

Viruses

While most people are aware of the dangers a virus can present to business, Mark Rogers from More Solutions says that as long as some common -sense principles are applied, any danger can be lessened substantially.

You could be forgiven for thinking that computers are getting more like their owners every year. Few could doubt that they seem to be getting cleverer, and unfortunately, most people are aware that they can also catch the computer equivalent of the common cold. However, while we all know that computer viruses exist, many of us lack knowledge of what they actually are, how they spread, and how to prevent or (if necessary) cure them.

Of course a computer virus is just a piece of software. Gardeners define weeds simply as plants growing in the wrong place, and computer viruses are similar, working like the applications you use every day, but doing things you did not want done. Usually it is simply their presence that is the problem, and the fact that they spread almost uncontrollably using resources not meant for them. Less often, but usually more worryingly, their impact can be more destructive.

Computer viruses are not a new phenomenon, although their methods of propagation have evolved dramatically since Internet use has become widespread. For a virus to jump from one computer to another has always required a transport mechanism, and while the floppy disk was effective a few years ago, the availability of direct connections between computers (with local networks, or LANs), and between those networks (the Internet) has simplified that transport dramatically. Furthermore, the increased power and functionality of computers has made it possible for viruses to do things they could never have done before.

Anti-virus software

Ironically, the increased power of computers and the connections between them is also the biggest weapon in our defence against viruses. We can run anti-virus programs that transparently check every e-mail we receive and every program we run for viruses, without the computing overhead being noticeable. Furthermore, we can keep ahead of virus outbreaks (or, more accurately, no more than one step behind them) by keeping our anti-virus software up to date, again transparently, using the Internet to download updates every few days. Updating your anti-virus software regularly is almost as important as installing the software in the first place.

Anti-virus software is therefore one of the most effective steps every business can (indeed must) take to protect itself from damage. The computer equivalent of immunization will keep most viruses at bay. It is remarkable that many of the viruses still being encountered today were first released months if not years ago, suggesting that many businesses still do not run up-to-date anti-viral software on their networks. However, just as in humans, viruses mutate and new ones are developed (thus being unrecognizable to the software sent to catch them, at least until their updates have arrived). Unfortunately a reliance on software protection alone is at best insufficient, and at worst brings a dangerous false sense of security.

Other measures

Viruses, and their cousins ‘Trojans’ and ‘worms’, rely for their spread on certain behaviours of their computer host, its operator, or both. Keeping the computer’s operating system and its applications updated (‘patched’) with security updates can go along way to limiting the ability of the computer to be an unwitting party to the viral spread.

The operators are a much bigger challenge. Trust is the biggest problem – most people trust (or even fear) their computer in situations they should not. Here are some common approaches designed to trick the unwary operator, all primarily delivered by e-mail:

- Looking like a joke, funny movie clip, screen saver, or similar.
- Appearing to have come from someone you know. (Very often viruses do actually come from people you know, as they often spread by working through address books, so trusting the source cannot be confused with trusting what he or she appears to have sent you.)
- Appearing to have come from some other trusted source, such as Microsoft. A recent trend has been to send fake security patches, cleverly using Microsoft’s corporate images and style of presentation in the e-mail to make it look official. Sometimes the sender’s e-mail address will give this away, but often this too is ‘spoofed’ to look like it came from Microsoft.[!list ends!]

Most of these approaches are properly called Trojans, as they are not infectious unless the attached program is run by the recipient, but this is encouraged by their pretending to be something they are not, as with the legendary wooden ‘gift’ horse of Troy. When activated they deliver some kind of payload, which increasingly includes ‘spyware’ which monitors your activity on the PC and attempts to collect passwords and credit card details to forward to someone else for their gain (and, inevitably, your loss). They then attempt to send copies of themselves to every e-mail address they can find on your system, by searching your address books and other sources on your PC.

