ООО «МКК КЕССАВ»

Адрес: 410065, г.Саратов, ул.Саперная, д.17

ИНН 6453128754 КПП 645301001 ОГРН 1136453002718

Рекомендации Клиентам ООО «МКК КЕССАВ» по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям.

Рекомендации по защите информации от воздействия вредоносного кода.

Общие рекомендации

Организуйте режим использования компьютера, с которого осуществляется использование систем дистанционного обслуживания, таким образом, чтобы исключить несанкционированное использование.

Используйте на вашем компьютере только лицензионное программное обеспечение, не устанавливайте программное обеспечение, полученное из сомнительных источников.

Рекомендуется ограничить права пользователя, использующего систему обслуживания, минимально необходимыми для работы с системой. Пользователь не должен обладать административными привилегиями.

Осуществляйте регулярный контроль состояния ваших счетов.

В сети Интернет получили широкое распространение специализированные вредоносные программы (трояны), обеспечивающие возможность похищения у пользователей систем дистанционного обслуживания файлов с секретными ключами электронной цифровой подписи (ЭЦП) и пароли. Трояны распространяются через электронную почту, по каналам сервисов мгновенной передачи информации, через принадлежащие злоумышленникам сайты. При этом злоумышленники похищают ключи ЭЦП, пароли доступа, что позволяет совершать операции от имени клиента.

При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

Своевременно обновляйте установленные программное обеспечение и операционную систему (установка критичных обновлений).

Обязательно установите и своевременно обновляйте на компьютере антивирусное программное обеспечение, но помните, что 100% защиты не обеспечивает ни одна программа.

Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы. Рекомендуется полная ежедневная проверка компьютера на наличие вирусов, иного вредоносного программного обеспечения. Исключить использование зараженного компьютера, вплоть до полного излечения от вирусов.

Антивирусное программное обеспечение должно регулярно обновляться.

Не отключайте антивирусное программное обеспечение ни при каких обстоятельствах.

При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам Сети Интернет.

При работе в Интернет не соглашайтесь на установку каких-либо сомнительных программ.

Не используйте для работы в системе дистанционного обслуживания компьютеры, расположенные в местах общего пользования (отелях, бизнес-центрах). Рекомендуется не использовать для работы с системой дистанционного обслуживания общедоступные каналы связи (например, Wi-Fi в кафе, отелях или аэропортах).

Не открывайте вложения электронных писем, полученные от неизвестных вам адресатов. Такие письма подлежат немедленному удалению.

По возможности, не сохраняйте пароль от системы дистанционного обслуживания в браузере.

При работе с системой дистанционного обслуживания обращайте внимание на адреса сайтов (убедитесь, что они являются официальными сайтами Общества).

Воздерживайтесь от использования программ онлайнового общения на компьютере, использующемся для работы в системе дистанционного обслуживания.

Исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер специальных «шпионских» программ. В частности, хорошей практикой является работа на компьютере от имени пользователя, не имеющего полномочий администратора.

Рекомендуем ограничить информационный обмен в сети Интернет только надежными информационными порталами и проверенными корреспондентами электронной почты.

Важно знать, что надежным средством обеспечения подлинности является цифровая подпись, а не строка адреса браузера или электронной почты. Часто в виде «интересной ссылки» в письме от якобы знакомого приходит вредоносная программа. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.

Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет.

Просим Вас отнестись с особым вниманием к расчетам в сети Интернет. Будьте внимательны: сайты мошенников могут быть почти точной копией тех, через которые Вы планировали осуществить платеж. Они созданы специально для получения Ваших персональных данных.

Если Вы обнаружили в сети Интернет ложный Web-сайт ООО «МКК КЕССАВ» (ООО), отличный от http://mkk-kessav.ru/, или с Вами пытаются связаться по электронной почте (электронная почта ООО «МКК КЕССАВ» - ooohotey2013@yandex.ru) или иным способом лица, с требованиями о предоставлении персональных идентификаторов доступа к системе дистанционного обслуживания, просьба немедленно сообщить об этом по телефону: 8 (8452) 45-16-87.

