РЕКОМЕНДАЦИИ
по соблюдению информационной безопасности клиентами АО «УК «Регионфинансресурс» в целях противодействия незаконным финансовым операциям

Настоящие Рекомендации по соблюдению информационной безопасности клиентами АО «УК «Регионфинансресурс» (далее - Организация) в целях противодействия незаконным финансовым операциям (далее – Рекомендации) разработаны в соответствии с требованиями Положения Банка России от 17.04.2019 № 684-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» и направлены на защиту информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям.

Рекомендации подлежат доведению до сведения клиентов Организации путем размещения на сайте Организации в сети Интернет.

Рекомендации по соблюдению информационной безопасности (совокупности мер, применение которых направлено на непосредственное обеспечение защиты информации, процессов, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты (здесь и далее термины из ГОСТ Р 57580.1-2017) 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.

В связи с тем, что требования информационной безопасности так же могут быть отражены в договорах, регламентах, правилах и иных документах Организации, регламентирующих предоставление услуг, настоящие Рекомендации действуют в части не противоречащей положениям внутренних документов.

В случае заключения договора с Организацией, клиентам рекомендуется внимательно изучить договор, приложения к договору и иные документы, связанные с исполнением договора, ознакомиться с разделами, посвященными информационной безопасности/конфиденциальности.

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

1.1. Клиенты Организации несут риски возможных финансовых потерь вследствие следующих обстоятельств:

- получение лицами, не обладающими правом осуществления финансовых операций от лица клиента, несанкционированного доступа к защищаемой информации;
- утрата, потеря (хищение) идентификаторов доступа клиента, с использованием которых, осуществляются финансовые операции;
- воздействие вредоносного кода на устройства клиента, с которых совершаются финансовые операции;
- совершение в отношении клиента иных противоправных действий, связанных с информационной безопасностью.

1.2. При осуществлении финансовых операций клиентам Организации следует принимать во внимание риск получения третьими лицами несанкционированного доступа

к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления. Такие риски могут быть обусловлены включая, но не ограничиваясь следующими событиями:

- кража пароля и/или иного идентификатора доступа и/или иных конфиденциальных данных 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 операции от имени клиента;
- использование злоумышленником утерянного или украденного устройства для получения идентификаторов доступа клиента, которые могут применяться Организацией в качестве дополнительной защиты от несанкционированных финансовых операций, что позволит им обойти защиту;
- кража или несанкционированный доступ к устройству, с которого клиент пользуется услугами Организации для получения злоумышленником данных и/или несанкционированного доступа к услугам Организации с этого устройства;
- получение пароля и/или иного идентификатора доступа, персональных данных и иных конфиденциальных данных клиента путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником Организации или техническим специалистом или использует иную легенду и просит клиента сообщить ему указанные конфиденциальные данные;
- направление злоумышленником поддельных почтовых сообщений (в том числе по электронной почте) с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;
- перехват электронных сообщений и получение несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если электронная почта клиента используется для информационного обмена с Организацией, или, в случае получения доступа к электронной почте клиента, отправка сообщений от имени клиента в Организацию.

1.3. Клиентам рекомендуется соблюдать профилактические мероприятия, направленные на повышение уровня информационной безопасности.

1.4. Организация не несет ответственности в случаях финансовых потерь, понесенных клиентами в связи с пренебрежением правилами информационной безопасности.

2. Меры по предотвращению несанкционированного доступа к защищаемой информации для снижения риска финансовых потерь.

2.1. Клиентам Организации следует предпринимать все доступные меры для предотвращения несанкционированного доступа к защищаемой информации, включая, но не ограничиваясь следующими мерами.

2.1.1. Обеспечение надлежащей защиты устройства, в случае его использования для получения услуг Организации и обмена информацией с Организацией:

- использование на устройстве только лицензионного программного обеспечения, полученного из доверенных источников;
- запрет на установку программ из непроверенных источников;

- использование средств защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран и др.;
- настройка прав доступа к устройству с целью предотвращения несанкционированного доступа;
- хранение, использование устройства способом, позволяющим избежать рисков его кражи и/или утери;
- своевременные обновления операционной системы, в частности обновления безопасности;
- активация парольной или иной защиты для доступа к устройству.

2.1.2. Обеспечение конфиденциальности защищаемой информации:

- хранение в тайне идентификационных данных в случае их получения от Организации, а при компрометации таких данных клиенту рекомендуется немедленно принять меры для их смены и/или блокировки и уведомить Организацию о такой компрометации;
- соблюдение принципа разумного раскрытия идентификационных данных (в том числе персональных данных), а в случае запроса у клиента указанной информации в связи с оказанием услуг Организацией, клиенту рекомендуется по возможности оценить ситуацию и уточнить полномочия запрашивающего лица и процедуру предоставления запрашиваемой информации через независимый канал связи, например, по контактному телефону Организации.

