комплекса Удостоверяющего центра на базе СКЗИ "Крипто-Ком 3.3" (СФ/124-2690 от 05.08.2015г.);
- двухфакторной аутентификации, авторизации, протоколирования событий;
- межсетевого экранирования, фильтрации и маршрутизации трафика систем ДБО;
- шифрования трафика, передаваемого через сеть Интернет (устанавливается защищенное TLS-соединение с сертификатом безопасности, выданным организацией COMODO SECURE™ для *.openbank.ru);
- электронной подписи (ЭП);
- ключевого носителя Рутокен ЭЦП, который обеспечивает безопасное хранение ключей электронной подписи во встроенной защищенной памяти без возможности их экспорта;
- генераторов одноразовых кодов (SMS-коды подтверждения) для физических лиц и SMS-оповещений о входе для юридических лиц;
- организационно-административных мероприятий.

Также ПАО Банк "ФК Открытие" имеет лицензию ЛСЗ №0011277 рег.№14520Н от 14 августа 2015г. на деятельность в области криптографии

Данный комплекс позволяет нам быть уверенными в эффективности применяемых средств защиты. Однако следует помнить, что важнейшим фактором, способствующим обеспечению безопасности, является ваша личная заинтересованность. Пожалуйста, будьте бдительны при пользовании онлайн-сервисами банка через мобильные устройства, персональные компьютеры, банкоматы и устройства самообслуживания.

Для Вашей безопасности, мы настоятельно рекомендуем соблюдать следующий комплекс мероприятий по защите информации:

при работе с интернет-банком:

- убедитесь, что на устройстве, с которого планируется осуществлять подключение в Интернет-Банк, должны быть установлены лицензионные, регулярно обновляемые операционная система, антивирусное программное обеспечение и web –браузер;
- на устройстве, с которого планируется осуществлять подключение в Интернет-Банк, должен быть настроен и использоваться локальный межсетевой экран, настроенный на работу только с необходимыми сетевыми ресурсами по поддерживаемым ими протоколам;
- устройство должно использовать процедуру аутентификации доступа к нему (требуется ввод логина и пароля);
- убедитесь, что для входа в Интернет-Банк требуется ввести только Имя пользователя, Пароль (Базовые аутентификационные данные) либо имя пользователя и пароль аккаунта социальных сетей Facebook, ВКонтакте (Дополнительные аутентификационные данные) и Одноразовый Пароль на вход (при использовании Одноразовых паролей);

- не передавайте Рутокен или PIN-код от него другим людям, не оставляйте устройство без присмотра, а в случае утери/кражи/поломки сообщите в Банк по тел. 8 (800) 700-78-77 (https://www.openbank.ru);
- убедитесь, что от антивирусного средства нет никаких сообщений о вирусах, а в случае появления признаков вируса незамедлительно прекратите работу в интернет-банке и сообщите в Банк по тел. 8 (800) 700-75-86 (https://online.openbank.ru/Business).

ВНИМАНИЕ: Наличие полей для ввода **полного** номера банковской карты, проверочного кода банковской карты или Номера телефона Клиента на главной странице означает, что вы попали на мошеннический сайт. Незамедлительно прекратите работу с мошенническим сайтом и сообщите об этом нам.

- ни при каких обстоятельствах, никогда и никому не сообщайте Пароль и Одноразовые пароли (при их использовании), пароли аккаунтов социальных сетей Facebook, ВКонтакте;
- перед Аутентификацией входа убедитесь, что в адресной строке браузера указан правильный адрес Интернет-Банка (https://online.openbank.ru);
- при использовании Одноразовых паролей: внимательно проверяйте информацию об Операции, полученную в СМС-сообщениях;
- убедитесь, что используется защищенное TLS-соединение (отсутствуют сообщения об ошибке сертификата, в браузере изображен значок закрытого замка или рядом с адресной строкой имеется поле, индицирующее корректность TLS-соединения).

