Computer viruses demystified

Viruses

Email

Internet

Mobile devices

Safety

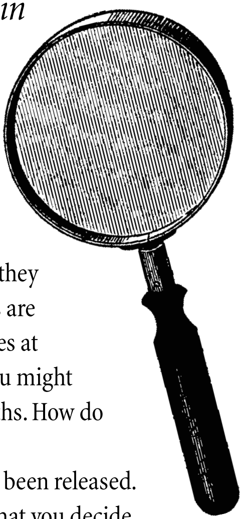
Reference

Computer viruses demystified

Contents

Why viruses matter

Computer viruses, hackers, crackers, data crime. They make headline news and – so the media claim – cost us millions. But do viruses and all the other nasties in cyberspace matter? Do they really do much harm?



If you're in any doubt, just try imagining what could happen in your office or home.

Imagine that no-one has updated your anti-virus software for a few months. When they do, you find that your accounts spreadsheets are infected with a new virus that changes figures at random. Naturally you keep backups. But you might have been backing up infected files for months. How do you know which figures to trust?

Now imagine that a new email virus has been released. Your company is receiving so many emails that you decide to shut down your email gateway altogether … and miss an urgent order from a big customer.

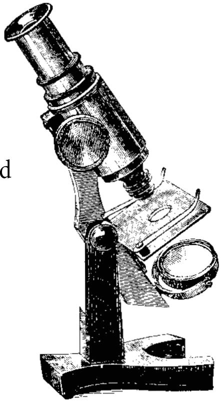
Suppose that you've been studying at home for an MBA. You've almost finished your dissertation when one of your children puts a new game on your PC and infects it. The virus deletes everything on the hard drive … including all your hard work.

Imagine that a friend emails you some files he found on the internet. You open them and trigger a virus that mails confidential documents to everyone in your address book … including your competitors.

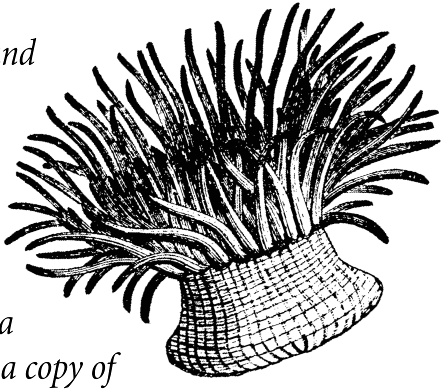
Finally, imagine that you accidentally send another company a report that carries a virus. Will they feel safe to do business with you again?

Such incidents have all happened. In every case, simple precautions, some of which cost nothing, could have prevented the problem.

This guide tells you what the risks are and how you can avoid them.



Viruses, Trojans and worms



In the mid-1980s Basit and Amjad Alvi of Lahore, Pakistan discovered that people were pirating their software. They responded by writing the first computer virus, a program that would put a copy of itself and a copyright message on any floppy disk copies their customers made. From these simple beginnings, an entire virus counter-culture has emerged. Today new viruses sweep the planet in hours and virus scares are major news. People are fascinated, but not always well-informed. Read on to see how viruses spread and how you can protect yourself.

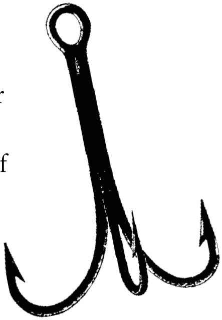
Viruses
Email
Internet
Mobile devices
Safety
Reference

What is a virus?

A computer virus is a computer program that can spread across computers and networks by making copies of itself, usually without the user's knowledge.

Viruses can have harmful side-effects. These can range from displaying irritating messages to deleting all the files on your computer.

How does a virus infect computers?



A virus program has to be run before it can infect your computer.

Viruses have ways of making sure that this happens. They can attach themselves to other programs or hide in code that is run automatically when you open certain types of files.

You might receive an infected file on a disk, in an email attachment, or in a download from the internet. As soon as you launch the file, the virus code runs. Then the virus can copy itself to other files or disks and make changes on your computer.

For details, see 'Boot sector viruses', 'Parasitic viruses' and 'Macro viruses' later in this chapter.

Trojan horses

Trojan horses are programs that do things that are not described in their specifications.

The user runs what they think is a legitimate program, allowing it to carry out hidden, often harmful, functions.

For example, *Troj/Zelu* claims to be a program for fixing the 'millennium bug' but actually overwrites the hard disk.

Trojan horses are sometimes used as a means of infecting a user with a computer virus.

Backdoor Trojans are programs that allow other computer users to take control of your PC over the internet.

Worms

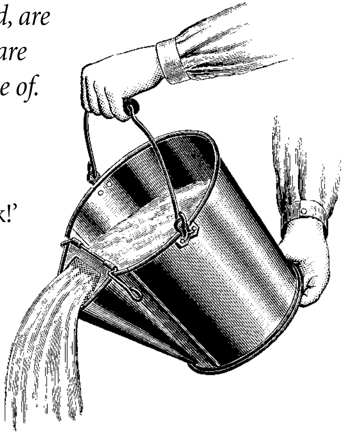
Worms are similar to viruses but do not need a carrier (like a macro or a boot sector).

Worms simply create exact copies of themselves and use communications between computers to spread.

Many viruses, such as *Kakworm* (*VBS/Kakworm*) or *Love Bug* (*VBS/LoveLet-A*), behave like worms and use email to forward themselves to other users.

What can viruses do?

