РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

(в соответствии с требованиями п.2 Положения ЦБ № 684-П)

В целях снижения риска реализации инцидентов информационной безопасности, которые могут привести к риску нарушения выполнения финансовых операций (клиента), технологических процессов Фонда и (или) нарушить конфиденциальность, целостность и доступность информации, следует принимать во внимание риск несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

Противоправные действия третьих лиц с целью реализации несанкционированного доступа к защищаемой информации и ее использования в корыстных целях:

- кража пароля и идентификатора доступа или иных конфиденциальных данных, например, CVV\CVC номера карты, ключей электронной подписи/шифрования посредством технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств;

- установка на устройство вредоносного кода, который позволит злоумышленникам осуществить финансовые операции от Вашего имени;

- кража или несанкционированный доступ к устройству, с которого Вы пользуетесь услугами/сервисами Фонда для получения данных и/или несанкционированного доступа к сервисам Фонда с этого устройства;

- получение пароля и идентификатора доступа и/или кодового слова и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником Фонда или техническим специалистом или использует иную легенду и просит Вас сообщить ему эти секретные данные, или направляет поддельные сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;

- перехват электронных сообщений и получение несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если Ваша электронная почта используется для информационного обмена с Фондом, а также получение доступа к вашей электронной почте, отправка сообщений от вашего имени в Фонд.

В связи с этим, рекомендуется соблюдать ряд профилактических мероприятий, направленных на повышение уровня информационной безопасности при использовании информационных систем для ведения бизнес-процессов Фонда.

1. Снижение риска финансовых потерь

1.1 Обеспечение защиты устройства, с которого Вы пользуетесь услугами Фонда.

К таким мерам могут быть отнесены:

- использование только лицензионного программного обеспечения, полученного из доверенных источников;
- запрет на установку программ из непроверенных источников;
- наличие средств защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран;
- настройка прав доступа к устройству с целью предотвращения несанкционированного доступа;
- хранение, использование устройства с целью избежать рисков кражи и/или утери;
- своевременные обновления операционной системы, особенно в части обновлений безопасности. Своевременные обновления снижают риски заражения вредоносным кодом;
- активация парольной или иной защиты для доступа к устройству.

1.2 Обеспечение конфиденциальности:

- хранение в тайне аутентификационных/идентификационных данных и ключевой информации, полученной от Фонда: пароли, кодовые слова, ключи электронной подписи/шифрования; в случае их компрометации необходимо немедленно принять меры для их смены и/или блокировки;
- соблюдение принципа разумного раскрытия информации о номерах счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVC\CVV кодах. В случае если у вас запрашивают указанную информацию в привязке к сервисам Фонда, по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через контактный телефон Фонда.

1.3 Проявление осторожности и предусмотрительности:

- будьте осторожны при получении электронных писем со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносным кодом. Вредоносный код, попав к Вам через электронную почту или интернет ссылку на сайт, может получить доступ к любым данным и информационным системам на Вашем устройстве;
- внимательно проверяйте адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под Фонд 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 из «незнакомых» источников (в т.ч. архивы с паролем, зашифрованные файлы/архивы), т.к. такого рода файлы не могут быть проверены антивирусным ПО в автоматическом режиме;

- при наличии контактного телефона, осуществляйте звонок только по данному номеру телефона или по номеру телефона, указанному в договоре или на официальном сайте Фонда.

- помните, что если Вы передаете Ваш телефон другим пользователям, они могут установить на него вредоносный код, а в случае кражи или утери телефона злоумышленники могут воспользоваться им для доступа к системам Фонда, которыми пользовались Вы.

2. Базовые меры безопасности при работе на компьютере:

- использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и т.д.);

- своевременно устанавливать актуальные обновления безопасности (операционных систем, офисных пакетов и т.д.);

- использовать антивирусное программное обеспечение, регулярно обновлять антивирусные базы;

- использовать сложные пароли при доступах к аппаратно-программным средствам.