АГРОПРОМКРЕДИТ
коммерческий банк

107023, г. Москва, ул. Электрозаводская, д. 27, стр. 5
Пресс-центр ОАО КБ «АГРОПРОМКРЕДИТ»
Тел.: +7 (495) 755-80-08, 8 (800) 100-80-08
E-mail: pressa@apkbank.ru
www.apkbank.ru

Открытое письмо

Дата: **28 апреля 2009 г.**

О выявлении попыток хищения денежных средств

Уважаемые клиенты!

За последние несколько месяцев в ряде российских банков были Выявлены попытки хищения денежных средств с расчетных счетов корпоративных клиентов путем совершения платежей с использованием системы электронного банкинга «iBank2».

О сложившейся ситуации

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

-ответственными сотрудниками предприятия, имевшими доступ к секретным ключам ЭЦП для системы электронного банкинга «iBank2», в том числе работающими или уволенными директорами, бухгалтерами и их заместителями;

-штатными ИТ-сотрудниками организаций, имевшими доступ к носителям с секретными ключами ЭЦП (дискеты, флэш-диски, жесткие диски и пр.), а также доступ к компьютерам, с которых осуществлялась работа по системе электронного банкинга «iBank2»;

-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 «iBank2»;

-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 секретных ключей ЭЦП и паролей.

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

Платежные поручения, успешно прошедшие проверку ЭЦП, но при этом абсолютно не свойственные конкретному клиенту, 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 секретных ключей ЭЦП клиента, не Вызывала подозрений у банка. Такие документы имели корректную ЭЦП, вполне обычные реквизиты получателей и типовое назначение платежа. Их исполнение банком приводило к хищению денежных средств с расчетного счета клиента. При этом вся ответственность за убытки безусловно и полностью возлагалась на клиента как единственного владельца секретных ключей ЭЦП.

О мерах по пресечению хищения и использования секретных ключей ЭЦП

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

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

Банк информирует Вас, что не осуществляет рассылку электронных писем с просьбой прислать секретный ключ ЭЦП или пароль. Банк не рассылает по электронной почте программы для установки на Ваши компьютеры.

Если Вы сомневаетесь в конфиденциальности своих секретных ключей ЭЦП, если есть подозрение об их компрометации (копировании), Вы должны немедленно заблокировать свои ключи ЭЦП. Это можно сделать двумя способами:
-позвонить в Банк и назвать блокировочное слово;
-прийти в Банк лично с документами, удостоверяющими личность.

Для продолжения работы в «iBank2» Вам потребуется сгенерировать и зарегистрировать в Банке новые ключи ЭЦП.

Внимание! Изменение пароля доступа к секретному ключу ЭЦП не защищает от использования злоумышленником ранее похищенного ключа.

Настоящим письмом Банк еще раз информирует Вас о необходимости строгого соблюдения правил информационной безопасности, правил хранения и использования секретных ключей ЭЦП и об ограничении по возможности доступа к персональным компьютерам, с которых осуществляется работа по системе электронного банкинга «iBank2».

Действия злоумышленников направлены на:
-похищение файла с секретным ключом ЭЦП;
-похищение пароля доступа к ключу;
-передачу в банк электронных платежных документов, заверенных похищенным ключом ЭЦП.

Для обеспечения безопасности Вашей работы с iBank2 требуется придерживаться приведенных ниже правил и рекомендаций.

Чтобы предотвратить хищение секретного ключа ЭЦП и пароля доступа к ключу, необходимо:

1. Использовать для хранения файлов с секретными ключами ЭЦП отчуждаемые носители: дискеты, флеш-носители, CD-диски, специализированные устройства. Отключать и извлекать носители с ключами ЭЦП в то время, когда они не используются для работы с iBank2.

2. По возможности ограничить доступ к компьютерам, используемым для работы с iBank2. На компьютерах, используемых для работы с iBank2, исключить посещение Интернет-сайтов сомнительного содержания, загрузку и установку сомнительного ПО и т. п.

3. Применять на рабочем месте (в рабочей локальной сети) надежные, по возможности лицензионные средства антивирусной защиты, обеспечить регулярное автоматическое обновления антивирусных баз.

4. Применять на рабочем месте специализированные программные средства безопасности: персональные файрволлы, достаточные (средние и Выше) параметры безопасности и конфиденциальности Вашего интернет-браузера и т.п.

5. Исключить обслуживание компьютеров, используемых для работы с iBank2, ненадежными ИТ-сотрудниками. При обслуживании компьютера ИТ-сотрудниками - обеспечивать контроль за Выполняемыми ими действиями. Никогда не передавать ключи ЭЦП ИТ-сотрудникам для проверки работы iBank2, проверки настроек взаимодействия с банком и т.п. При необходимости таких проверок только лично владелец ключа ЭЦП должен сам подключить носитель к компьютеру и лично ввести пароль, исключая его подсматривание.

6. При увольнении ответственного сотрудника, имевшего доступ к секретному ключу ЭЦП, обязательно заблокировать ключи ЭЦП и сгенерировать новые. При увольнении сотрудника,

имевшего технологический доступ к секретному ключу ЭЦП, обязательно заблокировать ключи ЭЦП и сгенерировать новые. При увольнении ИТ-специалиста, осуществлявшего обслуживание компьютеров, используемых для работы с iBank2, принять меры для проверки компьютеров на отсутствие вредоносных программ.

При возникновении любых подозрений на компрометацию (копирование) ключей ЭЦП или компрометацию среды исполнения (наличие в компьютере вредоносных программ)- обязательно заблокировать ключи ЭЦП и сгенерировать новые.

Если Вы заметили проявление необычного поведения ПО «iBank2» или какие-то изменения в интерфейсе программы - позвонить в банк и Выяснить, не связаны ли такие изменения с обновлением версии ПО. Если нет - возможно, изменения вызваны работой программы-шпиона. Обязательно сразу же заблокировать ключи ЭЦП и сообщить в Банк о ситуации.

Чтобы минимизировать риски нелегального использования ключей ЭЦП злоумышленниками, можно принять следующие дополнительные меры безопасности.

Для этого необходимо обратиться в Банк с просьбой разрешить работу с системой «iBank2» только с указанных Вами IP-адресов и IP-сетей. В список разрешенных Вы можете включить неограниченное количество IP-адресов и IP-сетей, чтобы обеспечить нормальную работу всех своих филиалов, площадок и пр. Бланк заявления на блокировку доступа содержится в пакете документов на подключение к системе Интернет-Банк находящемся на сайте банка. Также бланк заявления можно получить у ответственного сотрудника в Банке, обратившись в операционный отдел.

Попытки доступа с неразрешенного IP-адреса будут блокированы системой. Вы будете информированы Банком о попытке взлома. По Вашей просьбе Банк предоставит Вам IP-адреса, с которых были проведены попытки несанкционированного доступа для проведения дальнейшего расследования компетентными органами.

Для получения дополнительной информации обращайтесь в банковскую службу поддержки пользователей системы «iBank2».

С уважением,

ОАО КБ «АГРОПРОМКРЕДИТ»