Virus side-effects, often called the payload, are the aspect of most interest to users. Here are some of the things that viruses are capable of.



Messages *WM97/Jerk* displays the message 'I think (user's name) is a big stupid jerk!'

Pranks *Yankee* plays 'Yankee Doodle Dandy' at 5 pm.

Denying access *WM97/NightShade* password-protects the current document on Friday 13th.

Data theft *Troj/LoveLet-A* emails information about the user and machine to an address in the Philippines.

Corrupting data *XM/Compatable* makes changes to the data in Excel spreadsheets.

Deleting data *Michelangelo* overwrites parts of the hard disk on March 6th.

Disabling hardware *CIH* or *Chernobyl* (*W95/CIH-10xx*) attempts to overwrite the BIOS on April 26th, making the machine unusable.

Where are the virus risks?

Here are the points where your office is vulnerable.

The internet

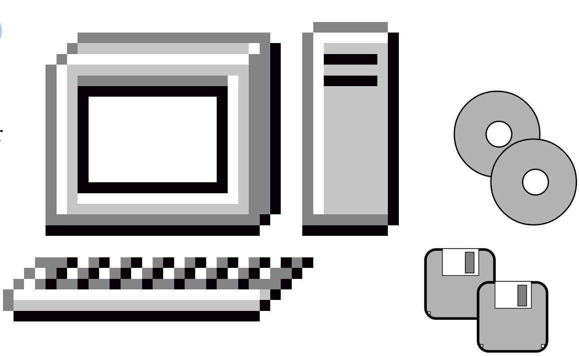
Downloaded programs or documents may be infected.

Documents and spreadsheets

These can contain macro viruses, which can infect and make changes to other documents or spreadsheets.

Programs

Programs that carry a virus can infect your machine as soon as you run them.



Email

Email can include infected attachments. If you double-click on an infected attachment, you risk infecting your machine. Some emails even include malicious scripts that run as soon as you preview the mail or read the body text.

Floppy disks and CDs

Floppy disks can have a virus in the boot sector. They can also hold infected programs or documents. CDs may also hold infected items.

Viruses
Email
Internet
Mobile devices
Safety
Reference

Viruses
Email
Internet
Mobile devices
Safety
Reference

Preventing viruses

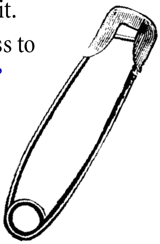
There are simple measures you can take to avoid being infected or to deal with viruses if you are infected.

Make users aware of the risks

Tell everyone in the organisation that they are at risk if they swap floppy disks, download files from websites or open email attachments.

Install anti-virus software and update it regularly

Anti-virus programs can detect and often disinfect viruses. If the software offers on-access virus checking, use it. On-access checking protects users by denying access to any file that is infected. See the 'Anti-virus software' section later in this chapter.



Keep backups of all your data

Make sure you have backups of all data and software, including operating systems. If you are affected by a virus, you can replace your files and programs with clean copies.

For details, see the 'Ten steps to safer computing' chapter.

Boot sector viruses

Boot sector viruses were the first type of virus to appear. They spread by modifying the boot sector, which contains the program that enables your computer to start up.

When you switch on, the hardware looks for the boot sector program – which is usually on the hard disk, but can be on floppy or CD – and runs it. This program then loads the rest of the operating system into memory.

A boot sector virus replaces the original boot sector with its own, modified version (and usually hides the original somewhere else on the hard disk). When you next start up, the infected boot sector is used and the virus becomes active.

You can only become infected if you boot up your computer from an infected disk, e.g. a floppy disk that has an infected boot sector.

Many boot sector viruses are now quite old. Those written for DOS machines do not usually spread on Windows 95, 98, Me, NT or 2000 computers, though they can sometimes stop them from starting up properly.

Form

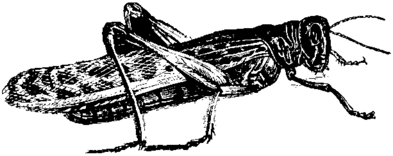
A virus that is still widespread ten years after it first appeared. The original version triggers on the 18th of each month and produces a click when keys are pressed on the keyboard.

Parity Boot

A virus that may randomly display the message 'PARITY CHECK' and freeze the operating system. The message resembles a genuine error message displayed when the computer's memory is faulty.

Parasitic viruses (file viruses)

Parasitic viruses, also known as file viruses, attach themselves to programs (or 'executables').



When you start a program infected with a file virus, the virus is launched first. To hide itself, the virus then runs the original program.

The operating system on your computer sees the virus as part of the program you were trying to run and gives it the same rights. These rights allow the virus to copy itself, install itself in memory or release its payload.

Parasitic viruses appeared early in virus history but they still pose a real threat. The internet has made it easier than ever to distribute programs, giving these viruses new opportunities to spread.

Jerusalem

On Friday 13th, deletes every program run on the computer.

CIH (Chernobyl)

On the 26th of certain months, this virus will overwrite part of the BIOS chip, making the computer unusable. The virus also overwrites the hard disk.

Remote Explorer

WNT/RemExp (*Remote Explorer*) infects Windows NT executables. It was the first virus that could run as a service, i.e. run on NT systems even when no-one is logged in.

Macro viruses

Macro viruses take advantage of macros, commands that are embedded in files and run automatically.

Many applications, such as word processing or spreadsheet programs, use macros.

A macro virus is a macro program that can copy itself and spread from one file to another. If you open a file that contains a macro virus, the virus copies itself into the application's startup files. The computer is now infected.

