РЕКОМЕНДАЦИИ ПО СОБЛЮДЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КЛИЕНТАМИ АО «РТ-ИНВЕСТ» В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ ФИНАНСОВЫМ ОПЕРАЦИЯМ

В соответствии с требованиями Положения Центрального Банка Российской Федерации от 17.04.2019 г. № 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» Акционерное общество «РТ-Инвест» (далее - Управляющая компания) доводит до сведения своих клиентов рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям, и информирует о следующем:

- 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.

Рекомендации по соблюдению информационной безопасности 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.

Управляющая компания информирует своих клиентов о возможных рисках, связанных с получением третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, и которые могут быть обусловлены, включая, но не ограничиваясь, следующими действиями:

- кража или несанкционированный доступ к устройству, с которого Вы пользуетесь услугами/сервисами Управляющей компании, и/или несанкционированный доступ к сервисам Управляющей компании с этого устройства, что может повлечь за собой получение третьими лицами доступа к защищаемой информации;

- кража пароля и идентификатора доступа или иных конфиденциальных данных, например, CVV/CVC номера карты, ключей электронной подписи/шифрования 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 финансовые операции от Вашего имени;

- использования злоумышленниками утерянного или украденного телефона (SIM карты) для получения СМС кодов, которые могут применяться Управляющей компанией в качестве дополнительной защиты от несанкционированных финансовых операций, что позволит им обойти защиту;

• получение пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, когда злоумышленник представляется работником Управляющей компании или техническим специалистом или использует иную легенду и просит Вас сообщить ему эти секретные данные, или направляет поддельные сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;

• перехвата электронных сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если Ваша электронная почта используется для информационного обмена с Управляющей компанией. Или в случае получения доступа к вашей электронной почте, отправка сообщений от Вашего имени в Управляющую компанию.

Несанкционированный доступ со стороны третьих лиц к защищаемой информации может повлечь:

• риски разглашения конфиденциальной информации: персональных данных клиента, сведений об операциях, другой значимой информации;

• риски совершения такими третьими лицами юридически значимых действий, включая, но не ограничиваясь, совершение финансовых операций от имени клиента, изменений регистрационных данных клиента, и иных действий, совершенных без воли клиента, и направленных против его интересов.

Управляющая компания информирует своих клиентов о мерах, позволяющих снизить риски 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, включая, но не ограничиваясь:

1. Обеспечьте защиту устройства, при помощи которого Вы пользуетесь услугами Управляющей компании и/или осуществляете финансовые операции, в том числе:

• используйте только лицензионное программное обеспечение, полученное из доверенных источников;

• установите запрет на установку программ из непроверенных источников;

• обеспечьте наличие средств защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран;

• не используйте устройства, используемые для осуществления финансовых операций, для работы с сомнительными и развлекательными сайтами;

• не работайте через открытые публичные и не проверенные wi-fi сети (кафе, отели, аэропорты, вокзалы и т.д.);

• не открывайте вложения, полученные в электронных письмах от неизвестных отправителей;

• обеспечьте надлежащее хранение, использование устройства во избежание рисков кражи и/или утери;

• настройте права доступа к устройству с целью предотвращения несанкционированного доступа.

2. Уделяйте особое внимание работе с паролями и иной аутентификационной/ идентификационной информацией, в том числе:

• используйте сложные пароли, длиной не менее 8 символов, состоящие из сочетания строчных и прописных букв, цифр и символов, воздержитесь от использования логинов и паролей, установленных ранее при работе с любыми иными ресурсами, сайтами, социальными сетями;

• регулярно меняйте пароли на всех устройствах и программах, включая сетевое оборудование;

• не пересылайте пароли по почте, СМС или иным образом, не храните в открытом виде в компьютерных файлах;

• храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Управляющей компании: 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 счетов, о Ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVV/CVC кодах. В случае, если у Вас запрашивают указанную информацию, в привязке к сервисам Управляющей компании по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон Управляющей компании, указанный на официальном сайте Управляющей компании в сети Интернет по адресу www.ukpir.ru; • не вводите персональную информацию на подозрительных сайтах и других неизвестных Вам ресурсах;

• внимательно проверяйте адресата, от которого пришло электронное письмо.

Входящее электронное письмо может быть от злоумышленника, который маскируется под представителей Управляющей компании или иных доверенных лиц.

3. При работе с ключами электронной подписи необходимо:

• использовать для хранения ключей электронной подписи внешние носители, настоятельно рекомендуется использовать специальные защищенные носители ключевой информации (ключевые носители), например: e-token, смарт-карта и т.п.;

• крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они (ключевые носители) не используются для работы.

Управляющая компания рекомендует применять следующие меры по защите информации от воздействия вредоносного кода, приводящего к нарушению штатного функционирования средств вычислительной техники, в целях противодействия незаконным финансовым операциям, включая, но не ограничиваясь:

• используйте технические устройства с установленным лицензионным программным обеспечением;

• своевременно обновляйте операционную систему, особенно в части обновлений безопасности, это позволит снизить риски заражения вредоносным кодом;

• установите и своевременно обновляйте на техническом устройстве лицензионное антивирусное программное обеспечение с функцией автоматического обновления вирусных баз;

• осуществляйте проверку жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода;

• при работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам, они могут привести к заражению Вашего устройства вредоносным кодом;

• рекомендуется подвергать предварительному антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USBнакопителях и т. п.); при наличии технической возможности сканирование внешних носителей информации должно осуществляться в автоматическом режиме;

• не заходите в системы удаленного доступа с недостоверных устройств, которые Вы не контролируете, на таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;

• ограничьте доступ к Вашему компьютеру, исключите (ограничьте) возможность дистанционного подключения к Вашему компьютеру третьим лицам;

• следите за информацией в прессе о последних критичных уязвимостях и о вредоносном коде;

• помните, что наличие «эталонной» резервной копии может облегчить и ускорить восстановление Вашего технического устройства.

При подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Управляющую компанию.