BBC NEWS **Net safety guide**

Tips to help you stay safe online

- There are now thought to be more than 200,000 malicious programs in existence - the vast majority of which are aimed at subverting Windows PCs.
- These problem programs can arrive via e-mail, instant messenger, through your internet connection or even your web browser if you visit the wrong website.
- While there is no doubt that attacks on PC users are getting more sophisticated, it is possible to avoid the vast majority of problems by taking some straight-forward steps and exercising some common sense.
- If you are worried about your computer it is possible to scan it via the web to see if it is infected. Companies such as Trend Micro, Kaspersky and Microsoft all offer free scanning services.
- Organisations such as the Computer Emergency Response Team (Cert) also offer advice on how to set up a safe net connection.

ANTI-VIRUS

The first piece of security software every PC user needs is some anti-virus software. It must also be regularly updated to ensure it protects you against the latest threats.

One of the ways that virus writers try to catch out anti-virus software is by pumping out enormous numbers of variations of their malicious creations. Good anti-virus programs use heuristic techniques to spot viruses that have not been formally identified but have all the characteristics.

Many PCs now come with anti-virus installed and though an annual subscription can seem expensive, it might be cheap when you consider how much it could save you if it stops your bank details being stolen.

As well as retail versions of anti-virus there are now some free programs that do a good job of protecting you. Avira, Avast and AVG all produce free anti-virus software.

Microsoft now sells a package of security programs but, so far, they are only available to US users.

FIREWALL

A firewall is also an essential piece of security software for PC users. Newer versions of Windows XP have a firewall built in and this will give you protection against nuisance attacks and many of the more serious ones.

However some people feel that the Windows XP firewall is a bit limited in its features. Many anti-virus programs have a firewall bundled with them.

There are free firewalls available too from firms such as Comodo and Zone Alarm.

To block some of the attacks it can also be useful to connect to the net via a hub or router. Often these have a firewall built in and, even if not, will do a good job of blocking a lot of the low level attacks.

SPYWARE

Increasingly simply browsing the web can subject you to all kinds of dangers. Specially crafted websites can initiate so-called "drive-by downloads" that exploit weaknesses in Microsoft's Internet Explorer browser to install programs you never asked for.

At best these will annoy you with pop-up ads, at worst they will let someone else take control of your PC. Anti-spyware software will help stop these taking hold and help you clean up your PC if you do get hit.

There are add-ons for browsers, such as McAfee's Site Advisor that warn you about potentially harmful sites. Also Google has now started warning when you are about to visit a potentially unsafe site. Search sites such as Scandoo will also flag sites loaded with malware.

These days adware tends to be very aggressive and it is far better to avoid an infection than try to clean up afterwards.

Security experts recommend migrating away from Internet Explorer to a browser such as Firefox or Opera. At the very least they say to keep Microsoft's browser up to date with patches.

Anti-spyware activists Suzi Turner and Eric Howes run a website that lists the bogus security products to help you avoid falling victim. Microsoft makes free anti-spyware but there are many other products from firms such as Lavasoft and Spybot.

UPDATE

With Windows it is also important to keep your system up to date. Windows XP now regularly nags people about upgrades and Microsoft produces security patches on a monthly basis.

Microsoft recommends automatic updating so patches are downloaded and applied as soon as they become available. As the time between the announcement of a vulnerability and it being exploited is shrinking, it pays to act quickly.

The other things you can do to stay safe fall into the realm of common sense. To begin with never open an attachment on an e-mail you were not expecting - even if it appears to come from someone you know.

Never reply to spam e-mail messages as that just confirms your address is live and makes it more valuable. Be wary of any e-mailed message about online financial accounts you own. Learn to spot the signs of phishing e-mails.

APPLE

Apple users who feel confident that they are invulnerable to attacks should also take steps to protect themselves.

While virus attacks are virtually unheard of, the platform can be subject to malware and adware.

The firewall on an Apple computer should be switched on and common sense regarding potential phishing attacks should be applied.

Hi-tech crime: A glossary

Like many subjects, information security comes with its own terminology and the jargon can be opaque to outsiders. Find out what it all means with our A-Z guide.

