РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ ОСУЩЕСТВЛЕНИЮ НЕЗАКОННЫХ ФИНАНСОВЫХ ОПЕРАЦИЙ

При обслуживании клиентов, в том числе при совершении клиентами операций с использованием электронного сервиса «Личный кабинет» на официальном сайте Фонда в сети Интернет (далее – Личный кабинет), Фонд использует современные и наиболее эффективные механизмы обеспечения информационной безопасности.

Необходимо помнить, что Личный кабинет, как и любой другой дистанционный способ взаимодействия с использованием сети Интернет, характеризуется повышенным уровнем риска получения третьими лицами несанкционированного доступа к идентифицирующей клиента информации (логин, пароль, проверочные коды) с целью совершения операций в Личном кабинете (в том числе, риск получения третьим лицом информации об операциях клиента, риск совершения третьим лицом несанкционированных клиентом операций).

В целях минимизации указанных рисков и во избежание неблагоприятных последствий клиенту следует руководствоваться следующими мерами безопасности.

МЕРЫ ПО ПРЕДОТВРАЩЕНИЮ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ:

- ***Сохраняйте в тайне Ваши логин, пароль, проверочные коды***. Не сообщайте эти данные даже сотрудникам Фонда. Сотрудники Фонда никогда не будут запрашивать Ваши реквизиты доступа в Личный кабинет. ***Если Вам позвонили, представились сотрудником Фонда и попросили сообщить Ваши логин, пароль – это действия мошенников, прекращайте разговор***.
- Периодически ***меняйте пароль***, а при возникновении у Вас подозрений о том, что пароль стал известен третьим лицам – незамедлительно измените пароль.
- Используйте для доступа в Личный кабинет только ***личные/доверенные*** стационарные компьютеры, мобильные телефоны, смартфоны, планшетные компьютеры, ноутбуки на которых установлено современное антивирусное программное обеспечение. Избегайте работы в Личном кабинете с использованием «недоверенных» компьютеров (в Интернет-кафе или с других общедоступных компьютеров) или с использованием публичных беспроводных сетей (бесплатный Wi-Fi и т.д.).
- ***Не допускайте бесконтрольного доступа посторонних лиц к устройствам***, используемым Вами для доступа в Личный кабинет, не оставляйте без присмотра устройство с открытым Личным кабинетом. Не закрывайте интернет-браузер с открытым Личным кабинетом, предварительно не произведя выход из Личного кабинета.
- Перед каждым сеансом использования Личного кабинета ***внимательно проверяйте адрес главной страницы Личного кабинета***, он должен соответствовать – **https://client.npf-sng.ru.** Другие адреса являются ЛОЖНЫМИ и свидетельствуют о наличии мошеннических действий.
- Для авторизации в Личном кабинете указывайте в соответствующих полях логин, пароль и проверочный код. На странице авторизации не должно быть никаких иных полей для ввода дополнительной информации (например, номер пенсионного счета, номер СНИЛС, код в связи с неисправностью Личного кабинета и т.д.). Если Личный кабинет запрашивает дополнительные сведения – это является вероятным признаком того, что Вы работаете на поддельном сайте. Необходимо немедленно прекратить работу и сообщить

о данном факте по телефону 8 (3462) 55-01-31 добавочный 9301 или на электронную почту QSite@npf-sng.ru.

- В случае утраты (потери, хищении) устройства, с которого осуществлялся доступ в Личный кабинет, незамедлительно измените пароль в Личном кабинете. 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.
- Не отключайте встроенные механизмы обеспечения безопасности и своевременно отслеживайте конфигурацию устройства на наличие постороннего программного обеспечения.
- ***Если Вы получили SMS-сообщение или сообщение на электронную почту от неизвестного Вам лица, содержащее информацию о блокировке Вашего Личного кабинета, о списании/зачислении денежных средств по Вашему пенсионному счету, другую информацию с просьбой перезвонить по указанному номеру телефона, перейти по ссылке в электронном письме или сообщить какие-либо сведения – это действия мошенников. Не выполняйте данные указания! Обязательно проверяйте любую информацию относительно услуг Фонда, поступившую от неизвестных лиц***.

Номер телефона, используемый Фондом для рассылки SMS-сообщений:	***AO-NPF-SNG***
Адрес электронной почты, используемый Фондом для рассылки сообщений:	***client@npf-sng.ru***

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНОГО КОДА:

- Для совершения финансовых операций используйте только те устройства, на которых установлено современное антивирусное программное обеспечение, своевременно обновляйте антивирусные базы. Антивирусное программное обеспечение должно запускаться автоматически с загрузкой операционной системы. Проверка устройства на наличие вирусов должна выполняться ежедневно.
- Не устанавливайте на устройство программное обеспечение, предварительно не проверив его на наличие вредоносного кода с использованием антивирусного программного обеспечения.
- При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
- Ограничьте информационный обмен в сети Интернет только с надёжными интернет-ресурсами по защищенному протоколу https и проверенными корреспондентами электронной почты.
- Своевременно устанавливайте обновления безопасности системного и прикладного программного обеспечения.
- При подозрениях на наличие вирусов на персональном компьютере или мобильном устройстве (в частности, неожиданных «зависаниях», перезагрузках, повышенной сетевой активности), полностью воздержитесь от осуществления финансовых операций с использованием этих устройств до исправления ситуации.