Уважаемые клиенты АО ВТБ Регистратор!

Доводим 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. В связи с тем, что требования информационной безопасности так же могут быть отражены в договорах, регламентах, правилах и иных документах Акционерного общества ВТБ Регистратор (далее – Регистратор), регламентирующих предоставление услуг/сервисов, настоящие Рекомендации действуют в части, не противоречащей положениям иных документов Регистратора.

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;
- рекомендаций по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники, в целях противодействия незаконным финансовым операциям.

Несанкционированный доступ к защищаемой информации происходит, как правило, посредством удаленного доступа к устройствам клиента в результате взлома защиты устройства клиента, кражи устройства 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 рисками получения несанкционированного доступа к защищаемой информации является Фишинг и его различные типы (в зависимости от каналов распространения):

АО ВТБ Регистратор
Ул. Правды, д.23
Москва, 127015,
Россия
Тел.:
+7(495)787-44-83
Факс: +7(495)787-44-83
info@vtbreg.ru

«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. Зачастую фишинг является лишь первым этапом многоступенчатой таргетированной атаки. Целью злоумышленника может быть понуждение пользователя установить какое-либо вредоносное программное обеспечение, например, программу для записи парольной информации (keylogger), удаленного доступа к компьютеру или вирус-шифровальщик.

Техника «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, использование IP для нелегальной торговли.

Техника «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.

Метод «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 Регистратором на адрес электронной почты и/или абонентский номер клиента, содержащих защищаемую информацию;
- риск совершения иных юридически значимых действий, включая включение и отключение услуг (включая платные услуги), внесение изменений в регистрационные данные клиента, использование счетов и находящихся на них активов для прикрытия иных действий, носящих противоправный характер, совершение иных действий против воли клиента;

- 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;
- 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;
- не рекомендуется взламывать мобильное устройство путем выполнения «jailbreak» или получения Root-прав (возможность получения прав суперпользователя операционной системы мобильного устройства), т.к. это отключает защитные механизмы, заложенные производителем мобильной платформы. В результате таких действий мобильное устройство становится уязвимым к заражению вредоносным ПО.

2) Парольная защита:

- длина пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.
- не используйте один и тот же пароль для разных сервисов;
- используете парольную или иную защиту для доступа к устройству (например, установив пин-код или используя биометрические системы аутентификации устройства);
- при работе с ключами электронной подписи (если это применимо к вашему договору) используйте 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.

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

3) Обеспечьте конфиденциальность:

- блокируйте устройство после использования, используйте настройки устройства, требующие ввода пароля для его разблокировки и использования;
- не передавайте третьим лицам и не оставляйте устройство без присмотра;
- храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Регистратора: пароли, СМС коды, кодовые слова, ключи электронной подписи/шифрования, а в случае компрометации немедленно примите меры
- храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Регистратора: пароли, СМС коды, кодовые слова, ключи электронной подписи/шифрования, а в случае компрометации немедленно примите меры для смены и/или блокировки и сообщите Регистратору;

- 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, в привязке к сервисам Регистратора по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон клиентской службы Регистратора.

4) Соблюдайте правила безопасности в сети Интернет:

- ссылки на электронные сервисы Регистратора размещаются на официальном сайте компании https://www.vtbreg.ru. Для установки мобильных приложений используйте официальные источники, указанные на сайте Регистратора;
- 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. В случае необходимости и возникновении сомнений проверяйте вложения и сайты на соответствующих бесплатных онлайн сервисах, например: https://www.virustotal.com/gui/home/upload;
- не сохраняйте пароли в памяти интернет-браузера, особенно, если к компьютеру есть доступ третьих лиц;
- не открывайте и не используйте сомнительные Интернет - ресурсы на устройстве.

5) 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. Используйте телефон и мобильную передачу данных 3G/LTE в качестве альтернативного способа доступа к Интернет.

6) Проявляйте осторожность и предусмотрительность:

- внимательно проверяйте адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под Регистратор или иных доверенных лиц, при этом адрес отправителя очень похож на настоящий, но отличается на один-два символа;
- будьте осторожны при получении электронных писем со ссылками и вложениями, они могут привести к заражению вашего устройства Вредоносным кодом.

- проверяйте реальные адреса гиперссылок, содержащихся в письме, наводя на них курсор. Адрес, куда ведёт ссылка будет отображён в строке состояния почтовой программы. Особое внимание обращать на длинные ссылки или на гиперссылки, привязанные к тексту;
- следите за информацией в прессе и на сайте Регистратора о последних критичных уязвимостях и о Вредоносном коде;
- осуществляйте звонок в Регистратор только по номеру телефона, указанному в договоре или на официальном сайте Регистратора. Имейте в виду, что от лица Регистратора 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.

Настоящие рекомендации подготовлены с учетом требований «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», утвержденных Банком России 20.04.2021 № 757-П.

АО ВТБ Регистратор
Ул. Правды, д.23
Москва, 127015,
Россия
Тел.:
+7(495)787-44-83
Факс: +7(495)787-44-83
info@vtbreg.ru