В целом, разработка и реализация комплекса мер по обеспечению информационной безопасности - сложная задача, требующая непрерывной работы квалифицированных специалистов. Однако, соблюдение перечисленных простых «гигиенических» мер позволяет существенно снизить риски, связанные с использованием систем

дистанционного обслуживания, с осуществлением платежей в сети Интернет и, в конечном итоге, предотвратить хищение Ваших денежных средств.

Рекомендации по снижению рисков получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.

Пользователям систем дистанционного обслуживания необходимо использовать дополнительные организационные меры по обеспечению информационной безопасности:

-Ключевые носители системы дистанционного обслуживания (дискета или флешка) должны храниться в сейфе, доступ к которому должен быть строго ограничен и предоставляться только уполномоченным лицам.

-Не рекомендуется использовать компьютер, на котором развернута программа дистанционного обслуживания (далее - компьютер), для просмотра посторонних (не относящихся к системе дистанционного банковского обслуживания) Интернет сайтов, работы с электронной почтой (особенно через общедоступные почтовые сервера: Mail.ru и т.д.), устанавливать игры и любые программы с пиратских дисков, просматривать видеофильмы, слушать музыку, загружать и устанавливать программы из Интернет, открывать и редактировать непроверенные антивирусом DOC, XLS, PDF файлы.

- В случае временного перерыва в работе с компьютером (совещание, обед и т.д.) необходимо завершить работу с программой дистанционного обслуживания, убрать в сейф ключевой носитель, выключить компьютер или заблокировать его клавиатуру и экран путем нажатия клавиш Ctrl-Alt-Del.

- Запрещается записывать пароли на бумажных листках (или в текстовых файлах на компьютере), оставлять их в легкодоступных местах (на рабочем столе), передавать неуполномоченным лицам. Если есть необходимость – храните все пароли записанными на одном листе, в сейфе, в опечатанном конверте.

Рекомендации по использованию парольной защиты

Не записывайте пароли, служащие для доступа к системе дистанционного обслуживания на бумажных носителях или в файлах на жестком диске вашего компьютера. Не сообщайте их другим лицам, в том числе вашим знакомым, друзьям, родственникам.

Используйте для доступа к системе дистанционного обслуживания сложные пароли, с наличием букв латинского алфавита в верхнем регистре (A-Z), букв латинского алфавита в нижнем регистре (a-z), цифр (0-9), специальных символов и знаков пунктуации (!@#$%^&*(),.?)

Не используйте простые пароли, представляющие собой осмысленные слова (password), дату рождения, номер телефона и т.д., последовательности повторяющихся на клавиатуре символов (qwerty), последовательности трех и более повторяющихся символов (77777777, 111adZZZ).

Рекомендации по использованию СМС подтверждений

При подтверждении ваших операций одноразовым СМС- кодом (паролем), всегда обращайте внимание на условия, реквизиты и иные данные поручения (иного вашего

распоряжения), которые вы подтверждаете, содержащиеся в полученном СМС-сообщении. Они должны соответствовать вашему волеизъявлению.

В случае утери мобильного телефона, незамедлительно обратитесь к оператору сотовой связи для блокировки вашей сим-карты.

Не устанавливайте на телефон, используемый для СМС-подтверждения, приложения из сомнительных источников.

Рекомендации по безопасному использованию мобильных приложений

Устанавливайте приложение исключительно по ссылкам в авторизованных магазинах приложений (App Store или Google Play).

Регулярно устанавливайте обновления безопасности для операционной системы вашего мобильного устройства.

Используйте лицензионные, постоянно обновляемые средства антивирусной защиты.

Используйте средства блокировки входа на ваше мобильное устройство (Пароль, Пин-код, TouchID, FaceID и иные).

Не посещайте с использованием мобильного устройства, сайты сомнительного содержания.

Не устанавливайте на мобильное устройство, программное обеспечение неизвестных разработчиков, распространяемое из сторонних источников (малоизвестных сервисов распространения приложений).

Не используйте приложение на мобильных устройствах, системная программная часть которых подверглась модификации, несанкционированной процедурам «Jailbreak», получению «Root»-прав, разблокировке загрузчика, установке версий операционных систем от неофициальных разработчиков).

При отсутствии необходимости, не используйте приложение для совершения операций по счету или совершения иных юридически значимых действий при подключении телефона к публичным сетям WiFi.