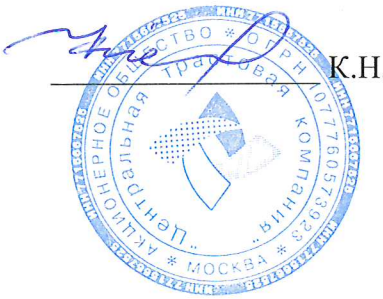
«УТВЕРЖДЕНЫ»

приказом генерального директора АО «Центротраст»
№ 6-2019/УК от 31.05.2019 г.



_____ К.Н. Кубушка

М.П.

Рекомендации клиентам Акционерного общества «Центральная трастовая компания» по защите информации в целях противодействия незаконным финансовым операциям

Москва
2019

1. Общие положения

1.1. Акционерное общество «Центральная трастовая компания» (далее - Управляющая компания) в соответствии с требованиями Положения Банка России от 17.04.2019 г. № 684-П доводит до сведения своих клиентов настоящие рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), уведомляет о возможных рисках получения несанкционированного доступа к защищаемой информации лицами, не обладающими правом такого получения, а также 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.

1.2. Кража учетных данных – это хищение личных данных клиента Управляющей компании в целях их незаконного использования для выполнения несанкционированных операций от имени клиента. Оптимальный способ защиты от кражи учетных данных состоит в умении распознавать способы этих злоумышленных действий для предотвращения таких ситуаций. При этом необходимо использовать комплексный подход, а вопросам информационной безопасности уделять достаточное внимание, как на стороне Управляющей компании, так и на стороне клиента.

2. Рекомендации по защите информации от воздействия вредоносного кода (вредоносная программа)

2.1 Вредоносная программа – это программа, наносящая вред мобильному устройству/компьютеру или иному устройству, на которых она запускается. Вредоносные программы способны самостоятельно (то есть без ведома владельца устройства), создавать свои копии и распространять их различными способами, что может привести к полному разрушению информации, хранящейся на устройстве, а также хищению личных данных клиента.

2.2 При наличии технической возможности на персональном компьютере клиента должно быть установлено программное обеспечение, которое должно регулярно обновляться. Рекомендуется установить по умолчанию максимальный уровень политики безопасности, то есть не требующий ответов пользователя при обнаружении вирусов. Лечение и удаления вирусов должно производиться в автоматическом режиме.

2.3 Не реже одного раза в неделю в автоматическом режиме должна производиться полная проверка жесткого диска персонального компьютера либо другого устройства, с использованием которого клиентом совершались действия в целях осуществления финансовой операции на предмет наличия вирусов и вредоносного кода. Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по средствам телекоммуникационных каналов, а также информацию на съемных носителях. При наличии технической возможности сканирование должно производиться в автоматическом режиме.

2.4 Рекомендуется не использовать компьютер, с которого клиент осуществляет операции с денежными средствами и иными активами, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания, так как именно через эти ресурсы сети Интернет чаще всего распространяют вредоносные программы.

3. Уведомление о рисках, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями третьих лиц

3.1. Клиенты Управляющей компании 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 (например, вследствие хищения) носителей информации, ключей электронной подписи, с использованием которых осуществляется взаимодействие с Управляющей компанией;

- воздействие вредоносного кода (вредоносных программ, приложений) на устройства клиента, с которых совершаются финансовые операции или осуществляется взаимодействие с Управляющей компанией (планшет, мобильный телефон и т.п., далее – устройство);

- совершение в отношении клиента иных противоправных действий.

3.2. При взаимодействии с Управляющей компанией и осуществлении операций клиентам следует принимать во внимание риск получения третьими лицами несанкционированного доступа к информации с целью осуществления ими несанкционированных операций с имуществом клиентов. Такие риски могут возникать, в том числе, вследствие следующих событий:

- кража пароля или иного идентификатора доступа, иных конфиденциальных данных, с помощью специальных устройств и/или вредоносного кода и использование злоумышленниками указанных данных для несанкционированного доступа;

- установка на устройство вредоносного кода, который позволит злоумышленникам осуществить операции от имени клиента Управляющей компании;

- кража или несанкционированный доступ к устройству, посредством которого клиент может пользоваться услугами Управляющей компании для получения данных и/или несанкционированного доступа к услугам с этого устройства.

