Рекомендации клиентам ООО «РЕГИОН Девелопмент» по соблюдению информационной безопасности в целях противодействия незаконным финансовым операциям

Настоящим ООО «РЕГИОН Девелопмент» (далее – «Общество») в целях противодействия незаконным финансовым операциям и в соответствии с Положением 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 17.04.2019 № 684-П), доводит до сведения клиентов Общества основные рекомендации (далее – «Рекомендации») о возможных рисках получения несанкционированного доступа к информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, а также о мерах по предотвращению несанкционированного доступа к защищаемой информации.

1. Риски, связанные с несанкционированным доступом к защищаемой информации, вредоносными кодами и иными противоправными действиями третьих лиц:

1.1. Получение лицами, не обладающими правом осуществления финансовых операций от лица клиента, несанкционированного доступа к защищаемой информации может повлечь за собой 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.

1.2. Повлечь за собой потерю защищаемой информации, а также получение лицами, не обладающими правом осуществления финансовых операций от лица клиента, несанкционированного доступа к защищаемой информации, разглашение конфиденциальной информации клиента, совершение 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, могут (включая, но не ограничиваясь) следующие обстоятельства:

- утрата (потеря, хищение) носителей ключей электронной подписи, кража пароля и идентификатора доступа или иных конфиденциальных данных, например, CVV\CVC номера карты, с использованием которых осуществляются финансовые операции, закрытого ключа, посредством технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;
- воздействие вредоносного кода на устройствах клиента, с которых совершаются финансовые операции (любое техническое средство, включая, но, не ограничиваясь, персональный компьютер, планшет, мобильный телефон и пр., далее – устройство), который позволит злоумышленникам осуществить операции от имени клиента Общества;
- кража, утеря или по иным причинам получение несанкционированного доступа к устройствам, с помощью которых клиент осуществляет вход в автоматизированные системы (далее - системы) для совершения финансовых операций или получения информации в отношении таких операций, что позволит злоумышленникам осуществить операции от имени клиента Общества или использовать конфиденциальные данные клиента в иных противоправных целях;
- получения несанкционированного доступа к электронной почте клиента, к выпискам, отчетам и прочей финансовой информации, получение возможности отправки сообщений Обществу от имени клиента, если электронная почта клиента используется для информационного обмена;
- получение злоумышленниками персональных данных клиента Общества, пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих конфиденциальных данных путем обмана и/или злоупотребления доверием. Описанный риск может реализоваться, помимо прочего, когда злоумышленник представляется сотрудником Общества или техническим специалистом или использует иную легенду и просит клиента сообщить ему указанные конфиденциальные данные или направляет поддельные почтовые сообщения с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;
- совершение в отношении клиента Общества иных противоправных действий.

1.3. Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) для доступа к системам несет Владелец учётных данных. Общество 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.

Клиентам Общества следует предпринять все доступные меры для предотвращения несанкционированного доступа к защищаемой информации. Для указанных целей клиентам Общества следует принять, помимо прочего, следующие меры:

2.1. Обеспечение надлежащей защиты устройства с помощью которого клиенты пользуются услугами и обмениваются информацией с Обществом:

- использование только лицензированного программного обеспечения, полученного из доверенных источников;
- запрет на установку программ из непроверенных источников, не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, скаченные с неизвестных сайтов в сети Интернет, присланные с неизвестных адресов электронной почты;использование средств электронной безопасности и защиты, таких как антивирус с регулярно и своевременно обновляемыми базами, персональный межсетевой экран, защита накопителя и прочих;
- настройка прав доступа к устройству таким образом, чтобы несанкционированный доступ к информации на таком устройстве был невозможен даже при утрате устройства владельцем;
- хранение и использование устройства способом, исключающим риски его кражи и/или утери;
- своевременное обновление операционной системы устройства;
- активация парольной или иной защиты для доступа к устройству;
- незамедлительное изменение учетных данных, используемых для доступа к услугам, после удаления с устройства обнаруженного вредоносного программного обеспечения;
- передача защищаемой информации клиентов только через безопасные беспроводные сети. Работая в общедоступных беспроводных сетях, клиентам не следует вводить учетные данные, используемые для доступа к услугам;
- не использовать на устройствах ПО неизвестных разработчиков, которые не гарантируют отсутствие скрытых возможностей по сбору информации с устройств;
- исключить использование средств удаленного администрирования на устройствах;
- не использовать устройства третьих лиц для подключения к Системам для совершения финансовых операций или получения информации в отношении таких операций;
- не работать в Системах с устройства, использующего подключение к общедоступной wi-fi сети.

2.2. Обеспечение конфиденциальности защищаемой информации:

- хранение в тайне аутентификационных/идентификационных данных и ключевой информации, полученных от Общества: паролей, СМС-кодов, кодовых слов, закрытых ключей, сертификатов. В случае компрометации указанных данных клиенту следует принять меры для смены таких данных и/или уведомления Общества об их компрометации;
- соблюдение принципа разумного раскрытия информации о номерах счетов, паспортных данных, номерах кредитных и дебетовых карт, CVC/CVV кодах. В случае запроса у клиента указанной информации в связи с оказанием услуг Обществом, клиенту следует по возможности оценить ситуацию и уточнить полномочия отправителя запроса и процедуру раскрытия информации через независимый канал связи, позвонив в Общество только по номеру телефона, указанному на официальном сайте Общества в сети Интернет по адресу: www.region-rd.ru.

