Приложение

к Приказу от 19.07.2019 № 167

Рекомендации

по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники в целях противодействия незаконным финансовым операциям для клиентов ООО МФК «КарМани»

В современном мире мобильный телефон, планшет, персональные компьютеры и ноутбуки превратились в устройства, содержащие не только колоссальные объемы персональных данных, сведений о личной человека, но и в средство управления финансами.

ООО МФК «КарМани» принимает необходимые и достаточные меры для поддержания уровня информационной безопасности со своей стороны, однако для достижения должного уровня информационной безопасности, необходимо так же соблюдения рекомендаций по защите информации со стороны клиентов, агентов и инвесторов, целью которых является минимизация рисков и возможного ущерба от действий со стороны злоумышленников.

Наибольшую опасность представляет кража Ваших учетных данных – паролей, логинов от электронной почты, банк-клиентов, социальных сетей, сайтов, которыми вы пользуетесь, мобильного приложения КарМани и личного кабинета. В этом случае, существует риск совершения операций от вашего имени лицами, не обладающими правом их осуществления.

Обновляйте устройства – производитель регулярно выпускает обновления безопасности для операционных систем телефонов и компьютеров, а так же для установленного на них иного программного обеспечения - почти каждое такое обновление устраняет серьезные уязвимости, которые могут эксплуатироваться злоумышленниками. Помните, что не обновляемое регулярно программное обеспечение и операционная система, практически всегда уязвимы. Правило обновления относится не только к устройствам, с которых вы выходите в Интернет или совершаете финансовые операции, но и к роутерам, маршрутизаторам, которые используются для подключения интернета, а также любым другим устройствам в домашней сети.

Избегайте использования для финансовых операций публичных WiFi сетей, особенно тех, которые не используют шифрование.

Не пользуйтесь сайтами, на которых отсутствует ssl-шифрование, для ввода и передачи любой информации с вашей стороны, особенно авторизации – данная информация передается в незашифрованном виде и может стать доступной злоумышленникам. Всегда проверяйте отсутствие предупреждений в браузере о недоверенных сертификатах либо их отсутствия на странице.

Не используйте сим-карты, которые не приобретены вами самостоятельно у операторов связи – на улице часто продают или раздают бесплатно сим-карты, оформленные на других лиц и доступ к которыми может быть в любое время заблокирован, а все сообщения будут приходить злоумышленникам.

Избегайте перехода по ссылкам и открытия файлов в сообщениях, полученных от неизвестных отправителей по электронной почте, смс, mms и мессенджерах. Приложения «получить наследство», «скачать счет», «посмотреть задолженность» могут привести к краже ваших данных и заражению устройства вредоносными программами. Более того, вредоносный код может быть получен даже от доверенных отправителей, например в случае

взлома их аккаунта, поэтому нужно также обращать внимание на изменившийся, например, стиль общения знакомого. И характер сообщения

Перед просмотром электронного письма проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты лишь схожий с официальным адресом компании.

Рекомендуется использовать официально купленную и регулярно обновляемую антивирусную защиту устройств, которые используются для пользования интернетом и совершения финансовых операций, однако нужно помнить, что антивирусная защита не является панацеей и не защищает 100% от вредоносного кода. Антивирус должен загружаться вместе с операционной системой и регулярно производить полную проверку диска, а также подключаемых внешних носителей (флешкарты, диски и т.п.)

Для дополнительной проверки файлов и ссылок можно использовать дополнительные бесплатные сервисы типа virustotal.com, где файл будет проверен антивирусами десятков производителей.

Устанавливайте программы и игры только из официальных репозиториев – google play, apple store, steam и т.п. Программы, скачанные с торрентов, сторонних сайтов могут быть инфицированы вредоносным программным обеспечением.

Не используйте права администратора на компьютере при обычной работе, не используете смартфоны с. полученными правами root для совершения финансовых операций.

Используйте шифрование на мобильных устройствах и ноутбуках – пинкод при включении, пароль для разблокировки экрана. В случае кражи или утери это позволит снизить опасность использования ваших данных злоумышленниками.

Используйте разные пароли в разных сервисах, избегайте использования простых паролей из цифр, сочетаний клавиш на клавиатуру, которые находится рядом (qwerty и т.п.). – такие пароли могут быть подобраны злоумышленниками за секунды. Меняйте пароль на домашнем WIFI, либо используйте длинные пароли.

Не пересылайте файлы с конфиденциальной информацией, особенно с паролями по электронной почте, мессенджерах и иных средствах коммуникации. Ваши пароли должны быть известны только вам.

Всегда обращайте внимание на системные уведомления и предупреждения программ, особенно об ошибках и критических событиях.

При подозрении на наличие вирусов на персональном компьютере (в частности, «зависаниях», перезагрузках, всплывающих баннеров, сетевой активности), рекомендуется воздержаться от совершения финансовых операций с устройства.

Помните, что ООО МФК «КарМани» не несет ответственности в случае возникновения финансовых потерь, понесенных в связи с нарушением и/или ненадлежащим исполнением рекомендаций по защите от вредоносного кода своих устройств для совершения финансовых операций.

Немедленно уведомляйте ООО МФК «КарМани» о любых признаках компрометации ваших учетных данных, утери (хищении) и телефона с приложением и подобных событиях любым доступным вам способом, а так же к оператору мобильной связи при необходимости блокировки и перевыпуска симкарты.