Акционерное общество
"Сити Инвест Банк"

Сити Инвест Банк

Памятка по безопасному использованию системы «Интернет-Клиент»

Уважаемый клиент!

В связи с тем, что злоумышленники могут получить доступ к Вашему счету вследствие кражи Ваших учетных данных (логин, пароль) и ключей электронной подписи с помощью вредоносного программного обеспечения, распространяемого через Интернет, просим ознакомиться с рядом правил, которые позволят минимизировать риски при работе с системой «Интернет-Клиент» (далее - Система).

- не сообщать конфиденциальную информацию о номере счета, паспорта, логине, пароле и др. посторонним. Сотрудник банка имеет право запросить Вашу персональную информацию только в случае, если Вы сами звоните в банк по телефонам, указанным на сайте. Также обращаем Ваше внимание, что АО «Сити Инвест Банк» не высылает писем по электронной почте с целью уточнить персональную информацию о клиенте;

- не передавать физические носители электронной цифровой подписи лицам, не обладающим правом их использования;

- соблюдать правила информационной безопасности, использовать лицензионное программное обеспечение, а также постоянно обновлять персональные средства защиты (межсетевые экраны, антивирусное программное обеспечение), средства обнаружения вредоносных программ и используемую операционную систему;

- не открывать компьютерные файлы, полученные из ненадёжных источников;

- не сохранять ключи электронной цифровой подписи на жестких дисках компьютеров;

- не оставлять физические носители электронной цифровой подписи в компьютерах, в периоды времени, когда использование их не требуется;

- использовать сложные пароли, избегая легко угадываемые варианты;

- не записывать свой логин и пароль к Системе там, где они могут стать доступными посторонним лицам;

- стараться не работать с Системой с общедоступных компьютеров, например, в Интернет-кафе. Если Вам пришлось воспользоваться системой с компьютера общего пользования, поменяйте пароль с личного компьютера при первой же возможности;

- не отправлять конфиденциальную информацию о средствах доступа к Системе и/или движении Ваших денежных средств по электронной почте – стандартное сообщение электронной почты не шифруется;

- следить за своими операциями. Выписка по счетам, полученная через Систему, позволит Вам своевременно обнаружить и оперативно известить Банк об имеющихся несоответствиях;

- правильно завершать работу в Системе: воспользуйтесь пунктом меню «Выход».

Внимание! Если Вы утратили пароль или ключи для доступа к Системе, или Вам стало известно, что кто-либо получил доступ к вышеуказанным данным, пожалуйста, немедленно сообщите об этом в Банк по телефону (812) 324-06-71 . Возможность работы с Системой будет заблокирована до разрешения инцидента.

Как показывает практика, в подавляющем большинстве случаев кража учетных данных и ключей электронной цифровой подписи происходит вследствие заражения компьютеров, используемых при работе с Системой, вирусами, «специализирующимися» на краже ключей, логинов и паролей пользователей.

В связи с этим настоятельно рекомендуем на этих компьютерах:

- установить и настроить антивирусное программное обеспечение, осуществляющее постоянный мониторинг работы программ;
- производить периодическую проверку компьютера при помощи антивирусного программного обеспечения другого разработчика (например: в качестве основного антивируса используется **Антивирус Касперского для Windows Workstation**, а для периодической проверки используется утилита **Dr.Web CureIt!**)
- установить и настроить межсетевой экран (firewall), позволяющий оградить ваш компьютер от интернет-атак и предотвратить попытки вредоносных приложений передать данные с вашего компьютера;
- не подключать внешние носители информации, кроме носителей, содержащих ключи Системы.

Просим учесть, что гарантировать полную защищенность компьютера от заражения вирусами можно только в том случае, если:

- установка операционной системы произведена с носителя, гарантированно не содержащего вирусы (например с лицензионного диска, распространяемого в составе коробочного продукта компанией Microsoft);
- установлено и настроено антивирусное программное обеспечение;
- установлен и настроен межсетевой экран;
- доступ к считывателям информации с внешних носителей ограничен;
- работа в сети Интернет осуществляется исключительно с Системой;
- компьютер является изолированным (т.е. не подключен к локальной вычислительной сети).
-

Кроме этого, эффективной мерой защиты от несанкционированного использования Системы является механизм использования одноразовых паролей. Одноразовые пароли (One-Time Passwords, OTP) — динамическая аутентификационная информация, генерируемая для единичного использования. OTP неуязвим для атаки сетевого анализа пакетов, что является значительным преимуществом перед запоминаемыми паролями. Генерация OTP производится с помощью аппаратных автономных генераторов **OTP-Token -** мобильных персональных устройств. Каждый OTP-Token проходит привязку к определенному пользователю клиента. Порядок использования OTP-Token описан в *«Кратком руководстве пользователя по работе с генератором одноразовых паролей OTP-Token».*

Дополнительной мерой по обеспечению безопасности является использование функции определения параметров операций, которые могут осуществляться Клиентом с использованием Системы.

В частности, установление максимально допустимых сумм переводов денежных средств за одну операцию (за период), фиксация перечня устройств, с использованием которых может осуществиться доступ к Системе на основе идентификаторов указанных устройств, задание временного интервала, в который могут проводиться переводы денежных средств с использование Системы, помогут Вам минимизировать риски при работе с Системой. Задать указанные выше параметры Системы Вы можете при заключении договора о дистанционном банковском обслуживании клиентов с использованием системы «Интернет-Клиент».

Более детальную информацию по возможностям обеспечения безопасности при работе с Системой Вы можете получить в службе технической поддержки АО «Сити Инвест Банк» по телефонам: **8 (812) 324-06-71**, **8 (812) 324-06-90** или по электронной почте **support@cibank.ru**