Приложение № 2

О рисках использования системы Интернет-банк и о соблюдении мер информационной безопасности, необходимых для обеспечения безопасной работы в системе Интернет-банк

Основным риском при использовании системы Интернет-банк является риск получения злоумышленником несанкционированного доступа к управлению счетом Клиента и к документам Клиента, передаваемым в Банк через систему Интернет-банк. Последствиями несанкционированного доступа могут быть списание денежных средств со счета Клиента или утечка конфиденциальной информации о совершаемых Клиентом операциях.

Способы несанкционированного доступа к системе Интернет-банк

Основными способами получения несанкционированного доступа к системе Интернет-банк являются:

– перехват злоумышленником управления компьютером клиента;

– кража Логина и Пароля Клиента для входа в систему Интернет-банк, а также закрытой части ключа электронной подписи Клиента;

– перехват данных, передаваемых Клиентом в Банк и получаемых Клиентом из Банка.

Получение несанкционированного доступа может быть осуществлено:

– штатными сотрудниками организации Клиента;

– нештатными сотрудниками, приходящими по вызову для обслуживания компьютеров организации Клиента;

– злоумышленниками, получившими доступ к компьютерам организации Клиента через сеть Интернет или иные каналы связи;

- в результате утраты (потри, хищения) устройства, с использованием которого клиентом осуществляются действия в целях осуществления банковских операций.

Признаки несанкционированного использования клиентского рабочего места системы Интернет-банк:

– наличие в системе нелегитимного платёжного поручения (платёжное поручение сформировано злоумышленником);

– наличие в системе не заказанных выписок, или иных документов (документы заказаны злоумышленником);

– «самостоятельная» (независимая от действий пользователя) работа компьютера: перемещение курсора, открытие и закрытие окон программ, заполнение форм и документов и пр. (управление компьютером захвачено злоумышленником);

– отсутствие доступа к системе Интернет-банк по причине неверного пароля (пароль изменен злоумышленником);

– нестабильная работа компьютера или полная его неработоспособность (последствия деятельности злоумышленника по уничтожению следов вторжения);

– не работает ключевой носитель (возможные последствия деятельности злоумышленника).

Данный перечень признаков несанкционированного использования системы Интернет-банк не является исчерпывающим. В зависимости от новых видов атак список может дополняться и корректироваться.

Компрометация закрытой части ключа электронной подписи (ключевого носителя).

К событиям, на основании которых принимается решение о компрометации, относятся, включая, но, не ограничиваясь, следующие события:

– потеря ключевых носителей (даже с их последующим обнаружением);

– увольнение сотрудников, имевших доступ к ключевым носителям;

– нарушение печати на сейфе с ключевыми носителями;

– случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);

- заражение компьютера вредоносным программным обеспечением.

Меры, необходимые для обеспечения безопасной работы в системе Интернет-банк

Клиенту, в целях снижения возможного риска несанкционированного использования рабочего места системы Интернет-банк и списания третьими лицами денежных средств со счета Клиента, необходимо выполнять следующие меры информационной безопасности:

1.Меры сетевой безопасности:

1.1. На компьютере должна быть установлена парольная защита на вход в BIOS и в операционную систему. Рекомендуется использовать в качестве пароля комбинацию знаков, смысл и последовательности которых трудно определить. При использовании смартфона или планшета необходимо настроить блокировку экрана способом, исключающих доступ к нему посторонних (PIN-код, графический ключ, отпечаток пальца и т.п.).

1.2. Перед установкой системы Интернет-банк на устройство, используемое для осуществления операций, необходимо проверить его на отсутствие вредоносного программного обеспечения и программ удаленного доступа (BeTwin, RAdmin и др.). Использование подобных программ несет большие риски, решение об их использовании организация принимает на свой страх и риск.

1.3. Не привлекать для администрирования и обслуживания компьютера, планшета, смартфона сотрудников посредством предоставления удаленного доступа.

1.4. Если компьютер установлен внутри локальной сети организации, провести мероприятия по защите локальной сети от зловредных воздействий со стороны сети Интернет. При выходе в Интернет рекомендуется использовать сетевые экраны, разрешив доступ только к доверенным ресурсам сети.

1.5. Включите систему фильтрации ложных web-узлов (антифишинг) в своем браузере либо в антивирусном программном обеспечении, если браузер ее не имеет —обновите браузер.

1.6. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам. Наилучшей практикой является отказ от использования электронной почты на устройствах с установленными рабочими местами системы Интернет-банк.

1.7. При вводе личной информации, ПОМНИТЕ, что любой веб-адрес в адресной строке Интернет- банка должен начинаться с «https». Если в адресе не указано «https», это значит, что вы находитесь на незащищенном веб-сайте, и вводить конфиденциальные данные нельзя.

