АО УК «ИНВЕСТСТРОЙ» (Лицензия на осуществление деятельности по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами от 26 октября 2010 года №21-000-1-00766) при осуществлении основной деятельности взаимодействует с пайщиками закрытых паевых инвестиционных фондов, и в силу особенностей вида лицензируемой деятельности, не использует дистанционных способов проведения финансовых операций пайщиков.

В рамках работы по обеспечению информационной безопасности АО УК «ИНВЕСТСТРОЙ» напоминаем пользователям сайта о необходимости следовать общим рекомендациям:

- Использовать на рабочем месте исключительно лицензионное программное обеспечение.

- Устанавливать все необходимые обновления безопасности, рекомендуемые производителем программного обеспечения, устанавливать запрет на установку программ из непроверенных источников.

- Устанавливать и регулярно обновлять лицензионное антивирусное программное обеспечение, регулярно проводить проверку на отсутствие вирусов.

- Не загружать приложения и данные из непроверенных источников, не посещать сайты сомнительного содержания.

- Не сообщать персональные данные (паспортные данные и иную информацию) лицам, которые путем обмана и (или) злоупотребления доверием, представляются сотрудниками или техническими специалистами АО УК «ИНВЕСТСТРОЙ», или используют иную легенду и просят Вас сообщить персональные данные, или направляют поддельные сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к негативным последствиям. По возможности оценивать ситуацию и уточнять полномочия и процедуру через независимый канал, например, по телефону АО УК «ИНВЕСТСТРОЙ», указанный на официальном сайте в сети Интернет по адресу http://www.investural.ru/

- Внимательно проверять адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под представителей АО УК «ИНВЕСТСТРОЙ» или иных доверенных лиц.

- Соблюдать принцип разумного раскрытия личной информации. Не вводить персональную информацию на подозрительных сайтах и других неизвестных ресурсах.

- Ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

- Обеспечить парольную защиту доступа к устройству. Использовать сложные пароли. В пароле не должны использоваться легко вычисляемые сочетания символов (например, последовательно расположенные на клавиатуре символы: «12345678», «QWERTY», имена, фамилии, номера телефонов, даты и т.п.), а также общепринятые сокращения («ИС», «USER» и т.п.).

- Следить за информацией в прессе о последних критичных уязвимостях и о вредоносном коде.

- Установить лицензионное антивирусное программное обеспечение, которое должно регулярно обновляться производителем. Осуществлять регулярный контроль его функционирования и не отключать ни при каких обстоятельствах. В случае возникновения подозрения на наличие на устройстве вредоносного программного обеспечения приостановить работу с финансовой информацией до устранения проблем и полного удаления вируса.

- Исключить использование средств удаленного администрирования на Вашем ПК (TeamViewer, AnyDesk и т.п.).

- Не открывать письма, полученные по электронной почте от неизвестных отправителей, не переходить по содержащимся в них ссылкам и не активировать вложения. Проявлять бдительность по отношению к письмам с вложениями и ссылками, даже если отправитель вам известен. Не отвечать на сообщения/звонки, в которых запрашиваются личные сведения, а также не вводить персональную информацию на подозрительных сайтах и других неизвестных Вам ресурсах.

- Помнить, что наличие резервной копии дисков может облегчить и ускорить восстановление технического устройства.

- При подозрении на несанкционированный доступ и (или) компрометацию устройства сменить пароль, воспользовавшись другим доверенным устройством и (или) заблокировать доступ.

Рекомендации по соблюдению информационной безопасности 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. Информация, связанная с деятельностью АО УК «ИНВЕСТСТРОЙ» предоставляется по адресу: 620000, Екатеринбург, ул. Февральской революции, д. 15 и публикуется в сети Интернет по адресу: http://www.investural.ru/