

Viruses

- Does your computer ever act erratically when you're not doing anything (fan starts up, lights flash)?
- Do you share files online?
- Do you open email attachments?
- Do you transfer data from computer to computer?
- Do you use email or the internet on your phone?

If you answered yes to any of the above questions then your computer equipment may be at risk from virus infection.



Description

“The overall number of malicious code threats in circulation as of the end of 2007 is 1,122,311”

– Symantec Internet Security Threat Report Vol. XVIII - 2008

A computer virus is software or coding written for the sole purpose of infecting a computer. The effects can range from the irritating but harmless, such as humorous text or pictures being displayed on your monitor to the more malicious sort that will send offensive emails to clients and delete all of the files on your hard disk

Viruses are most commonly spread via email. Before email appeared viruses were spread through the sharing of floppy disks. Disks and memory sticks present a similar threat. Computers can also be infected via file sharing and from websites asking to install software.

An email based virus can scan your address book and forward the virus to all of your friends, family and clients. In this way a virus can circle the globe in a matter of hours.

Viruses also come in the form of worms. A worm is different to a virus in that it is self replicating and does not need a host medium. A typical virus will spread via email or an infected file but a worm can be released on to a computer and could in theory spread to all computers connected to the internet if unchecked.

It is not just computers and laptops that can become infected; mobile technology is also at risk from becoming infected.

“It is estimated that 64 million smart phones i.e. PDAs and mobiles with increased functionality, were sold worldwide in the first part of 2008”

– Gartner 2008

CASE STUDY

Accountants, Birmingham

The business is a small family owned accountants with a list of longstanding clients. In 2005 they were hit by a virus known as the ‘Blackworm’ or ‘Nyxem.E’ which spreads via email attachments and once in place, corrupts files rendering them useless. The virus targeted Microsoft Word documents and Excel spreadsheets. For a company reliant on the Microsoft Office package, the virus was extremely damaging. Blackworm also disables the security features of installed anti-virus software allowing further infections from other viruses.

It was discovered that the virus was spread via an attachment from a spam email, opened by an employee. From the original computer it spread through the network to the other computers in the company until they were all infected. It then destroyed all .xls (spreadsheet) and .doc (word document) files stored on the hard drives, replacing them with the text “DATAError [46 0E 94 93 F4 K6]”.

The loss of client data would have been enough to close the business down. Fortunately they had a backup system in place. At the end of each week, all data was collated from each employees computer over the network and copied to a DVD, then dated and then stored safely offsite. Although all of the data from each computer had been lost, it could be recovered from the backup DVD’s. The business was able to recover the majority of files from the backup, although, they still effectively lost the three days work following the most recent backup.

The infected email bypassed the network security as it was delivered by email (a trusted application) and although updates were installed regularly, this virus had been created and circulated since the last update. The consequences highlighted a need for staff training in dealing with suspicious email and a review of backup procedure to increase frequency and a regular audit to ensure files could be retrieved.

Solutions

- + Install anti-virus and set updates to automatic
- + Exercise caution about who or what you allow to access your computer
- + Ensure you have a backup system in place, that backups are carried out regularly and stored offsite
- + Ensure clients, colleagues and employees are aware of infected emails and attachments and to not open any unsolicited mail
- + Do not install anything from a website when asked to unless it can be verified as safe
- + Ensure your software firewall is turned on, to block attacks
- + If sharing files, exercise extreme caution about what is shared and ensure up to date anti-virus is in operation
- + If using Microsoft Windows, ensure you have the updates set to automatic. Updates and patches should be set to automatic for all software
- + Consider a firewall for your server to ensure that attacks are stopped before accessing the network
- + If you notice one computer is infected, quickly disconnect it from the network to stop infection of other machines
- + Share examples and experiences of viruses with other users in the network to raise awareness
- + If infected, disconnect your computer from the internet. There is a danger that the virus could spread to all of your clients via your contacts list

Business Type	Method of Attack	Negative Consequences	Solution	Cost
BASIC + Not linked to the internet + Administration only	+ Via media storage device (memory stick/optical disk)	+ Loss of company data. Business may be unable to continue after the loss of valuable data such as payroll, client lists, electronic documents etc + Disruption to work + Destruction of software	+ Install anti-virus + Limit access to your computer + Ensure you have a backup system see 'Disaster Recovery' flyer	+ Low cost + No cost + Low - High cost
ONLINE COMPUTER USER + Single machine linked to the internet + Receive email/transact online (includes laptops, smartphones, Blackberrys, PDA's)	The same as above but also: + Via email + Via 'free download' from website + Via infected website + Via file sharing	As above	Solutions the same as above but also: + Ensure clients, colleagues and employees understand risk of infected email + Do not install anything from a website + Ensure personal firewall is turned on + Exercise extreme caution if file sharing + Ensure all updates and patches are set to automatic + Install the latest web browser	+ No cost + No cost + No cost + No cost + No cost
NETWORKED + Same as above, but a collection of computers form a network (The risk increases as there are potentially more staff, increased computer business activity, therefore increased exposure to the risks)	Risks the same as above but also: + Via networked computer	As above but also: + If one computer is infected, then all computers on a network may be infected	Solutions the same as the above but also: + Install a hardware firewall for your server + Stop the virus spreading by disconnecting infected machine from network + Share examples and experiences of viruses	+ Low-High cost + No cost + No cost
ONLINE TRADER + Uses an e-commerce strategy to sell products to a global audience (Risk is again generally enhanced as the business and turnover is totally reliant on computer systems functioning correctly)	Risks the same as above	As above but also: + The virus may spread to clients via your mailing lists + Loss of clients' sensitive information + Damage to company reputation and loss of business + Damage to company website	Solutions the same as above but also: + By disconnecting the infected machine from the network, you'll also protect your clients from potentially being infected	+ No cost

Useful Websites

- <http://www.ktn.qinetiq-tim.net/>
- <http://www.berr.gov.uk/whatwedo/sectors/infosec>
- <http://www.bcrc-uk.org>
- <http://www.businesslink.gov.uk>
- <http://www.getsafeonline.org/>
- <http://www.sophos.com/security>
- <http://zdnet.co.uk/toolkits/securitythreats>

Internet Security Packages

- Includes: anti-virus, anti-spyware, a firewall and anti-spam
- <http://www.symantec.com/en/uk/norton/>
 - <http://www.mcafee-online.com/uk/store/>
 - <http://www.kaspersky.co.uk/store>
 - <http://uk.trendmicro.com/uk/home/>