Пожалуйста, при любых подозрениях на мошеннические web-сайты, имитирующие Интернет-Банк, мошеннические СМС-сообщения или телефонные звонки, в которых неизвестные лица представляются как работники Банка, убедительно просим вас обратиться к нам в Банк по телефону, указанному на обратной стороне Аутентификационной или иной банковской карты, принадлежащей «Открытию», либо по телефону, указанному на сайте Банка в сети Интернет по адресу https://www.openbank.ru

при работе в мобильном банке:

- убедитесь, на мобильном устройстве, с которого планируется осуществлять подключение к Мобильному Банку, должны быть установлены лицензионные, регулярно обновляемые операционная система, антивирусное программное обеспечение (если операционная система подвержена вирусным атакам);
- мобильное устройство не должно быть подвергнуто операциям повышения привилегий / взлома операционной системы устройства (jail-break, rooting);
- вы должны использовать процедуру аутентификации доступа к мобильному устройству (ввод пароля для разблокировки мобильного устройства), прежде чем приступить к совершению операций через Мобильный Банк;
- установленный пароль для входа в Мобильный Банк должен быть сложен для угадывания (отличаться от последовательности одинаковых символов, даты или года вашего рождения и т.д.);
- ни при каких обстоятельствах, никогда и никому не сообщайте пароль для входа в Мобильный Банк;
- используя мобильное устройство, с которого получаете доступ к Мобильному Банку, осуществляйте избирательную навигацию в сети Интернет, и старайтесь не посещать неизвестные вам сайты, устанавливать сомнительные приложения;

- не подключайте мобильное устройство к компьютерам, безопасность которых (обеспечение доверенных сред, лишенных удаленного управления и установленных / запущенных вредоносных программ) не можете гарантировать;
- не модифицируйте и не изменяйте Мобильный Банк, устанавливайте приложение только из официальных хранилищ AppStore и Google Play.

Пожалуйста, не храните на мобильном устройстве критичную информацию в незащищенном/незашифрованном виде и не оставляйте мобильное устройство без присмотра. В случае утери или кражи мобильного устройства немедленно смените все пароли и обратитесь к оператору сотовой связи для блокировки SIM-карты.

при работе с банковскими картами и устройства самообслуживания:

- при получении SMS-сообщений о блокировке карты или об операциях, которые вы не совершали, срочно перезвоните на официальный номер банка 8 (800) 700-78-77 (https://www.openbank.ru);
- ни при каких обстоятельствах не сообщайте кому-либо (в том числе сотруднику банка) конфиденциальную информацию о вашей пластиковой карте: ПИН-код, полный номер карты, срок действия, коды CVV2/CVC2;
- обязательно установите суточный лимит на сумму операций, проводимых по карте или её реквизитам, а также подключите услугу оповещения о проводимых операциях посредством sms-сообщений;
- запомните ПИН-код карты и уничтожьте ПИН-конверт (при наличии). Если запоминание ПИН-кода является затруднительным, запишите его в неявном виде;
- никогда не вводите ПИН-код при совершении операции в сети Интернет;
- ни при каких обстоятельствах не передавайте карту для использования третьим лицам, в том числе родственникам;
- регулярно получайте выписки по карте и контролируйте все операции, совершенные с использованием карты или ее реквизитов;
- перед использованием банкомата осмотрите его на наличие дополнительных мошеннических устройств (накладок), расположенных в месте набора ПИН-кода и в месте (прорезь), предназначенном для приема Карт. Если из этого, что-то вам покажется подозрительным, воздержитесь от использования Карты в данном банкомате;
- набирайте ПИН-код таким образом, чтобы люди, находящиеся в непосредственной близости от Вас, в том числе стоящие за вами в очереди к банкомату, не смогли его увидеть. При наборе ПИН-кода прикрывайте клавиатуру рукой;
- в момент получения денежных средств не отвлекайтесь на телефонные звонки и разговоры, чтобы не стать жертвой мошеннических действий. Дождитесь выдачи денег, заберите и пересчитайте их.

Для обеспечения сохранности средств на карте и снижения рисков при получении наличных денежных средств мы установили ограничения на операции в странах повышенного риска: Австралия, Вьетнам, Гонконг, Индонезия, Камбоджа, Китай, Лаос, Малайзия, Монголия, Мьянма, Республика Корея, Сингапур, Филиппины, Шри-Ланка, Япония.

Документы:

- Федеральный закон от 06 апреля 2011 года № 63-ФЗ "Об электронной подписи"
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Федеральный закон от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне»
- Положение Банка России от 9 июня 2012 г. N 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
- Письмо Банка России от 05.08.2013 N 146-Т «О рекомендациях по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети «Интернет»