РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНОГО КОДА В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ ФИНАНСОВЫМ ОПЕРАЦИЯМ

В рамках Договора с АО НПФ «Пенсионные решения» (далее - Фонд) клиентам Фонда (далее – Участники) предоставляется возможность оформлять заявления и получать информацию по счетам через Личный кабинет клиента на сайте Фонда (далее - Личный кабинет).

Использование Личного кабинета сопряжено с возможными рисками получения несанкционированного доступа к конфиденциальной информации лицами, не обладающими правом доступа к ней.

К конфиденциальной информации Участника относятся:

- информация о балансе денежных средств на счетах;
- информация о совершенных перечислениях денежных средств;
- информация, содержащаяся в оформленных Участником заявлениях;
- информация ограниченного доступа, в том числе, персональные данные и иная информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении деятельности Фонда.

Уведомление Фонда об изменении и, соответственно, неактуальности обрабатываемых Фондом персональных данных клиента является обязанностью Участника. В случае изменения персональных данных, обрабатываемых Фондом, Участник или его представитель обязан уведомить об этом Фонд путем направления соответствующего обращения и предоставить в Фонд актуальные сведения.

Ниже приведены рекомендуемые Фондом меры по снижению рисков получения несанкционированного доступа к конфиденциальной информации Клиента.

Важно! Передача другому лицу (в том числе, работнику Фонда) СМС-кодов от Личного кабинета или иной контрольной информации, предназначенной для доступа и подтверждения операций через Личный кабинет, предоставляет данному лицу доступ к конфиденциальной информации и возможность оформлять заявления в Фонд.

При любых подозрениях на мошенничество (получение от Фонда SMS/Push/e-mail-сообщения о якобы совершенной операции или SMS/Push/e-mail-сообщение, которое вызывает сомнения), следует незамедлительно обратиться в Фонд по номерам телефонов, указанных на официальном сайте Фонда:

Для звонков из Москвы

+7 495 933-47-66

Для звонков из других регионов России

8 800 200-47-66

МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В ЛИЧНОМ КАБИНЕТЕ НА САЙТЕ ФОНДА

Для первичного входа в Личный кабинет требуется ввести номер телефона и паспортные данные Участника.

Для повторного входа в Личный кабинет требуется ввести только номер телефона и полученное на него смс с разовым паролем.

Внимание! Если для повторного входа в Личный кабинет предлагается дополнительно ввести любую другую информацию или дополнительные данные (данные платёжных карт, данные паспорта или иных документов, другую информацию), это указывает на мошенничество! В таких случаях необходимо немедленно прекратить сеанс работы в Личном кабинете и срочно обратиться в Фонд по номерам, указанным на официальном сайте Фонда:

Для звонков из Москвы

+7 495 933-47-66

Для звонков из других регионов России

8 800 200-47-66

При работе в Личном кабинете всегда проверяйте, что с сайтом установлено защищенное соединение (https://npfpens.ru/lk/login): справа или слева (в зависимости от используемого Вами браузера) в адресной строке браузера должно быть изображение запертого замка, обозначающее наличие защищенного соединения.
Должны использоваться только надежные и проверенные точки доступа Wi-Fi. Не рекомендуется подключаться к популярным и/или бесплатным точкам доступа Wi-Fi. Точки доступа Wi-Fi, для подключения к которым не требуется ввод пароля, могут представлять повышенную опасность в связи с возможными действиями мошенников, направленными на получение доступа к конфиденциальной информации.

Для исключения компрометации конфиденциальной информации и хищения средств, запрещено подключать к услугам Фонда номера телефонов, оформленные на другое лицо.

Запрещено устанавливать на устройства, которые используются для доступа к Личному кабинету, приложения, полученные по ссылкам от непроверенных или неизвестных источников.

Фонд не рассылает ссылки или указания на установку приложений через сообщения SMS, Push, MMS или e-mail.
На всех устройствах, используемых для доступа к Личному кабинету (стационарный или переносной компьютер, мобильное устройство):

- должно использоваться современное антивирусное программное обеспечение и выполняться регулярное обновление баз данных (сигнатур);
- должна регулярно выполняться полная антивирусная проверка устройства для своевременного обнаружения вредоносных программ;
- должны своевременно устанавливаться обновления операционной системы, рекомендуемые компанией - производителем;
- должен осуществляться контроль конфигурации устройства и установленных приложений;
- по возможности, должно использоваться дополнительное лицензионное программное обеспечение, позволяющее повысить уровень защиты устройства: персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «СПАМ»-рассылок и пр.