When you next open a file using the same application, the virus infects that file. If your computer is on a network, the infection can spread rapidly: when you send an infected file to someone else, they can become infected too.

A malicious macro can also make changes to your documents or settings.

Macro viruses infect files used in most offices and some can infect several file types, such as Word or Excel files. They can also spread to any platform on which their 'host' application runs. Above all, they spread easily because documents are exchanged frequently via email and websites.

WM/Wazzu

Infects Word documents. It moves between one and three words and inserts the word 'wazzu' at random.

OF97/Crown-B

Can infect Word, Excel and PowerPoint files. When it infects a Word document, it turns off macro protection in the other Office 97 applications, so that it can infect them.

Viruses
Email
Internet
Mobile devices
Safety
Reference

Anti-virus software

Anti-virus software can detect viruses, prevent access to infected files and often eliminate the infection. Here is an introduction to the different kinds of software available.

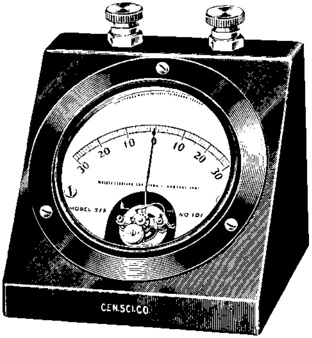
Scanners

Virus scanners can detect, and often disinfect, the viruses known at the time the scanner is released. Scanners are easily the most popular form of anti-virus software but they have to be updated regularly to recognise new viruses.

There are *on-demand* and *on-access* scanners. Many anti-virus packages offer both.

On-demand scanners let you start or schedule a scan of specific files or drives.

On-access scanners stay active on your machine whenever you are using it. They check files as you try to open or run them.



Viruses
Email
Internet
Mobile devices
Safety
Reference

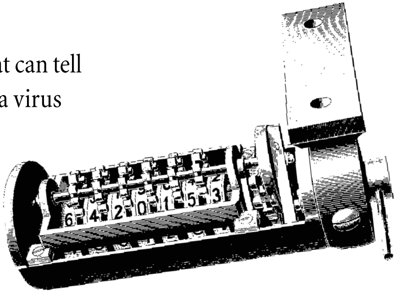
Checksummers

Checksummers are programs that can tell when files have been changed. If a virus infects a program or document, changing it in the process, the checksummer should report the change.

The good thing about checksummers is that they do not need to know anything about a virus in order to detect its presence. For that reason, checksummers do not need regular updating.

The bad thing about checksummers is that they cannot tell the difference between a virus and a legitimate change, so false alarms are likely. Checksummers have particular problems with documents, which can change frequently.

In addition, checksummers can only alert you after infection has taken place, they cannot identify the virus, and they cannot provide disinfection.



Heuristics

Heuristic software tries to detect viruses – both known and unknown – by using general rules about what viruses look like. Unlike conventional scanners, this software doesn't rely on frequent updates about all known viruses.

However, if a new kind of virus emerges, the software will not recognise it and will need to be updated or replaced.

Heuristics can be prone to false alarms.

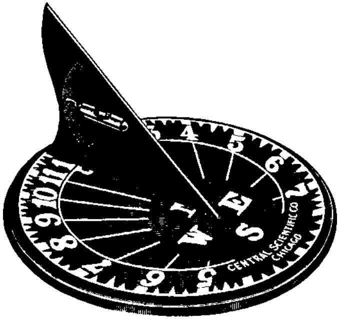
A brief history of viruses

1949 Mathematician John von Neumann suggests that computer programs could reproduce.

1950s Bell Labs develop an experimental game in which players use malicious programs to attack each other's computers.

1975 Sci-fi author John Brunner imagines a computer 'worm' spreading across networks.

1984 Fred Cohen introduces the term 'computer virus' in a thesis on such programs.



1986 The first computer virus, *Brain*, is allegedly written by two brothers in Pakistan.

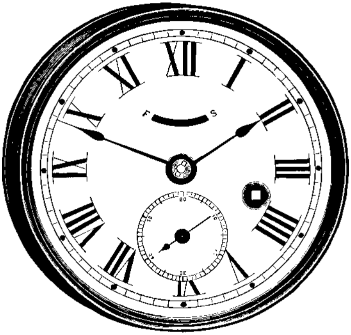
1987 The *Christmas tree* worm paralyses the IBM worldwide network.

1988 The *Internet worm* spreads through the US DARPA internet.

1990 Mark Washburn writes *1260*, the first 'polymorphic' virus, which mutates (i.e. change its form) each time it infects.

1992 There is worldwide panic about the *Michelangelo* virus, although very few computers are infected.

1994 *Good Times*, the first major virus hoax, appears.



1995 The first macro virus, *Concept*, appears. In the same year, Australian virus writers produce the first virus specifically written for Windows 95.

1998 *CIH* or *Chernobyl* becomes the first virus to paralyse computer hardware.

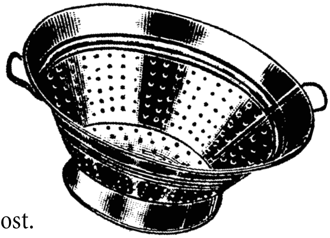
1999 *Melissa*, a virus that forwards itself by email, spreads worldwide. *Bubbleboy*, the first virus to infect a computer when email is viewed, appears.

2000 *Love Bug* becomes the most successful email virus yet. The first virus appears for the Palm operating system, although no users are infected.

