РЕКОМЕНДАЦИИ
по защите информации в целях противодействия незаконным финансовым операциям

Настоящие рекомендации разработаны для клиентов АО «НПФ «Волга-Капитал» в целях выполнения требований Положения Банка России от 17.04.2019 № 684-П «Об установлении обязательных требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

1. О возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления:

АО «НПФ Волга-Капитал» предоставляет своим клиентам сервис Личный кабинет на официальном сайте Фонда в сети Интернет по адресу: https://www.volga-capital.ru (далее – Личный кабинет). Личный кабинет позволяет передавать информацию в электронной форме и обеспечивает возможность получения клиентами сведений о состоянии пенсионного счета и бланков необходимых заявлений, и совершения иных действий.

Фонд принимает все необходимые и достаточные организационные и технические меры для защиты персональной информации наших клиентов от неправомерного или случайного доступа, их уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ней третьих лиц.

Мы заботимся о том, чтобы пользоваться Личным кабинетом для клиентов Фонда было не только удобно, но и максимально безопасно. И постоянно нейтрализуем новые угрозы, используя только самые современные и эффективные средства защиты.

Однако очень многое зависит и от Вас – наших клиентов. Личный кабинет, как и любой дистанционный способ взаимодействия в сети Интернет связан с риском получения третьими лицами несанкционированного доступа к персональной информации клиента и совершения несанкционированных клиентом операций. Обратите внимание на несколько важных правил по безопасной работе в Интернете, чтобы избежать указанные риски.

2. 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:

2.1. Никому не сообщайте Ваши данные для входа в Личный кабинет (логин, пароль, одноразовые пароли из СМС), в том числе коллегам или тем, кто представляется сотрудниками Фонда.

2.2. Регулярно меняйте пароль для работы со своими учетными данными в Личном кабинете. Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов. При возникновении у Вас подозрений о том, что пароль стал известен третьим лицам – незамедлительно измените пароль.

2.3. Если в процессе работы Вы столкнулись с тем, что ранее действующий пароль не

срабатывает и не позволяет Вам войти в Личный кабинет, как можно быстрее обратитесь в Фонд для получения инструкций по смене пароля.

2.4. Не записывайте и не храните логин и пароль в общедоступных местах.

2.5. Не сохраняйте информацию о Вашем пароле на любых электронных носителях, включая Ваши персональные устройства, а также воздержитесь от использования функции автозаполнение в установках вашего браузера. Это поможет не сохранять данные (пароль пользователя, имя пользователя и др.) в электронной форме, что предотвратит их использование третьими лицами через дистанционные каналы.

2.6. Используйте разные уникальные пароли для различных web-сайтов и систем, на которых Вы вводите конфиденциальные данные.

2.7. Используйте для доступа в Личный кабинет только личные/доверенные стационарные компьютеры, мобильные телефоны, смартфоны, планшетные компьютеры, ноутбуки (далее - устройство) на которых установлено современное антивирусное программное обеспечение. Избегайте работы в Личном кабинете на устройствах с общим доступом или через публичные точки доступа к сети Интернет (в том числе Интернет кафе, бесплатный Wi-Fi и.т.д.).

2.8. Ограничьте доступ посторонних лиц к устройствам для входа в Личный кабинет. Не оставляйте без присмотра устройство с открытым Личным кабинетом. Всегда корректно завершайте работу в Личном кабинете через кнопку «Выход».

2.9. Перед каждым сеансом использования Личного кабинета внимательно проверяйте адрес главной страницы, он должен соответствовать – http://www.volga-capital.ru. Другие адреса являются ЛОЖНЫМИ и свидетельствуют о наличии мошеннических действий.

2.10. Для авторизации в Личном кабинете указывайте в соответствующих полях логин, пароль. 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 в АО НПФ «Волга-Капитал» о данном факте по телефону 8 (843) 273-13-14 или на электронную почту info@volga-capital.ru с пометкой «Срочно!»

2.11. Используйте для работы в Личном кабинете защищенный паролем персональный компьютер с установленным антивирусным программным обеспечением и обновлениями безопасности операционной системы. Вход в систему с чужого компьютера не является безопасным.

2.12. Регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ и устанавливайте только лицензионное программное обеспечение (операционная система, приложения), полученное из проверенных и надежных источников, своевременно устанавливайте все обновления программного обеспечения, повышающие безопасность

2.13. На устройстве, используемом Вами для доступа в Личный кабинет необходимо использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), обеспечить регулярную своевременную установку обновлений, выпускаемых разработчиками, операционной системы, web-браузеров (Microsoft Internet Explorer, Mozilla FireFox, Opera и т.д.) и иного прикладного программного обеспечения;

2.14. На устройстве, используемом Вами для доступа в Личный кабинет необходимо исключить посещение WEB- сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т.п. Использование нелицензионного программного обеспечения повышает риск получения несанкционированного доступа злоумышленников;

2.15. 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.

2.16. В случае передачи устройства, на котором ранее осуществлялся доступ в Личный кабинет, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред клиенту;

3. *Рекомендации по защите информации от воздействия вредоносного кода:*

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

3.1. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

3.2. Пользуйтесь устройствами с установленным лицензионным программным обеспечением.

3.3. Своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений).

3.4. Не используйте права администратора при отсутствии необходимости; в повседневной практике входите в систему с учетной записью пользователя, не имеющего прав администратора.

3.5. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ; старайтесь периодически просматривать журнал и реагировать на ошибки.

3.6. Не используйте на устройстве, предназначенном для доступа в Личный кабинет, средства удаленного администрирования.

3.7. Обязательно установите и своевременно обновляйте на устройстве антивирусное программное обеспечение. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т. е. не требующий ответов пользователя при обнаружении вирусов. Лечение (удаление) зараженных файлов производится антивирусным средством в автоматическом режиме.

3.8. Не реже одного раза в неделю в автоматическом режиме осуществляйте полную проверку устройства на предмет наличия вирусов и вредоносного программного кода. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного средства.

3.9. Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы.

3.10. Рекомендуется подвергать антивирусному контролю 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 должно осуществляться в автоматическом режиме.

3.11. При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам сети Интернет.

3.12. При работе в Интернете не соглашайтесь на установку каких-либо сомнительных программ.

3.13. Воздерживайтесь от использования программ онлайнового общения на устройстве, используемом для работы в Личном кабинете.

3.14. Исключите возможность установки посторонними лицами (гостями, посетителями) на устройство специальных «шпионских» программ.

3.15. Ограничьте информационный обмен в сети Интернет только надежными информационными порталами и проверенными корреспондентами электронной почты. Старайтесь не использовать

устройство, с которого Вы осуществляете выход в Личный кабинет, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.

3.16 Важно знать, что надежным средством обеспечения подлинности является цифровая подпись, а не строка адреса браузера или электронной почты. Часто в виде «интересной ссылки» в письме от якобы знакомого приходит вредоносная программа. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.

3.17. При подозрениях на наличие вирусов на устройстве (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), воздержитесь от использования Личного кабинета до исправления ситуации.