Since it is important to the success of the Trojan that it is not recognized by its recipient, several increasingly ingenious methods of disguise are used. As well as collecting e-mail addresses from your PC, other details such as typical e-mail subjects can be collected and used to make the recipients of the resulting e-mail look more like it really did come from you. At least one even took the step of forwarding a random document from the PC with the e-mail, which could result in sensitive information being leaked to competitors or customers alike.

Potential damage

The biggest concern that many people have is that a virus could damage their PC in some way. In truth, physical damage is pretty much impossible, although formatting the computer's hard disk and deleting all the important data can be pretty devastating to both the individual and the organization he or she works for. As well as taking steps to avoid virus infection and thus avoid this potential damage, it is important that important data be backed up regularly so that its loss is much less significant.

The damage to a reputation that can be caused by sending confidential documents to the wrong people, or the damage to trust and respectability from just propagating a benign virus, are more serious threats to a computer literate business. This, combined with the costs of downtime assessing damage and restoring back-ups, are the real reasons why prevention is much better than cure.

Virus hoaxes

No introduction to computer viruses would be complete without mentioning hoax viruses. Since we have established that the biggest potential threat from a real virus can be to an organization's reputation, it can be true that hoax viruses have the potential to cause real damage to a business despite their false basis.

Hoax viruses usually take the form of an e-mail warning about something that is not a real threat. If they are believed, as they often are, they get forwarded by well-meaning recipients to all their colleagues and friends, often spreading as far if not further than a real virus might.

Some example hoaxes include:

- Simple lies, detailing serious but non-existent (and often technically implausible) threats. Probably the best known is the 'Good Times' virus hoax, which has been doing the rounds for many years now.
- Hoax warnings about legitimate programs. A good example is slfnbk.exe, a benign program on most Windows PCs that most people do not use and would not be aware of. The hoax warns of a serious and potentially damaging virus, and describes how this file is a sign of an infection. People follow the instructions to find that the file is indeed there, and delete it, glad that they caught it in time (and then forwarding the hoax on). If the hoax refers to a program that is genuinely important to the system operation the hoax can cause as much damage as a real virus.

Since these are not real viruses, they are not 'detected' by anti-virus programs. The hoaxes often play on this, describing how the threat is so new that most anti-virus programs will not detect it, thus adding to the urgency with which the hoax gets forwarded.

The 'cure' for hoaxes is remarkably simple, but few people think to use it. Typing a few key words from the hoax (such as 'slfnbk' in the example above) into an Internet search engine such as Google will quickly show plenty of references to the hoax. In any

case, anti-virus software writers do not send random warnings around by e-mail, any more than organizations like Microsoft send security update patches out by e-mail. A cool head and a quick check can be the best antidote to many threats.

Many non-virus hoaxes also exist, which can be just as damaging to reputations if forwarded without at least basic checks of their validity. Many claim something to the effect that ‘for every person you send this e-mail to, <insert large corporation here> will donate <sum of money> to <very worth cause>’.

Summary

- Computer viruses can be pervasive and damaging, but most serious problems are easily avoided with preventative action. Up to date anti-virus software and common sense are essential in equal parts.
- Many viruses do so little that a first scan for viruses can throw up several (even hundreds) which have lay dormant and unnoticed for years, and a panic response will usually do far more harm than the virus itself.
- However, the most important lesson to learn is that while actual damage to data is a tangible but relatively small risk, the real danger from viruses is the damage they cause to reputations, and this more than anything else is why they cannot be ignored.

Mark Rogers is a senior developer at More Solutions Ltd, a company dedicated to designing and deploying software solutions for industries using the Internet as a communications medium. With many applications involving stand-alone, unattended equipment installed miles from the nearest IT department, security and reliability are essential aspects of their business.

For further information contact More Solutions Ltd, 6 Belgic Square, Fengate, Peterborough, PE1 5XF, Tel: 0845 45 89 555, E-mail: mark@more-solutions.co.uk, Web: www.more-solutions.co.uk