СТРАХОВАЯ МЕДИЦИНСКАЯ КОМПАНИЯ
АСТРАМЕД-МС

Юридический адрес: 620073, г. Екатеринбург, ул. Крестинского, 46А, оф. 303
Почтовый адрес: 620014, г. Екатеринбург, ул. 8 Марта, д.37, тел. (343) 380-53-96, 385-90-14, факс: (343) 385-90-16
www.astramed-ms.ru, e-mail: info@astramed-ms.ru

В соответствии с требованиями Положения 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 (утв. Банком России 20.04.2021 №757-П), СМК «АСТРАМЕД-МС» (АО) (далее - Компания) доводит до вашего сведения информацию о возможных рисках, связанных с получением третьими лицами несанкционированного доступа к защищаемой информации, и основные рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (далее - Вредоносный код), в целях противодействия незаконным финансовым операциям (далее Рекомендации).

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

Целью Рекомендаций являются доведение до вас информации:

- о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

- 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, и своевременному обнаружению воздействия Вредоносного кода.

Несанкционированный доступ к защищаемой информации происходит, как правило, посредством удаленного доступа к устройствам клиента в результате взлома защиты устройства клиента или получения данных для проведения / подтверждения проведения операций с помощью метода социальной инженерии (методы доступа к защищаемой информации, основанной на психологии людей), а также в следствии заражения устройства клиента Вредоносным кодом.

Оптимальным способом защиты от методов социальной инженерии является умение распознать злоумышленные действия. Основными способами получения несанкционированного доступа к защищаемой информации являются:

«**Фишинг**» - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных компаний, а также личных сообщений внутри различных сервисов, например, от имени финансовых организаций или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и счетам клиента, в том числе доступ в личный кабинет.

«**Троянский конь**» - разновидность вредоносной программы, проникающая в компьютер под видом легального программного обеспечения. В данную категорию входят программы, осуществляющие различные неподтверждённые пользователем действия: сбор информации банковских карт

и её передачу злоумышленнику, её использование, удаление или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в целях майнинга и т.д.

«**Кви про Кво**» - используется для внедрения вредоносного программного обеспечения в устройства. Злоумышленники звонят клиенту, представляются сотрудниками техподдержки компании и опрашивают клиентов на наличие каких-либо технических неисправностей в устройстве клиента. Если неисправности имеются, злоумышленники просят клиента ввести определенную команду, после чего появляется возможность запуска вирусного программного обеспечения.

«**Дорожное яблоко**» - состоит в адаптации «троянского коня» и требует обязательного применения какого-то физического носителя информации. Злоумышленники могут предоставить клиенту загрузочные внешние носители информации, подделанные под носители с интересным и/или уникальным контентом.

Основные риски получения несанкционированного доступа к устройствам клиента:

- риск совершения финансовых операций с активами клиентов, в том числе путем формирования и отправки от имени клиента распоряжения на проведение финансовой операции, а также риск перехвата сообщений, отправляемых Компанией на адрес электронной почты и/или абонентский номер клиента, содержащих защищаемую информацию;
- риск повреждения программного обеспечения клиента, а также риск искажения, изменения, искажения, уничтожения или шифрования информации об активах клиента или данных самого клиента;
- риск разглашения конфиденциальной информации.

Рекомендации по защите информации от воздействия Вредоносного кода

1) Обеспечьте защиту устройства:

- используйте только лицензионное программное обеспечение, полученное из доверенных источников;
- не совершайте установку программ из непроверенных источников;
- для повседневной работы за компьютером не используйте учетную запись с правами администратора;
- установите средства защиты, такие как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран;
- настройте право доступа к устройству с целью предотвращения несанкционированного доступа;
- своевременно обновляйте операционную систему, особенно в части обновлений безопасности;
- используете парольную или иную защиту для доступа к устройству;
- не используйте на компьютере, предназначенного для обмена информацией и документами с Компанией, средства удаленного администрирования;
- при работе с ключами электронной подписи используйте для хранения ключей электронной подписи внешние носители, настоятельно рекомендуется использовать специальные защищенные носители ключевой информации (ключевые носители), например: eToken, смарт-карта и т.п.

Рекомендуется регулярно менять пароли для работы со своими учетными данными в различных системах. Длина пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

2) Обеспечьте конфиденциальность:

- блокируйте устройство после использования, используйте настройки устройства, требующие ввода пароля для его разблокировки и использования;
- не используйте функцию запоминания логина и пароля в браузерах;

- не используйте одинаковые логины и пароли для доступа к различным системам, для уменьшения последствий при компрометации одного из паролей;
- регулярно производите смену паролей. Рекомендуемый период смены пароля не реже 1 раза в квартал
- не передавайте третьим лицам и не оставляйте устройство без присмотра;
- храните в тайне аутентификационные/идентификационные данные и ключевую информацию: пароли, СМС коды, 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 договоров, номерах ваших счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVC\CVV кодах, в случае если у вас запрашивают указанную информацию, по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал.

3) Соблюдайте правила безопасности в сети Интернет:

- при использовании систем удостоверьтесь в том, что сертификат безопасности сайта действителен, а соединение происходит в защищенном режиме (адресная строка браузера начинается с https, либо используется значок в виде замка);
- при наличии на устройстве программ фильтрации сетевого трафика (брандмауэра) держите его включённым и блокируйте все незнакомые или подозрительные подключения;
- не отвечайте на подозрительные сообщения, полученные с неизвестных адресов;
- не устанавливайте и не сохраняйте подозрительные файлы, программы, полученные из ненадежных источников, скаченные с неизвестных сайтов в сети Интернет, присланные с неизвестных адресов электронной почты;
- не соглашайтесь на предложения установки неизвестного программного

обеспечения во всплывающих окнах на сайтах;

- не открывайте и не используйте сомнительные Интернет - ресурсы на устройстве.

4) Контроль подключения:

- не используйте устройства третьих лиц для подключения к системам для совершения финансовых операций или получения информации в отношении таких операций;
- не работайте в системах с устройства, использующего подключение к общедоступной wi-fi сети.

5) Проявляйте осторожность и предусмотрительность:

- будьте осторожны при получении электронных писем со ссылками и вложениями, они могут привести к заражению вашего устройства Вредоносным кодом. Вредоносный код, попав к вам через электронную почту или интернет ссылку на сайт, может получить доступ к любым данным и информационным системам на вашем устройстве;
- внимательно проверяйте адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под Компанию или иных доверенных лиц;
- будьте осторожны при просмотре/работе с интернет сайтами, так как Вредоносный код может быть загружен с сайта;
- следите за информацией в прессе и на сайте Компании о последних критичных уязвимостях и о Вредоносном коде;
- осуществляйте звонок в Компанию только по номеру телефона, указанному в договоре или на официальном сайте Компании. Имейте в виду, что от лица Компании не могут поступать звонки или сообщения, в которых от вас требуют передать СМС-код, пароль, номер счета, кодовое слово и т.д.

- имейте в виду, если вы передаете ваш телефон и/или устройство другим пользователям, они могу установить на него Вредоносный код, а в случае

кражи или утери злоумышленники могут воспользоваться им для доступа к системам Регистратора, которыми пользовались вы.