2.1.3. Проявление осторожности и предусмотрительности:

- клиентам Организации рекомендуется проявлять должную осторожность в следующих случаях:
  - при получении электронных писем со ссылками и вложениями, так как они могут привести к заражению устройства клиента вредоносным кодом;
  - при получении электронных писем с вложениями в виде архивов с файлами, защищенных паролем, или зашифрованных файлов/архивов, так как в таких файлах может быть вредоносный код;
  - при просмотре/работе с интернет-сайтами, так как вредоносный код может быть загружен с сайта.

  С помощью вредоносного кода, попавшего к клиенту через электронную почту или ссылку в сети Интернет, злоумышленник может получить доступ к любым данным на зараженном устройстве клиента.
- клиентам Организации рекомендуется внимательно проверять адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под Организацию или иных доверенных лиц;
- клиентам Организации рекомендуется следить за информацией в прессе и на сайте Организации о последних критичных уязвимостях и о вредоносном коде и принимать такую информацию к сведению;
- клиентам Организации рекомендуется осуществлять звонки и направлять почтовые сообщения (в том числе электронные) в Организацию только по номеру телефона, почтовому и электронному адресам, указанным на сайте Организации

в сети Интернет. От лица Организации не могут поступать звонки или сообщения, в которых от клиента требуют предоставить идентификаторы доступа;

- клиентам Организации не следует предоставлять доступ к устройству третьим лицам, так как в этом случае клиент несет риск загрузки такими лицами на устройство вредоносного кода.
- в случае утраты устройства клиентам рекомендуется для предотвращения использования злоумышленниками устройства для доступа к услугам Организации от лица клиента:
  - незамедлительно проинформировать Организацию по контактному номеру телефона и/или адресу электронной почты, указанным на сайте Общества в сети Интернет;
  - по возможности оперативно с учетом прочих рисков и особенностей использования устройства заблокировать доступ к устройству, а также сменить идентификатор(ы) доступа к услугам Организации, лично обратившись в Организацию.
- при подозрении на несанкционированный доступ и/или компрометацию устройства клиентам рекомендуется сменить идентификатор(ы) доступа, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Организацию;
- в случае получения услуг Организации через устройство, клиентам рекомендуется использовать для этих целей отдельное устройство, доступ к которому есть только у клиента;
- клиентам рекомендуется использовать сложный пароль для входа на устройство, и не хранить пароль в открытом виде на компьютере/мобильном устройстве;
- клиентам рекомендуется поддерживать в актуальном состоянии свою контактную информацию, предоставленную Организации, чтобы в случае необходимости представитель Организации мог оперативно связаться с клиентом.

2.1.4. При работе на персональном компьютере клиентам рекомендуется:

- использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и т.д.);
- своевременно устанавливать актуальные обновления безопасности (операционные системы, офисные пакеты и т.д.);
- использовать антивирусное программное обеспечение, регулярно обновлять антивирусные базы;
- использовать специализированные программы для защиты информации (персональные межсетевые экраны и средства защиты от несанкционированного доступа), средства контроля конфигурации устройств;
- использовать сложный пароль для входа на компьютер, и не хранить пароль в открытом виде на компьютере;
- ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

2.1.5. При работе с мобильным устройством клиентам рекомендуется:

- не оставлять свое Мобильное устройство без присмотра, чтобы исключить его несанкционированное использование;
- использовать только официальные мобильные приложения, установленные с помощью магазина приложений;
- не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в SMS-сообщениях, Push-уведомлениях или по электронной почте, в том числе от имени Организации;
- установить на мобильном устройстве сложный пароль для входа и не хранить пароль в открытом виде.

2.1.6. В случае обмена информацией с Организацией через сеть Интернет клиентам рекомендуется:

- не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам;
- не вводить персональную информацию на подозрительных сайтах и других неизвестных клиенту ресурсах;
- Не посещать сайты сомнительного содержания;
- не сохранять пароли в памяти интернет-браузера, если к устройству имеют доступ третьи лица;
- не нажимать на баннеры и всплывающие окна, возникающие во время работы в сети Интернет;
- не открывать файлы, полученные (скачанные) из неизвестных источников и имеющие неизвестное «расширение».

2.2. При подозрении в несанкционированном обращении для получения услуг Организации от имени клиента, клиенту необходимо незамедлительно обратиться в Организацию по контактному телефону: **+7 (495) 256-80-41** и/или адресу электронной почты: **rfr@yk-rfr.ru**