Безопасное использование электронной почты

Сегодня доступ в интернет имеет практически каждый. Кому-то он необходим для выполнения служебных обязанностей, кто-то использует его для учебы, для игр и просмотра фильмов, но практически всех активных пользователей глобальной сети объединяет одно — использование электронной почты.

При быстром ритме современной жизни электронная почта стала важным средством коммуникации. Используя электронную почту, мы можем моментально отправлять и получать письма, документы, программы, фотографии, любые файлы. Кроме того, для регистрации на большинстве ресурсов требуется привязка Вашей электронной почты.

Однако не стоит забывать, что по электронной почте могут приходить не только «полезные» письма. Они могут содержать ссылки на сайты злоумышленников, целью которых является выведать у пользователя важную информацию, или вредоносные файлы, которые, попав на компьютер, могут доставить много неприятностей.

Основной мотив злоумышленника — получение денег. Используя электронную почту в качестве инструмента для совершения злонамеренных действий, он может:

- продавать взломанные аккаунты для рассылки спам-сообщений;
- использовать взломанный аккаунт электронной почты для восстановления паролей других учетных записей, при регистрации которых использовался взломанный адрес (банкинг, соцсети, игровые аккаунты и т.п.)
- использовать информацию из личной или деловой переписки в различных схемах мошенничества;
- вымогать деньги, шантажируя владельца аккаунта;
- рассылать спам-сообщения с адреса взломанной электронной почты.

Использование электронной почты без соблюдения определенных мер безопасности может угрожать безопасности вашего компьютера и тем самым нанести вред вам.

Письма, приходящие по электронной почте, могут содержать вредоносные файлы или ссылки, ведущие на зараженные сайты. При открытии такого файла или переходе по ссылке вирус попадает на компьютер пользователя.

Для защиты компьютера от заражения вирусом необходимо:

– установить на компьютер средство антивирусной защиты и регулярно обновлять антивирусные базы;
– регулярно обновлять операционную систему и программное обеспечение, установленные на компьютере;
– не переходить по ссылкам из подозрительных писем;
– не открывать письма с вложениями, полученные от неизвестных отправителей.

Злоумышленник может попытаться угадать пароль от электронной почты путем перебора наиболее часто встречающихся комбинаций, например 12345, qwerty, p@ssw0rd и т.п., сейчас в открытом доступе можно найти огромное количество собранных баз данных с десятками и сотнями тысяч наиболее часто используемых паролей. Пароли, состоящие из фамилии, даты рождения, номера телефона также могут быть легко угаданы. Подобрав пароль, злоумышленник получает полный доступ к почте жертвы.

Чтобы оградить свою электронную почту от рук злоумышленника, рекомендуется:

– создать сложный пароль;
– менять пароли;
– не хранить пароль на компьютере;
– не использовать основной адрес электронной почты для регистрации на каких-либо ресурсах;
– придумать разные пароли для разных сайтов;
– указать контрольный вопрос и номер телефона для восстановления пароля электронной почты.

Для восстановления пароля электронной почты рекомендуется выбрать контрольный вопрос и задать для него ответ. Однако стоит помнить, что если ответ на контрольный вопрос будет очевидным, то злоумышленник сможет легко его угадать.

Рекомендуется использовать уникальный вопрос и легко запоминающийся ответ, который будете знать только вы и который трудно угадать.

По электронной почте могут приходить письма, якобы от лица администратора соцсети или от сотрудников банка — с просьбой прислать свои логин и пароль, например якобы для восстановления после сбоя базы данных, или с просьбой перейти по ссылке для подтверждения адреса электронной почты. Зачастую, перейдя по ссылке, можно обнаружить запрос на ввод данных (пароля, логина, номера банковской карты и т. п.). При этом страница сайта внешне может быть похожа на ресурс, которым вы привыкли пользоваться (соцсеть, интернет-банкинг). Однако если обратить внимание на адрес такой страницы, то можно заметить, что он незначительно отличается от оригинального, например вместо «о» может стоять «0» или вместо «l» — «I».

Как только запрашиваемые данные будут введены на такой лжестранице, они сразу же попадут в руки злоумышленника, который сможет воспользоваться ими в своих корыстных целях.

Для того чтобы этого избежать, необходимо руководствоваться несколькими простыми правилами:

– не отвечайте на письма от неизвестных отправителей;
– не переходите по ссылкам, содержащимся в письмах;
– не сообщайте приватную информацию, запрашиваемую в письмах, приходящих по электронной почте.

Не рекомендуется сообщать пароль от почты кому бы то ни было. Если в какой-то момент вам пришлось предоставить друзьям или коллегам доступ к своему электронному ящику или если у вас возникло подозрение, что кто-то посторонний узнал ваш пароль, — необходимо как можно скорее его сменить.

При подключении к незащищенным точкам доступа передаваемые данные не шифруются, поэтому злоумышленник может перехватить их при помощи ноутбука с Wi-Fi-адаптером. Используя специальную программу для «перехвата трафика», злоумышленник сможет увидеть все данные, передаваемые по такой сети, в частности пароль от электронной почты.

Для того чтобы обезопасить себя от перехвата паролей рекомендуется:

– не пользоваться открытыми Wi-Fi-сетями для доступа к электронной почте, соцсетям и прочим ресурсам, требующим ввода пароля;
– использовать VPN при подключении к открытым точкам доступа Wi-Fi;
– отключить общий доступ к файлам на устройстве.

Если не соблюдать указанные выше рекомендации, взлом почтового ящика может стать для Вас неприятным сюрпризом.

Скорее всего, ваш почтовый ящик взломали, если:
– не удается войти в электронную почту (пароль не подходит);
– вам сообщили, что с вашего адреса приходят письма, которых вы не отправляли (или в папке «Отправленные» появились такие подозрительные письма);
– исчезли письма, которых вы не удаляли;
– письма, которых вы не читали, помечены как прочитанные;
– установлен пароль на папку «Входящие».

В этом случае необходимо:
– проверить компьютер на вирусы;
– попробовать восстановить пароль по секретному вопросу, с помощью дополнительного адреса или номера мобильного телефона (если это удастся, нужно немедленно сменить пароль и секретный вопрос);
– обратиться в службу поддержки и сообщить о проблеме.