ПАМЯТКА
по безопасной работе в системе «Интернет-Банк»

В системе Интернет-Банк используются современные механизмы и средства обеспечения информационной безопасности. Безопасность обмена электронными документами обеспечивается посредством шифрования данных и наложения электронной подписи для обеспечения целостности, и аутентичности (доказательства авторства) документов в системе.

Соблюдение приведенных ниже рекомендаций позволит обеспечить безопасность расчетов в системе Интернет-банк и свести риски мошенничества и финансовые потери к минимуму.

Меры безопасности при работе с системой Интернет-Банк:

- Самостоятельно генерируйте ключи для работы в системе Интернет-Банк, никому не доверяйте выполнение этой процедуры;
- Храните ключевые носители (токены) в сейфе, исключающем несанкционированный доступ к ним;
- Не допускайте постоянного подключения к компьютеру токенов; по завершении работы в системе Интернет-Банк или при перерыве в работе извлекайте ключевой носитель из устройства. Не передавайте свой ключевой носитель третьим лицам, не оставляйте его без присмотра;
- Пароль на доступ к секретному ключу должен быть известен только Вам, ни при каких обстоятельствах не передавайте свой пароль никому, включая сотрудников Банка. Используйте сложные пароли, состоящие из заглавных и строчных букв, цифр и специальных знаков;
- Используйте антивирусное программное обеспечение и следите за его регулярным обновлением. Регулярно выполняйте антивирусную проверку на своем компьютере для своевременного обнаружения вредоносных программ;
- Используйте только лицензионное программное обеспечение (ПО). Обновляйте системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ;
- Используйте и своевременно обновляйте специализированное ПО, позволяющее повысить уровень защищенности Вашего компьютера – персональные межсетевые экраны, средства защиты от несанкционированного доступа и пр. Настройте межсетевой экран таким образом, чтобы запретить соединение с сетью Интернет по протоколам ftp, smtp, сделав исключение только для конкретных почтовых серверов, где зарегистрирована Ваша электронная почта;
- При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не открывайте прикрепленные к письму файлы и не переходите по содержащимся в таких письмах ссылкам. Помните, что письмо с непонятным содержанием, даже отправленное с известного Вам адреса, скорее всего, является спамом или фишингом;
- Не давайте разрешения неизвестным Вам программам на доступ в сеть Интернет. При работе в сети Интернет не давайте согласия на установку на Вашем компьютере каких-либо дополнительных программ. Если Ваш браузер предлагает вам запустить или установить неизвестное Вам программное обеспечение – отвечайте отказом;

- Не работайте на компьютере под учетной записью с правами администратора. Учетная запись с правами администратора может использоваться только для установки и настройки системы Интернет-Банк;
- Не используйте компьютер, с которого производится работа с системой Интернет-Банк, для посещения других Интернет-сайтов. Использование компьютера для посещения посторонних Интернет-ресурсов значительно повышает риск его заражения вредоносными программами;
- Не допускайте установку на компьютер программ удаленного управления (Team Viewer, Ammyy Admin, Remote Administrator, VNC и т.п.), заблокируйте на нем работу встроенного сервиса удаленного доступа к рабочему столу;
- Блокируйте компьютер в случае покидания рабочего места (даже кратковременного); в случае длительного отсутствия и по окончании рабочего дня выключайте компьютер;
- Проверяйте подлинность сайта, на котором Вы осуществляете работу с системой Интернет-Банк. Часто мошенники делают сайты, внешне похожие на сайт Банка, но имеющие другой (отличающийся на одну-две буквы) адрес;
- Ограничьте физический доступ к компьютерам, с которых осуществляется работа с ПО системы Интернет-Банк, не допускайте его использование посторонними лицами;
- Не пользуйтесь системой Интернет-Банк в интернет-кафе, а также там, где Вы не уверены в безопасности компьютеров;
- Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте сотрудникам Банка обо всех подозрительных или несанкционированных операциях;
- При возникновении любых подозрений на компрометацию (возможность ознакомления с ключевыми материалами постороннего человека) секретных ключей электронной подписи, при утрате ключевого носителя или обнаружении неизвестных Вам операций по счету – незамедлительно сообщите в Банк и заблокируйте доступ к системе Интернет-Банк.

Хищение денежных средств с расчетного счета возможно при получении злоумышленниками доступа к секретным ключам электронной подписи (ЭП) и паролям с целью направления в Банк платежных поручений, заверенных от Вашего лица **похищенным ключом ЭП**. Таким образом, в Банк могут поступать не вызывающие подозрений платежи, направленные злоумышленниками с использованием корректных и действующих секретных ключей ЭП Клиента, имеющие вполне обычные реквизиты получателей и типовые назначения платежа. И правомерное, в данном случае, исполнение таких платежей Банком приведёт к хищению денежных средств с Вашего расчетного счета.

Важно понимать, что Банк не имеет доступа к Вашим секретным ключам ЭП и не может от Вашего имени сформировать корректную ЭП под электронным платежным поручением. Вся ответственность за конфиденциальность Ваших секретных ключей ЭП полностью лежит на Вас, как единственных владельцах секретных ключей ЭП.

Для получения информации обращайтесь в Банк по телефонам:
8 499 968-94-23 или 8 800 770-79-20 (Бесплатный звонок по России).