Правила безопасного использования систем дистанционного банковского обслуживания и сервисов электронного документооборота, предоставляемых ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» клиентам – юридическим лицам, индивидуальным предпринимателям и физическим лицам, занимающимся в установленном законодательством Российской Федерации порядке частной практикой, в рамках соответствующих договоров (соглашений)

Правила безопасного использования систем дистанционного банковского обслуживания и сервисов электронного документооборота, предоставляемых ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» клиентам – юридическим лицам, индивидуальным предпринимателям и физическим лицам, занимающимся в установленном законодательством Российской Федерации порядке частной практикой, в рамках соответствующих договоров (соглашений), определены Банком в целях информирования клиента о рисках, связанных с использованием указанных систем и сервисов (далее – Система ДБО), и о мерах, которые необходимо принимать клиенту для снижения возможных рисков при совершении операций по банковским счетам.

1. Термины

Социальная инженерия – это метод манипуляции действиями человека, заключающийся в использовании слабостей человеческого фактора в целях незаконного получения личной информации (учетных или банковских данных) или несанкционированного доступа к компьютеру жертвы с целью установки на него Вредоносного ПО. Мошенники часто прибегают к подобной практике, так как с помощью нее значительно проще добыть учетные данные, нежели получить их путем взлома системы безопасности.

Фишинг – один из видов интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей: логинам, паролям, данным лицевых счетов и банковских карт. В основном, используется метод проведения массовых рассылок от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих.

Вредоносное ПО (malware) – это назойливые или опасные программы, предназначенные для тайного доступа к устройству без ведома его владельца. Целями такого доступа могут быть как удаленное управление устройством, так и подмена составляемых пользователем платежных поручений.

2. Риски использования систем дистанционного банковского обслуживания

Использование систем дистанционного банковского обслуживания неизбежно сопряжено с рисками получения несанкционированного доступа злоумышленников к устройствам пользователей систем дистанционного банковского обслуживания, заражения устройств Вредоносным ПО, использования методов Социальной инженерии, Фишинга и реализации прочих угроз, способных привести к финансовым потерям клиентов или несанкционированного доступа к банковской тайне.

3. Для снижения риска несанкционированного доступа к Системе ДБО и мошеннических действий посторонних лиц необходимо обязательно принимать следующие меры предосторожности:

3.1. Обеспечить безопасность ключей электронной подписи (ЭП):

3.1.1. Сохранить используемый ключ ЭП только на токен.

3.1.2. Хранить и использовать ключевые носители, в том числе токен с ключами ЭП, в условиях, исключающих несанкционированный доступ к ним посторонних лиц.

3.1.3. Извлекать токен с ключами ЭП из компьютера каждый раз после завершения их использования. Не допускать (даже на минимальное время) нахождение токена с ключами ЭП:

– подключенным к компьютеру, если не осуществляется доступ в Систему ДБО и подписание расчетных (платежных) и иных документов;

– в открытом доступе (например, на столе), когда он не находится в зоне прямой видимости. В случае необходимости отлучиться от рабочего места необходимо поместить токен с ключами ЭП в сейф.

3.1.4. Не передавать ключи ЭП посторонним лицам.

3.1.5. Выделить отдельный компьютер или сервер для работы с Системой ДБО.

3.1.6. Не осуществлять доступ к Системе ДБО с гостевых рабочих мест (интернет-кафе и т. д.). В противном случае риск хищения и дальнейшего неправомерного использования ключа ЭП и другой аутентификационной информации повышается.

3.1.7. Не отвечать на письма, запрашивающие конфиденциальную информацию, в том числе содержащие просьбу прислать ключи ЭП и/или пароль доступа к Системе ДБО.

3.2. Обеспечить безопасность средств доступа к Системе ДБО:

3.2.1. Не применять простые пароли, а использовать сложные комбинации длиной не менее 8 (Восьми) символов, состоящие из строчных и прописных букв, цифр, не расположенных на клавиатуре последовательно, и специальных символов (!, @, ?, < и т. п.). Рекомендуется использовать парольные фразы, которые обладают достаточной длиной и легко запоминаются.

3.2.2. Осуществлять регулярную смену пароля доступа к Системе ДБО и пин-кода на токен (не реже одного раза в шесть месяцев). Обеспечить использование паролей и пин-кодов, известных только лицам, уполномоченным работать с Системой ДБО.

3.2.3. Пароль доступа к Системе ДБО следует вводить вручную, не сохраняя его в компьютере.

3.2.4. Не назначать пароль, используемый для доступа к Системе ДБО, в любых других системах и сервисах.

3.2.5. Не сообщать логин и/или пароль, используемые для доступа к Системе ДБО, пин-код на токен посторонним лицам.

3.3. На компьютере, который используется для работы с Системой ДБО, следует:

3.3.1. Применять только лицензионное программное обеспечение, в том числе средства антивирусной защиты, обеспечивая при этом регулярное обновление антивирусных баз, а также еженедельную полную антивирусную проверку.

При подозрении на наличие вирусов, в частности, при неожиданном прекращении реагирования программ или всей операционной системы на действия пользователя («зависание» компьютера), снижении скорости работы, самопроизвольных перезагрузках, подозрительной сетевой активности, иных сбоях необходимо воздержаться от использования Системы ДБО и принять меры по проверке на наличие вирусов и их удалению при обнаружении.

Обнаружение вредоносных программ на компьютере, используемом для работы с Системой ДБО, относится к событиям компрометации ключей ЭП. В этом случае необходимо незамедлительно обратиться в Банк в порядке, предусмотренном соответствующим договором / соглашением о дистанционном банковском обслуживании.