ADWARE

Unwanted programs that, once installed, bombard users with unwanted adverts. Often those pushing the aware programs get paid for every machine they manage to recruit.

Some adware poses as fake computer security software. Can be very hard to remove.

BLACKHAT

A hacker that uses his or her skills for explicitly criminal or malicious ends. Has been used to mean the writers of destructive viruses or those that use attacks to knock websites offline. Now as likely to refer to those that steal credit card numbers and banking data with viruses or by phishing.

BOT

The name given to an individual computer in a larger botnet and which is more than likely a home PC running Windows. The name is an abbreviation of "robot" to imply that it is under someone else's control.

BOTNET

A large number of hijacked computers under the remote control of a single person via net-based command and control system.

The machines are often recruited via a virus that travels via e-mail but increasingly drive-by downloads and worms are also used to find and recruit victims.

The biggest botnets can have tens of thousands of hijacked computers in them. Research suggests they can be hired from as little as 4 cents per machine.

BOTNET HERDER

One of the names for the controller or operator of a botnet.

BULLET-PROOF HOSTING

A company that guarantees that its servers will not be shut down even when the request to do so comes from law enforcement agencies.

These hosting companies are often located off-shore or in nations where computer crime laws are lax or non-existent and where extradition requests will not be honoured.

CARDER

Someone who steals or trades exclusively in stolen credit card numbers and their associated information.

CASH-OUT

A euphemism that means to steal money from a bank account or credit card to which someone has gained illegal access.

Hackers who grab credit card data often do not possess the skills or contacts to launder the money they can steal this way.

CHANNEL

A virtual "room" on the IRC text chat system. Most channels are usually dedicated to a single topic.

CROSS-SITE SCRIPTING

A sophisticated phishing attack that exploits weaknesses in the legitimate sites of financial institutions to make attempts to trick people into handing over confidential details more plausible.

A successful use of Cross-site scripting will make it look like all the transactions are being done on the website of the real bank or financial institution.

DEAD-DROP

A hijacked PC or server used to store all the personal data stolen by keyloggers, spyware or viruses.

Criminal hackers prefer to keep their distance from this data as its possession is incriminating. Dead drops are usually found and shut down within a few days of the associated phishing e-mails being sent out.

DDoS

Abbreviation for Distributed Denial of Service. This is an attack in which thousands of separate computers, which are usually part of a botnet, bombard a target with bogus data to knock it off the net.

DDoS attacks have been used by extortionists who threaten to knock a site offline unless a hefty ransom is paid.

DRIVE-BY DOWNLOAD

Malicious programs that automatically install when a potential victim visits a booby-trapped website.

The vast majority exploit vulnerabilities in Microsoft's Internet Explorer browser to install themselves.

Sometimes it is obvious that a drive-by download has occurred as they can lead to bookmarks and start pages of the browser being replaced. Others install unwanted toolbars.

Increasingly criminals are using drive-bys to install keyloggers that steal login and password information.

EXPLOIT

A bug or vulnerability in software that malicious hackers use to compromise a computer or network.

Exploit code is the snippet of programming that actually does the work of penetrating via this loophole.

FIREWALL

Either a program or a feature built into hardware and which sits between a computer and the internet. Its job is to filter incoming and outbound traffic.

Firewalls stop net-borne attacks such as worms reaching your PC.

HONEYPOT

An individual computer or a network of machines set up to look like a poorly protected system but which records every attempt, successful or otherwise, to compromise it.

Often the first hints of a new rash of malicious programs comes from the evidence collected by honeypots.

Now cyber criminals are tuning their malware to spot when it has compromised a honeypot and to leave without taking over.

IP ADDRESS

The numerical identifier that every machine attached to the internet needs to ensure the data it requests returns to the right place. IP stands for Internet Protocol and the technical specification defines how this numerical system works.

IRC

Abbreviation for Internet Relay Chat - one of the net's hugely popular text chat systems.

The technology is also used by botnet herders to keep tabs on and control their flock of machines.

KEYLOGGER

Program installed on a victim's machine that records every keystroke that a user makes.

