Уважаемые клиенты!

В целях выполнения требований Положения Банка России от 17 апреля 2019 г. № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций», а также в целях предупреждения последствий недобросовестных действий третьих лиц, противодействия проведению незаконных финансовых операций в отношении ваших активов и защиты вашей информации от воздействия вредоносных кодов, ООО МФК «ОТП Финанс» настоятельно рекомендует вам соблюдать приведенные ниже рекомендации и принимать меры, изложенные в них.

Рекомендации по безопасному использованию мобильных приложений

1. Используйте только официальные мобильные приложения, доступные в App Store и Google Play.

2. Регулярно устанавливайте обновления операционной системы вашего мобильного устройства.

3. Используйте лицензионные, постоянно обновляемые средства антивирусной защиты.

4. Используйте средства блокировки входа на ваше мобильное устройство (пароль, PIN-код, TouchID, FaceID и иные).

5. Отключите отображение содержимого SMS-сообщений на экране заблокированного устройства (в случае кражи или утери смартфона злоумышленники легко смогут получить доступ к денежным средствам на ваших счетах, даже если телефон будет заблокирован).

6. Установите PIN-код на SIM-карту (в случае кражи или утери смартфона злоумышленники легко смогут получить доступ к денежным средствам на ваших счетах, переставив SIM-карту в свой телефон).

7. Никому не сообщайте пароль для доступа в приложение и одноразовый SMS-код подтверждения операций (**даже сотрудникам финансового учреждения**).

8. Не храните пароль для доступа в приложение на своем мобильном устройстве в открытом виде.

9. Завершайте сеанс работы в приложении при помощи кнопки «Выход» сразу после проведения всех необходимых операций.

10. Не посещайте сайты сомнительного содержания с устройства, на котором установлено мобильное приложение.

11. При отсутствии крайней необходимости, не используйте приложение для совершения операций по счету при подключении телефона к публичным сетям Wi-Fi.

Рекомендации по безопасному использованию интернет-банкинга

1. Исключите возможность несанкционированного доступа к компьютеру, на котором вы используете интернет-банкинг.

2. Используйте на вашем компьютере только лицензионное программное обеспечение; не устанавливайте программное обеспечение, полученное из сомнительных источников.

3. Установите на вашем компьютере лицензионное средство антивирусной защиты, работающее в автоматическом режиме. Не реже одного раза в неделю проводите полное антивирусное сканирование компьютера. В случае обнаружения подозрительные файлы должны быть удалены, а при невозможности удаления - заблокированы.

4. Следите за регулярными обновлениями операционной системы, браузера и антивирусных баз на вашем компьютере.

5. Всегда используйте встроенные средства межсетевого экранирования операционной системы (брандмауэр или firewall).

6. После окончания работы в интернет-банкинге всегда завершайте сессию (кнопка «Выход»).

7. Не пользуйтесь интернет-банкингом на компьютерах, расположенных в местах общего пользования (отелях, бизнес-центрах).

8. Помните, что сотрудники финансовых учреждений никогда не звонят клиентам и не предлагают помощь в устранении технических проблем, не запрашивают и не предлагают ввести коды, пароли или иные данные.

Рекомендации по использованию парольной защиты

1. Не записывайте пароли для доступа в интернет-банкинг на бумажных носителях или в файлах на жестком диске вашего компьютера. Не сообщайте их другим лицам, в том числе вашим знакомым, друзьям, родственникам.

2. Используйте для доступа в интернет-банкинг сложные пароли, содержащие буквы латинского алфавита в верхнем регистре (A-Z), буквы латинского алфавита в нижнем регистре (a-z),цифры (0-9), специальные символы и знаки пунктуации (!@#$%^&*(),.?).

3. Не используйте простые пароли, представляющие собой имена людей, дату рождения, номер телефона и т.д., последовательности повторяющихся на клавиатуре символов (qwerty), последовательности трех и более повторяющихся символов (77777777, 111!!!ZZZ).

Рекомендации по защите при использовании сети Интернет

1. Не посещайте сайты сомнительного содержания на компьютере, с которого осуществляется доступ в интернет-банкинг.

2. Не используйте для работы в интернет-банкинге общедоступные каналы связи (например, Wi-Fi в кафе, отелях или аэропортах).

3. Не открывайте вложения электронных писем, полученные от неизвестных вам адресатов.

4. Не сохраняйте пароль для входа в интернет-банкинг в браузере.

5. При использовании интернет-банкинга убедитесь, что вы заходите на официальный сайт.

Рекомендации по использованию SMS-подтверждений

1. При подтверждении ваших операций одноразовым SMS-кодом (паролем), всегда проверяйте, верны ли реквизиты операции.

2. Если у вас сменился номер телефона, обязательно измените его в интернет-банкинге.

3. Не переходите по ссылкам, приходящим в SMS-сообщениях из недостоверных источников, в том числе на известные сайты.