- несанкционированное получение злоумышленниками персональных данных клиента. Описанный риск может реализоваться, помимо прочего, когда злоумышленник представляется сотрудником Управляющей компании или техническим специалистом, или использует иную легенду и просит клиента сообщить ему конфиденциальные данные или направляет поддельные почтовые сообщения с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;

- перехват почтовых сообщений и получение несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если электронная почта клиента используется для информационного обмена с Управляющей компанией. В случае получения доступа к почте клиента - отправка сообщений Управляющей компании от его имени.

3.3. Описанные выше риски, связанные с утратой и компрометацией учётных данных несет владелец таких данных.

4. Рекомендуемые меры по предотвращению несанкционированного доступа к защищаемой информации

4.1. Клиентам Управляющей компании рекомендуется предпринять все доступные меры для предотвращения несанкционированного доступа к защищаемой информации.

4.2. Меры по надлежащей защите устройства, с помощью которого клиенты пользуются услугами Управляющей компании и обмениваются с ней информацией, включают:

- использование только лицензированного программного обеспечения, полученного из доверенных источников.

- обеспечение запрета на установку программ из непроверенных источников.

- использование средств электронной безопасности и защиты, таких как антивирус с регулярно и своевременно обновляемыми базами, персональный межсетевой экран, защита накопителя и прочие;

- 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 Управляющей компании, 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 Управляющей компании.

4.3. Меры по обеспечению конфиденциальности защищаемой информации, в том числе:

- хранение в тайне идентификационных данных и ключевой информации, полученных от Управляющей компании. В случае компрометации указанных данных клиенту следует принять меры для смены таких данных и/или уведомления Управляющей компании об их компрометации;

- соблюдение принципа разумного раскрытия информации о номерах счетов, паспортных данных, иной информации. В случае запроса у клиента указанной информации в связи с оказанием услуг Управляющей компанией, клиенту следует по возможности оценить ситуацию и уточнить полномочия отправителя запроса и процедуру предоставления информации непосредственно у Управляющей компании.

4.4. Клиенту Управляющей компании 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, который, попав к клиенту через почту или ссылку на сайт в сети Интернет, может получить доступ к любым данным и информационным системам на зараженном устройстве.

4.4.1. Следует внимательно проверять отправителя электронных сообщений. Входящее сообщение может быть от злоумышленника, который маскируется под Управляющую компанию или иных доверенных лиц;

4.4.2. Клиентам Управляющей компании не рекомендуется заходить на сайты, в системы удаленного доступа с непроверенных устройств, которые клиент не имеет возможности контролировать.

4.4.3. При наличии в средствах массовой информации и на сайте Управляющей компании сведений о последних критичных уязвимостях и о вредоносном коде, клиентам рекомендуется принимать такую информацию к сведению.

4.4.4. При обращении в Управляющую компанию клиенту рекомендуется осуществлять звонок только по номеру телефона, указанному на сайте Управляющей компании в сети Интернет.

4.4.5. 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 Управляющей компании от лица клиента.

4.4.6. Клиенту рекомендуется использовать для связи с Управляющей компанией отдельное, максимально защищенное устройство, доступ к которому есть только у клиента.

4.4.7. Контактная информация, предоставленная клиентом Управляющей компании, должна поддерживаться в актуальном состоянии для того, чтобы в случае необходимости представитель Управляющей компании мог оперативно связаться с клиентом.

4.4.8. В случае использования клиентом при взаимодействии с Управляющей компанией

электронной подписи, клиенту рекомендуется:

- использовать для хранения ключей электронной подписи внешние носители;

- 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, не хранить пароли в текстовых документах на устройстве.

4.5. При работе с защищаемой информацией 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 и средства защиты от несанкционированного доступа;

- использовать сложные пароли;

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

4.6. При работе с мобильным устройством необходимо:

- не оставлять устройство без присмотра, чтобы исключить его несанкционированное использование;

- использовать только официальные мобильные приложения, загруженные при помощи официальных магазинов приложений;

- не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в смс-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Управляющей компании;

- установить на устройстве пароль для доступа к устройству.

4.7. При обмене информацией 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 не вызывающих доверие сайтах и других неизвестных клиенту ресурсах;

- исключить посещение сайтов сомнительного содержания;

- не сохранять пароли в памяти интернет-браузера, если третьи лица имеют доступ к компьютеру;

- не нажимать на баннеры и всплывающие окна, возникающие во время работы в сети Интернет;

- открывать файлы только известных клиенту расширений.

4.8. При подозрении в компрометации электронной подписи или несанкционированном движении активов клиенту следует незамедлительно обращаться в Управляющую компанию по телефону и/или адресу электронной почты, указанным на официальном сайте Управляющей компании в сети Интернет.