Рекомендации по защите информации
в целях противодействия незаконным финансовым операциям

Акционерное общество «Негосударственный пенсионный фонд «Первый промышленный альянс» (далее – Фонд) в соответствии с требованиями Положения Банка России от 17.04.2019 № 684-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» информирует:

- о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

- 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[1].

1. Риски получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

Любой дистанционный способ взаимодействия в сети Интернет связан с риском получения третьими лицами несанкционированного доступа к персональной информации клиента и риском совершения несанкционированных клиентом операций.

[1] Вредоносный код - программный код, приводящий к нарушению штатного функционирования средства вычислительной техники

2. Меры 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.

Для предотвращения указанных рисков необходимо соблюдать несколько важных правил:

- никому не раскрывайте Ваши аутентификационные данные (логины, пароли и т.п.) и не храните их на устройстве в открытом виде;
- используйте разные уникальные пароли для различных web-сайтов и систем, на которых вводите конфиденциальные данные, регулярно меняйте пароли для работы со своими учетными данными;
- не храните учетные записи и пароли в местах, где они могут стать легкой добычей мошенников;
- свои персональные данные предоставляйте только доверенным организациям и только в случаях, когда Вам понятна цель передачи персональных данных и условия их обработки, а также Вами подписано согласие на обработку персональных данных;
- устанавливайте на устройство только лицензионное программное обеспечение;
- регулярно устанавливайте исправления и обновления, чтобы обеспечить актуальность программ, особенно в части обновлений безопасности - обновления снижают риски заражения вредоносным кодом, злоумышленники часто используют старые уязвимости;
- обязательно установите и своевременно обновляйте на устройстве средства антивирусной защиты;
- никому не передавайте устройство, так как незаметно от Вас на него может быть установлен вредоносный код;

- при работе в сети Интернет не соглашайтесь на установку каких-либо сомнительных программ;

- регулярно создавайте резервные копии устройства и храните их на отдельных доверенных носителях информации;

- при работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам. Настройте их автоматическую проверку антивирусом при получении;

- ограничьте информационный обмен в сети Интернет только надежными информационными порталами и проверенными корреспондентами электронной почты;

- внимательно проверяйте адрес электронной почты отправителя электронного письма. Злоумышленники могут маскироваться под доверенных отправителей изменяя одну или несколько букв в адресе электронной почты;

- не используйте общедоступные wi-fi сети при осуществлении финансовых операций.

В случае утраты (потери, хищении) устройства незамедлительно измените пароли для работы со своими учетными данными. При наличии технической возможности включите шифрование данных на устройстве.

Также если к данному устройству были привязаны банковские карты, незамедлительно обратитесь в банк для их блокировки и дальнейшей замены.