Удостоверьтесь, что адрес сайта введён правильно и вы не зашли на мошеннический сайт с похожим адресом. Например, вместо окончания «ru» злоумышленник может зарегистрировать ложный сайт «faktura.ру» или вместо «faktura.ru» сделать ложный сайт «factura.ru» и узнать ваш пароль, для доступа к системе «Интернет-банк», когда он будет там введён.

1.8. Не давайте разрешения неизвестным программам выходить в интернет.

1.9. При работе в Интернете не соглашайтесь на установку каких-либо дополнительных программ от недоверенных издателей.

1.10. Не используйте компьютер, планшет, смартфон, на котором установлено рабочее место системы Интернет-банк, не по назначению, например, для игр, просмотра фильмов и т.п.

1.11. Для повышения степени безопасности эксплуатации системы Интернет-банк можно сообщить в Банк список доверенных IP-адресов, с которых возможен вход в систему. Возможность входа в систему с IP-адресов, не входящих в список доверенных в этом случае будут полностью исключены.

2. Меры по защите от вредоносного программного обеспечения:

2.1. Установить на компьютере, планшете, смартфоне антивирусное программное обеспечение. Обновление баз данных антивирусного программного обеспечения должно осуществляться ежедневно, либо по мере выхода новых официальных версий баз данных.

2.2. Антивирусное программное обеспечение должно быть запущено постоянно с момента загрузки устройства. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов.

2.3. Должны быть установлены последние пакеты обновлений (Service Packs), актуальные патчи безопасности, критичных обновлений операционной системы и браузеров, обновление которых должно проводиться регулярно.

2.4. Необходимо своевременно обновлять, используемое для работы с системой Интернет-банк программное обеспечение. Установку обновлений необходимо производить только с официальных сайтов разработчиков соответствующего программного обеспечения.

2.5. В операционной системе должна быть отключена функция AutoRun.

2.6. Не используйте права администратора при отсутствии необходимости. В повседневной практике входите в систему как пользователь, не имеющий прав администратора.

2.7. Необходимо исключить установку на компьютер, планшет, смартфон нелицензионного и полученного из не заслуживающих доверия источников программного обеспечения.

2.8. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривайте журнал и реагируйте на ошибки.

2.9. Контролируйте конфигурацию устройства, чтобы вовремя обнаружить его несанкционированное использование или изменения. Например, появление в списке нового программного обеспечения, которое было установлено без вашего ведома.

3. Меры, направленные на защиту от копирования (хищения) ключевой и парольной информации:

3.1. Храните носители ключей (смарт-карты, дискеты, флэш-карты и другие носители с записанными ключами) в месте, недоступном посторонним лицам (сейфе и т.д.). Исключите хранение ключей на жестком диске, в сетевых каталогах и прочих общедоступных ресурсах.

3.2. Храните в тайне пароль доступа к ключу, а также Логин и Пароль для доступа в систему Интернет-банк, исключите их запись на стикерах, носителях ключей и т.п.

3.3. Не передавайте ключи электронной подписи и не сообщайте Логин и Пароль доступа к системе Интернет-банк кому-либо.

3.4. Извлекайте ключевой носитель сразу после окончания сеанса работы с системой Интернет-банк.

3.5. Юридические лица во всех случаях увольнения или смены лиц, допущенных к ключам электронной подписи, Логину и Паролю, а также руководителей юридического лица, которые подписывали доверенности о допуске пользователей к ключам электронной подписи, логинам и паролям, должны заменить карточку с образцами подписей и оттиска печати, ключи электронной подписи, Логин и Пароль.

3.6. Минимизируйте количество пользователей, которые имеют право доступа к компьютеру, планшету, смартфону с установленным рабочим местом системы Интернет-банк, ограничив его кругом лиц, непосредственно использующих систему Интернет-банк.

3.7. Не используйте функцию автозаполнения (пароль пользователя, имя пользователя, пароль на токен и др.) это предотвратит использование данных сторонними лицами.

3.8. Сотрудники Банка никогда не запрашивают по телефону, электронной почте или через SMS сообщения никакой конфиденциальной информации (ключи, пароли и пр.)! Не выполняйте никаких рекомендаций, особенно связанных с вводом каких-либо данных на любых страницах, открытых вашим браузером. Работники банка не обращаются к Клиентам по телефону с предложениями попытаться войти в систему еще раз или ввести еще один код подтверждения, не пытаются узнать у Клиентов пароли или код подтверждения. Ни при каких обстоятельствах не сообщать данную информацию!

4. Меры по контролю несанкционированных списаний:

4.1. Необходимо контролировать доставку пакета электронных документов и результаты его обработки. Для этого связь с Банком должна повторяться по прошествии времени, достаточного для обработки Банком пришедших пакетов документов.

