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

Информация о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления:

1) Несанкционированный доступ к устройствам (т.е. любому техническому средству, включая, но, не ограничиваясь, компьютер, ноутбук, планшет, мобильный телефон, с помощью которого клиент может взаимодействовать с Фондом (далее – Устройства), влечет риск получения третьими лицами несанкционируемого доступа к защищаемой информации.

2) Несакционированный доступ со стороны третьих лиц к защищаемой информации может повлечь за собой риски разглашения конфиденциальной информации: персональных данных клиента, сведений об операциях, о состоянии счета, другой значимой информации.

3) Несакционированный доступ со стороны третьих лиц к защищаемой информации может повлечь совершение такими третьими лицами юридически значимых действий, включая, но, не ограничиваясь, совершение финансовых операций от имени клиента, изменений регистрационных данных клиента, и иных действий, совершенных без воли клиента, и направленных против его интересов.

Информация о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.

При использовании программного обеспечения на Устройствах рекомендуется:

1) Использовать на Устройствах антивирусное программное обеспечение (ПО), поддерживать версию антивирусного ПО и входящих в его состав баз вирусных определений в актуальном состоянии.
2) Регулярно проводить полную проверку Устройств на вирусы и вредоносный код.
3) Прекратить использование Устройства в случае обнаружения вирусов и вредоносного кода, до момента полного удаления вирусов и вредоносного кода.
4) Использовать программное обеспечение, которое отслеживает и борется с программой Spyware. Spyware — вид программного обеспечения, которое пытается запомнить ваши клавиатурные последовательности и передать их третьим лицам.
5) Использовать firewall при входе в Интернет или установить персональный firewall на вашем компьютере.

Использовать на Устройствах исключительно лицензионное ПО и операционные системы:

1) Регулярно устанавливать обновления безопасности ПО и операционной системы, используемых на Устройствах.
2) Не использовать на Устройствах ПО неизвестных разработчиков, которые не гарантируют отсутствие скрытых возможностей по сбору информации с устройств.
3) Исключить использование средств удаленного администрирования на Устройствах.

В целях безопасности использования паролей рекомендуется:

1) Выбирать пароли самостоятельно. Проводить регулярную смену паролей.

2) Использовать сложные пароли, требующие ввода заглавных и прописных букв, цифр и специальных символов, в общем количестве не менее 8 символов. Не рекомендуется в качестве паролей использовать имена близких лиц, домашних животных, даты рождения и т.п., которые могут быть легко подобраны злоумышленниками.
3) Не сохранять пароли в текстовых файлах на Устройстве либо иных электронных носителях.
4) Не хранить пароль совместно с Устройством.
5) Не передавать третьим лицам пароли, коды доступа к Устройству.
6) Не использовать функцию запоминания логина и пароля в браузерах, так как эти данные могут быть скомпрометированы.
7) Совершать операции только с личного Устройства в целях сохранения конфиденциальности персональных данных и иной защищаемой информации.

Соблюдение правил безопасности в сети Интернет:

1) При работе с Устройством в сети Интернет удостовериться в том, что сертификат безопасности сайта действителен, а соединение происходит в защищенном режиме (адресная строка браузера начинается с https, либо используется значок в виде замка).
2) При наличии на Устройстве программ фильтрации сетевого трафика (брандмауэра) держать его включённым и блокировать все незнакомые или подозрительные подключения.
3) Не отвечать на подозрительные сообщения, полученные с неизвестных адресов.
4) Не устанавливать и не сохранять подозрительные файлы, программы, полученные из ненадежных источников, скаченные с неизвестных сайтов в сети Интернет, присланные с неизвестных адресов электронной почты.
5) Не открывать и не использовать сомнительные Интернет - ресурсы на Устройстве.

Осуществление контроля подключения:

1) Не работать с Устройств, использующих подключение к общедоступной wi-fi сети.

Дополнительные рекомендации:

1) Для связи с Фондом по телефону и e-mail необходимо использовать контактные данные, указанные на официальном сайте Фонда в сети Интернет.
2) Не передавать никакой персональной и иной информации конфиденциального характера при получении писем по электронной почте от якобы представителей Фонда и иных финансовых организаций, если получение таких писем инициировано не Вами, не переходите по ссылкам в таких письмах, не открывайте вложенные приложения (такие ресурсы могут содержать вредоносное программное обеспечение), не звоните по телефонам, указанным в подобных письмах, и не отвечайте на них. Для связи используйте номера телефонов, адреса электронной почты, формы обратной связи, указанные на официальном сайте Фонда.