Ежедневно мы получаем значительное число электронной корреспонденции: информационные сообщения, различные уведомления и предложения, личную почту. Мы, не задумываясь, переходим по прикреплённым ссылкам в письмах, загружаем файлы и фотографии, пересылаем необходимые данные. При этом мы не учитываем, что количество информации о нас, содержащейся в электронном почтовом ящике, прирастает ежедневно, ведь именно к электронной почте «привязаны» учётные записи практически всех сервисов, и взлом электронной почты позволяет получить к ним доступ.

В ежедневном потоке сообщений злоумышленникам не составляет никакого труда спрятать письма, реальная цель которых не сообщить значимую информацию, а добыть её у пользователя или вынудить совершить какие-либо действия. Стоит понимать, что любая информация, которой мы обмениваемся в Интернете, представляет потенциальную ценность, если знать, как правильно ей воспользоваться.

Первым шагом на пути повышения уровня безопасности при работе со своей электронной почтой является использование надёжного пароля, известного только вам. Конечно, встречаются ситуации, когда кто-то просит сообщить пароль от почтового аккаунта, но, делая это, стоит помнить о том, что под видом того, кого вы хорошо знаете, могут действовать злоумышленники, получив доступ к его аккаунту.

Вводить логин и пароль от электронной почты в достаточной мере безопасно лишь на официальном сайте почтового сервиса или в почтовой программе. Обращайте внимание непосредственно на адрес страницы, где предлагается ввести реквизиты для доступа, поскольку внешний вид ресурса можно подделать и единственным способом в этом удостовериться является правильность написания адреса почтового сервиса. Если данные будут введены на небезопасном сайте, то с высокой долей вероятности ими воспользуются злоумышленники.

Используя электронную почту, всегда должны настораживать:

- любые требования и просьбы сообщить пароль или иные персональные данные, поступившие даже от знакомого лица или якобы от представителя службы безопасности;
- любые письма с требованиями ввести или отправить свой пароль от онлайн-банка или реквизиты банковской платёжной карты. Этими сведениями должен владеть только держатель карты и даже сотруднику банка их сообщать не стоит;
- всплывающие окна, в том числе с предложениями поучаствовать в беспроигрышных акциях, а также письма с

неоправданными пометками «Срочно!» и невнятно сформулированной темой письма. Помните: чем соблазнительнее предложение, тем выше вероятность того, что оно мошенническое.

Немаловажное значение в обеспечении безопасного использования электронной почты является внимательное отношение к содержимому входящей корреспонденции. Прикреплённые файлы обычно воспринимаются как рабочий инструмент и подозрения не вызывают, из-за чего на расширение файла внимание обращается в последнюю очередь (расширение объясняет системе, какие действия необходимо выполнить с этим файлом):

*.doc - документ Word;

*.bat - пакетный файл, содержащий последовательность исполняемых команд;

*.exe - исполняемый файл, запускающий определённую программу;

*.vbs - сценарий, написанный на языке Visual Basic, также используется для выполнения команд и программ в Windows;

*.js - JavaScript; открывая такой файл, запускается определённая последовательность действий;

*.scr - файлы с этим расширением используются в системе Windows как заставка экрана.

Файл, открытый (запущенный) или загруженный из ненадёжного источника, может запустить на компьютере определённые действия, направленные на получение конфиденциальной пользовательской информации, использование ресурсов компьютера для совершения противоправной деятельности, а также на причинение вреда самому пользователю, в том числе путём шифрования данных на его компьютере. Стоит запомнить, что открытие любых исполняемых (запускающих выполнение определённых процессов) файлов, полученных по электронной почте – это всегда риск, и перед его открытием стоит как минимум проверить его расширение. Файлы с расширениями .exe, .js, .vbs, .scr и т.д., а также с двойными расширениями .txt.exe, .pdf.scr, .doc.js, mp3.vbs, .jpg.exe потенциально угрожают вашей информационной безопасности. Любые файлы с неизвестными и непонятными расширениями должны вызывать опасение и их необходимо проверять антивирусом, предварительно сохранив файл на диск, не открывая его.

Для того чтобы обезопасить себя и свою электронную почту, рекомендуется:

- использовать сложные пароли, состоящие из букв, цифр и специальных символов, никому и ни под каким предлогом его не сообщая;

- обращать внимание на адрес ресурса, на котором находитесь. Перейдя по подозрительной ссылке, рекомендуется не вводить свою конфиденциальную информацию и не загружать какие-либо файлы;
- не хранить в электронной переписке сведения о банковской платёжной карте;
- не открывать и не запускать подозрительные файлы с неизвестными расширениями, а также исполняемые файлы с расширениями .exe, .vbs, .js, .scr и т.д;
- использовать двухфакторную систему идентификации, привязав электронную почту к абонентскому номеру телефона. При её использовании авторизация с применением нового устройства будет невозможна без введения кода, поступающего в смс-сообщении.