Internet Security

Posted At : October 16, 2009 12:10 PM | Posted By : Andrea
Related Categories: security, Internet news, Jargon Buster

Jargon Buster - Spam Scams

What is Spam?

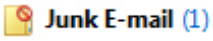
Spam, E-mail spam, or junk E-mail is the abuse of electronic mail systems, to send unsolicited bulk messages to as many recipients as possible. Several billion spam email messages are received every day, causing confusion and frustration in its victims. Unfortunately, spam has evolved over the years and can now do a lot more than just annoy us. Fortunately however, Computer Internet Security has also evolved and if kept updated, can help block both spam and the viruses, spyware, adware and malware that can attack your computer. So don't panic - just be extra cautious and aware!

What are viruses, spyware, malware and adware?

They're all software programmes that can attack your computer without your knowledge or consent, contaminate your operating system or data files, disrupt your privacy and dramatically reduce your computers working speed. **Viruses** are programs that can copy themselves and infect your computer. **Spyware** is computer software, which can obtain information from your computer. **Malware** is software designed to infiltrate or damage your computer system and **Adware** is software that can load itself onto your computer, track your browsing habits and pop up advertisements. All four can be a real pain in the hard drive to computer users and website builders alike.

Watch out for the Warning Signs!

There are warning signs, which you can watch out for: such as



receiving emails accusing you of sending spam, spotting emails in your "outbox" that you know you didn't send or your computer working unusually slowly. The most immediate defence however is being very careful with the emails you receive. You must be especially wary of Emails with attachments, links or images, which, when clicked on or opened, can install hidden software, which then allows spammers to spy on your Internet activity, steal personal information, and use your computer to send further spam to all your address book contacts without your knowledge. This involuntary recruitment of computers creates networks, known as a "botnets" or Robotic Networks. A botnet could include hundreds of thousands of home computers all sending emails. Spammers obtain E-mail addresses from chatrooms, websites, customer lists, newsgroups and viruses which pilfer address book contacts.

Scams, Cheats, Traps and Frauds.

Spam is also used to circulate Scams or Bogus Offers. These Scams can be very cleverly disguised with beguiling authenticity to make them look legitimate. Some already know certain pieces of information such as names, business names, account names etc., others offer an invitation to a website offering full details, claims and promises. Some give testimonials from supposedly successful millionaires and winners. All need to be ignored and reported and forwarded to the FTC at spam@uce.gov.

The Top Scams currently in circulation are:

The "Foreign Funds" Scam, offering huge payments in return for help to access money in foreign countries.

Phishing Emails, claiming to be from businesses or organisations you actually deal with such as your Internet service provider (ISP), website host, bank, online payment service or other online accounts you may have such as ebay or amazon. You may be asked to "update," "validate," or "confirm" your account information including usernames and passwords. Once they have your details, they have an open door to all your information! ***Reason8, along with most online businesses will NEVER ask you for your username, password or login***

information by email, so if you receive an email asking for this information, even if it looks legitimate, forward it to the authorities or the company it is claiming to have come from.

and; Work at Home Schemes, Weight Loss Claims, Foreign Lotteries, Cure All Products, Cheque Overpayment Scams, Pay in Advance Credit Offers, Debt Relief and Investment Schemes.
All of which are scams to watch out for.

You can help to secure your computer by:
Using anti-virus and anti-spyware software and keeping it up to date.
Use caution when opening any attachments or downloading files from emails. *If you're not expecting it or you don't know what it is – DON'T OPEN IT!*
Use a firewall to protect your computer while it's connected to the Internet.
Disconnect from the Internet when you're away from your computer *by Shutting Down or putting your computer into Sleep Mode.*
Only download free software from sites you trust. *Many free software applications such as games are free because they carry spyware.*
Check your "sent items" or "outbox" regularly for strangers. *If you find strange or unknown messages in your outbox, your computer could be infected.*
Take action straight away if you think your computer is infected. *Disconnect from the Internet, Run a complete scan with up to date anti-virus and anti-spyware software. Report it to your Internet Service Provider , forward the email to the FTC* ***(Federal Trade Commission)*** *at* spam@uce.gov*.and change any important passwords, if you suspect that any have been compromised.*