Viruses
Email
Internet
Mobile devices
Safety
Reference

The hidden costs of viruses

Viruses don't just corrupt or delete data. They can also harm your business in less obvious ways.



Everyone knows about viruses that delete everything on the hard drive or corrupt documents. Such effects are serious, but you can soon recover if you have good backups. More serious are some of the less visible side-effects.

For example, viruses can prevent computers from working or force you to shut down the network. During this time, working hours - and so revenue - are being lost.

Some viruses interrupt the communications business depends on. *Melissa* or *ExploreZip*, which spread via email, can generate so much mail that servers crash. Even if this doesn't happen, companies sometimes react to the risk by shutting down their mail servers anyway.

There is a threat to confidentiality too. *Melissa* can forward documents, which may contain sensitive information, to anyone in your address book.

Viruses can seriously damage your credibility. If you send infected documents to customers, they may refuse to do business with you or demand compensation. Sometimes you risk embarrassment as well as a damaged business reputation. *WM/Polypost*, for example, places copies of your documents in your name on alt.sex usenet newsgroups.

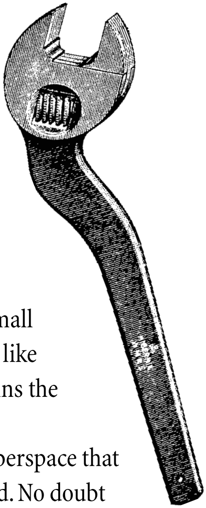
Who writes viruses?

If your computer, or your network, is hit by a virus, the first thing you're likely to say - expletives apart - is 'Why do people write these viruses?'

At first glance, there seems to be little incentive for writing viruses. Virus writers don't gain in financial or career terms; they rarely achieve real fame; and, unlike hackers, they don't usually target particular victims, since viruses spread too indiscriminately.

Virus writing is easier to understand if you compare it to forms of delinquency such as graffiti or vandalism.

Virus writers tend to be male, under 25 and single. Their self-esteem is bound up with the approval of their peer group, or at least of a small electronic community. Virus-writing exploits, like graffitti art, are a kind of performance that wins the writer status.



Viruses also give their writers powers in cyberspace that they could never hope to have in the real world. No doubt that's why virus writers choose names inspired by heavy metal music or fantasy literature, which thrive on similar illusions of prowess and potency.

Viruses
Email
Internet
Mobile devices
Safety
Reference

Is virus writing always wrong?

Most of us take it for granted that viruses are simply a bad thing, but is that necessarily true?

Many viruses are 'harmless' or take the form of jokes. Others alert us to security flaws in software. Some people argue that viruses could even be useful, e.g. by distributing bug fixes. Unfortunately, the idea of 'harmless' viruses doesn't stand up to scrutiny.

First, viruses make changes on users' computers without their consent and sometimes without their knowledge. That's unethical – and illegal in many countries – whether the intention is good or bad. You shouldn't interfere with somebody else's computer, any more than you would borrow their car without telling them – even if you did change the oil.

Secondly, viruses don't always perform as the author intends. If a virus is badly written, it can cause unforeseen problems. Even if it's harmless on the operating system it was written for, a virus may be highly destructive on other platforms or on systems developed in future.

Proof-of-concept

Sometimes people write viruses to prove that a new kind of virus is possible. These are known as proof-of-concept viruses. They do not usually have side-effects (a payload) and shouldn't be released onto other users' computers.

Research?

Virus writers like to claim that they are doing research. Yet viruses are often poorly written, they are released at random on unsuspecting users, and there's no way to collect the results. This can hardly be called research.

Virus hoaxes

If you have been warned about viruses called 'Good Times', 'Budweiser Frogs' or 'How to give a cat a colonic', you are the victim of a hoax. Virus hoaxes, especially email hoaxes, are commonplace and can be just as costly in terms of time and money as the real thing.

Viruses
Email
Internet
Mobile devices
Safety
Reference

What are hoaxes?

Hoaxes are reports of non-existent viruses. Typically, they are emails which do some or all of the following:

- Warn you that there is an undetectable, highly destructive new virus.
- Ask you to avoid reading emails with a particular subject line, e.g. Join the Crew or Budweiser Frogs.
- Claim that the warning was issued by a major software company, internet provider or government agency, e.g. IBM, Microsoft, AOL or the FCC.
- Claim that a new virus can do something improbable. For instance, *A moment of silence* says that 'no program needs to be exchanged for a new computer to be infected'.
- Use techno-babble to describe virus effects, e.g. *Good Times* says that the virus can put the PC's processor into 'an nth-complexity infinite binary loop'.
- Urge you to forward the warning to other users.

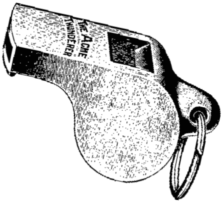
The hoax that wasn't

On April 1, 2000 an email headed *Rush-Killer virus alert* began circulating. It warned of viruses that take over the modem and dial 911 (the US emergency number), and urged you to forward the warning. The email had all the hallmarks of a hoax. Yet the virus was real. It was one of the *BAT/911* viruses which spread through Windows shares and do call 911. It's difficult to tell a hoax from a real warning; you should follow the advice in 'What can be done about hoaxes?' at the end of this chapter.

Why are hoaxes a problem?

Hoaxes can be as disruptive and costly as a genuine virus.

