

Осторожно, Интернет!

Работу выполнила
Белоблоцкая Алёна
ученица 10 класса
МОУ СОШ №13 им. Р. А. Наумова



Опасности Интернета

Что такое Интернет знает каждый, о нем наслышан даже никогда не бывавший в нем человек. Это всемирная база данных, которая не имеет границ и национальностей. Любой человек из любой страны мира может легко и быстро получить доступ к интересующей его информации в Интернете. Многие наверно помнят то время, когда чтобы найти нужную информацию в библиотеке, нужно было потратить несколько часов на утомительные поиски. Или найти нужную программу в магазине, тоже подчас нелегко. В Интернете это легко и просто, а главное быстро! Но далеко не каждый пользователь знает и догадывается, что наряду с большими преимуществами, Интернет таит в себе и большие опасности. Их достаточно много.

Вирусы

Вирусы – программы, добавляющие свой вредоносный код в другие программы, тем самым, заражая их чтобы получить управление зараженными программами.

Поймав в Интернете вирус, Вы рискуете потерять ценную для Вас информацию или хуже того вывести из строя компьютер. Некоторые вирусы способны переписать без Вашего согласия системную BIOS или загрузочные сектора жесткого диска, в результате чего становится невозможным загрузить компьютер. Кроме того, вирусы способны самостоятельно распространяться по локальному компьютеру и по сети, заражая другие компьютеры.



Троянские программы

Троянские программы (Trojans или Trojans Horses) представляют собой программы, выполняющие несанкционированные пользователем действия на компьютере. В зависимости от условий, троянские программы уничтожают информацию на жестком диске, приводят систему к зависанию, воруют конфиденциальную информацию (например, пароли доступа к Интернету, к почте и т.д.) Часто троянские программы представляют собой утилиты скрытого удаленного администрирования (backdoors). В отличие от вирусов, троянские программы не являются вирусами в традиционном понимании понятия «вирус». Они не могут самостоятельно распространяться, не заражают программы и не портят их. Поэтому троянские программы распространяются злоумышленниками под видом полезного программного обеспечения.

Программы-шпионы

Программы-шпионы (Spyware) собирают информацию о Вашем компьютере, об установленном программном обеспечении, о Ваших предпочтениях в Интернете и отсылают по заложенному в них адресу. В основном это делается, для того чтобы в дальнейшем украсть регистрационную информацию программ. Ведь ни для кого не секрет, что в России не принято платить за программное обеспечение. Подавляющее большинство пользователей пользуется похищенными регистрационными данными. Интернет предпочтения пользователей собирают маркетинговые службы некоторых сайтов. О наличии программ-шпионов на своем компьютере, Вы можете и не догадываться.

Программы-рекламы

Программы-рекламы (Adware) представляют собой программный код, включенный без ведома пользователя в рабочий интерфейс программы. Помимо того, что программы-рекламы показывают информацию рекламного содержания, они могут изменять стартовую страницу браузера на свою, создают неконтролируемый пользователем трафик и, как и программы-шпионы, могут передавать своему разработчику персональные данные пользователя без его ведома. Программы-рекламы способны нарушить политику безопасности и привести к прямым финансовым потерям.

ФИШИНГ

Фишинг (Phishing) – вид Интернет мошенничества. Потенциальной жертве злоумышленник посылает письмо, оформленное под официальное, например, от банка или какой либо компании, специализирующейся на предоставлении каких либо услуг. В этом письме Вам предлагается пройти на тщательно подготовленный и оформленный под официальный сайт, на котором Вам необходимо указать Вашу конфиденциальную финансовую информацию. Например, пароли доступа к Вашей персональной банковской страничке или номер кредитной карточки. Передав на фишинг-сайт Вашу конфиденциальную информацию, злоумышленник получит ее и не замедлит ею воспользоваться. Политика таких сайтов кража Вашей финансовой и другой информации.

Спам

Спам (Spam) – массовая несанкционированная рассылка писем пользователю без его на то согласия, часто рекламного и агитационного содержания. Спам, помимо нагрузки на почтовый сервер, отвлекает пользователя от работы, повышает трафик. Спам-письма могут привести на мошеннические фишинг-сайты.

Некоторые правила, которые МОГУТ СНИЗИТЬ РИСК ЭТИХ опасностей

- Установите на свой компьютер антивирусную программу!
- Старайтесь, по мере возможности, регулярно обновлять базы Вашей антивирусной программы.
- Установите на свой компьютер персональный межсетевой экран (брандмауэр)!
- НИКОГДА не открывайте скачанный с Интернета файл, не проверив сначала его антивирусом!
- НИКОГДА и ни под каким предлогом не отвечайте на спам-письма!
- Старайтесь обновлять Ваши программы, если разработчики в них обнаружили уязвимости.
- Ограничьте круг лиц, допущенных к работе с Вашим компьютером.

ИСТОЧНИКИ

- www.megakomp.info
- http://go.mail.ru/search_images