Приложение к письму
департамента информатизации и
связи Краснодарского края
от 22.08.2023 № 86-06-04-4336/23

Рекомендации по парольной защите:

– в качестве пароля рекомендуется использовать последовательности длинной не менее 12 символов;

– для формирования паролей требуется использовать алфавит, состоящий из строчных и прописных символов латинского алфавита, цифр, а также специальных символов (!, @, #, $, % и т.д.);

– генерацию новых паролей необходимо осуществлять на основе псевдослучайных функций;

– пароли, содержащие имена, названия городов, клички животных, номера телефонов, даты рождения, общепринятые слова и выражения, а также пароли типа "p@ssw0rd123", "qwerty12345", являются ненадежными;

– обновление паролей необходимо производить не реже, чем раз в 90 дней (при смене пароля необходимо менять его полностью, не ограничиваясь добавлением нескольких символов к прежнему паролю);

– необходимо настроить механизмы защиты от подбора аутентификационных данных, использовать меры по временной блокировке учетных записей;

– пароли недопустимо записывать на бумажных носителях и хранить в доступных местах;

– недопустимо хранить пароли в текстовых файлах на автоматизированных рабочих местах: в документах, на рабочих столах, а также на файловых серверах в общих каталогах, хранение аутентификационных данных допустимо только в криптографически защищенном виде;

– при возможности требуется включить двухфакторную аутентификацию;

Рекомендации по антивирусной защите:

– необходимо производить регулярное обновление используемого общесистемного и прикладного программного обеспечения;

– рассмотреть возможность замены используемого программного обеспечения и операционных систем, официальная поддержка которых прекращена производителем. В случае отсутствия такой возможности проводить периодическую корректировку настроек программного обеспечения и используемых средств защиты информации в целях минимизации возможностей эксплуатации уязвимостей;

– отказаться от использования незащищенных протоколов "HTTP", "TELNET", "FTP" и "SNMP" (версии 1 и 2);

– использовать отечественное сертифицированное антивирусное программное обеспечение и регулярно проверять компьютер на наличие вирусов;

– регулярно производить обновления баз антивирусного программного обеспечения.

Рекомендации по антивирусной защите мобильных устройств:

Вирусы на мобильных устройствах способны открывать удаленный доступ к устройствам пользователей, красть логины и пароли от банковских приложений, аккаунтов пользователей, перехватывать аутентификационную информацию из сообщений.

Факт заражение устройства возможно определить в том числе по следующим признакам:

– устройство зависает, самопроизвольно выключается или перезагружается;

– устройство само завершает работу приложений;

– устройство показывает различные всплывающие окна;

– теряется часть объема памяти, как оперативной, так основного

хранилища устройства.

В целях защиты мобильных устройств рекомендуется:

– использовать антивирусное программное обеспечение и регулярно его обновлять;

– не переходить по ссылкам, полученным от незнакомцев, не устанавливать приложения по их просьбе;

– скачивать приложения исключительно из проверенных источников;

– обновлять операционную систему мобильных устройств;

– избегать использование общедоступных Wi-Fi сетей.

Рекомендации по противодействию фишинговым рассылкам:

Фишинговые письма могут содержать вредоносные вложения (архивы, текстовые и исполняющие файлы), предложение перехода на сторонние ресурсы, например, в целях принятия участия в онлайн конференциях или ознакомления с копиями бухгалтерских документов.

Конечная цель таких запросов может быть различной, начиная от рекламы коммерческих образовательных программ и обеспечения прохождения интернет трафика на рекламных страницах, заканчивая попытками внедрения вредоносного программного обеспечения.

Фишинговые рассылки могут направляться как на адреса рабочей и личной электронной почты, так и в сообщения через мессенджеры и социальные сети.

Для того, чтобы не стать жертвой фишинговых рассылок рекомендуется:

– не использовать личную электронную почту в служебных целях;

– с подозрением относиться к любым письмам с вложениями и ссылками, полученными от неизвестных отправителей;

– обязательно проверять известные URL-адреса, по которым рекомендуется перейти, на наличие незначительных ошибок в написании;

– использовать безопасные https-соединения;

– получив подозрительное сообщение от имени знакомого отправителя, но с незнакомого адреса электронной почты, либо номера телефона стоит связаться с отправителем каким-либо альтернативным способом;

– внимательно относиться к сообщениям, содержащим гиперссылки;

– перед пересылкой писем от незнакомых источников необходимо производить проверку источников таких запросов, принадлежность домена, к которому относится адрес электронной почты отправителя, а также принадлежность домена и хостинга интернет ресурса, на который предлагается перейти, согласно таким письмам.

Рекомендации по защите личной информации:

– регулярно менять пароли от аккаунтов в социальных сетях и почтовых ящиков, не использовать один и тот же пароль для разных сервисов.

– использовать дополнительный (специальный) почтовый ящик для регистрации на сайтах, маркетплейсах, социальных сетях;

– при онлайн покупках в информационно-телекоммуникационной сети "Интернет" рекомендуется использовать отдельную банковскую карту с небольшим объемом средств;

– ознакамливаться с политикой конфиденциальности сайтов;

– закрыть свои аккаунты в социальных сетях и включить двухфакторную аутентификацию;

– не выкладывать в социальных сетях личную информацию и фотографии документов;

– не принимать cookie-файлы на сайтах автоматически.