ПАМЯТКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В связи с опасностью несанкционированного доступа или проникновения вредоносных программ, а также в целях противодействия осуществления противоправных финансовых операций злоумышленниками, ООО «Страховой брокер «Мирное небо» (далее - Общество) сообщает следующее:

1. Рекомендации по защите информации от воздействия программных кодов, приводящего к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям

1.1. Рекомендуется работа на устройстве под учетной записью пользователя без прав администратора (в случае десктопных операционных систем). Также рекомендуется внимательное отношение к всплывающим запросам на предоставление доступа установленному программному обеспечению (в случае мобильных операционных систем).

1.2. На Вашем устройстве должно быть установлено лицензионное антивирусное программное обеспечение (ПО), которое должно регулярно обновляться.

Рекомендуется установить по умолчанию максимальный уровень политик безопасности, не требующих ответов пользователя при обнаружении вирусов.

Лечение (удаление) зараженных файлов должно производиться антивирусным ПО в автоматическом режиме.

1.3. 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 должна осуществляться согласно расписанию, выставленному в настройках антивирусного ПО.

1.4. 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.

1.5. При обмене электронными почтовыми сообщениями (эксплуатации почтовых клиентов) необходимо применять антивирусное ПО, поддерживающее проверку почтовых клиентов.

1.6. При возникновении подозрения на заражение устройства компьютерным вирусом (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.) или нарушения работоспособности компьютера необходимо осуществить внеплановую проверку на наличие вредоносного ПО (желательно с использованием двух антивирусных ПО). После удаления вирусов и восстановления работоспособности компьютера необходимо произвести смену паролей, удовлетворяющим требованиям п. 4.1 настоящей Памятки.

1.7. Рекомендуется не открывать файлы, полученные по электронной почте от неизвестных отправителей.

2. Информация о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления

При осуществлении финансовых операций следует принимать во внимание риски финансовых потерь, связанные с получением несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, а также с воздействием вредоносных программ.

Указанные риски могут быть обусловлены, включая, но не ограничиваясь, следующими ситуациями:

2.1. Кража идентификатора и пароля доступа (в том числе SMS-кодов) или иных конфиденциальных данных посредством технических средств и (или) вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа.

2.2. Установка на устройство вредоносной программы, которая позволит злоумышленникам осуществить операции от Вашего имени.

2.3. Кража или несанкционированный доступ к устройству, с которого Вы осуществляете финансовые операции для получения данных и (или) несанкционированного доступа к сервисам с этого устройства.

2.3. Получение идентификатора доступа, пароля, SMS-кодов и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д., путем обмана и (или) злоупотребления доверием, методом «социальной инженерии» (звонки «службы безопасности банка», «правоохранительных органов» и т.д.), когда злоумышленник использует какую-либо легенду и просит Вас сообщить ему конфиденциальные данные; или направляет поддельные почтовые сообщения или письмо на бумажном носителе по почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства.

2.3. Перехват сообщений электронной почты и получение несанкционированного доступа к отчетам и прочей финансовой информации, если Ваша электронная почта используется для информационного обмена такой информацией.

В случае получения доступа к Вашей электронной почте - несанкционированная рассылка сообщений от Вашего имени.

К основным причинам возникновения рисков получения несанкционированного доступа к защищаемой информации относятся:

- неограниченный доступ третьих лиц к Вашему устройству;
- неограниченный доступ третьих лиц к информации о паролях и логинах, используемых для доступа к информационным ресурсам;
- несоблюдение режима конфиденциальности в отношении защищаемой информации в информационно-телекоммуникационной сети «Интернет»;
- утрата (потеря, хищение) Вашего устройства;
- отсутствие непроверенного программного обеспечения;
- отсутствие действующего актуального антивирусного ПО с актуальными вирусными базами;
- несоблюдение рекомендаций по защите информации, в том числе содержащихся в настоящей Памятке.

Перечень причин возникновения рисков получения несанкционированного доступа к защищаемой информации, указанных в настоящей Памятке, не является исчерпывающим. Причины возникновения рисков получения несанкционированного доступа к защищаемой информации зависят от конкретной ситуации и (или) обстоятельств.

3. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов информационно-телекоммуникационной сети «Интернет»

3.1. Мошеннический или поддельный web-сайт - это небезопасный web-сайт, где под каким-либо предлогом предлагается ввести конфиденциальную информацию (аутентификационные данные).

Указанные web-сайты могут являться почти точной копией официальных web-сайтов известных организаций, которым Вы доверяете (например, сайта кредитной организации), и предназначены для сбора конфиденциальной информации обманным путем.

3.2. Интернет-сайт Общества имеет следующий адрес: http://www.ib-ps.ru.

Общество не оказывает финансовых услуг посредством Интернет-сайта или других общедоступных средств автоматизации.

Интернет-сайт Общества не содержит форм для авторизации в личном кабинете. Остерегайтесь похожих названий Интернет-сайта.

3.3. Мошенники могут изменить адрес электронной почты в преднамеренных целях, поэтому перед просмотром электронного письма всегда проверяйте адрес электронной почты отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса электронной почты Общества, отличаясь от него только на один символ. Официальный адрес электронной почты Общества - info@ib-ps.ru, сотрудники Общества могут присылать электронные письма с персонифицированных электронных адресов и в этом случае домен отправителя имеет указание - @ib-ps.ru.

3.4. Внимательно читайте текст электронного письма. Электронные письма от известных компаний, как правило, не содержат орфографических или грамматических ошибок.

Если Вы видите слова на иностранном языке, специальные символы и т.д., возможно, это - электронное письмо, отправленное мошенниками.

3.5. Старайтесь действовать рационально. 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 Вашему счету или Вашим данным угрожает опасность, если Вы немедленно не предпримете действия, выгодные злоумышленникам.

3.6. Внимательно анализируйте ссылки (например, на virustotal.com).

Поддельные ссылки могут быть почти точной копией подлинных, при этом они могут перенаправить Вас на мошеннический Интернет-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с «http://» вместо «https://»), не переходите по ней.

4. Информация о мерах по предотвращению несанкционированного доступа к защищаемой информации третьими лицами

4.1. Рекомендуется регулярно менять пароли для работы со своими учетными данными в различных системах.

Длина Вашего пароля должна содержать не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

В качестве пароля не рекомендуется использовать даты рождения, имена родственников, клички питомцев и т.п.

4.2. Рекомендуется использовать уникальные пароли для различных Интернет-сайтов и систем, на которых хранятся и обрабатываются Ваши конфиденциальные данные (например, портал государственных и муниципальных услуг, личный кабинет, онлайн-банкинг и т.д.).

4.3. В случае компрометации или подозрении на компрометацию пароля, рекомендуется незамедлительно сменить пароль на новый, удовлетворяющий требованиям, указанным в п. 4.1 настоящей Памятки.

4.4. Никому передавайте и не разглашайте свои пароли, а также иные данные, необходимые для аутентификации.

4.5. Рекомендуется установить пароли на учетные записи пользователей операционной системы на компьютере.

4.6. Рекомендуется установить на устройство актуальное антивирусное ПО и своевременно обновлять ПО и антивирусные базы.

4.7. Рекомендуется включить блокировку экрана для мобильных устройств и отключить показ любых паролей при вводе.

4.8. Рекомендуется исключить возможность физического доступа посторонних лиц к устройству, с которого Вы осуществляете доступ к сайтам и информационным системам.

4.9. Рекомендуется применять на устройстве для работы специализированные программные и аппаратные средства безопасности: средства защиты от несанкционированного доступа, персональные межсетевые экраны, антишпионское программное обеспечение и т.п., обеспечить регулярное автоматическое обновление программного обеспечения этих средств.

4.10. На устройстве, с которого осуществляется доступ к Интернет-сайтам и информационным системам, содержащим конфиденциальную информацию, рекомендуется исключить посещение Интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т.п.

Использование нелицензионного программного обеспечения повышает риск получения несанкционированного доступа злоумышленников с целью хищения информации.

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