3.3.2. Установить межсетевой экран (особенно для пользователей широкополосного доступа к Интернету) с разрешением соединений с Банком и ограниченным числом сайтов сети Интернет для проведения обновлений программного обеспечения, а также ограничить доступ к компьютеру, предназначенному для работы с Системой ДБО из локальной сети (кроме систем, передающих в Систему ДБО платежи в соответствии с установленными клиентом внутренними процессами).

3.3.3. Обеспечивать своевременную (по возможности автоматическую) загрузку и установку всех последних обновлений операционных систем, а также регулярное обновление другого системного и прикладного программного обеспечения по мере появления новых версий.

3.3.4. Исключать возможность посещения сайтов сети Интернет сомнительного содержания, загрузку и установку нелицензионного программного обеспечения.

3.3.5. Если на компьютере, используемом для доступа к Системе ДБО, также используется электронная почта, не использовать ссылки, указанные в подозрительных письмах, полученных по электронной почте, всегда вводить адрес через браузер. Одним из способов мошеннических действий является рассылка писем с указанием ссылок на поддельные web-сайты, имеющие похожие адреса, например, m**c**b.ru вместо истинного m**k**b.ru.

3.3.6. Осуществлять антивирусную проверку любых файлов и программ, загружаемых на компьютер, используемый для доступа к Системе ДБО.

3.3.7. Не допускать работу в операционной системе под учетной записью, имеющей права администратора, следует использовать учетную запись с ограниченными правами.

3.3.8. Не допускать отсутствие пароля на вход в операционную систему / использование простых паролей для всех учетных записей, имеющих право входа в операционную систему. Регулярно осуществлять смену паролей.

3.3.9. Не использовать средства удаленного (дистанционного) доступа. Заблокировать возможность использования таких средств с помощью межсетевого экрана (программного и/или

аппаратного). Администрирование компьютера, используемого для доступа к Системе ДБО, следует осуществлять локально с использованием физического доступа администратора к компьютеру.

3.3.10. Осуществлять проверку корректности посещаемого (указанного) в браузере адреса web-страницы Системы «Ваш Банк Онлайн» (https://vbo.mkb.ru / https://vbo2.mkb.ru) до введения своих учетных данных (логина и пароля) для доступа в Систему «Ваш Банк Онлайн».

3.3.11. Обеспечить возможность доступа к компьютеру только уполномоченных лиц.

3.3.12. Обеспечить контроль конфигурации устройств, с использованием которых осуществляется доступ к Системе ДБО. В этих целях рекомендуется использовать специализированное программное обеспечение для контроля целостности системных и прикладных файлов (например, свободно распространяемое программное обеспечение OSSec).

3.4. На мобильном устройстве, которое используется для работы с Системой ДБО, следует:

3.4.1. Устанавливать обновления операционной системы. Воздержаться от использования мобильного устройства в случае отсутствия поддержки его операционной системы.

3.4.2. Не устанавливать на устройство программное обеспечение, распространяемое не через официальные магазины.

3.4.3. Установить пин-код для защиты доступа к операционной системе устройства.

3.4.4. Воздержаться от посещений подозрительных сайтов и установки подозрительного программного обеспечения (даже из магазинов производителей).

3.4.5. Не разглашать третьим лицам используемые пин-коды и одноразовые пароли.

3.5. Незамедлительно обратиться в службу Банка, осуществляющую техническую поддержку Систем ДБО (Контакт-центр), при возникновении любой нестандартной ситуации при входе или в процессе работы в Системе ДБО.

3.6. Незамедлительно обратиться в Контакт-центр и уведомить Банк в порядке, установленном соответствующим договором о дистанционном банковском обслуживании, при возникновении угрозы несанкционированного доступа к Системе в случаях компрометации ключей ЭП.

3.7. В дополнение к обязательным мерам, направленным на снижение риска несанкционированного доступа к Системе ДБО, рекомендуется:

3.7.1. Заблокировать использование Системы ДБО на определенный период времени в случае планируемого длительного ее неиспользования.

3.7.2. Осуществить разделение прав доступа в Систему ДБО между разными рабочими местами: например, на одном рабочем месте осуществляется создание и подписание документов электронной подписью, а на другом месте – отправка в Банк.

3.7.3. Связаться с операционистом и уточнить последние направленные в Банк с использованием Системы ДБО расчетные (платежные) документы в случае неожиданного «зависания» компьютера в момент работы с Системой ДБО и последующего его полного отказа в работе.

4. Фрод-мониторинг

Под фрод-мониторингом понимаются процедуры, направленные на идентификацию и дополнительную валидацию с клиентами платежей, являющихся по мнению Банка потенциально мошенническими.

В целях валидации Банк может осуществлять приостановку обработки поступившего платежа с последующей связью с клиентом посредством телефонных звонков. При этом операторы Банка обладают полной информацией о направленном платеже и сами называют ее для подтверждения клиентом.

В случае возникновения подозрений о легитимности звонка (например, звонящий пытается вынудить клиента самостоятельно назвать информацию о платежах, не обладая ей) клиенту необходимо запросить внутренний номер звонящего сотрудника Банка и осуществить обратный звонок на номер Контакт-центра для последующий связи с указанием внутреннего номера. Кроме того, в случае подозрительного звонка клиенту необходимо уведомить Банк о содержании разговора, дате и времени звонка, номере телефона, с которого осуществлялся звонок.