Документ утвержден Приказом Председателя правления
Кредитного потребительского кооператива
«Союз банковских служащих»
Приказ №93 о/д от 25.07.2019

Рекомендации по защите информации от воздействия вредоносных кодов для получателей финансовых услуг КПК «СБС»

В целях выполнения требований Положения Банка России от 17 апреля 2019 г. N 684-П "Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций" Кредитный потребительский кооператив «Союз банковских служащих» (далее - Кооператив) доводит до получателей финансовых услуг Кооператива информацию о мерах по предотвращению несанкционированного доступа к защищаемой информации с целью осуществления финансовой операции лицами, не обладающими правом осуществления финансовой операции, а также приводит список рекомендаций по защите информации от воздействия вредоносного кода (компьютерные вирусы, «трояны», «руткиты» и т.п.), о мерах соблюдения информационной безопасности и способах предотвращения хищения.

Банк России отмечает участившиеся случаи несанкционированного доступа к защищаемой информации и широкое распространение специализированных вредоносных программ. И как следствие – осуществление незаконных финансовые операции, доступ к защищаемой информации, а также ее искажение, модификация, уничтожение, блокирование или несанкционированное копирование с использованием устройств мобильной связи (далее УМС) – мобильных телефонов, смартфонов, планшетов и т.п., без согласия лиц, обладающих правом осуществления финансовой операции или доступа к такой информации.

Получатели финансовых услуг Кооператива, использующие компьютеры и УМС для совершения действий в целях осуществления финансовых операции, необходимо учитывать следующие рекомендации для предотвращения случаев несанкционированного доступа:

Пароли

- Установите надежный пароль. Используйте, по возможности, биометрические данные для разблокировки экрана УМС;
- Используйте сложный пароль для входа: не рекомендуется использовать дату рождения, имя, фамилию и прочие часто используемые комбинации. Рекомендуется, чтобы пароль содержал латинские буквы верхнего и нижнего регистра, специальные символы и цифры. Минимум – 8 символов;
- Не сообщайте никому свое кодовое слово, кроме случаев, когда в организацию, осуществляющую финансовую услугу (далее – Организация), позвонили Вы сами по официальному телефону Организации;
- Не разглашайте пароли и коды подтверждения даже сотрудникам Организации. Пароли и коды подтверждения спрашивают только мошенники;
- Никогда не вводите пароли для отмены операции. Если вы с этим столкнулись, покиньте сайт и срочно обратитесь в Организацию.
- При любых подозрениях на компрометацию паролей (постоянных или разовых) посторонними лицами (в т.ч. представившимися сотрудниками Организации) или запросах на выполнение неинициированных Вами операций, следует незамедлительно обратиться в службу помощи Организации;
- Не сохраняйте пароли доступа и логины в памяти браузера, а вводите их заново.

Программы

- Используйте только лицензионное программное обеспечение;
- Используйте только официальные приложения Организаций;
- Не производите установку программного обеспечения из непроверенных источников;
- При установке приложений обращайте внимание на полномочия, которые они запрашивают. Будьте осторожны, если приложение просит права на чтение адресной книги, отправку SMS-сообщений и доступ к интернету — оно может быть опасным;
- Проводите регулярную установку обновлений программного обеспечения, по мере их выпуска производителем;
- Используйте антивирусную программу и регулярно проверяйте устройство на вирусы;
- Установите автоматическое обновление антивирусных баз и операционной системы УМС, компьютера и т.д.;
- Никогда не отключайте брандмауэр Windows;
- Используйте дополнительные средства защиты информации (межсетевые экраны и т. п.);
- Отключите режим автозапуска сменных носителей;
- Используйте для повседневной работы пользователя с ограниченными, минимальными правами. Не работайте на компьютере с правами администратора;
- Отключите на компьютере, с которого ведется работа, гостевые учетные записи и возможность дистанционного управления;
- На компьютере не должно быть учетных записей (пользователей) с пустыми паролями;
- Покидая рабочее место, необходимо блокировать компьютер (CTRL+ALT_DEL –> блокировать компьютер или сочетание клавиш WIN+L);
- Не оставляйте без присмотра работников сторонних организаций, которые производят сервисные работы на компьютере.

Работа в сети (рассылки, смс, звонки и т.д.)

