Рекомендации клиентам по повышению безопасности ДБО

В последнее время в средствах массовой информации участились упоминания о хищениях денежных средств с использованием систем дистанционного банковского обслуживания (ДБО). В связи с этим АО "Банк "Агророс" рекомендует Вам провести аудит безопасности ваших компьютеров и мобильных устройств, с помощью которых Вы пользуетесь системой ДБО, и принять меры по снижению рисков использования системы ДБО.

Возможные риски при использовании систем ДБО

Действия злоумышленников, направленные на хищение денежных средств с использованием систем дистанционного банковского обслуживания всегда предполагают несанкционированное использование программного обеспечения и электронных ключей. Передаваемая в банк информация подписывается электронной подписью. Документы с недостоверной подписью банк не обрабатывает. Механизм электронных подписей, основанный на паре открытых и секретных ключей, исключает возможность подделки как самой подписи, так и подписанных ей данных. Поэтому основная задача злоумышленника – воспользоваться настоящими электронными ключами для подписи нелегального документа, а основная задача владельца ключа - не допустить несанкционированного использования своего электронного ключа. Владелец электронного ключа несет полную ответственность за обеспечение его безопасного использования.

Электронные ключи всегда защищаются паролем. Чтобы воспользоваться украденными ключами похитителю необходимо либо подобрать, либо украсть пароль. Для кражи конфиденциальных данных на компьютере нелегально запускается шпионская программа (троян). Такие программы, как правило, попадают в компьютер случайно под видом безобидных программ запускаемых пользователем либо по принципу вируса через интернет или с зараженных сменных носителей (дискеты, флешки, компакт-диски). Но не исключена и адресная атака с целенаправленным заражением компьютеров внутри сети лицом, имеющим доступ к компьютерам организации. Шпионская программа может отслеживать действия пользователя, искать и копировать файлы, которые являются электронными ключами, перехватывать и сохранять все вводимые пароли, отправлять собранную информацию злоумышленнику через интернет и даже предоставлять ему полный контроль над компьютером при помощи удаленного управления. В этом случае преступник видит экран атакуемого компьютера и может им управлять удаленно точно так же, как и оператор, непосредственно работающий на этом компьютере. Преступник может создать свой документ на вашем компьютере, в надежде что оператор, обычно работающий с системой, не заметит нелегальный документ в большом объеме отправляемых платежей, подпишет и отправит его сам.

Если электронные ключи хранятся в файлах на диске, злоумышленник может скопировать эти файлы чтобы самостоятельно подписать документ, используя программу на своем компьютере, поэтому хранение электронных ключей в файлах небезопасно. Наиболее безопасном носителем для хранения электронных ключей являются микропроцессорные устройства со встроенными криптографическими функциями (токены). АО "Банк "Агророс" использует в своей системе ДБО токены eToken одного из ведущих российских разработчиков и поставщиков средств аутентификации, формирования ЭП, продуктов и решений для информационной безопасности - компании Аладдин. Электронные ключи, созданные внутри eToken, не являются файлами, извлечь и скопировать их невозможно. Подписание документов электронной подписью происходит внутри самого устройства, исходные данные передаются внутрь смарт-карты, а подписанные возвращаются обратно. Поэтому злоумышленнику потребуется украсть само устройство eToken, либо воспользоваться удаленным управлением компьютером с подключенным, бесконтрольно оставленным на длительное время eToken.

Методы снижения рисков

Повысьте свой уровень компьютерной грамотности. При необходимости, пройдите компьютерные курсы на уровне "продвинутого пользователя". Недопустимо держать eToken постоянно подключенным к компьютеру. Недопустимо оставлять без присмотра компьютер с подключенным токеном. Подключать токен следует только непосредственно перед входом на сайт ДБО. После окончания работы токен следует отключать от компьютера. Также для исключения возможности несанкционированного использования мобильных банковских услуг не оставляйте свой телефон (мобильное устройство) без присмотра.

