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

В рамках Договора с АО «НПФ Сбербанка» (далее Фонд) клиентам Фонда предоставляется возможность совершать операции и получать информацию по счетам через Удаленные каналы обслуживания, к которым относятся:

- Личный кабинет клиента на сайте Фонда (далее Личный кабинет);
- Личный кабинет в мобильном приложении Фонда (далее Мобильное приложение).

Использование Удаленных каналов обслуживания сопряжено с возможными рисками получения несанкционированного доступа к конфиденциальной информации лицами, не обладающими правом доступа к ней. К конфиденциальной информации Клиента относятся:

- информация об остатках денежных средств на счетах;
- информация о совершенных перечислениях денежных средств;
- информация, содержащаяся в оформленных Клиентом распоряжениях;
- информация, необходимая для удостоверения Клиентами права распоряжения счетами;
- информация ограниченного доступа, в том числе персональные данные и иная информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении деятельности негосударственного пенсионного фонда.

Уведомление Фонда об изменении и, соответственно, неактуальности обрабатываемых Фондом персональных данных Клиента является обязанностью Клиента. В случае изменения персональных данных Клиента, обрабатываемых Фондом, Клиент или его представитель обязан уведомить об этом Фонд путем направления соответствующего обращения, в том числе в виде электронного документа через сервис Личного кабинета, и предоставить в Фонд актуальные сведения.

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

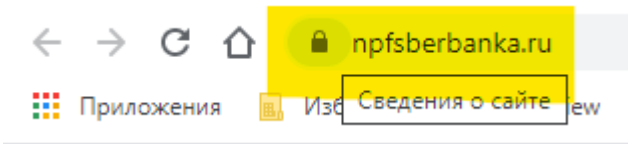
Важно! Передача другому лицу (в том числе работнику Фонда) Логина и Пароля от Личного кабинета, Сбербанк ID или иной контрольной информации, предназначенной для доступа и подтверждения операций через Удаленные каналы обслуживания, предоставляет данному лицу доступ к конфиденциальной информации и возможность проводить операции по счетам.

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 Контактный центр Фонда по номеру телефона, указанному на официальном сайте Фонда: **8 (800) 555-00-41**

МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В ЛИЧНОМ КАБИНЕТЕ НА САЙТЕ ФОНДА

Для входа в Личный кабинет требуется ввести Логин (Идентификатор пользователя) и Пароль. В качестве Логина могут использоваться номер мобильного телефона, адрес электронной почты или СНИЛС, указанные при заключении Договора. Также возможен вход с помощью Сбербанк ID или через портал ГосУслуг. Для входа в Личный кабинет не требуется вводить никакой дополнительной информации.

Внимание! Если для 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 номеру 8 (800) 555-00-41.



При работе в Личном кабинете всегда проверяйте, что с сайтом установлено защищенное соединение (https://lk.npfsb.ru, https://npfsberbanka.ru/): 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 не проверенных 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 «Выход» в меню.

МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В ЛИЧНОМ КАБИНЕТЕ В МОБИЛЬНОМ ПРИЛОЖЕНИИ ФОНДА

При утрате мобильного устройства, на которое установлено Мобильное приложение, (далее Мобильное устройство) следует незамедлительно обратиться к оператору сотовой связи для блокировки SIM-карты и в Контактный центр Фонда для приостановки доступа Мобильного приложения.

При внезапном прекращении работы SIM-карты следует незамедлительно обратиться к своему оператору сотовой связи за уточнением причин: в отношении Вас возможно осуществление мошеннических действий (несанкционированный перевыпуск SIM-карты).

При смене номера телефона, зарегистрированного для доступа к Мобильному приложению, следует незамедлительно обратиться в Фонд и сообщить о смене номера.

Оставленное без присмотра Мобильное устройство может привести к несанкционированному использованию Мобильного приложения или утечке конфиденциальной информации. По возможности, на Мобильном устройстве должен быть установлен пароль (графический ключ, TouchID, FaceID) для доступа к устройству.

Должно использоваться только официальное Мобильное приложение, доступное в официальных магазинах приложений производителей мобильных платформ. В поле «разработчик мобильного приложения» должен быть указан НПФ Сбербанка.

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.

Работа в Мобильном приложении должна завершаться путем выбора пункта «Выход» в меню.

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 контактный центр Фонда по номеру телефона, размещенному на официальном сайте Фонда: **8 (800) 555-00-41**