***Рекомендации по защите информации при использовании систем электронного документооборота.***

В сети Интернет получили широкое распространение специализированные вредоносные программы (трояны), обеспечивающие возможность похищения у пользователей систем дистанционного банковского обслуживания (ДБО) персональных данных, проведения мошеннических операций в системе с целью кражи денежных средств и т.п. Трояны распространяются по открытым каналам сети Интернет через электронную почту, по каналам сервисов мгновенной передачи информации, через принадлежащие злоумышленникам сайты. При этом злоумышленники похищают пароли доступа к электронным ключам (АСП, ЭЦП, ЭП). В связи с этим Банк рекомендует:

1. При работе с системой ДБО не использовать параллельно иные ресурсы сети Интернет (социальные сети, электронную почту, ICQ-приложения, СКАЙП и т.п.);
2. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам;
3. Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением (операционная система, офисные приложения и т.п.);
4. Своевременно обновляйте установленные программное обеспечение и операционную систему (установка критичных обновлений безопасности);
5. Обязательно установите и своевременно обновляйте на компьютере антивирусное программное обеспечение, но помните, что 100% защиты не обеспечивает ни одна программа;
6. Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы и обновляться не реже 1 раза в день.
7. Рекомендуется полная ежедневная проверка компьютера на наличие вирусов, иного вредоносного программного обеспечения. При подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), следует воздержаться от использования систем ДБО до удостоверения в отсутствии на ПК вредоносного ПО.
8. Перед выходом в сеть Интернет для выполнения работы не связанной с использованием системы ДБО, необходимо выключить систему ДБО, извлечь из компьютера ключевой носитель и поместить его в надежное место хранения.
9. При работе в сети Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам сети Интернет, не соглашайтесь на установку каких-либо сомнительных программ, воздерживайтесь от использования программ онлайнового общения на компьютере, который используется для работы в системе ДБО.
10. Исключите возможность установки посторонними лицами (гостями, посетителями, приходящими программистами) на компьютер специальных «шпионских» программ. В частности, хорошей практикой является работа на компьютере от имени пользователя, не имеющего полномочий администратора.
11. Рекомендуем ограничить информационный обмен в сети Интернет только надёжными информационными порталами и проверенными корреспондентами электронной почты.

Важно знать, что часто под видом «интересной ссылки» в письме от якобы знакомого приходит вредоносная программа, запускаемая самим пользователем при первом нажатии на ссылку. Важно помнить, что вредоносная программа может скрываться под всплывающим окном рекламной ссылки на интересующем вас интернет-сайте.

***Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет*.**

Отнестись с особым вниманием к расчетам в сети Интернет. Будьте внимательны: сайты мошенников могут быть почти точной копией тех, через которые Вы планировали осуществить платеж. Они созданы специально для получения Ваших персональных данных и платежных реквизитов.

Если Вы обнаружили в сети Интернет подложные Web-сайты ЗАО «ИК Банк», с адресами, отличающимися от **http://tib.ru** прекратите работу с ними и обратитесь к техническим специалистам банка в Департамент информационных технологий ЗАО «ИК Банк» по телефону: **(843) 231-72-62.**

Разработка и реализация комплекса мер по обеспечению информационной безопасности - сложная задача, требующая непрерывной работы квалифицированных специалистов. Однако, соблюдение перечисленных простых мер позволяет существенно снизить риски, связанные с использованием систем ДБО, с осуществлением платежей в сети Интернет в конечном итоге, предотвратить хищение Ваших денежных средств.

***Рекомендации по снижению рисков получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.***

Пользователям систем ДБО необходимо использовать дополнительные организационные меры по обеспечению информационной безопасности:

1. Ключевые носители системы ДБО (дискета или флешка) должны храниться в сейфе, доступ к которому должен быть строго ограничен и предоставляться только уполномоченным лицам. Хорошей практикой является хранение вышеуказанных носителей в сейфе в опечатанном контейнере.
2. Не рекомендуется использовать компьютер, на котором развернута программа ДБО (далее -компьютер), для просмотра посторонних (не относящихся к системе ДБО) Интернет сайтов, работы с электронной почтой (особенно через общедоступные почтовые сервера: Mail.ru и т.д.), устанавливать игры и любые программы с пиратских дисков, просматривать видеофильмы, слушать музыку, загружать и устанавливать программы из Интернет, открывать и редактировать непроверенные антивирусом DOC, XLS, PDF файлы.
3. В случае временного перерыва в работе с компьютером (совещание, обед и т.д.) необходимо завершить работу с программой ДБО, убрать в сейф ключевой носитель, выключить компьютер или заблокировать доступ путем нажатия клавиш Ctrl-Alt-Del.
4. Запрещается записывать пароли на бумажных листках (или в текстовых файлах на компьютере), оставлять их в легкодоступных местах (на рабочем столе), передавать неуполномоченным лицам. Если есть необходимость – храните все пароли записанными на одном листе, в сейфе, в опечатанном конверте.
5. В случае любых кадровых перестановок лиц, имевших доступ к компьютеру и ключам, при подозрении в несанкционированном доступе (локально или по сети) неуполномоченных лиц к компьютеру, ключам, программе ДБО, паролям или других случаях компрометации системы ДБО Вам необходимо связаться со специалистами банка, сообщить название Вашей организации, номер счета и детально описать что произошло. Это позволит нам оперативно заблокировать доступ к Вашему счету через систему ДБО.