If users do forward a hoax warning to all their friends and colleagues, there can be a deluge of email. This can overload mail servers and make them crash. The effect is the same as that of the real *Love Bug* virus, but the hoaxer hasn't even had to write any computer code.



It isn't just end-users who overreact. Companies who receive hoaxes often take drastic action, such as closing down a mail server or shutting down their network. This cripples communications more effectively than many real viruses, preventing access to email that may be really important.

False warnings also distract from efforts to deal with real virus threats.

Hoaxes can be remarkably persistent too. Since hoaxes aren't viruses, your anti-virus software can't detect or disable them.

Which came first?

A hoax can inspire a real virus threat, or vice versa. After the *Good Times* hoax made the headlines, some virus writers waited until it had been debunked and then wrote a **real** virus with the same name (anti-virus firms call it *GT-Spoof*).

What can be done about hoaxes?

Hoaxes, like viruses or chain mail, depend on being able to spread themselves. If you can persuade users to break the chain, you limit the harm done.

Have a company policy on virus warnings

The solution may be a company policy on virus warnings. Here is an example:

‘Do not forward any virus warnings of any kind to ANYONE other than *the person responsible for anti-virus issues*. It doesn’t matter if the virus warnings come from an anti-virus vendor or have been confirmed by a large computer company or your best friend. ALL virus warnings should be sent to *name of responsible person* only. It is their job to notify everybody of virus warnings. A virus warning which comes from any other source should be ignored.’

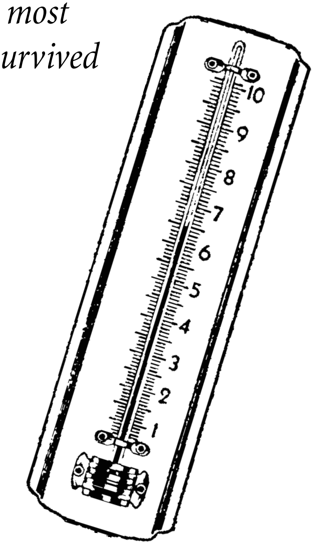
As long as users follow the policy, there will be no flood of emails and the company expert will decide whether there is any real risk.

Keep informed about hoaxes

Keep informed about hoaxes by visiting the hoaxes pages on our website: www.sophos.com/virusinfo/hoaxes

Top 10 viruses

Which viruses are the most successful ever? Here is our selection of those that travelled furthest, infected most computers ... or survived the longest.



Love Bug

(VBS/LoveLet-A)

The Love Bug is probably the best-known virus. By pretending to be a love letter, it played on users' curiosity, spreading around the world in hours.

First seen:	May 2000
Origin:	The Philippines
AKA:	Love Letter
Type:	Visual Basic Script worm
Trigger:	On initial infection
Effects:	The original version sends an email with the subject line 'I LOVE YOU' and the text 'kindly check the attached love letter coming from me'. Opening the attachment allows the virus to run. If Microsoft Outlook is installed, the virus tries to forward itself to all addresses in the Outlook address book. It can also distribute itself to other newsgroup users, steal user information and overwrite certain files.

Form

Form featured in the top ten viruses for eight years and is still widespread. On DOS and early versions of Windows, it behaved inconspicuously, so it spread widely.

First seen:	1991
Origin:	Switzerland
Type:	Boot sector virus
Trigger:	18th of the month
Effects:	Produces a click every time you press a key. Can prevent Windows NT computers from working.

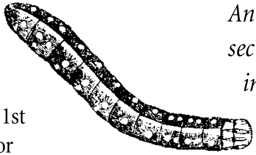
Kakworm

(VBS/Kakworm)

Kakworm made it possible for users to become infected just by viewing infected email.

First seen: 1999

Type: Visual Basic Script worm



Trigger: On initial infection (for most effects) or 1st of any month (for Windows shutdown side-effect)

Effects: The worm arrives embedded in an email message. If you are using Outlook or Outlook Express with Internet Explorer 5, the machine can be infected when you open or preview the infected email. The virus changes the Outlook Express settings so that the virus code is automatically included with all outgoing mail. On the 1st of any month after 5 pm, it displays the message 'Kagou-Anti_Kro$oft says not today' and shuts down Windows.

Anticmos

Anticmos is a typical boot sector virus. It was widespread in the mid-1990s and frequently appeared in the top ten viruses.

First seen: January 1994

Origin: First detected in Hong Kong, but believed to originate in China.

Type: Boot sector virus

Trigger: Random

Effects: Tries to erase information about the type of floppy and hard disk drives installed.

Melissa

(WM97/Melissa)

Melissa is an email virus that uses psychological subtlety to spread rapidly. It appears to come from someone you know and to include a document you would definitely want to read. As a result, Melissa spread worldwide within a single day.

First seen: March 1999

Origin: A 31-year-old US programmer, David L Smith, posted an infected document on an alt.sex usenet newsgroup

Type: Word 97 macro virus; also Word 2000 aware

Trigger: On initial infection

Effects: Sends a message to the first fifty addresses in all the address books accessible by Microsoft Outlook, using the current user's name in the subject line. There is an attachment containing a copy of the infected document. If the minute and day are the same when the document is opened (e.g. 10.05 am on the 5th), the virus adds text about the game Scrabble to the document.

New Zealand

New Zealand was easily the commonest virus in the early 1990s.

