Приложение № 26 к Регламенту брокерского обслуживания ООО «БК РЕГИОН»

Уведомление 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 и защите информации от воздействия вредоносных кодов

I. Уведомление о рисках информационной безопасности, связанных с несанкционированным доступом к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, и воздействием вредоносных кодов.

В соответствии с требованиями 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 (утв. Банком России 17.04.2019 № 684-П) ООО «БК РЕГИОН» (далее – РЕГИОН) настоящим РЕГИОН доводит до сведения своих клиентов

- рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям.

- информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

- информацию о возможных рисках, связанных с использованием электронной подписи при подписании электронных документов и передаче таких документов по защищенным и/или открытым каналам связи;

- информацию 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.

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 кодов. Указанные риски могут быть обусловлены, включая, но не ограничиваясь, следующими ситуациями:

a. Кража пароля и идентификатора доступа или иных конфиденциальных данных, например, закрытого ключа посредством технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа.

b. Установка на устройство вредоносного кода, который позволит злоумышленникам осуществить операции от Вашего имени.

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

d. Получение пароля, идентификатора доступа и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником РЕГИОНА или техническим специалистом или использует иную легенду и просит Вас сообщить ему эти секретные данные; или направляет поддельные почтовые сообщения или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привес к компрометации устройства;

e. Перехвата почтовых сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если Ваша почта используется для информационного обмена с РЕГИОНОМ. В случае получения доступа к вашей почте, отправка сообщений от Вашего имени в РЕГИОН.

Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) для доступа к информационным системам РЕГИОНА несет Клиент.

РЕГИОН не несет ответственность в случаях финансовых потерь, понесенных Клиентами в связи с пренебрежением правилами информационной безопасности.

II. Рекомендуемые меры по предотвращению несанкционированного доступа к защищаемой информации и защите информации от воздействия вредоносных кодов.

1. Обеспечьте защиту устройства, с которого вы пользуетесь услугами РЕГИОНа, к таким мерам включая, но не ограничиваясь могут быть отнесены:
   - Использование только лицензированного программного обеспечения, полученного из доверенных источников.
   - Запрет на установку программ из непроверенных 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 предотвращения несанкционированного доступа.
   - Хранение, использование устройства с целью избежать рисков кражи и/или утери.
   - Своевременные обновления операционной системы.
   - Активация парольной или иной защиты для доступа к устройству.
   - В случае обнаружения злонамеренного программного обеспечения на компьютере после его удаления незамедлительно смените логин и пароль.
   - Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины.
2. Обеспечьте конфиденциальность:
   - Храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от РЕГИОНА: пароли, закрытые ключи, сертификаты, а в случае компрометации немедленно примите меры для смены и/или блокировки;
   - Соблюдайте принцип разумного раскрытия информации о номерах счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVC кодах, в случае если у вас запрашивают указанную информацию, в привязке к сервисам РЕГИОНА по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон контакт центра РЕГИОНА.
3. Проявляйте осторожность и предусмотрительность:

- 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.
- Внимательно проверяйте адресата, от которого пришло письмо. Входящее письмо может быть от злоумышленника, который маскируется под РЕГИОН или иных доверенных лиц.
- Будьте осторожны при просмотре/работе с интернет сайтами, 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.
- 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 иных общедоступных специализированных источниках о последних известных критичных уязвимостях и вредоносных кодах.
- Осуществляйте звонок в РЕГИОН только по номеру телефона, указанному в договоре. Важно учесть, что от лица РЕГИОНА не могут поступать звонки или сообщения, в которых от Вас требуют передать СМС-код, пароль, номер карты, кодовое слово и т.д.
- 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 РЕГИОНА, которыми пользовались Вы.
- При утере, краже телефона, планшета, персонального компьютера, используемого для доступа к системам РЕГИОНА необходимо:
    a. незамедлительно проинформировать РЕГИОН через отдел по работе с клиентами;
    b. целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить сим карту;
    c. сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в отдел по работе с клиентами РЕГИОНА.
- При подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в РЕГИОН, в отношении ключевой информации, если это уместно для Вашей услуги – отозвать скомпрометированный закрытый ключ, в соответствии с правилами, отраженными в договорных и/или процедурных документах;
- Помните, что наличие резервной копии может облегчить и ускорить восстановление Вашего устройства;
- 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.
- Регулярно выполняйте резервное копирование важной информации.
- Поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.

4. При работе с ключами электронной подписи необходимо:
    - В случае хранения секретных ключей электронной подписи на внешнем ключевом носителе крайне внимательно относиться к внешнему 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 компьютере.
5. При работе на компьютере необходимо:
    - 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.
6. При работе с мобильным устройством необходимо:
    - Не оставлять свое мобильное устройство без присмотра, чтобы исключить несанкционированное использование;
    - Использовать только официальные мобильные приложения;
    - Не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в SMS-сообщении, Push-уведомлении или по электронной почте, в том числе от имени РЕГИОНА;
    - Установить на мобильном устройстве пароль для доступа к устройству.
7. При обмене информацией через сеть Интернет необходимо:
    - 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 Вам ресурсах;
    - Ограничить посещения сайтов сомнительного содержания;
    - Не сохранять пароли в памяти интернет-браузера, если к компьютеру есть доступ третьих лиц;
    - Не нажимать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;
    - Открывать файлы только известных Вам расширений (docx, png, xlsx и т.д.).

При подозрении в компрометации ключей или несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов необходимо незамедлительно обращаться в РЕГИОН (тел. 495-777-29-64 доб. 636)

Настоящее уведомление составлено в двух экземплярах, один из которых находится у Клиента, другой - у РЕГИОНА.

Настоящим Клиент подтверждает факт уведомления 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 и защите информации от воздействия вредоносных кодов

Клиент:_____ Подпись _____/ _____/ "__" _____ 20__ года

мп