Рекомендации

по защите информации от воздействия программных кодов

В соответствии с требованиями Положения Банка России от 20.04.2021 № 757- П «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» ООО «УК «ИНТЕЛЛЕКТ-КАПИТАЛ» доводит до вашего сведения основные рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям.

Рекомендации по соблюдению информационной безопасности 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.

Риск реализации инцидентов информационной безопасности - нежелательные или неожиданные события защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов, технологических процессов и/или нарушения конфиденциальности, целостности и доступности информации вследствие:

* несанкционированного доступа к вашей информации лицами, не обладающими правом осуществления финансовых операций;
* потери (хищения) носителей ключей электронно-цифровой подписи, с использованием которых, осуществляются финансовые операции;
* воздействия вредоносного кода на устройства, с которых совершаются финансовые операции;
* совершения в отношении вас иных противоправных действий, связанных с информационной безопасностью.

Возможные риски

Риски несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, могут быть обусловлены в том числе следующим:

* кража конфиденциальных данных, например, CVV\CVC номера карты посредством технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;
* установка на используемое устройство вредоносного кода, который позволит злоумышленникам осуществить финансовые операции от вашего имени;
* кража или несанкционированный доступ к устройству, с которого вы осуществляете финансовые операции для получения данных и/или несанкционированного доступа к используемым сервисам с этого устройства;
* получение конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником финансовой организации или техническим специалистом, или использует иную легенду и просит вас сообщить ему эти секретные данные; или направляет поддельные сообщения с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства.

**Рекомендуемые меры по предотвращению несанкционированного доступа**

В целях снижения риска реализации инцидентов информационной безопасности рекомендуется соблюдать ряд профилактических мероприятий, направленных на повышение уровня информационной безопасности при осуществлении финансовых операций посредством автоматизированных систем.

Обеспечьте защиту устройства, с которого вы пользуетесь услугами финансовых организаций, в том числе:

* используйте только лицензионное программное обеспечение, полученное из доверенных источников;
* используйте антивирусную программное обеспечение, регулярно обновляйте антивирусные базы;
* используйте специализированные программы для защиты информации (персональные межсетевые экраны и средства защиты от несанкционированного доступа), средства контроля конфигурации устройств;
* ограничьте доступ к устройству, исключите (ограничьте) возможность дистанционного подключения к устройству третьим лицам;
* установите сложные пароли и регулярно их меняйте;
* своевременно устанавливайте актуальные обновления безопасности (операционные системы, офисные пакеты и т.д.);
* при работе на смартфоне отключите прием сообщений MMS. Прием MMS является серьезной уязвимостью вашего смартфона.
* не передавайте ваше устройство третьим лицам, они могу установить на него вредоносный код.

Обеспечьте конфиденциальность ваших персональных данных:

* соблюдайте принцип разумного раскрытия информации о номерах счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVC\CVV кодах;
* не вводите персональную информацию на подозрительных сайтах и других неизвестных вам ресурсах;
* не используйте социальные сети для отправки конфиденциальной информации, она может быть перехвачена злоумышленниками;
* при использовании программ для мгновенного обмена сообщениями (мессенджеров) всегда включайте функцию «сквозного» шифрования.
* не отправляйте ваши данные вместе с паролями по электронной почте. Используете разные ресурсы для отправки данных и пароля.

При работе в сети Интернет проявляйте осторожность и предусмотрительность:

* не подключайтесь к публичным сетям Wi-Fi. Надежней использовать мобильную сеть Интернет. Не допускайте автоматического подключения устройства к сетям Wi-Fi без вашего согласия;
* не передавайте личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины, данные платежных карт и прочую конфиденциальную информацию.
* не используйте программы-помощники переключения раскладок и исправления ошибок ввода. Такие программы сохраняют все набираемые символы и, тем самым, могут перехватывать пароли и конфиденциальные данные;
* убедитесь, что в адресной строке браузера указан верный адрес сайта финансовой организации;
* остерегайтесь веб-страниц, которые требуют установить программное обеспечение. Отменяйте установку, если вместе с требуемым приложением предполагается установка других программ;
* не открывайте файлы, полученные(скачанные) из недоверенных источников, они могут привести к заражению вашего устройства вредоносным кодом. Помните, что архивные файлы с паролем и зашифрованные файлы/архивы не могут быть проверены антивирусным ПО в автоматического режиме. Вредоносный код, попав к вам через электронную почту или интернет ссылку на сайт, может получить доступ к любым данным и информационным системам на вашем устройстве;
* не сохраняйте пароли в памяти интернет-браузера, если к компьютеру есть доступ третьих лиц;
* не нажимайте на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;
* ограничьте посещения сайтов сомнительного содержания.

Используйте дополнительные меры безопасности:

* 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;
* при подозрении на несанкционированный доступ и/или компрометацию устройства смените пароль, воспользовавшись другим доверенным устройством и/или заблокируйте доступ;
* для ответа на контрольный вопрос, необходимый для восстановления доступа к вашему устройству и/или аккаунту не используйте личные данные, такие как даты, фамилия или последние цифры номера телефона и т.п.;
* создайте резервную копию, это облегчит и ускорит восстановление вашего устройства;
* используйте для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у вас.