Рекомендации по защите информации

Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее – вредоносный код), в целях противодействия незаконным финансовым операциям.

ООО Сбережения плюс (далее – Организация) ставит своей целью обеспечить предоставление услуг на высоком и профессиональном уровне. Для автоматизации предоставления услуг используются информационные технологии. Информационные технологии несут в себе присущие им риски информационной безопасности. Организация доводит до сведения клиентов следующие рекомендации по защите информации, в том числе о мерах по предотвращению несанкционированного доступа к защищаемой информации, например, при утрате (потере, хищении) клиентом устройства, с использованием которого клиентами совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода:

1) Требования информационной безопасности отражены в документах, оформляемых для предоставления Организацией той или иной услуги. Внимательно ознакомьтесь с разделом, посвященным информационной безопасности. Указанные ниже рекомендации не гарантируют обеспечение защиты информации, однако позволят снизить риски киберугроз. Под устройством далее по тексту понимается любое устройство: компьютер, смартфон, ноутбук и т.д., удовлетворяющее требованиям Организации, для использования услуг удаленного доступа. Там, где речь идет именно о телефоне, явно в тексте используется термин «телефон».

2) Обеспечьте защиту устройства, с которого вы пользуетесь услугами Организации, к таким мерам включая, но не ограничиваясь могут быть отнесены:
   - Использование только лицензированного программного обеспечения, полученного из доверенных источников.
   - Запрет на установку программ из непроверенных источников.
   - Наличие средства защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран, шифрование, защита информации от потери и воровства и другие средства защиты информации.
   - Настройка прав доступа к устройству с целью предотвращения несанкционированного доступа.
   - Хранение, использование устройства с минимизацией риска кражи и/или утери устройства.
   - Своевременные обновления операционной системы, особенно в части обновлений безопасности. Имейте в виду, что обновления снижают риски заражения. Злоумышленники часто используют старые уязвимости.
   - Активация парольной или иной защиты для доступа к устройству.

3) Обеспечьте конфиденциальность:
   - Храните в тайне аутентификационные данные и ключевую информацию, полученные от Организации: пароли, СМС-коды, кодовые слова, закрытые ключи, сертификаты. В случае компрометации/подозрения на компрометацию таких данных, немедленно примите меры для их смены и/или блокировки.

4) Дополнительно:
   - Будьте осторожны при получении писем со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносным кодом. Вредоносный код, попав к Вам через почту или Интернет-ссылку на сайт, может получить доступ к любым данным и информационным системам на вашем устройстве.
   - Внимательно проверяйте адресата, от которого пришло письмо. Входящее письмо может быть от злоумышленника, который маскируется под Организацию или иных доверенных лиц.

- Будьте осторожны при просмотре/работе с интернет сайтами, так как вредоносный код может быть загружен с сайта.
- Будьте осторожны с файлами в архиве с паролем, так как в таком файле может быть вредоносный код.
- Не используйте системы и сервисы Организации на непроверенных устройствах, которые вы не контролируете. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию.
- Анализируйте информацию в прессе и на сайте Организации о последних критичных уязвимостях и о вредоносном коде.
- При наличии в рамках вашего продукта сервиса контактного центра, осуществляйте звонок только по номеру телефона, указанному в договоре. И имейте в виду, что от лица Организации не могут поступать звонки или сообщения, в которых от Вас требуют передать СМС-код, пароль, номер карты, кодовое слово и т.д.; Кодовое слово может быть запрошено только, если Вы сами позвонили в контактный центр.
- Имейте в виду, что если Вы передаете Ваш телефон и/или устройство другим лицам, они могу установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам и сервисам Организации, которыми пользовались Вы. В связи с этим при утере, краже телефона, используемого для получения СМС-кодов или доступа к системам и сервисам Организации с Мобильного приложения необходимо: 1) незамедлительно проинформировать Организацию через контактный центр, 2) целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить сим-карту, а также сменить пароль в Мобильное приложение.
- При подозрении на несанкционированный доступ и/или компрометацию устройства – необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Организацию.
- Помните, что наличие резервной копии может облегчить и ускорить восстановление Вашего устройства.
- Лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у Вас.
- Контролируйте свой телефон, используемый для получения СМС-кодов. В случае выхода из строя сим-карты, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи.
- Анализируйте выписки, остатки по Вашим счетам, выявляйте расхождения, в случае их наличия обращайтесь в Организацию для выяснения причин.