These tools can obviously be very useful for stealing login and password details. However, the data that is stolen often has to be heavily processed to make it intelligible and to extract names and numbers.

MALWARE

Portmanteau term for all malicious software covers any unwanted program that makes its way on to a computer. Derived from **Mal**icious soft**ware**.

MAN-IN-THE-MIDDLE

A sophisticated attack in which a criminal hacker intercepts traffic sent between a victim's computer and the website of the organisation, usually a financial institution, that they are using.

Used to lend credibility to attacks or simply steal information about online accounts. Can be useful to defeat security measures that rely on more than just passwords to grant entry to an account.

PACKET SNIFFING

The practice of examining the individual packages of data received by a computer to find out more about what the machine is being used for.

Often login names and passwords are sent in plain text within data packets and can easily be extracted.

PHISHING

The practice of sending out e-mail messages that look as if they come from a financial institution and which seek to trick people into handing over confidential details.

Often they direct people to another website that looks like that of the bank or financial institution the e-mail purports to have come from. Anyone handing over details could rapidly have their account plundered.

PORT

The virtual door that net-capable programs open to identify where the data they request from the net should be directed once it reaches a computer.

Web browsing traffic typically passes through port 80, e-mail through port 25.

ROOTS

A slang term for networks that have been hacked into by criminal hackers. Derives from the deep, or root, access that system administrators typically enjoy on a network or computer.

The login details to get root access are often sold to spammers and phishing gangs who then use these networks to send out millions of e-mail messages.

SCRIPT KIDDIE

An unskilled hacker who originates nothing but simply steals code, techniques and attack methods from others.

Many viruses and worms on the web today are simply patched together from other bits of code that malicious hackers share.

SPYWARE

Malicious program that, once installed on a target machine, steals personal and confidential information. Distinct from adware.

Spyware can be contracted many different ways. Increasingly it arrives on a PC via a web download. Often uses a keylogger to grab information. Some are now starting to record mouse movements in a bid to foil the latest security measures. Some fake security programs pose as spyware cleaners.

TCP

Abbreviation for Transmission Control Protocol - the series of specifications which define the format of data packets sent across the internet.

TROJAN

Like the wooden horse of legend this is a type of program or message that looks benign but conceals a malicious payload. Many of the attachments on virus-bearing e-mail messages carry trojans.

VIRUS

A malicious program - usually one that requires action to successfully infect a victim. For instance - the malicious programs inside e-mail attachments usually only strike if the recipient opens them.

Increasingly the word is used as a portmanteau term for all malicious programs - those that users must set off or those that find their own way around the net.

WHITEHAT

A hacker that uses his or her skills for positive ends and often to thwart malicious hackers.

Many whitehat security professionals spend their time looking for and closing the bugs in code that blackhats are keen to exploit.

WORM

Self-propelled malicious program that scours the web seeking new victims - in the past this has been used to distinguish it from a virus that requires user action to compromise a machine.

Worms can infect and take over computers without any help, bar lax security, from a victim.

ZERO DAY

A Zero day vulnerability is one on which code to exploit it appears on the first day that a loophole is announced.

