О противодействии хищению денежных средств

Уважаемые клиенты! Внимание!

В банковской сфере страны продолжают выявляться попытки хищения денежных средств с расчетных счетов корпоративных клиентов, использующих системы электронного банкинга, в том числе и систему «iBank 2», при этом часть из них предотвратить не удается. Как следствие, клиент сталкивается с непростой процедурой возврата денежных средств, заключающейся во взаимодействии с правоохранительными органами, судами различных инстанций и банком, клиентом которого он является.

Анализ выявленных ситуаций показал, что хищения денежных средств с расчетных счетов осуществляются:

- ответственными сотрудниками предприятия, имеющими доступ к носителям ключей ЭП системы электронного банкинга «iBank 2», в том числе работающими или уволенными (при несвоевременном предоставлении уведомления о блокировании ключа проверки ЭП в банк);
- штатными ИТ-сотрудниками организаций, имевшими доступ к носителям с ключами ЭП (usb-токенами), а также доступ к компьютерам, с которых осуществлялась работа по системе электронного банкинга «iBank 2»;
- нештатными ИТ-специалистами, приходящими по вызову, и выполняющими профилактику и подключение к интернет, установку и обновление бухгалтерских и справочных программ, установку и настройку другого программного обеспечения на компьютерах, с которых осуществляется работа по системе электронного банкинга «iBank 2»;
- **злоумышленниками путем заражения компьютеров клиентов специальными вирусными программами через уязвимости системного и прикладного ПО (операционные системы, Web-браузеры, почтовые клиенты и пр.) с последующим дистанционным похищением паролей и использованием ключей ЭП.**

Действия злоумышленников направлены на:

- заражение компьютера для дистанционного использования подключенного usb-токена;
- похищение пароля доступа к ключу;
- передачу в банк подложных электронных платежных документов, заверенных ключом ЭП.

Во всех выявленных случаях злоумышленники тем или иным образом получали доступ к ключам ЭП и паролям и направляли в банк платежные поручения с корректной электронной подписью.

Платежные поручения, успешно прошедшие проверку ЭП, в большинстве случаев были замечены банковскими сотрудниками, сочтены подозрительными и отвергнуты на этапе принятия решения об исполнении документов.

В то же время часть платежей, направленных злоумышленниками с использованием действующих ключей ЭП клиента, не вызывала подозрений у банков. Такие документы имели корректную ЭП, вполне обычные реквизиты получателей и типовое назначение платежа. Их исполнение банком приводило к хищению денежных средств с расчетного счета клиента.

Важно понимать, что Банк не имеет доступа к Вашим ключам ЭП и не может от Вашего имени сформировать корректную ЭП под электронным платежным поручением.

Вся ответственность за конфиденциальность Ваших ключей ЭП полностью лежит на Вас, как на единственных владельцах ключей ЭП.

Банк НЕ осуществляет рассылку электронных писем с просьбой прислать ключ ЭП или пароль. Банк НЕ рассылает по электронной почте программы для установки на Ваши компьютеры.

Если Вы сомневаетесь в конфиденциальности своих ключей ЭП, если есть подозрение об их компрометации, Вы должны немедленно заблокировать свои ключи ЭП. Это можно сделать двумя способами:

- позвонить в Банк и назвать блокировочное слово;
- прийти в Банк лично с документами, удостоверяющими личность.

Для продолжения работы в «iBank 2» Вам потребуется сгенерировать и зарегистрировать в Банке новые ключи ЭП.

О мерах по пресечению хищения и несанкционированного использования ключей ЭП.

В целях предотвращения хищения ключей ЭП у клиентов банка, регистрация ключей ЭП клиентов с правом подписи осуществляется **только** на USB-токенах.

Настоятельно рекомендуем Вам **после завершения сеанса работы** с Internet-Банкином или РС-Банкингом **извлекать USB-токен из USB-порта** персонального компьютера.

Использование USB-токенов **исключает хищение** ключей ЭП, **но возможны попытки хищений средств со счета путем дистанционного подключения злоумышленника к Вашему компьютеру.**

В целях уменьшения риска доступа сразу к двум ключам подписи платежных документов (директора и главного бухгалтера) при подключении USB-токена к компьютеру, на котором происходит обработка платежных документов системы «iBank 2», рекомендуем ключи подписи платежных документов директора и главного бухгалтера компаний сохранять на разные USB-токены и при формировании платежных документов использовать их последовательно (желательно на разных компьютерах).

Программное обеспечение системы Интернет-Банкинга «iBank2» **НИКОГДА** не выводит на экраны компьютера сообщение о временной неработоспособности системы. Сообщения типа: ***«Ошибка. Технические работы. Окончание xx.xx.xxxx в xx:xx», «На сервере банка ведутся профилактические работы»,*** свидетельствуют о том, что Ваш компьютер заражен троянской программой.

В случае появления такого рода сообщений на Вашем компьютере необходимо извлечь USB-токен, выйти из системы, выключить компьютер и немедленно связаться с сотрудником Банка.

Банк осуществляет проверку подозрительных платежей по установленным банком правилам, но надеется, что Вы так же будете бдительны.