Ханты-Мансийский
Негосударственный
Пенсионный
Фонд

УТВЕРЖДАЮ
Исполнительный вице-президент
АО «Ханты-Мансийский НПФ»
_____Угорелов Ю.С.
«04» июня 2019 г.

**Рекомендации для клиентов фонда**
**по мерам снижения риска получения несанкционированного доступа к носителям и устройствам, защищаемой информации при работе на сайте фонда, а так же своевременному обнаружению воздействий вредоносного кода и защите информации от воздействий вредоносного кода**

## 1. Общие положения

1.1. Кража учетных данных – хищение личных данных клиента Фонда и их незаконное использование для выполнения несанкционированных действий от имени клиента на сайте фонда. Оптимальный способ защиты от кражи учетных данных состоит в умении распознавать способы этих злоумышленных действий для предотвращения таких ситуаций.

1.2. Риски получения несанкционированного доступа к информации прежде всего связаны с использованием ложных ресурсов сети Интернет (фишинговых сайтов) с целью осуществления перехвата учетных данных (логинов и паролей) лицами, не обладающими правом распоряжения этими учетными данными, а также воздействием вредоносного кода.

1.3. «Фишинг» – попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

1.4. Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах, с которых осуществляется работа с системой, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения (далее – ПО) либо на перехват информации, в том числе паролей.

1.5. Средства и методы защиты информации, применяемые в Фонде, позволяют обеспечить необходимый уровень безопасности при работе на сайте фонда и предотвратить мошеннические действия недоброжелателей при условии

выполнения клиентами рекомендаций, изложенных в данном документе.

## 2. Рекомендации по защите информации от воздействия вредоносного кода

2.1. На персональном компьютере Клиента должно быть установлено антивирусное ПО.

2.2. Антивирусное ПО должно регулярно обновляться. 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.

2.3. Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного средства.

2.4. 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.

2.5. При использовании сети Интернет для обмена почтовыми сообщениями необходимо применять антивирусное ПО, разработанное специально для почтовых клиентов.

2.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа ПО, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т. п.) рекомендуется приостановить работу с системой до полного устранения неисправностей.

2.7. Не открывайте файлы, полученные по электронной почте от неизвестных отправителей.

## 3. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

3.1. Мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете (например, Фонда), и предназначены для сбора конфиденциальной информации обманным путем.

3.2. Перед просмотром электронного письма всегда проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты в

официальном формате, который является почти точной копией адреса настоящей компании. Изменить адрес электронной почты отправителя очень просто, поэтому будьте бдительны.

3.3. Внимательно читайте текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это – электронное письмо, отправленное мошенниками.

3.4. Опасайтесь безличных обращений, таких как «Уважаемый пользователь», или обращения по адресу электронной почты. В настоящем электронном письме Фонд всегда приветствует Вас, обращаясь по имени и фамилии либо по названию компании. Типичное фишинговое письмо начинается с обезличенного приветствия.

3.5. Старайтесь сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Вас действовать быстро и необдуманно. Многие поддельные сообщения электронной почты пытаются убедить Вас в том, что Вашей информации в кабинете угрожает опасность, если Вы немедленно не обновите критически важные данные.

3.6. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не переходите по этой ссылке.

## 4. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

4.1. Рекомендуем регулярно менять пароль для работы со своими учетными данными в системе Личного кабинета. Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

4.2. Рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, на которых Вы вводите конфиденциальные данные (например, сведения о Вашем профиле в Личном Кабинете, в электронной почте и т. д.).

4.3. В том случае, если Вы обнаружили, что Ваш пароль от Личного кабинета скомпрометирован, рекомендуем Вам незамедлительно сменить пароль на новый, известный только Вам, удовлетворяющий требованиям п. 4.1.

4.4. Если в процессе работы Вы столкнулись с тем, что ранее действующий пароль не срабатывает и не позволяет Вам войти в систему, необходимо как можно быстрее обратиться в Контактный центр фонда для получения информации по смене пароля.

4.5. Никому не разглашайте пароль от Личного кабинета. Фонд не рассылает электронных писем, SMS или других сообщений с просьбой уточнить Ваши конфиденциальные данные (в т.ч. пароли, логины, номера договоров и т.п.).

4.6. Не пересылайте файлы с конфиденциальной информацией для работы в Личном кабинете по электронной почте или через SMS-сообщения.

4.7. Рекомендуем исключить возможность доступа к компьютеру, с которого Вы осуществляете работу в авторизованной(открытой Вами) системе Личного кабинета, посторонних лиц.