РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ КОДОВ

СКПК «Ссудо-Сберегательный Союз» (далее – Кооператив) предоставляет своим членам возможность получать информацию по договорам, заключенным с Кооперативом, и подавать заявки на заем через:

- Личный кабинет клиента на сайте Кооператива (далее - Личный кабинет);
- Личный кабинет в мобильном приложении Кооператива (далее - Мобильное приложение).

Использование Личного кабинета сопряжено с возможными рисками получения несанкционированного доступа к конфиденциальной информации лицами, не обладающими правом доступа к ней.

К конфиденциальной информации Клиента относятся:

- информация об остатках денежных средств по Договорам личных сбережений;
- информация об остатках задолженности по Договорам займов;
- информация ограниченного доступа, в том числе персональные данные и иная информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении деятельности Кооператива.

Ниже приведены рекомендуемые Кооперативом меры по снижению рисков получения несанкционированного доступа к конфиденциальной информации Клиента.

Важно! Передача другому лицу (в том числе работнику Кооператива) Логина и Пароля от Личного кабинета, предназначенной для доступа в Личный кабинет, предоставляет данному лицу доступ к конфиденциальной информации.

МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В ЛИЧНОМ КАБИНЕТЕ НА САЙТЕ КООПЕРАТИВА

Для входа в Личный кабинет требуется ввести Логин и Пароль. Для входа в Личный кабинет не требуется вводить никакой дополнительной информации.

Внимание! Если для входа в Личный кабинет предлагается дополнительно ввести любую другую информацию или дополнительные данные (данные платёжных карт, данные паспорта или иных документов, другую информацию), это указывает на мошенничество! В таких случаях необходимо немедленно прекратить сеанс работы в Личном кабинете и срочно обратиться в Кооператив по номерам, указанным на официальном сайте Кооператива.

При работе в Личном кабинете всегда проверяйте, что с сайтом установлено защищенное соединение: справа или слева (в зависимости от используемого Вами браузера) в адресной строке браузера должно быть изображение запертого замка, обозначающее наличие защищенного соединения.

Должны использоваться только надежные и проверенные точки доступа Wi-Fi. Не рекомендуется подключаться к популярным и/или бесплатным точкам доступа Wi-Fi. 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 конфиденциальной информации.

Для исключения компрометации конфиденциальной информации и хищения средств запрещено привязывать к Личному кабинету номер телефона, оформленное на другое лицо.

Запрещено устанавливать на устройства, которые используются для доступа к Личному кабинету, приложения, полученные по ссылкам от не проверенных или неизвестных источников.

Кооператив не рассылает ссылки или указания на установку приложений через сообщения SMS, Push, MMS или e-mail.

На всех устройствах, используемых для доступа к Личному кабинету (стационарный или переносной компьютер, мобильное устройство):

- должно использоваться современное антивирусное программное обеспечение и выполняться регулярное обновление баз данных (сигнатур);
- должна регулярно выполняться полная антивирусная проверка устройства для своевременного обнаружения вредоносных программ;
- должны своевременно устанавливаться обновления операционной системы, рекомендуемые компанией-производителем;
- должен осуществляться контроль конфигурации устройства и установленных приложений;
- по возможности, должно использоваться дополнительное лицензионное программное обеспечение, позволяющее повысить уровень защиты устройства: персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «СПАМ»-рассылок и пр.

Доступ в Личный кабинет должен завершаться путем выбора пункта «Выход» в меню.

МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В ЛИЧНОМ КАБИНЕТЕ В МОБИЛЬНОМ ПРИЛОЖЕНИИ КООПЕРАТИВА

При утрате мобильного устройства, на которое установлено Мобильное приложение, (далее Мобильное устройство) следует незамедлительно обратиться к оператору сотовой связи для блокировки SIM-карты и в Кооператив для приостановки доступа Мобильного приложения.

При смене номера телефона, зарегистрированного для доступа к Мобильному приложению, следует незамедлительно обратиться в Кооператив и сообщить о смене номера.

Оставленное без присмотра Мобильное устройство может привести к несанкционированному использованию Мобильного приложения или утечке конфиденциальной информации. По возможности, на Мобильном устройстве должен быть установлен пароль (графический ключ, TouchID, FaceID) для доступа к устройству.

Должно использоваться только официальное Мобильное приложение, доступное в официальных магазинах приложений производителей мобильных платформ. В поле «разработчик мобильного приложения» должен быть указан «Sintechno».

На Мобильном устройстве:

- должно использоваться современное антивирусное программное обеспечение и выполняться регулярное обновление баз данных (сигнатур);
- должна регулярно выполняться полная антивирусная проверка устройства для своевременного обнаружения вредоносных программ;
- должны своевременно устанавливаться обновления операционной системы, рекомендуемые компанией-производителем;
- не должны использоваться права «суперпользователя» (root), не предусмотренные компанией-разработчиком и отключающие защитные механизмы;
- должен осуществляться контроль конфигурации устройства и установленных приложений: не должны устанавливаться приложения, ссылки для установки которых пришли в SMS/Push/e-mail-сообщениях, в том числе, якобы, от имени Кооператива.

Работа в Мобильном приложении должна завершаться путем выбора пункта «Выход» в меню.