МЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ «EUROLINK»

Для обеспечения безопасности работы в системе дистанционного банковского обслуживания (далее - Система) Банком применяются следующие методы защиты:

- шифрование канала связи с использованием протокола SSL и сертификата, подписанного удостоверяющим центром VeriSign или Thawte;
- одноразовые сеансовые ключи;
- рассылка sms уведомлений об операциях в Системе .

В связи с участившимися случаями 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 АО АКБ «ЕВРОФИНАНС МОСНАРБАНК» настоятельно рекомендует физическим лицам – пользователям Системы соблюдать следующие меры информационной безопасности.

При организации рабочего места для работы с Системой:

- Старайтесь по возможности не пользоваться Системой с гостевых рабочих мест (интернет-кафе и пр.). При использовании недоверенных компьютеров значительно возрастает риск кражи ваших учетных данных (логина/пароля, сеансовых ключей). При утере мобильного телефона с номером (SIM-картой) или отдельно SIM-карты, на номер которой посредством SMS-сообщений Вам направляется информация о движениях по счету, необходимо незамедлительно обратиться в Банк для блокировки сервиса SMS-оповещения.

- Никогда не сообщайте по телефону одноразовые ключи со скретч-карты. Даже сотрудникам Банка.

- Не оставляйте компьютер с активной Системой без присмотра. Выходите из Системы, даже если необходимо отойти на непродолжительное время. Не оставляйте карту с сеансовыми ключами без присмотра. Не допускайте доступ посторонних лиц к компьютеру, с которого Вы осуществляете работу с Системой.

- Не работайте на компьютере из-под учетной записи, обладающей административными правами в системе. Для повседневной работы создайте учетную запись с ограниченными правами.

- Не сохраняйте Ваши пароли в браузере.

- Используйте на постоянной основе антивирусное программное обеспечение с последней актуальной версией баз. Регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ. Регулярно устанавливайте обновления операционной системы и браузера Интернет (посредством которого осуществляется доступ к Системе).

- Действия вредоносного кода (вирусы, программы шпионы и т.п.) могут быть направлены на получение и передачу третьим лицам информации о ваших учетных данных и одноразовых ключах, с целью дальнейшего их использования в мошеннических операциях.

- Установите и настройте персональный брандмауэр (firewall) на Вашем компьютере, что позволит предотвратить несанкционированный доступ к информации на компьютере.

- Используйте лицензионное программное обеспечение из проверенных и надежных источников.

- Не устанавливайте обновления системного программного обеспечения или браузера Интернет, полученные от имени Банка по электронной почте или другим способом, не открывайте ссылки в таких почтовых сообщениях. Получив такое сообщение, незамедлительно сообщите об этом Банку.

При работе в Системе:

- Вход в Систему рекомендуется осуществлять по ссылке с официального сайта Банка. При этом необходимо всегда проверять, что соединение осуществляется по безопасному протоколу HTTPS на адрес dbo.efbank.ru. Адресная строка браузера при переходе на подлинный сайт Системы должна поменять цвет на зеленый. В сертификате сервера в поле субъект должно быть указано название сервера (CN = dbo.efbank.ru) и организация, на имя которой выдан сертификат (O = Evrofinance Mosnarbank). В поле издатель должна быть указана организация, выдавшая сертификат VeriSign или Thawte. В качестве примера смотрите приложение №1.

- В случае пропажи Логина, Пароля, Таблицы сеансовых ключей, незамедлительно обратитесь в Банк с просьбой о блокировке Системы, с последующей заменой Логина, Пароля, Таблицы сеансовых ключей.

- Обращайте внимание на изменения привычных страниц входа в Систему. Если Вы сомневаетесь в том, что содержимое страницы получено с официального сервера Банка, попробуйте открыть ту же страницу Системы на другом компьютере, который подключен к другой сети или позвоните в Банк для уточнения информации о внесенных изменениях на официальном сайте.
- Внимательно контролируйте все операции, совершенные в Системе.

- Регулярно проводите сверку финансовых операций, выполненных в Системе в течение дня с целью выявления ошибочных или подозрительных операций.

- После окончания работы в Системе обязательно закройте окно Системы с помощью кнопки «Выход».

- Периодически производите замену пароля для входа в Систему.

- Ни при каких условиях не сообщайте информацию о Вашем пароле никому, включая сотрудников Банка, родственников.

- Не сохраняйте информацию о Вашем пароле на вход в Систему на любых носителях, включая диск Вашего компьютера.

- Стирайте защитный слой со значения сеансового ключа на Таблице сеансовых ключей непосредственно перед его использованием.

Первые признаки, по которым можно определить факт заражения компьютера вредоносным кодом или факт получения к нему несанкционированного доступа третьими лицами:

- В Системе присутствуют действия, которые Вы не совершали.

- Подозрительная активность на компьютере, на котором осуществляется работа с Системой (самопроизвольные движения курсора/указателя мыши, открытие/закрытие окон, набор текста и т.п.).