4.2. Следует регулярно контролировать состояние своих счетов и незамедлительно информировать обслуживающее подразделение Банка обо всех подозрительных или несанкционированных операциях, но не позднее дня, следующего за днём получения от Банка уведомления о совершённой операции, об их использовании без согласия Клиента.

4.3. В случае неожиданного выхода из строя компьютера (планшета, смартфона), либо пропадания на нём программного обеспечения системы Интернет-банк, необходимо прекратить работу на нём, отключив его от всех видов сетей, включая локальную корпоративную сеть, и модемов, срочно запросить в Банке выписку по счету. При обнаружении несанкционированных платежных операций написать заявление в Банк, а также обратиться с соответствующим заявлением в правоохранительные органы. устройства не восстанавливайте до проведения технической экспертизы.

4.4. В случае обнаружения несанкционированного доступа к компьютеру с установленным рабочим местом системы Интернет-банк, подозрительных операций, установлении фактов компрометации закрытой части ключа электронной подписи, утрате (потери, хищения) устройства, применяемого для осуществления банковских операций:

- срочно связаться с Банком и проинформировать об имеющихся подозрениях или фактах;
- проверить легитимность всех выполненных за последнее время платежей;
- направить в Банк заявление о блокировке операций в системе Интернет-банк;
- произвести смену ключей электронной подписи.

4.5. Необходимо выполнять незамедлительную блокировку и смену ключей электронной подписи, паролей для доступа в случаях их компрометации, а также по истечении срока действия ключей с периодичностью, установленной договорами и документацией.

4.6. Необходимо заменять ключи электронной подписи, Логины и Пароли во всех случаях увольнения или смены руководителей Клиента, подписывавших распоряжения (доверенности) о предоставлении сотрудникам Клиента, полномочий подписания электронной подписью, аналогом собственноручной подписи электронных документов.

4.7. Подключите sms-информирование, чтобы оперативно узнать о несанкционированном переводе и своевременно сообщить о мошеннической операции (компрометации ключа электронной подписи или Логина и Пароля). Используйте разные устройства для работы в Интернет-банке и получения уведомлений о совершённых операциях. Например, если доступ в систему Интернет-банк осуществляется с планшета и на него же придёт SMS о переводе, то в случае заражения его вредоносным программным обеспечением SMS-сообщение может быть удалено и вы о переводе не узнаете.

5. Меры по поддержанию уровня информационной безопасности:

5.1. Для обеспечения высокого уровня информационной безопасности при эксплуатации системы Интернет-банк у Клиента должен быть назначен ответственный, который осуществляет:

- постоянный контроль соблюдения мер информационной безопасности, предусмотренных настоящей памяткой, документацией на систему и средства защиты;
- выявление, устранение и информирование руководства Клиента обо всех выявленных нарушениях;
- контроль над устранением выявленных нарушений;
- документирование результатов проведенных работ и проверок.

Для работы с ПРОСТОЙ ЭП / АСП:

1. Запомните, что для входа в Интернет-банк вам требуется вводить только ваш логин и пароль. Не нужно вводить номер вашего мобильного телефона, номер вашей банковской карты или CVV2/CVC2 код для входа или дополнительной проверки персональной информации в Интернет-банке.
2. Никогда и ни при каких обстоятельствах не сообщайте никому свои пароли для входа в Интернет- банк или для подтверждения платежей, а также номера ваших карт и CVV2/CVC2 коды.
3. Обязательно сверяйте текст SMS-сообщений, содержащий пароль, с деталями выполняемой вами операции. Если в SMS указан пароль для платежа, который вы не совершали или вам предлагают его ввести/назвать, чтобы отменить якобы ошибочно проведенный по вашему счету платеж, ни в коем случае не вводите его в Интернет-банке и не называйте его, в том числе сотрудникам банка.
4. В случае утери мобильного телефона, на который приходят разовые пароли, немедленно заблокируйте SIM-карту / войдите в Интернет-банк и удалите телефон из списка зарегистрированных устройств для получения PUSH-сообщений.
5. Запишите контактный телефон вашего банка в адресную книгу или запомните его. В случае если в личном кабинете Интернет-банка вы обнаружите телефон, отличный от записанного, в особенности, если вас будут призывать позвонить по этому телефону для уточнения информации, либо по другому поводу, будьте бдительны и немедленно позвоните в банк по ранее записанному вами телефону. Также для этих целей подойдет телефон, указанный на вашей банковской карте.
6. Устанавливайте мобильные приложения Faktura.ru только из авторизованных магазинов приложений App Store и Google Play. Используйте антивирусное программное обеспечение, в случае, если оно доступно для вашего телефона/смартфона.
7. Избегайте регистрации номера вашего мобильного телефона, на который приходят SMSсообщения с разовым паролем, в социальных сетях и других открытых источниках.