БОЛЬШОЙ

АКЦИОНЕРНОЕ ОБЩЕСТВО
МЕЖРЕГИОНАЛЬНЫЙ НЕГОСУДАРСТВЕННЫЙ
ПЕНСИОННЫЙ ФОНД

Рекомендации по соблюдению информационной безопасности клиентами АО МНПФ «БОЛЬШОЙ» в целях противодействия незаконным финансовым операциям

В соответствии с требованиями Положения Банка России от 20.04.2021 № 757-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» АО МНПФ «БОЛЬШОЙ» (далее – Фонд) доводит до сведения своих Клиентов рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям.

Рекомендации по соблюдению информационной безопасности не гарантируют обеспечение конфиденциальности, целостности и доступности информации, но позволяют снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации.

Фонд информирует своих клиентов о возможных рисках, связанных с получением третьими лицами несанкционированного доступа к конфиденциальной информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, и которые могут быть обусловлены, включая, но не ограничиваясь, следующими действиями:

- Кража или несанкционированный доступ к устройству, с которого Вы пользуетесь услугами/сервисами Фонда, и/или несанкционированный доступ к сервисам Фонда с этого устройства, что может повлечь за собой получение третьими лицами доступа к конфиденциальной информации;
- Кража пароля и идентификатора доступа или иных конфиденциальных данных, например, CVV/CVC номера карты, ключей электронной подписи/шифрования посредством технических средств и/или вредоносного кода; и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;
- Установка на устройство вредоносного кода, который позволит злоумышленникам осуществить финансовые операции от Вашего имени;
- Использования злоумышленниками утерянного или украденного телефона (SIM карты) для получения SMS-сообщений с кодами, которые могут применяться Фондом в качестве дополнительной защиты от несанкционированных финансовых операций, что позволит им обойти защиту;
- Получение пароля и идентификатора доступа и/или кода из SMS-сообщения и/или кодового слова и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, когда злоумышленник представляется работником Фонда или техническим специалистом или использует иную легенду и просит Вас сообщить ему эти секретные данные, или направляет поддельные сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;
- Перехвата электронных сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если Ваша электронная почта используется для информационного обмена с Фондом. В случае получения доступа к вашей электронной почте, возможность отправки сообщений от Вашего имени в Фонд.

Несанкционированный доступ со стороны третьих лиц к конфиденциальной информации Клиента может повлечь:

- Риск совершения злоумышленниками от имени Клиента юридически значимых действий;
- Риск разглашения злоумышленниками конфиденциальной информации Клиента;
- Риски нарушения целостности либо доступности информации на устройстве Клиента;
- Риски повреждения либо несанкционированного изменения программного обеспечения, установленного на устройстве Клиента.

В настоящее время злоумышленники часто используют методы с применением вредоносного программного обеспечения для получения несанкционированного доступа к конфиденциальной информации Клиента. К вредоносному программному обеспечению относятся:

- Файловые вирусы (разрушают структуру файлов и приводят их в негодность);
- Вирусы-шифровальщики (после проникновения на компьютер шифруют все файлы и требуют деньги за их дешифровку);
- Вирусы-блокировщики (блокируют любые действия на компьютере, требуя денежный выкуп);
- Вирусы-ботнеты (скрытно подключают компьютер к вредоносной сети и используют его в качестве распространения вирусов);
- Рекламные вирусы (загружают рекламу и требуют за ее блокировку и удаление выплату денег;
- Троянские программы (проникают в компьютер и совершают кражу значимой информации).

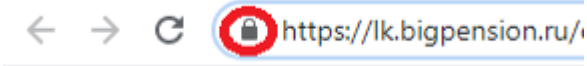
Фонд информирует своих клиентов о мерах, позволяющих снизить риски несанкционированного доступа к конфиденциальной информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого Клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода, включая, но не ограничиваясь:

1. **Обеспечьте защиту устройства, при помощи которого Вы пользуетесь услугами Фонда и/или осуществляете финансовые операции, в том числе:**

- Используйте только лицензионное программное обеспечение, полученное из доверенных источников;
- Установите запрет на установку программ из непроверенных источников;
- Обеспечьте наличие средств защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран;
- Не используйте устройства, используемые для осуществления финансовых операций, для работы с сомнительными и развлекательными сайтами;
- Не работайте через открытые публичные и не проверенные Wi-Fi сети (кафе, отели, аэропорты, вокзалы и т.д.);
- Не открывайте вложения, полученные в электронных письмах от неизвестных отправителей;
- Обеспечьте надлежащее хранение и использование устройства во избежание рисков кражи и/или утери;
- Настройте права доступа к устройству с целью предотвращения несанкционированного доступа.

2. **Уделяйте особое внимание работе с паролями и иной аутентификационной/ идентификационной информацией, в том числе:**

- Используйте сложные пароли, длиной не менее 8 символов, состоящие из сочетания строчных и прописных букв, цифр и символов, воздержитесь от использования логинов и паролей, установленных ранее при работе с любыми иными ресурсами, сайтами, социальными сетями;
- Регулярно меняйте пароли на всех устройствах и программах, включая сетевое оборудование;
- Не пересылайте пароли по почте, в SMS-сообщении или иным образом. Не храните пароли в открытом виде в файлах на компьютере;
- Храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Фонда: пароли, кодовые слова, ключи электронной подписи/шифрования, а в случае компрометации немедленно примите меры для смены и/или блокировки;
- Соблюдайте принцип разумного раскрытия информации о номерах счетов, о Ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVV/CVC кодах;
- При работе в Личном кабинете на сайте Фонда всегда проверяйте, что с сайтом установлено защищенное соединение (**https://lk.bigpension.ru**) справа или слева (в зависимости от используемого Вами браузера), в адресной строке браузера должно быть изображение закрытого замка, обозначающее наличие защищенного соединения.



- Не вводите персональную информацию на подозрительных сайтах и других неизвестных Вам ресурсах;
- Внимательно проверяйте адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под представителей Фонда или иных доверенных лиц.

3. **При работе с ключами электронной подписи необходимо:**

- Использовать для хранения ключей электронной подписи внешние носители, настоятельно рекомендуется использовать специальные защищенные носители ключевой информации (ключевые носители), например: e-token, смарт-карта и т.п.;
- Крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они (ключевые носители) не используются для работы.

Фонд рекомендует применять следующие меры по защите информации от воздействия вредоносного кода, приводящего к нарушению штатного функционирования средств вычислительной техники, в целях противодействия незаконным финансовым операциям, включая, но не ограничиваясь:

- Используйте технические устройства с лицензионным программным обеспечением;
- Своевременно устанавливайте обновления для операционной системы, особенно относящиеся к обновлениям безопасности, это позволит снизить риски заражения вредоносным кодом;
- Установите и своевременно обновляйте 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 открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам, они могут привести к заражению Вашего устройства вредоносным кодом;
- Рекомендуется подвергать предварительному антивирусному сканированию любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB накопителях и т. п.), при наличии технической возможности сканирование внешних носителей информации должно осуществляться в автоматическом режиме;
- Не заходите в системы удаленного доступа с недостоверных устройств, которые Вы не контролируете, на таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;
- Ограничьте доступ к Вашему компьютеру, исключите (ограничьте) возможность дистанционного подключения к Вашему компьютеру третьим лицам;
- Следите за информацией в прессе о последних критичных уязвимостях и о вредоносном коде;
- Помните, что наличие «эталонной» резервной копии может облегчить и ускорить восстановление Вашего технического устройства.

При подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Фонд.