РЕКОМЕНДАЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, В ТОМ ЧИСЛЕ, ПО СНИЖЕНИЮ РИСКОВ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА

В связи с участившимися случаями проведения мошеннических операций по переводу денежных средств с использованием систем дистанционного банковского обслуживания через сеть Интернет и в целях предотвращения несанкционированного доступа к Счетам Клиента со стороны злоумышленников Банк настоятельно рекомендует физическим лицам - пользователям Системы соблюдать следующие меры информационной безопасности:

- Использовать на постоянной основе антивирусное программное обеспечение с последней актуальной версией баз (на всех устройствах, с которых осуществляется доступ в Систему и/или на которые приходит sms/push уведомление).
- Регулярно выполнять антивирусную проверку для своевременного обнаружения вредоносных программ (на всех устройствах, с которых осуществляется доступ в Систему и/или на которые приходит sms/push уведомление).
- Регулярно устанавливать обновления операционной системы и браузера Интернет (посредством которого осуществляется доступ к Системе) (на всех устройствах, с которых осуществляется доступ в Систему и/или на которые приходит sms/push уведомление).
- Не устанавливать на устройства, с которых осуществляется доступ в Систему, программы для удаленного управления (Team Viewer, Ammyy Admin, AnyDesk, VNC и т.п.).
- Блокировать доступ к устройствам (например, к USB-токенам), посредством которых осуществляется доступ к Системе, на время неактивности и не оставлять разблокированные устройства без присмотра, т.к. этим могут воспользоваться злоумышленники.
- Осуществлять вход в Систему посредством прямого набора адреса сайта Системы в строке браузера или переходить по ссылке на корпоративном Интернет-сайте Банка. При этом всегда проверять, что соединение осуществляется по безопасному протоколу https на адрес домена Банка *.efbank.ru. В адресной строке должен появиться значок закрытого замка. При нажатии на замок должна появляться информация о действующем сертификате сайта Системы (безопасное подключение-данные сертификата) выданном на доменное имя *.efbank.ru.
- Не пользоваться Системой с гостевых рабочих мест (интернет-кафе и пр.) и с открытых гостевых точек WiFi не защищенных шифрованием (без WPA2), т.к. в таком случае возможен перехват злоумышленниками всего вашего трафика, в том числе парольной информации.
- Устанавливать обновления системного программного обеспечения или браузера только через процедуру обновления, встроенную в операционную систему (Windows).
- Не сохранять Логин и Пароль Системы в памяти браузера.
- Не хранить Логин и Пароль Системы в открытом виде на устройствах, с которых осуществляется доступ в Систему.
- Использовать приложения на смартфонах, полученные только из проверенных и официальных источников (Apple Store, Google Play/ Play Market, сайт Банка).
- Регулярно, не реже одного раза в день получать и проверять информацию о зарегистрированных Распоряжениях и о состоянии Счетов.

Банк рекомендует Клиенту учитывать риски при работе с Системой через сеть Интернет и понимать, что использование только антивирусного программного обеспечения не дает 100% гарантии защиты от проведения злоумышленником мошеннических операций в Системе.

В случае если у Вас перестала работать сим-карта, свяжитесь со своим оператором сотовой связи и выясните причину. Возможно, злоумышленники получили клон (дубликат) Вашей сим-карты.

Следует учитывать самые распространенные на сегодняшний день схемы мошенничества в сети Интернет:

- «Социальный инжиниринг» - злоумышленники рассылают сообщения посредством SMS/электронной почты или звонят от имени Банка и под различными предлогами пытаются получить от Клиента Логины, Пароли, Ф.И.О, номера счетов, карт, пин-кодов и т.д.
- «Фишинг» – Клиенту присылается по почте или иным способом ссылка на поддельный сайт, который может визуально не отличаться от подлинного, с просьбой ввести Логин, Пароль на доступ к Системе и другие данные под любым предлогом (истек срок действия пароля, необходимость пройти дополнительную авторизацию, разблокировка заблокированного доступа и т.п.).
- Заражение вредоносным кодом - происходит через распространение вредоносных программ через Интернет-ресурсы, например, сайты социальных сетей или посредством спам-рассылки через электронную почту. После заражения Системы Клиента вирусом или «трояном» злоумышленник получает полный контроль над Системой.

При использовании Системы необходимо помнить, что:

В случае выявления Клиентом подозрительных операций в Системе необходимо незамедлительно связаться со Службой клиентской поддержки Банка по номеру телефона, опубликованному на корпоративном Интернет-сайте Банка.