В случае неожиданного выхода из строя (выключения, пропадания изображения) компьютера во время работы с системой Клиент-Банк немедленно отключите eToken от компьютера. Используйте надежный, современный компьютер. При внезапном прекращении работы SIM-карты Вашего мобильного устройства необходимо обратиться к оператору сотовой связи за уточнением причин.

Недопустимо оставлять eToken без присмотра либо передавать его третьим лицам. В нерабочее время следует хранить токен в запертом сейфе.

Для упрощения подключения и отключения токена рекомендуется использовать кабель USB-удлинителя один конец которого постоянно подключен к компьютеру, а второй выведен на стол рядом с мышью и клавиатурой. Токен можно отключать от компьютера в любой момент без выполнения "безопасного извлечения" устройства.

Используйте компьютер, на котором установлена система Клиент-Банк только для работы с банком и бухгалтерского учета. Не устанавливайте на этом компьютере никакое программное обеспечение без особой необходимости. Не запускайте неизвестные программы, не открывайте почтовые вложения. Не используйте компьютер для игр и интернет-серфинга. В случае необходимости работы через Internet, используйте только проверенные сайты по заранее определенному списку адресов.

Если вы пользуетесь системой ДБО на смартфоне или планшете, рекомендуем иметь два устройства, одно для входа и осуществления операций в системе, другое для получения одноразовых паролей. Если произойдет утеря либо кража смартфона, то злоумышленник не сможет получить SMS с паролем для осуществления операций или доступа в Систему ДБО.
Используйте лицензионную операционную систему Windows. Своевременно устанавливаете все обновления на операционную систему. Используйте встроенные средства обеспечения безопасности (брандмауэр Windows).

Используйте современное лицензионное антивирусное программное обеспечение, которое имеет режим постоянного файлового мониторинга, контролирует сетевой трафик, электронную почту. Своевременно обновляйте антивирусные базы. Подпишитесь на автоматические обновления. Предпочтительнее отечественные разработки, так как они более адаптированы под специфические угрозы.

Используйте надежные пароли. Надежный пароль должен иметь длину не менее 8 символов, содержать буквы из различных регистров (заглавные и строчные) и цифры. Не используйте в пароле только цифры. Не используйте словарные слова. Не используйте очевидные сочетания (имя, фамилия, дата рождения, номер телефона). Меняйте пароли каждые 3-4 месяца и немедленно после любого подозрения на компрометацию. Исключите хранение записанных на бумажный носитель логина/пароля компьютера или системы ДБО в общедоступных местах.

Отключите режим автозапуска на сменных носителях (CD, флешки и т.п.). Всегда проверяйте посторонние сменные носители на отсутствие вирусов и иных вредоносных программ, а так же свои флешки, если они подключались к чужим компьютерам. Не устанавливайте на компьютер непроверенные (без крайней необходимости - никакие) системы удаленного управления, не разрешайте подключения к компьютеру как к удаленному рабочему столу.

Не устанавливайте никакие надстройки и плагины (например от поисковых служб Яndex, Google и т.п., дополнительные панели, например Mail.Ru, различные "ускорители интернет" и прочие, не обусловленные крайней необходимостью) в программу интернет-браузер, которая используется для доступа к системе ДБО.

Не работайте на компьютере с правами Администратора. Используйте для повседневной работы только пользователя с ограниченными, минимальными полномочиями. Административные полномочия в операционной системе следует использовать только Системным Администраторам для решения задач администрирования или для установки и настройки ОС и программного обеспечения.

Администратору сети организации следует организовать работу сети таким образом, чтобы исключить возможность неограниченного прямого подключения компьютеров внутри сети к ресурсам интернет. Используйте proxy-сервер. Блокируйте все внешние подключения. Разрешайте прямой доступ только по определенным IP адресам и на определенные порты.
Не отвечайте на подозрительные письма с просьбой выслать секретный ключ ЭП, пароль и другие конфиденциальные данные. Напоминаем, что Банк никогда не осуществляет рассылку электронных писем с компьютерными программами или с просьбой предоставить конфиденциальную информацию. Ответственность за сохранение ключа ложится на пользователя системы.