Доступ в Личный кабинет должен завершаться путем выбора пункта «Выйти» в меню.

На Мобильном устройстве:

- должно использоваться современное антивирусное программное обеспечение и выполняться регулярное обновление баз данных (сигнатур);
- должна регулярно выполняться полная антивирусная проверка устройства для своевременного обнаружения вредоносных программ;
- должны своевременно устанавливаться обновления операционной системы, рекомендуемые компанией-производителем;

- не должны использоваться права «суперпользователя» (root), не предусмотренные компанией-разработчиком и отключающие защитные механизмы;
- должен осуществляться контроль конфигурации устройства и установленных приложений: не должны устанавливаться приложения, ссылки для установки которых пришли в SMS/Push/e-mail-сообщениях, в том числе, якобы, от имени Фонда.

ЗАЩИТА ОТ SMS/PUSH/E-MAIL МОШЕННИЧЕСТВА

Мошеннические SMS/Push/e-mail сообщения, как правило, информируют о совершенном переводе (списании) денежных средств или содержат другую информацию, побуждающую перезвонить на указанный в SMS/Push/e-mail сообщении номер телефона, пройти по ссылке или открыть вложенный файл для уточнения информации. Зачастую такие сообщения замаскированы под официальные сообщения Фонда, а мошенники представляются сотрудниками службы безопасности или специалистами службы технической поддержки Фонда и в убедительной форме предлагают срочно провести какие-либо действия или предоставить конфиденциальную информацию.

В случае получения подозрительных SMS/Push/e-mail сообщений запрещено:

- перезванивать на номера телефонов, проходить по ссылкам, указанным в подозрительном сообщении, или открывать прилагаемые файлы и архивы;
- предоставлять конфиденциальную информацию (Фамилия, Имя, Отчество, данные паспорта или иных документов, реквизиты платёжных карт (номер карты, срок ее действия, ПИН, CVV2/CVC2/ППК2), Контрольная информация, Логин (Идентификатор пользователя) и Пароль от Личного кабинета), в том числе, посредством направления ответных SMS/Push/e-mail сообщений.

Следует незамедлительно обратиться в Фонд по номерам телефонов, размещенных на официальном сайте Фонда:

Для звонков из Москвы
+7 495 933-47-66

Для звонков из других регионов России

8 800 200-47-66

МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНОГО КОДА, ПРИВОДЯЩЕГО К НАРУШЕНИЮ ШТАТНОГО ФУНКЦИОНИРОВАНИЯ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ (ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ):

- Необходимо использовать технические устройства с лицензионным программным обеспечением;
- Необходимо своевременно устанавливать обновления для операционной системы, особенно относящиеся к обновлениям безопасности, это позволит снизить риски заражения вредоносным кодом;
- Необходимо установить и своевременно обновлять лицензионное антивирусное программное обеспечение с функцией автоматического обновления вирусных баз;
- Осуществляйте проверку жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода не реже одного раза в неделю;
- При работе с электронной почтой не следует открывать письма и вложения к ним, полученные от неизвестных отправителей, не следует переходить по содержащимся в таких письмах ссылкам, они могут привести к заражению устройства вредоносным кодом;
- Не следует заходить в системы удаленного доступа с недостоверных устройств, на таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;
- Следите за информацией в прессе о последних критичных уязвимостях и о вредоносном коде!

МЕРЫ БЕЗОПАСНОСТИ В СЛУЧАЕ УТЕРИ/КРАЖИ УСТРОЙСТВ, С КОТОРЫХ ОСУЩЕСТВЛЯЕТСЯ ДОСТУП К ЛИЧНОМУ КАБИНЕТУ

Утеря или кража устройств, с которых осуществляется вход в Личный кабинет, может нести угрозу несанкционированного доступа к нему и утечке персональных данных и/или другой чувствительной информации. В случае утери или кражи устройств, с которых выполнялся вход в Личный кабинет, следует незамедлительно обратиться в Фонд по номерам телефонов, размещенных на официальном сайте Фонда:

Для звонков из Москвы

+7 495 933-47-66

Для звонков из других регионов России

8 800 200-47-66