



# Банк Проминвестрасчет

## Рекомендации по обеспечению безопасности при работе в Сети Интернет

\* Не запускайте у себя на компьютере программ из ненадежных источников и не открывайте приложения к письмам, даже если письмо пришло от Вашего хорошего знакомого: в них могут быть спрятаны вирусы или троянские кони. Сначала сохраните это приложение в файл и проверьте его антивирусной программой. Помните, что злоумышленники могут прибегнуть к разнообразным приемам, чтобы обманом получить у Вас информацию об идентификационных параметрах.

\* Не надо верить всем сообщениям о новых страшных вирусах, появившихся в Интернет, особенно если в сообщении сказано, что надо распространить эту информацию всем Вашим знакомым. Это сообщение может оказаться носителем вируса или просто компьютерной шуткой.

\* Если Вы получили письмо от незнакомого человека или организации, то знайте, что скорее всего это спам - назойливые рекламные письма - и письмо попало в Ваш ящик не по ошибке, а специально.

\* Обязательно установите на ВСЕ компьютеры антивирусную программу для защиты от троянских коней и вирусов в режиме резидентного монитора (тогда она будет проверять все запускаемые программы и открываемые документы автоматически).

\* Ограничьте доступ к Вашему компьютеру с помощью программ управления доступом

\* Делайте резервные копии системных файлов и важных данных и храните их в безопасном месте (не на жестком диске Вашего компьютера). В случае сбоя жесткого диска или вирусной атаки это позволит Вам быстро продолжить работу.

\* Помните, что программы, которыми Вы пользуетесь при работе в Интернет, могут содержать ошибки безопасности ("дыры"). Эти ошибки могут позволить злоумышленнику заблокировать Ваш компьютер или получить несанкционированный доступ к нему через Интернет. Производители операционных систем и прикладных программ регулярно публикуют информацию об обнаруженных "дырах" и исправленные версии программ. Проверьте, что Вы установили ВСЕ исправления для используемых Вами программ, и если нет - сделайте это как можно скорее. Следите за публикациями о новых обнаруженных ошибках в программах и оперативно устанавливайте исправления для них.

\* Не думайте, что вирусы и троянские кони могут находиться только в программах, загруженных из Интернета - как показывает печальный опыт покупателей пиратских CD, на них все чаще появляются программы, также зараженные вирусами или троянскими конями. Если уж Вы купили CD, проверьте его хорошей антивирусной программой с последней антивирусной базой данных.

## **О попытках хищения денежных средств со счетов корпоративных клиентов с использованием системы электронного банкинга «iBank 2»**

За последние несколько месяцев в российских банках были выявлены случаи хищения (предотвращенные и свершившиеся) денежных средств с расчетных счетов корпоративных клиентов путем совершения электронных платежей по системе «iBank 2».

Для предотвращения хищения средств необходимо строго соблюдать порядок работы в системе «iBank 2»:

- \* соблюдать правила информационной безопасности, регламент доступа к компьютерам для работы в системе <iBank 2>, регламент работы с секретными ключами ЭЦП клиента;
- \* использовать только лицензионное системное и прикладное ПО, оперативно его обновлять;
- \* использовать и оперативно обновлять персональный межсетевой экран (firewall), антивирусное ПО, средства обнаружения вредоносных программ;
- \* при использовании клиентом двух секретных ключей ЭЦП (ключ ЭЦП директора с правом первой подписи, и ключ ЭЦП главного бухгалтера с правом второй подписи) осуществлять работу с системой <iBank 2> на двух отдельных компьютерах с хранением секретных ключей ЭЦП на двух отдельных USB-токенах;
- \* Клиентам у которых два ключа подписи хранятся на одном USB-токене необходимо в банке получить второй USB-токен и на нем сгенерировать ключ со второй подписью;
- \* периодически обновлять версию java с сайта [www.java.com](http://www.java.com).

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

1. **Ответственными сотрудниками корпоративных клиентов**, имевшими доступ к секретным ключам ЭЦП организации. Как правило, это уволенные директора, бухгалтеры и их заместители, а также совладельцы организации.

2. **Штатными ИТ-сотрудниками корпоративных клиентов**, имевшими технический доступ к носителям (дискеты, флеш-носители, жесткие диски и пр.) с секретными ключами ЭЦП клиентов, а также доступ к компьютерам клиентов, с которых осуществлялась работа по системе электронного банкинга «iBank 2».

3. **Нештатными, проходящими по вызову, ИТ-специалистами**, обслуживающими компьютеры корпоративного клиента, с которых осуществлялась работа по системе электронного банкинга «iBank 2».

Как правило, это проходящие ИТ-специалисты, осуществляющие профилактику и подключение к Интернет, установку и обновление бухгалтерских и информационно-правовых программ, установку, обновление и настройку другого ПО.

4. **Злоумышленниками путем заражения через Интернет компьютеров корпоративных клиентов вредоносными программами**. Используя уязвимости системного и прикладного ПО (операционные системы, Web-браузеры, почтовые клиенты и пр.), злоумышленники заражали компьютеры корпоративных клиентов троянскими программами с последующим дистанционным похищением секретных ключей ЭЦП клиента и паролей.

Во всех выявленных случаях злоумышленники тем или иным образом получали доступ к секретным ключам ЭЦП и паролям корпоративного клиента и направляли в банк платежные поручения с корректной ЭЦП клиента.

Успешно прошедшие проверку ЭЦП, но при этом подозрительные, абсолютно не свойственные данному клиенту платежные поручения в большинстве случаев пресекались банковскими операционистами на этапе принятия решения об исполнении документов.

В то же время часть платежей, направленных злоумышленниками с использованием действующих секретных ключей ЭЦП клиента, не вызвала 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.

Отдельную группу составляют ситуации, когда банки не соблюдают регламент регистрации сертификатов открытых ключей ЭЦП клиентов. В подобных случаях банковские сотрудники закрепляют за клиентом сертификат открытого ключа ЭЦП, созданного злоумышленником. В результате злоумышленник получает возможность управлять счетом корпоративного клиента. При таких хищениях ответственность за убытки полностью несет банк.