- Убедитесь, что адресная строка сайтов начинается с префикса https://, это означает, что установлено защищенное соединение;
- Не посещайте интернет-ресурсы сомнительного содержания;
- Контролируйте состояние счёта путем просмотра выписки;
- Не открывайте подозрительные ссылки от неизвестных отправителей: мошенники могут заразить ваш компьютер или телефон вирусом и украсть ваши данные;
- Не устанавливайте приложения по ссылкам из СМС/ММС-сообщений или электронной почты, даже если в сообщении утверждается, что оно от Организации;
- При получении от близких или друзей сообщений с просьбой о финансовой помощи – свяжитесь с ними лично по телефону, не переводите деньги, пока не убедитесь, что просьба действительно исходит от них (сообщения могут быть результатом взлома аккаунта или вируса на телефоне);
- Используйте только надежные и проверенные точки Wi-Fi. Не рекомендуется подключаться к популярным и/или бесплатным точкам доступа Wi-Fi, если Вы не уверены в достоверности имени точки доступа. Обращаем Ваше внимание, что точки доступа Wi-Fi, для подключения к которым не требуется ввод пароля, могут представлять повышенную опасность в связи с возможными действиями мошенников, направленными на получение доступа к Вашим персональным данным. Специальные приложения применяют механизмы защиты своих данных при передаче, а так как публичные беспроводные сети сравнительно труднее контролировать, то у злоумышленников появляется больше возможностей для попыток обхода защитных механизмов. Для работы необходимо использовать подключение к сети Интернет через мобильного оператора или через доверенную защищенную беспроводную сеть;
- Будьте бдительны при получении сообщений или звонков, особенно если:

- Вы получили сообщение в СМС-мессенджере или по электронной почте о проведении или отмене операций, которых вы не совершали;
- Вас настойчиво и убедительно (с элементами жалости или запугивания) просят совершить действия, которые вы не планировали совершать или не понимаете их смысл;
- Если вам представляются работниками Организации и запрашивают коды и пароли из СМС якобы для отписки от услуг, аутентификации, отмены операции или разблокировки карты;

- Не совершайте необдуманные действия, не перезванивайте по номерам, указанным в сообщении, и не проводите действий в банкоматах и терминалах по инструкциям, полученным по телефону. Всегда уточняйте полученную информацию только по телефонам, указанным на оборотной стороне карты или на сайте банка (телефонам контактного центра).

Телефон, планшет (УМС) или компьютер

- Не рекомендуется оставлять своё УМС без присмотра и/или передавать его для использования третьим лицам, в том числе родственникам, т.к. на нём может быть совершён ряд действий, направленных на получение доступа к операционной системе, мобильному банку или перевод средств мошеннику. Например, злоумышленник может установить программное обеспечение с вредоносным кодом, настроить переадресацию СМС-сообщений на другое УМС, произвести перевод средств третьему лицу или оплату услуг;
- В случае изменения номера УМС не забывайте оповестить об этом Организацию. Контроль сообщений об операциях является одним из ключевых элементов безопасности. В случае внезапного приостановления работы сим-карты (блокировки сим-карты) необходимо в кратчайшие сроки обратиться к оператору мобильной связи и в Организацию, поскольку возможно изготовление злоумышленниками дубликата сим-карты;
- В случае утери (кражи, иного хищения) УМС следует незамедлительно сообщить оператору связи об утрате доступа к УМС для дальнейшей блокировки сим-карты, обратиться в правоохранительные органы. Также рекомендуется оповестить всех третьих лиц, оказывающих вам финансовые услуги посредством УМС, об утере (кражи, иного хищения) УМС для последующей блокировки доступа через данное УМС к каналам связи с такими лицами;
- В случае появления подозрения на заражение компьютера вредоносным кодом немедленно прекратите работу, извлеките носители ключей электронной подписи и проведите полную проверку устройства, проверку компьютера желательно проводить, произведя загрузку «чистой» операционной системы (с диска аварийного восстановления).

Помните, что Организация не несет ответственности в случае возникновения финансовых потерь, понесенных Клиентом в связи с нарушением и/или ненадлежащим исполнением им требований по защите от вредоносного кода своих автоматизированных рабочих мест (компьютера, ноутбука и т.д.) для доступа к системе дистанционного банковского обслуживания.

Председатель правления КПК «СБС» А.Ф. Фисунов