Пожалуйста, прочитайте эту страницу внимательно. Несоблюдение этих простых правил может привести к тому, что все Ваши пароли станут известны другим, нужная информация исчезнет с диска и нормальная работа компьютера будет нарушена. Будьте осторожны!

Никогда не запускайте программы, полученные по электронной почте. Это может показаться смешным, но это действительно опасно, даже если письмо прислал хорошо известный Вам человек. Если есть подозрение что это вирус или Троян, просто удалите письмо.

Не доверяйте даже «солидным» адресам, типа support@mail.ru или webmaster@mail.ru. Почтовые сервера никогда не рассылают программ своим пользователям, однако адрес отправителя очень легко подделать и многие этим пользуются, чтобы под видом службы поддержки рассылать вирусов или Троянов.

Никому не отдавайте свой пароль! Если Вам пришло письмо с требованием сообщить все данные о себе, включая пароль от вашего электронного ящика, ни в коем случае не отдавайте пароль, даже если это письмо пришло с адреса webmaster или support. Не доверяйте доводам вроде «устранения технических проблем с Вашим ящиком» и не бойтесь угроз Ваш ящик закрыть. Это наглая попытка собрать пароли никакого отношения к службе поддержки не имеет. К сожалению, адрес отправителя очень легко подделать. Почтовые сервера никогда сами не просят пользователей прислать действующий пароль к почтовому ящику.

Открывая полученные файлы MS Office (Word — .doc, Excel — .xls и т.д.) не разрешайте использование макросов.

Старайтесь пользоваться самими свежими почтовыми программами. В любой из них периодически находятся «дырки» в безопасности, и злоумышленники тут же ими пользуются. В свежих версиях, как правило, эти ошибки исправляются. Популярные программы: Outlook Express, Netscape Messenger, web-интерфейс Mail.ru, опять же, — бесплатны, так что не пренебрегайте этим советом. Н

Например, Вы можете получить по почте письмо такого вида: «Привет! Меня зовут Даша, мне 19 лет, симпатичная. Давай познакомимся. Можешь посмотреть мою фотку». К письму прикреплен файл с «фоткой», которая на самом деле и является тем самым трояном. Запустив эту программу, Вы, может быть, и увидите фотографию, но заодно и отдадите этой самой Даше все свои данные. И скорее всего не Даше, а злоумышленнику, который не прочь попользоваться Сетью за Ваш счет.

Также в сети очень распространен такой способ выманивая паролей. Злоумышленник заводит себе почтовый ящик на mail.ru с адресом, похожим на служебный: pass_robot_support@mail.ru и т.д. или любой другой. Далее злоумышленник рассылает письмо тем, пароль от чьих почтовых ящиков он хочет получить, либо создает страничку и рассылает ссылку на нее. Текст письма или странички всегда разный, но смысл такой: в Mail.Ru дыра, отправьте на адрес pass_robot_support@mail.ru (адрес может быть совершенно любым, главное — похожим на служебный) имя Вашего почтового ящика, пароль к нему, а также имя чужого почтового ящика, от которого Вы хотите получить пароль, тогда в ответ на такой запрос Вы получите пароль от интересующего Вас почтового ящика. Этот трюк рассчитан на тех, кто хочет получить пароль от чужого почтового ящика, и настолько доверчив, чтобы пропустить мимо самое главное: что на адрес злоумышленника (в нашем примере это pass_robot_support@mail.ru) человек собственными руками отправляет пароль от своего почтового ящика!!! Таким образом, неудавшийся «хакер» после отправки такого письма псевдо-роботу может попрощаться со своим почтовым ящиком.