При увольнении сотрудника пользователь должен удаляться из системы ДБО. При увольнении IT-специалиста, обслуживавшего компьютеры с установленной системой ДБО, обязательно проверьте компьютеры на отсутствие вредоносных программ. Исключите обслуживание компьютера ненадежными IT-сотрудниками. Контролируйте все действия, выполняемые IT-сотрудниками с системой ДБО.

При потере мобильного телефона (мобильное устройство) с подключенной услугой системы интернет клиент-банк, необходимо срочно обратиться к оператору сотовой связи для блокировки SIM-карты и в Контактный Центр Банка по телефонам 8(8452) 44-19-19; 8(800) 222-44-19 для блокировки доступа к услугам программного комплекса услуги системы ДБО.

При смене номера телефона, на который подключена услуга системы интернет клиент-банк, Вам необходимо обратиться в Банк и отключить указанную услугу от старого номера телефона и подключить услугу на новый номер. Помните, что операторы сотовой связи могут передать номер телефона другому абоненту, если он будет неактивным длительное время.

Не используйте мобильные телефоны, у которых изменены заводские настройки в части доступа к операционной системе – Jail Break, Root и пр. Данные процедуры отключает защитные механизмы, заложенные производителем.

Запомните адрес страницы, а так же внешний вид окон системы ДБО в которых требуется вводить секретную информацию (имена, пароли). Не вводите никакие конфиденциальные

данные, если адрес страницы отличается или окно (цвета, размеры, расположение элементов, логотип и т.п.) выглядит не так, как обычно.

В системе ДБО Интернет Клиент-Банк существует режим подтверждения каждого отправленного платежа с помощью уникального кода, который банк отправляет на мобильный телефон клиента. Платеж принимается к обработке только после ввода клиентом кода, полученного в SMS сообщении. Использование одноразовых SMS кодов для подтверждения документов повышает безопасность системы, хотя несколько усложняет отправку платежей, поскольку требуется ждать получения кода и вводить его с клавиатуры.
Не используйте для получения одноразовых SMS кодов смартфоны, планшетные компьютеры или иные устройства с возможностью выхода в интернет и установки дополнительного программного обеспечения. Для максимальной безопасности приобретите и используйте специально для ДБО самый простой телефон только с функциями звонков и SMS. Следует постоянно контролировать входящие сообщения на этом телефоне.
В системе ДБО есть так называемый "белый список" получателей платежа. То есть заранее предоставляемый в банк список пар "БИК банка/Номер счета получателя", отправка платежей на которые считается безопасной. Если получатель находится в "белом списке" платеж принимается в обработку без дополнительных подтверждений. Если получатель платежа не находится в данном списке, банк может затребовать дополнительное подтверждение, например SMS кодом. Использование "белого списка" совместно с SMS подтверждениями повышает безопасность и минимизирует дополнительные действия для отправки платежей.

Доступ к системе ДБО может быть ограничен по IP адресам. Если в организации клиента заключен договор с провайдером на выделение фиксированных IP адресов рекомендуется указывать эти адреса в заявке на подключение ДБО, чтобы исключить возможность входа в систему с других адресов. Если адреса выделяются динамически, то такое ограничение использовать невозможно.

Регулярно контролируйте состояние своих счетов и незамедлительно информируйте обслуживающее подразделение Банка обо всех подозрительных или несанкционированных операциях. В случаях подозрений на мошеннические действия в системе ДБО, незамедлительно обращайтесь в правоохранительные органы.

Банк обеспечивает безопасность системы со своей стороны, но обеспечить полную безопасность работы системы без соблюдения Вами собственной информационной безопасности невозможно!