Приложение № 29 к РОФР, № 24 к РДО

Утверждено Приказом №1/29-11-2019 от 29.11.2019 г.
редакция, действующая с 16 декабря 2019 г.

РЕКОМЕНДАЦИИ по обеспечению информационной безопасности при использовании информационных технологий

ООО ВТБ Капитал Брокер (далее – Организация) ставит своей целью обеспечить предоставление услуг на высоком и профессиональном уровне. Для автоматизации предоставления услуг используются информационные технологии. Информационные технологии несут в себе присущие им риски информационной безопасности. ООО ВТБ Капитал Брокер доводит до сведения Клиентов (Депонентов) нижеследующие рекомендации по защите информации, в том числе о мерах по предотвращению несанкционированного доступа к защищаемой информации, например, при утрате (потере, хищении) Клиентом (Депонентом) устройства, с использованием которого Клиентами (Депонентами) совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода:

1. Требования информационной безопасности отражены в документах, оформляемых для предоставления Организацией той или иной услуги. Внимательно ознакомьтесь с разделом, посвященным информационной безопасности.
2. Обеспечьте защиту устройства, с которого вы осуществляете финансовые операции. к таким мерам могут относиться, включая, но не ограничиваясь:
   - наличие лицензированного программного обеспечения, полученного из доверенных источников;
   - наличие средства защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран, защита накопителя;
   - настройка прав доступа к устройству с целью невозможности несанкционированного доступа;
   - хранение, использование устройства с целью избежать рисков кражи и/или утери;
   - запрет на установку приложений из непроверенных источников.
3. Дополнительно:
   - будьте осторожны при получении писем со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносным кодом. Вредоносный код, попав к Вам через почту или интернет ссылку на сайт, может получить доступ к любым данным и информационным системам на вашем устройстве;
   - имейте в виду, что мошенники могут создавать поддельные сайты, используя схожую цветовую гамму и название Организации, направлять поддельные письма, как бы от лица Организации, будьте максимально внимательны;
   - внимательно проверяйте адресата, от которого пришло письмо. Входящее письмо может быть от злоумышленника, который маскируется под Организацию или иных доверенных лиц, в том числе и под представителей органов власти;
   - будьте осторожны при просмотре интернет сайтов, так как вредоносный код может быть загружен с сайта;
   - будьте осторожны с файлами в архиве с паролем, так как в таком файле может быть вредоносный код;
   - контролируйте необходимость обновления операционной системы в части обновлений безопасности. Имейте в виду, что обновления снижают риски заражения. Злоумышленники часто используют старые уязвимости;

- не заходите в системы удаленного доступа с недоверенных устройств, которые вы не контролируете. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;
- анализируйте информацию в прессе и на сайте Организации о последних критичных уязвимостях и о вредоносном коде;
- храните в тайне аутентификационные данные, полученные от Организации: пароли, СМС коды, кодовые слова, закрытые ключи, сертификаты, а в случае компрометации немедленно примите меры для смены и/или блокировки;

- при наличии в рамках вашего продукта сервиса контакт центра, осуществляйте звонок только по номеру телефона, указанному в договоре, для осуществления звонков в Организацию используйте телефон Организации из Регламента обслуживания на финансовых рынках. И имейте в виду, что от лица Организации не могут поступать звонки или сообщения, в которых от Вас требуют передать СМС-код, пароль, номер карты, кодовое слово и т.д.;
  - кодовое слово может быть запрошено только, если, Вы сами позвонили по телефонным номерам, указанным в регламенте обслуживания на финансовых рынках;
  - имейте в виду, что, 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, которыми пользовались Вы. В связи с этим при утере, краже телефона, используемого для получения СМС кодов или доступа к системам организации с Мобильного приложения:
    1) незамедлительно проинформировать Организацию через телефоны Организации, указанные в регламенте обслуживания на финансовых рынках;
    2) целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить сим карту, а также сменить пароль в Мобильное приложение. При утере иного устройства или подозрении на несанкционированный доступ – сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Организацию;
  - лучше всего использовать для финансовых операций отдельное, максимально защищенное, устройство, доступ к которому есть только у Вас;
  - контролируйте свой телефон. В случае выхода из строя сим карты, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи;
  - анализируйте выписки, остатки по Вашим счетам, выявляйте расхождения, в случае наличия - обращайтесь в Организацию для выяснения причин.