РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО)

14.01.2020 г. г. Махачкала

«О предоставлении рекомендаций
для клиентов системы ДБО «iBank2»»

В связи с необходимостью снижения рисков воздействия вредоносного кода и повышения уровня безопасности при работе с системой дистанционного банковского обслуживания «iBank2» (Интернет-банком) Комитет по информационной безопасности РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО) информирует клиентов системы ДБО «iBank2» о необходимости применения рекомендаций по защите информации от воздействия вредоносного кода (Приложение 1 к данному письму). В случае возникновения вопросов по применению рекомендаций просим Вас позвонить в Комитет по информационной безопасности по номеру 8 (8722) 51-70-44.

Председатель Правления **К.А.Абдурахманов**

Приложение 1
К информационному письму
«О предоставлении рекомендаций
для клиентов системы ДБО «iBank2»»

Рекомендации
Клиентам РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО) по защите информации при пользовании системой дистанционного банковского обслуживания «iBank2»

Рекомендации по защите информации от воздействия вредоносного кода

В сети Интернет получили широкое распространение специализированные вредоносные программы (трояны), обеспечивающие возможность похищения у пользователей систем дистанционного банковского обслуживания файлов с секретными ключами электронной подписи (ЭП) и пароли. Трояны распространяются через электронную почту, по каналам сервисов мгновенной передачи информации, через принадлежащие злоумышленникам сайты. При этом злоумышленники похищают ключи ЭП, пароли доступа, что позволяет совершать операции от имени клиента.

При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.

Своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений).

Обязательно установите и своевременно обновляйте на компьютере антивирусное программное обеспечение, но помните, что 100% защиты не обеспечивает ни одна программа.

Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы. Рекомендуется полная ежедневная проверка компьютера на наличие вирусов, иного вредоносного программного обеспечения. Исключить использование зараженного компьютера, вплоть до полного излечения от вирусов.

При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам сети Интернет.

При работе в сети Интернет не соглашайтесь на установку каких-либо сомнительных программ.

Воздерживайтесь от использования программ онлайнового общения на компьютере, использующемся для работы в системе дистанционного банковского обслуживания.

Исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер специальных «шпионских» программ. В частности, хорошей практикой является работа на компьютере от имени пользователя, не имеющего полномочий администратора.

Рекомендуем ограничить информационный обмен в сети Интернет только надёжными информационными порталами и проверенными корреспондентами электронной почты.

Важно знать, что надёжным средством обеспечения подлинности является электронная подпись, а не строка адреса браузера или электронной почты. Часто в виде «интересной ссылки» в письме от якобы знакомого приходит вредоносная программа. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте. Важно знать, что ни одна антивирусная программа не обеспечивает 100% защиты.

При подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), полностью воздержаться от использования систем дистанционного банковского обслуживания и проведения платежей до исправления ситуации.

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

Просим Вас 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.

Если Вы обнаружили в сети Интернет ложный Web-сайт РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО), отличный от https:\\www.psib.ru, или с Вами пытаются связаться по электронной почте или иным способом лица, с требованиями о предоставлении персональных идентификаторов доступа к системе дистанционного банковского обслуживания, просьба немедленно сообщить об этом в отдел внедрения и сопровождения программных средств РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО) по телефону: 8 (8722) 62-16-94.

В целом, разработка и реализация комплекса мер по обеспечению информационной безопасности - сложная задача, требующая непрерывной работы квалифицированных специалистов. Однако, соблюдение перечисленных простых «гигиенических» мер позволяет существенно снизить риски, связанные с использованием систем дистанционного банковского обслуживания, с осуществлением платежей в сети Интернет и, 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

При подключении к сети Интернет велика вероятность заражения используемого оборудования вредоносными программами, который распространены в сети и используются злоумышленниками для кражи у пользователей систем дистанционного банковского обслуживания файлов с секретными ключами электронной подписи (ЭП) и паролей. Использование лицензионного антивирусного программного обеспечения со своевременным автоматическим обновлением позволит существенно снизить риски потери защищаемой информации. Пользователям систем дистанционного банковского обслуживания необходимо использовать дополнительные организационные меры по обеспечению информационной безопасности:

1) Ключевые носители системы дистанционного банковского обслуживания (usb-токен) 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. Целостность печати (пломбы) должна ежедневно, в начале рабочего дня, контролироваться руководителем организации или уполномоченным лицом. После завершения работы ключевой носитель помещается в контейнер и заново опечатывается (пломбируется) уполномоченным лицом.

2) Не рекомендуется использовать компьютер, на котором развернута программа дистанционного банковского обслуживания (далее - компьютер), для просмотра посторонних (не относящихся к системе дистанционного банковского обслуживания) Интернет сайтов, работы с электронной почтой (особенно через общедоступные почтовые сервера, например, Mail.ru), 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) необходимо завершить работу с программой дистанционного банковского обслуживания, убрать в сейф ключевой носитель, выключить компьютер или заблокировать его клавиатуру и экран 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 дистанционного банковского обслуживания, паролям или других случаях компрометации системы дистанционного банковского обслуживания Вам необходимо связаться со специалистами кредитной организации, сообщить название Вашей организации, номер счета и детально описать, что произошло. Это позволит нам оперативно заблокировать доступ к Вашему счету через систему дистанционного банковского обслуживания.