«УТВЕРЖДЕНО»
Приказом Генерального директора от «03» июля 2021 года
Общества с ограниченной ответственностью
Микрокредитная компания «ТВОИ ПЛЮС»

РЕКОМЕНДАЦИИ

по противодействию совершения незаконных финансовых операций при нарушении штатного функционирования средства вычислительной техники

1. Общие положения.

В соответствии с требованиями Положения Банка России от 20.04.2021 N 757-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" Общество с ограниченной ответственностью Микрокредитная компания «ТВОИ ПЛЮС» (далее по тексту – «Общество») доводит до Вашего сведения основные рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям.

Рекомендации по соблюдению информационной безопасности (совокупности мер, применение которых направлено на непосредственное обеспечение защиты информации, процессов, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты (здесь и далее термины из ГОСТ Р 57580.1-2017) не гарантируют обеспечение конфиденциальности, целостности и доступности информации, но позволяют в целом снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации.

В связи с тем, что требования информационной безопасности так же могут быть отражены в договорах, регламентах, правилах и иных документах Общества, регламентирующих предоставление услуг/сервисов, настоящие Рекомендации действуют в части, не противоречащей положениям внутренних документов.

2. Общие рекомендации.

В целях снижения риска реализации инцидентов информационной безопасности (ГОСТ Р 57580.1-2017) – нежелательные или неожиданные события защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов (клиента), технологических процессов Общества и (или) нарушить конфиденциальности, целостности и доступности информации вследствие:

- несанкционированного доступа к вашей информации лицами, не обладающими правом осуществления значимых (критичных) операций (в т.ч. финансовых);
- потери (хищения) носителей ключей электронной подписи, с использованием которых, осуществляются критичные (финансовые) операции;
- воздействия вредоносного кода на устройства, с которых совершаются критичные (финансовые) операции;
- совершения в отношении Вас иных противоправных действий, связанных с информационной безопасностью.

Рекомендуется соблюдать ряд профилактических мероприятий, направленных на повышение уровня информационной безопасности при использовании объектов информатизации (совокупности объектов, ресурсов, средств и систем обработки информации, в т.ч. автоматизированных систем, используемых для обеспечения информатизации бизнес-процессов (ГОСТ Р 57580.1-2017)) Общества. Внимательно изучите договор, приложения к договору и иные документы, связанные с исполнением договора, ознакомьтесь с разделами, посвященными информационной безопасности/конфиденциальности.

При использовании мобильного телефона рекомендуется придерживаться следующих советов:

- При взаимодействии с Обществом указывайте в качестве основного номера телефона номер, который принадлежит Вам лично (договор на услуги сотовой связи заключен на Ваше имя). Устанавливайте мобильное приложение Общества на телефонный аппарат, который принадлежит Вам и постоянно находится в Вашем распоряжении.
- Включите запрос кода-пароля SIM-карты при включении телефона.
- При поддержке телефоном соответствующей функции, выполните следующие действия:
  1) Включите блокирование экрана телефона после определенного времени неактивности.
  2) Включите запрос кода-пароля телефона, отпечатка пальца или графического ключа для

разблокирования телефона.

3) Установите запрет на отображение информации из вновь поступивших сообщений на экране блокировки.
4) Включите и настройте функцию поиска, удаленного блокирования и удаленной очистки потерянного телефона.
5) Установите запрет на установку в телефон приложений из ненадежных источников.

- При установке новых приложений на телефон обращайте внимание на запрашиваемые ими разрешения. Не давайте приложениям разрешение на чтение СМС, если такой доступ не нужен им для выполнения их основных функций.
- Не переходите по ссылкам из СМС сообщений, если Вы не ждали такие сообщения.
- Регулярно обновляйте операционную систему телефона и установленные в телефоне приложения (не отключайте автоматическое обновление).
- В случае утраты телефона воспользуйтесь функцией поиска телефона, если ранее ее активировали. Если с использованием функции поиска найти телефон не удалось или Вы ранее не активировали эту функцию, обратитесь с паспортом в офис своего сотового оператора для блокирования утерянной вместе с телефоном СИМ-карты и выпуска новой.
- Если на утерянном телефоне установлено мобильное приложение Общества, дополнительно к действиям, указанным в предыдущем абзаце, с любого телефона обратитесь на горячую линию Общества по номеру телефона 88003338652, 88124263717 и попросите оператора «отвязать» утерянный телефон от вашей учетной записи в системе дистанционного обслуживания.

3. Защита от вирусов

Вирусы – это программы для компьютеров или мобильных устройств, предназначенные для нанесения вреда.

Функционал вирусов может быть разным: показ нежелательной рекламы, кража паролей (в том числе, из СМС-сообщений) и данных банковских карт, совершение незаконных финансовых операций от имени клиента.

Практически все вирусы имеют функцию собственного распространения или заражения всех доступных им устройств.

Отсутствие вирусов на устройствах (компьютерах, сотовых телефонах, планшетах), с которых Вы работаете с системами дистанционного обслуживания Общества, является залогом безопасности Ваших денежных средств.

Во избежание заражения вирусами Вашего компьютера, следуйте таким советам:

1) Регулярно обновляйте операционную систему и установленные в ней приложения (включите автоматическое обновление).
2) Установите и регулярно обновляйте (не отключайте автоматическое обновление) антивирусную программу.
3) Не открывайте файлы и не переходите по ссылкам, пришедшим в сообщениях электронной почты, служб мгновенных сообщений (Skype, WhatsApp, Viber и т.п.) и социальных сетей, которые Вы не ждете.
4) Проверяйте антивирусной программой файлы, полученные из Интернет или со съемных носителей («USB-накопителей») до их использования.

Во избежание заражения вирусами Вашего мобильного устройства:

1) Регулярно обновляйте операционную систему и установленные в ней приложения (не отключайте автоматическое обновление).
2) Не открывайте файлы и не переходите по ссылкам, пришедшим в сообщениях электронной почты, служб мгновенных сообщений (Skype, WhatsApp, Viber и т.п.) и социальных сетей, которые Вы не ждете.
3) Установите запрет на установку в телефон приложений из ненадежных источников.

Генеральный директор
ООО МКК «ТВОИ ПЛЮС»
Брюквин С. В.