First seen: Late 1980s

Origin: New Zealand

AKA: Stoned

Type: Boot sector virus

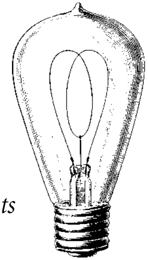
Trigger: Once in 8 times, if booted from a floppy

Effects: Displays the message 'Your PC is now Stoned!'. Puts a copy of the original boot sector in a sector that is last in the root directory of a 360K disk. This can damage larger disks.

Concept

(WM/Concept)

Concept achieved instant success by being shipped accidentally on official Microsoft software. It was the first macro virus found in the wild and one of the commonest viruses in 1996-1998. The virus takes control with its AutoOpen macro, which Word runs automatically, and carries out infection with its FileSaveAs macro, which runs when Word saves a document. Many variants exist.



First seen:	August 1995
Virus type:	Macro virus
Trigger:	None
Effects:	When you open an infected document, a dialog box titled 'Microsoft Word' and containing the figure 1 appears. The virus includes the text 'That's enough to prove my point' but this is never displayed.

CIH (Chernobyl)

(W95/CIH-10xx)

CIH was the first virus to damage computer hardware. Once it overwrites the BIOS, the computer cannot be used until the BIOS chip is replaced.

First seen:	June 1998
Origin:	Written by Chen Ing-Hau of Taiwan
Type:	Parasitic virus that runs on Windows 95 computers
Trigger:	April 26th, with variants which trigger on June 26th or the 26th of any month
Effects:	Tries to overwrite the BIOS and then overwrites the hard disk.

Parity Boot

Parity Boot spreads on the boot sectors of floppy disks. Its success shows that boot sector viruses, which were commonest in the 1980s and early 1990s, can still thrive. This virus was still among the most commonly reported as recently as 1998. It was particularly common in Germany, where it was distributed on a magazine cover-disk in 1994.

First seen:	March 1993
Origin:	Possibly Germany
Type:	Boot sector virus
Trigger:	Random
Effect:	Displays the message ‘PARITY CHECK’ and freezes the computer. This mimics a genuine memory error. As a result, users often think that there is a problem with their computer’s RAM (Random Access Memory).

Happy99

W32/Ska-Happy99

Happy99 was the first well-known virus to spread itself rapidly by email.

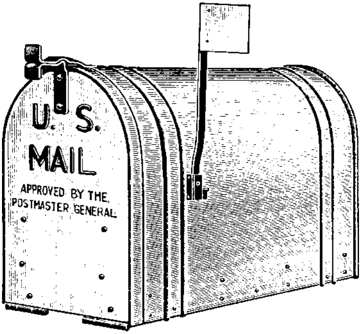
First seen:	January 1999
Origin:	Posted to a newsgroup by French virus writer ‘Spanska’
Type:	File virus that runs on Windows 95/98/Me/NT/2000 computers.
Trigger:	None
Effect:	Displays a fireworks effect and the message ‘Happy New Year 1999’. The virus also modifies the file wsock32.dll in the Windows system directory so that whenever an email is sent, a second message including the virus is sent too.

Viruses
Email
Internet
Mobile devices
Safety
Reference

Email

If you asked most people to name a single virus, the chances are it would be the Love Bug or Melissa. What these headline-hitting viruses have in common is that they spread around the world by email.

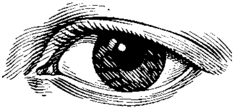
Email is now the biggest source of viruses. Why is this?



As long as viruses were transferred by floppy disk, they spread slowly. Companies could ban disks or insist on having them virus-checked. Email has changed all that. Now you can exchange files much more quickly and infecting your PC is as easy as clicking on an icon – or easier. Conventional viruses can spread faster and new kinds of virus exploit the workings of email programs.

Can you get a virus just by reading email?

Some users think they are always safe to open email as long as they don't look at attachments. This is no longer necessarily true.



Viruses such as *Kakworm* and *Bubbleboy* can infect users when they read email. They look like any other message but contain a hidden script that runs as soon as you open the email, or even look at it in the preview pane (as long as you are using Outlook with the right version of Internet Explorer). This script can change system settings and send the virus to other users via email.

Microsoft have issued a patch that eliminates this security weakness. To download it, visit www.microsoft.com/technet/security/bulletin/ms99-032.asp

Email hoaxes

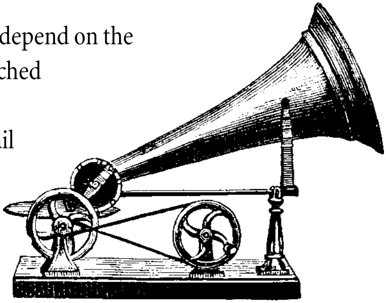
Email is a popular medium for hoaxes. These are bogus virus reports that urge you to forward the message to everyone you know.

An email hoax can spread across networks like a virus and can cause a mail overload. The difference is that the hoax doesn't need virus code; it simply depends on users' credulity. For more information, see the 'Virus hoaxes' chapter.

Viruses that spread automatically by email

The most successful viruses today are those that spread themselves automatically by email.

Typically, these viruses depend on the user clicking on an attached document. This runs a script that uses the email program to forward infected documents to other email users. *Melissa*, for example, sends a message to the first fifty addresses in all address books that Microsoft Outlook can access. Other viruses send themselves to every address in the address book.



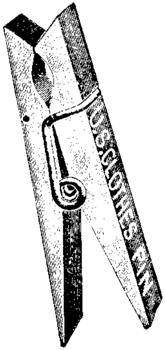
What is spam?

