Рекомендации клиентам по защите информации

Уважаемые Клиенты!

Акционерное общество «Акционерный Банк «РОССИЯ» (далее – Банк) настоящим информирует клиентов, находящихся на депозитарном и брокерском обслуживании в Банке, а также клиентов, которым Банк оказывает услуги доверительного управления на рынке ценных бумаг, далее совместно именуемые Клиенты, о возможных рисках несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, используемого в целях осуществления финансовой операции, и необходимости ее защиты от воздействия вредоносного кода[1].

Возможные риски получения несанкционированного доступа к защищаемой информации

При осуществлении финансовых операций следует принимать во внимание риски финансовых потерь, связанные с получением несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, а также с воздействием вредоносных программ:

Кража аутентификационных данных (логин, пароль и т.п.) или иных конфиденциальных данных посредством программно-аппаратных средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа.

Установка на устройство вредоносной программы, которая позволит злоумышленникам осуществить операции от Вашего имени.

Кража или несанкционированный доступ к устройству, с которого Вы пользуетесь сервисами Банка для получения данных и/или несанкционированного доступа к сервисам с этого устройства.

Перехват сообщений электронной почты и получение несанкционированного доступа к отчетам и прочей финансовой информации, если Ваша почта используется для информационного обмена такой информацией.

К основным причинам возникновения рисков получения несанкционированного доступа к защищаемой информации относятся:

- неограниченный доступ третьих лиц к устройству;
- неограниченный доступ третьих лиц к аутентификационным данным (логин, пароль и т.п.);
- утрата (потеря, хищение) устройства;
- использование недоверенного программного обеспечения;
- отсутствие действующего актуального антивирусного программного обеспечения с актуальными вирусными базами.

Указанные риски и перечень причин не являются исчерпывающими.

Рекомендации по защите информации от вредоносного кода

Применение мер антивирусной защиты позволит обеспечить защиту информацию от воздействия вредоносного кода и (или) программ. Банком рекомендуется:

- использовать актуальные сертифицированные версии антивирусных средств защиты;
- регулярно обновлять антивирусные средства защиты и базы данных вирусов;
- проверять на наличие вирусов отчуждаемые (съемные) носители информации (например, USB-накопитель);
- выполнять сканирование персонального компьютера и (или) устройства на предмет наличия вирусов и вредоносного программного кода;

[1] Вредоносный код - программный код, приводящий к нарушению штатного функционирования средства вычислительной техники

- регулярно создавать резервные копии важных файлов и системных областей жестких дисков;
- не открывать файлы, полученные по электронной почте, от неизвестных отправителей.

Не рекомендуется запускать на исполнение файлы, полученные из сомнительных источников и предварительно не проверенные антивирусными программами.

Применяйте профилактическую защиту от загрузочных вирусов, которая заключается в отказе от загрузки операционной системы с гибких дисков и установке в BIOS вашего компьютера защиты загрузочного сектора от изменений.

Применяйте профилактическую защиту от макровирусов (разновидность компьютерных вирусов, разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office), в этом случае при запуске документа поступит сообщение о присутствии в загружаемом документе макросов (потенциальных вирусов) и предложение о запрете загрузки.

Рекомендации по защите информации от несанкционированного доступа путем использования ресурсов сети Интернет

При осуществлении финансовых операций рекомендуется:

- исключить использование информационно-телекоммуникационной сети Интернет через общедоступные/публичные точки доступа;
- убедиться, что вы находитесь на официальной странице/сайте;
- проверять адрес электронной почты отправителя письма, вложения и ссылки в письме;
- при работе в сети Интернет запретить установку каких-либо сомнительных программ.

Мошеннические и поддельные ссылки или фишинговые web-сайты могут быть почти точной копией подлинных, и предназначены для сбора конфиденциальной информации обманным путем.

Дополнительно Вы можете применять профилактическую защиту от вирусов и скриптов путем запрета в браузере получение скриптов на локальный компьютер, либо путем использования межсетевого экрана и модуля проверки скриптов, не переходите по сомнительным ссылкам, своевременно обновляйте базы системы безопасности операционной системы и приложений.

Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

При использовании мобильных устройств и (или) программных комплексов применяйте защиту паролем с учетом следующего:

- пароль должен быть сложным;
- рекомендуется использовать уникальные пароли для различных web-сайтов и систем;
- осуществляйте регулярную смену паролей;
- не сообщайте и не доверяйте аутентификационные данные (логин, пароль и т.п.) третьим лицам.

При доступе к мобильным устройствам рассмотрите возможность использования биометрических систем защиты. Рекомендуется исключить возможность физического доступа посторонних лиц к устройству.

Банк настоятельно рекомендует своим Клиентам предпринимать меры, направленные на предотвращение несанкционированного доступа к защищаемой информации и программным комплексам, включая, но не ограничиваясь программными комплексами, с помощью которых вами совершались (совершаются) действия в целях осуществления финансовых операций.