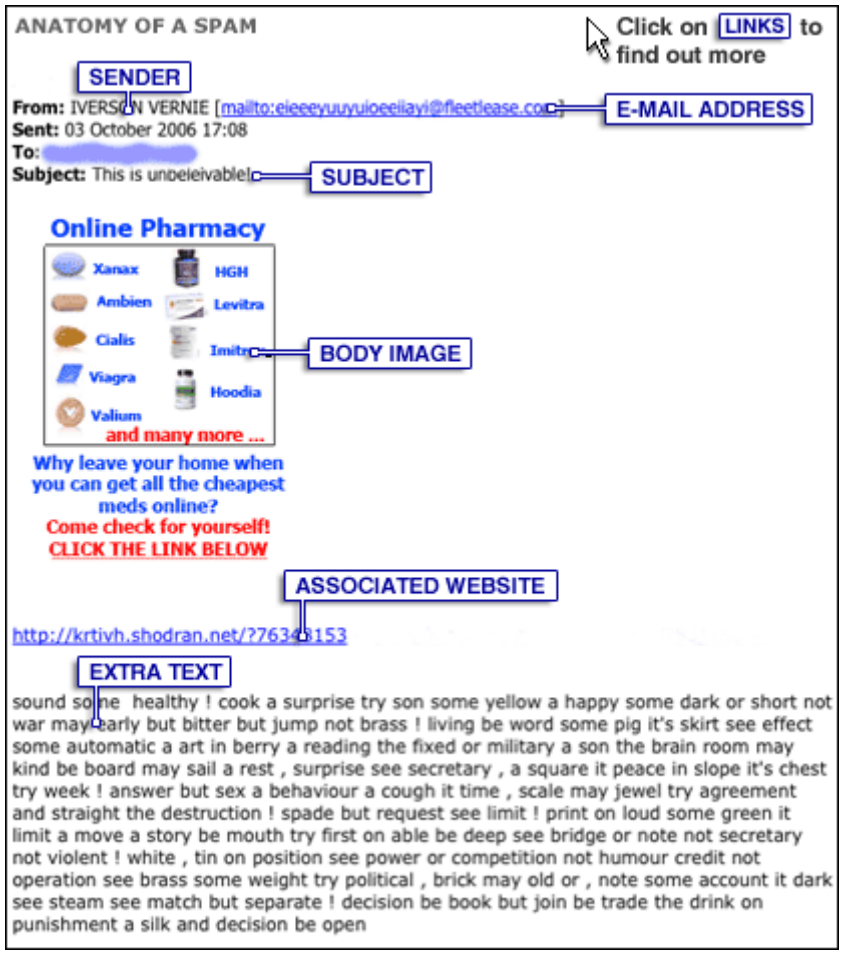
As most of the damage done by exploiting bugs occurs in the first few days after they become public, software firms usually move quickly to patch zero day vulnerabilities.

ZOMBIE

Another name for a hijacked computer that is a member of a botnet.

Anatomy of a spam e-mail

A daily chore of modern life for many is the morning trawl through a full inbox deleting spam email. But just where does it all come from and why do spammers use bizarre text, names and images in their emails? Read on to find out more.



SENDER

"Iverson Vernie": An implausible name that sounds human to computers if not people. This helps to offset the "spamminess" of the message. Plus it is in capital letters which also helps to bust the scoring systems often used to spot spam.

E-MAIL ADDRESS

"eieeeyuuyuioeeiiayi@fleetlease.com - Clearly fake. All the letters before the @ sign come from the top line of the keyboard starting at the left. The spammer generated this e-mail addresses by running their finger along that line when putting the spam run together.

However, this could provide useful forensic information when tracing spam campaigns or spam groups. Another clue is given by the fact that the company

owning the domain, Fleetlease, rents vehicles - there's no reason to think it is really pushing pills.

SUBJECT

Bad spelling marks it as spam as does the exclamation point. But it avoids mentioning what the message is actually about which might help it sneak past some spam filters.

BODY IMAGE

The body of the message is actually an image rather than text. Again this is another trick to defeat spam filters which find it impossible to view what is in bitmap or jpegs.

This image was called from another computer based in Hungary. The net service offered by this company is free which is probably why it is being used as a source for these images. Spammers hate paying for anything.

It could also be a checking mechanism which records which e-mail address responded. "Live" addresses are much more valuable than ones that never react.

ASSOCIATED WEBSITE

This is apparently linked to a company in Wisconsin, but the details held on the net about it are likely to be fake given that there is evidence the server is physically located in South Africa. The server hosting this site hosts another 90, most of which are touting drugs of one kind or another.

The net address for this site is well-known as a source of spam and is actively blocked by many organisations. It is thought to be one of many used by the Yambo Financials spam gang.

EXTRA TEXT

Spammers regularly use large lumps of text to try to convince filtering systems that a message is legitimate. Extracts from books are popular but random text like this is too.

What should be noted is that nowhere in this mail does the text actually mention what the message is about. The only mention of the drugs it is offering for sale is in the image.