Альфа НПФ

Рекомендации по защите информации в целях противодействия незаконным финансовым операциям и своевременному обнаружению воздействия вредоносного кода

Фонд принимает все необходимые и достаточные организационные и технические меры для защиты персональных данных клиентов от неправомерного или случайного доступа, их уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий с ними третьих лиц.

При пользовании порталом пользователям необходимо помнить о возможных рисках несанкционированного доступа к обрабатываемой в нем информации и соблюдать рекомендуемые Фондом меры по снижению рисков получения несанкционированного доступа к конфиденциальной информации.

Меры, позволяющие снизить риски 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.

1. Используйте официальный сайт, расположенный по адресу: https://alfanpf.ru Внимательно проверяйте адрес сайта при его посещении, злоумышленники создают копии сайта для кражи ваших персональных данных и денежных средств (фишинговые сайты). Примеры поддельных сайтов: https://alfanpr.ru, https://alfnpf.ru. Обращайте внимание на наличие безопасного соединения. В адресной строке браузера должен быть указан протокол https.
2. Используйте антивирусные программы.

   Используйте на Ваших компьютерах и мобильных устройствах антивирусные программы (при наличии технической возможности). Своевременное обновление антивирусных баз повышает шанс обезопасить Ваши устройства от вредоносных программ. Регулярно выполняйте полную антивирусную проверку устройств.
3. Своевременно устанавливайте обновления операционной системы, рекомендуемые производителем.
4. Используйте только надежные и проверенные точки доступа Wi-Fi.

   Не используйте сомнительные или общедоступные точки доступа Wi-Fi, для подключения к которым не требуется ввод пароля.
5. Обеспечивайте безопасность пароля.

   Используйте надежные пароли от личного кабинета клиента. При формировании пароля рекомендуется использовать буквы верхнего и нижнего регистров, цифры, специальные символы. Используйте пароли длиной не менее 8 символов. периодически меняйте пароль на новый (не реже одного раза в год). Не передавайте третьим лицам пароли и коды подтверждения из смс. Не храните пароли в блокнотах, ежедневниках и на других бумажных носителях, а также в заметках на мобильных устройствах.

При любых подозрениях на мошенничество, следует незамедлительно обратиться в Контактный центр Фонда по телефонным номерам, указанным на официальном сайте Фонда.