Spam is unsolicited email, often advertising get-rich-quick schemes, home-working jobs, loans or pornographic websites. Spam often comes with fake return information, which makes it more difficult to deal with the perpetrators. Such mail should simply be deleted.

Viruses
Email
Internet
Mobile devices
Safety
Reference

The risks of attachments

The greatest security risk at present isn't email itself but email attachments.



Any program, document or spreadsheet that you receive by email could carry a virus; launching such an attachment can infect your computer.

Unfortunately, email attachments are a popular way to exchange information. Many users think it's 'harmless fun' to circulate screensavers, greetings cards, animations or joke programs. However, such files can carry viruses.

Even an attachment that appears to be a safe type of file, e.g. a file with a .txt extension, can pose a threat. That 'text file' may actually be a malicious VBS script with the file extension (.vbs) hidden from view.

The *VBS/Monopoly* worm is an example of a malicious program disguised as entertainment. It masquerades as a 'Bill Gates joke'. It is (it displays a Monopoly board with Microsoft images in it) but it also emails itself to other users and forwards your system details to specific email addresses, threatening the confidentiality of sensitive information.

Email interception and forgery

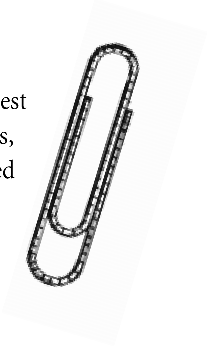
Email interception involves other users reading your email while it is in transit. You can protect yourself with email encryption.

Email forgery means sending mail with a forged sender's address or tampering with contents. You can protect yourself by using digital signatures.

How to stop email viruses

Viruses
Email
Internet
Mobile devices
Safety
Reference

Have a strict policy about email attachments



Changing your (and other users') behaviour is the simplest way to combat email threats. Don't open any attachments, even if they come from your best friend. Don't be tempted by promises of instant gratification or 'harmless fun'. If you don't know something is virus-free, treat it as if it's infected. You should have a company policy that ALL attachments are authorised and checked with anti-virus software before being launched.

Disable Windows Scripting Host

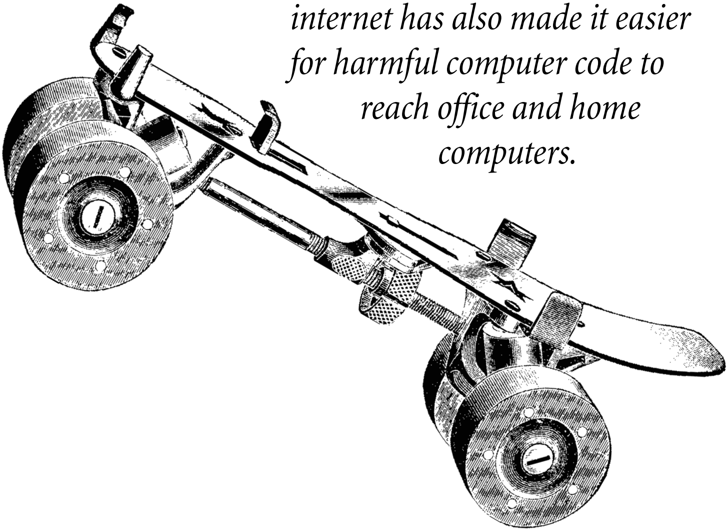
Windows Scripting Host (WSH) automates certain actions, such as running VBS or Java script, on Windows computers. However, WSH allows viruses like *Love Bug* to spread. You can probably do without WSH (but consult your network administrator first). For instructions on turning it off, see www.sophos.com/support/faqs/wsh.html. Remember that every time you update Windows or Internet Explorer, WSH will be re-enabled.

Use anti-virus software

Use on-access anti-virus software on the desktop and at the email gateway. Both arrangements can protect against viruses sent via email.

The internet

The internet has made more information available to more people more quickly than ever before. The downside is that the internet has also made it easier for harmful computer code to reach office and home computers.



Click and infect?

The internet has increased the risk of infection.

Ten years ago, most viruses spread via floppy disks. Spreading in this way was slow and depended on users making a conscious effort to run new programs. If the virus had side-effects that were too obvious, it was unlikely to affect many users. Now that the internet is so widely used, everything has changed.

Sharing software over the net is easy. A click of the mouse attaches a program to an email and it's easy to detach and run it. Users can just as easily place a program on a web page, which anyone can download. So file (or 'parasitic') viruses, which target programs, can thrive on the net.

The viruses that really benefit, though, are macro viruses, which affect documents. Users frequently download documents or spreadsheets, or exchange them by email. All you have to do to infect your computer is to click on a downloaded file or email attachment.

When you use the internet, open documents with a viewer that ignores macros, and don't run programs that don't come from a trustworthy source.

Can I be infected just by visiting websites?

Visiting a website is less hazardous than opening unknown programs or documents. There are risks, though. The threat depends on the types of code used in the site and the security measures taken by service providers and by you. Here are the main types of code you will encounter.

HTML

Web pages are written in HTML (Hypertext Markup Language). This language lets web authors format their text and create links to graphics and to other pages. HTML code itself can't carry a virus. However, web pages can contain code that launches applications or opens documents automatically. This introduces the risk of launching an infected item.

ActiveX

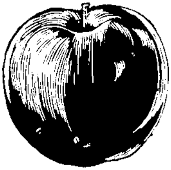
ActiveX is a Microsoft technology for web developers used only on computers running Windows.

ActiveX applets, used to create visual effects on webpages, have full access to resources on your computer, which makes them a potential threat. However, digital signatures, which prove that an applet is authentic and hasn't been tampered with, do provide limited security.