- Необъяснимое замедление работы компьютера или «зависания» программ или операционной системы.

- Изменение адреса для соединения с Системой.

- Изменение IP адреса, с которого осуществлялось подключение к Системе.

- Невозможно получить доступ к Системе по причине несовпадения пароля на вход в Систему.

- Изменился внешний вид интерфейса Системы.

Что необходимо сделать в случае появления подозрения на несанкционированный доступ к компьютеру третьих лиц:

- Выйти из Системы.
- Выключить компьютер.
- Обратиться в Банк для смены пароля и/или приостановления/ограничения дистанционного обслуживания в Системе и/или для блокирования Таблицы сеансовых ключей.

- При оформлении письменного заявления обязательно опишите обстоятельства компрометации пароля, разовых ключей или факт несанкционированного доступа, либо другую информацию по фактам, вызвавшим Ваши подозрения.

Возобновить доступ в Систему можно будет в офисе Банка при личном обращении Клиента.

Обращаем Ваше внимание!

Банк рекомендует Клиентам учитывать следующие 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 на компьютере Клиента.

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

- Социальный инжиниринг - злоумышленники рассылают SMS сообщения 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, необходимо пройти дополнительную авторизацию, разблокировать заблокированный доступ 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 компьютера вирусом или трояном злоумышленник получает полный контроль над Системой.

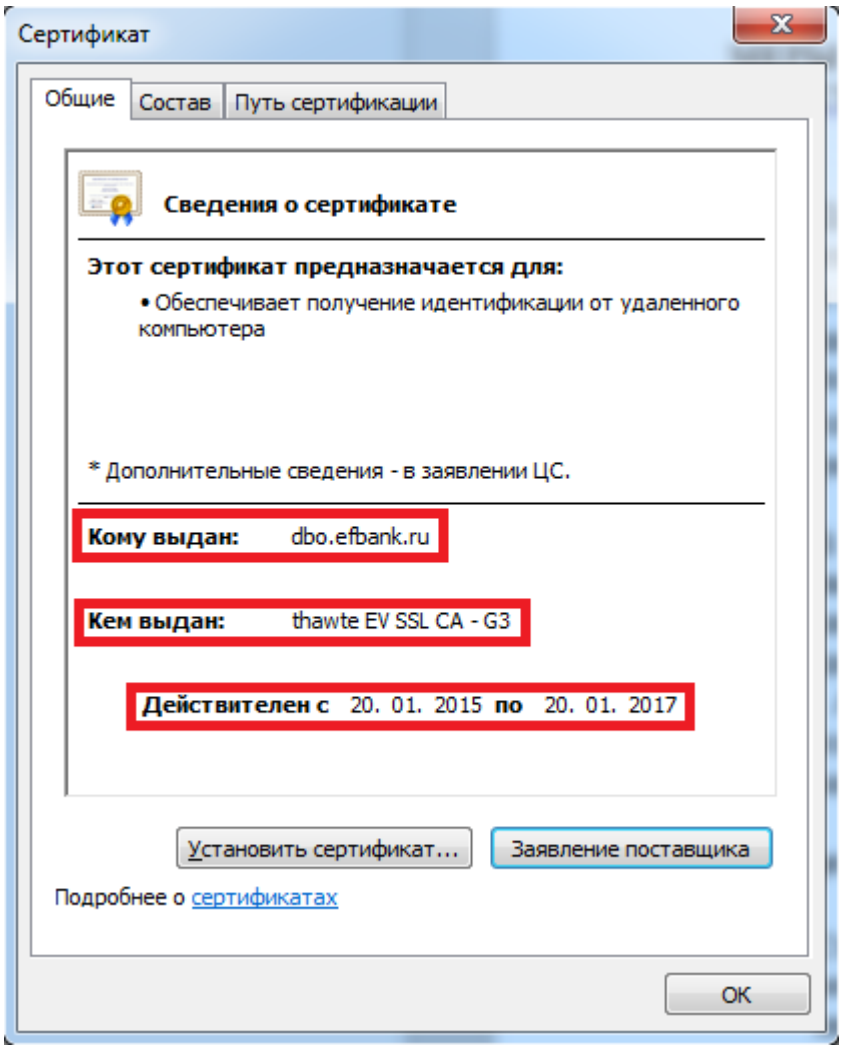
При использовании Системы необходимо помнить, что:

Банк не рассылает сообщения посредством SMS или электронной почты с запросом получения данных Клиентов или данных о Системе.

Информирование Банком по SMS (при подключении данной услуги) осуществляется только по факту получения Банком по Системе распоряжения от Клиента и об исполнении полученного распоряжения.

В случае выявления Клиентом подозрительных операций в Системе необходимо незамедлительно связаться со Службой клиентской поддержки по телефонам: 8-800-200-8-600(звонок бесплатный) и +7 (495) 733-93-75.

Сведения о сертификате (приложение 1)



Адресная строка браузера Internet Explorer