2.3. Проявление осторожности и предусмотрительности:

Клиенту Общества следует проявлять повышенную осторожность в следующих обстоятельствах:

а) при получении электронных сообщений со ссылками и вложениями, так как они могут привести к заражению устройства клиента вредоносным кодом;

б) при просмотре/работе с сайтами в сети Интернет, так как вредоносный код может быть загружен с сайта;

в) при получении файлов в архиве с паролем, так как в таком файле может быть вредоносный код.

Вредоносный код, попав к клиенту через почту или ссылку на сайт в сети Интернет, может получить доступ к любым данным и информационным системам на зараженном устройстве.

- следует внимательно проверять отправителя электронных сообщений. Входящее сообщение может быть от злоумышленника, который маскируется под Общество или иных доверенных лиц;
- клиентам Общества не следует заходить в системы удаленного доступа с ненадежных устройств, которые клиент не контролирует. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;
- при наличии в средствах массовой информации и на сайте Общества сведений о последних критичных уязвимостях и о вредоносном коде, клиентам рекомендуется принимать такую информацию к сведению;
- при обращении в контакт-центр Общества клиенту следует осуществлять звонок только по номеру телефона, указанному на сайте Общества в сети Интернет указанному на официальном сайте Общества в сети Интернет по адресу: www.region-rd.ru;
- при предоставлении клиентом доступа к устройству третьим лицам клиент несет риск загрузки такими лицами на устройство вредоносного кода. В случае утраты устройства злоумышленники могут воспользоваться им для доступа к системам Общества от лица клиента;
- при утрате телефона, используемого для получения СМС-кодов или доступа к системам Общества, клиенту необходимо совершить следующие действия:

а) проинформировать Общество по телефону контакт-центра и/или адресу электронной почты, указанным на сайте Общества в сети Интернет;

б) по возможности оперативно с учетом прочих рисков и особенностей использования телефона клиента заблокировать и перевыпустить сим-карту;

в) сменить пароль, воспользовавшись другим доверенным устройством, и/или заблокировать дистанционный доступ к услугам Общества, обратившись в Общество;

- при подозрении на несанкционированный доступ и/или компрометацию устройства клиенту необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать дистанционный доступ к услугам Общества, обратившись в Общество, в отношении ключевой информации, если это уместно для оказываемого клиенту Обществом вида услуг – отозвать скомпрометированный закрытый ключ;
- клиенту рекомендуется использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у клиента;
- в случае выхода из строя сим-карты, используемой для получения СМС-кодов, клиенту следует незамедлительно обратиться к своему сотовому оператору для уточнения причин неработоспособности сим-карты и восстановления связи;
- контактная информация, предоставленная клиентом Обществу, должна поддерживаться в актуальном состоянии для того, чтобы в случае необходимости представитель Общества мог оперативно связаться с клиентом.

2.4. <u>При работе с ключами электронной подписи необходимо:</u>

- использовать для хранения секретных ключей электронной подписи внешние носители;
- крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они не используются для работы;
- использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи, требующие ввода заглавных и прописных букв, цифр и специальных символов, в общем количестве не менее 8 символов. Не рекомендуется в качестве паролей использовать имена близких лиц, домашних животных, даты рождения и т.п., которые могут быть легко подобраны злоумышленниками;
- не хранить пароли в текстовых файлах на устройстве либо иных электронных носителях, не хранить пароль совместно с устройством;.
- выбирать пароли самостоятельно. Проводить регулярную смену паролей;
- не передавать третьим лицам пароли, коды доступа к устройству, а также пароли доступа в системы.

2.5. <u>При работе с защищаемой информацией на персональном компьютере необходимо:</u>

- 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 сложные пароли;
- ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

2.6. <u>При работе с мобильным устройством необходимо:</u>

- не оставлять устройство без присмотра, чтобы исключить его несанкционированное использование;
- использовать только официальные мобильные приложения, загруженные при помощи официального магазина приложений;
- не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие не от имени Общества в смс-сообщении, Push-уведомлении или по электронной почте;
- блокировать устройства после использования;
- использовать настройки устройства, требующие ввода пароля для его разблокировки и использования.

2.7. <u>При обмене информацией через сеть Интернет и использовании программного обеспечения на устройстве необходимо:</u>

- 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;
- исключить посещение сайтов сомнительного содержания (не открывать и не использовать сомнительные Интернет - ресурсы на устройстве);
- не сохранять пароли в памяти Интернет-браузера, если третьи лица имеют доступ к компьютеру;

- открывать файлы только известных расширений.
-

Для связи с Обществом по телефону и или электронной почте необходимо использовать только номер телефона и адрес электронной почты, указанные на официальном сайте Общества в сети Интернет по адресу: www.region-rd.ru.

Если по контексту настоящих Рекомендаций подразумевается, что предоставление услуг Общества может иметь дистанционных характер, то такие условия настоящих Рекомендаций применяются, только в случае если Обществом предоставляются подобные услуги.