More website code

Java

People sometimes worry unduly about Java viruses on the internet. They do so because they confuse Java applets, which are used to create effects on web pages, with Java applications and Java scripts.



Applets are generally safe. They are run by the browser in a secure environment known as a 'sandbox'. Even if a security flaw lets an applet escape, a malicious applet cannot spread easily. Applets usually flow from a server to users' computers, not from one user to another (you tell your friends to visit a site, rather than sending them a copy of an applet). In addition, applets are not saved on the hard disk, except in the web cache.

If you do encounter a harmful applet, it is most likely to be a Trojan, i.e. a malicious program pretending to be legitimate software.

Java applications are simply programs written in the Java language. Like any other program, they can carry viruses. You should treat them with the same caution as you would use with other programs.

Java script is active script embedded in HTML code in web pages. Like any other script, it can carry out operations automatically, which carries risks. You can disable active scripts (see 'Safety on the net' at the end of this chapter).

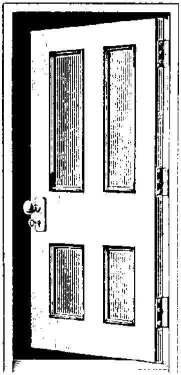
VBS script

VBS (Visual Basic Script) can run as soon as a page is viewed, depending on the browser used. You don't have to do anything to launch it.

This script is used by email worms such as *Kakworm* and *Bubbleboy*, but can just as well be run from web pages.

Backdoor Trojans

A backdoor Trojan is a program that allows someone to take control of another user's PC via the internet.



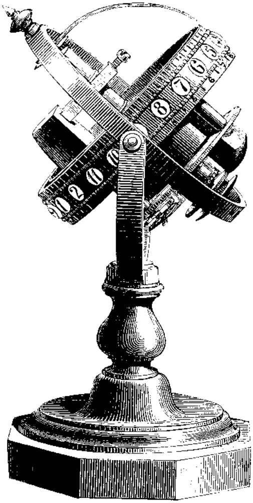
Like other Trojans, a backdoor Trojan poses as legitimate or desirable software. When it is run (usually on a Windows 95/98 PC), it adds itself to the PC's startup routine. The Trojan can then monitor the PC until it makes a connection to the internet. Once the PC is on-line, the person who sent the Trojan can use software on their computer to open and close programs on the infected computer, modify files and even send items to the printer. *Subseven* and *BackOrifice* are among the best known backdoor Trojans.

Are cookies a risk?

Cookies do not pose a direct threat to your computer or the data on it. However, they do theaten your confidentiality: a cookie enables a website to remember your details and keep track of your visits to the site. If you prefer to remain anonymous, you should use the security settings on your browser to disable cookies.

Attacks on web servers

End-users aren't the only ones at risk on the internet. Some hackers target the web servers which make websites available.



A common form of attack involves sending so many requests to a web server that it slows down or crashes. When this happens, genuine users can no longer gain access to the websites hosted by the server.

CGI (Common Gateway Interface) scripts are another weak point. These scripts run on web servers to handle search engines, accept input from forms, and so forth. Hackers can exploit poorly-implemented CGI scripts to take control of a server.

Safety on the net

If you want to use the internet safely, you should do the following:

Have a separate network for internet machines

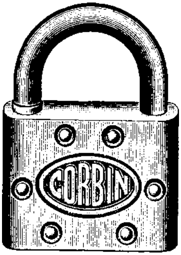
Maintain separate networks for those computers that are connected to the internet and those that are not. Doing so reduces the risk that users will download infected files and spread viruses on your main network.

Use firewalls and/or routers

A firewall admits only authorised traffic to your organisation. A router controls the flow of packets of information from the internet.

Configure your internet browser for security

Disable Java or ActiveX applets, cookies, etc., or ask to be warned that such code is running. For example, in Microsoft Internet Explorer, select **Tools|Internet Options|Security| Custom Level** and select the security settings you want.

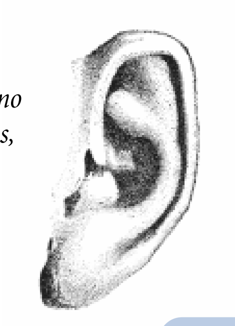


Mobile phones and palmtops

The last decade brought the world (wide web) to your desktop; the next will bring it to your mobile phone. You can already access internet-like sites and services on the new generation mobiles and the technology is developing fast. But as it becomes easier to transfer data – even on the move – the risk is that new security threats will emerge too.

Do mobile phone viruses exist?

At the time of writing, there is no virus that infects mobile phones, despite media stories and hoaxes.



There *have* been viruses that send messages to phones. For example, *VBS/Timo-A*, a worm that spreads itself by email, also uses the modem to send text (SMS) messages to selected mobile numbers. The notorious *Love Bug* virus is also capable of forwarding text to fax machines and mobiles. However, these viruses can't infect or harm the mobile phone.

Things might change as mobile phones become more sophisticated.

Do mobile devices put data at risk?

Mobile devices are not as safe a place for data as a PC:

- They are easily lost or stolen.
- Interruptions in power can cause data loss.
- Data is not backed up.

As mobile devices become more complex, they could also become vulnerable to viruses or to hackers.

WAP phones and viruses

The most talked-about new technology in this field is WAP (Wireless Application Protocol).

WAP provides internet-type information and services for mobile phones and organisers. It is based on the same model as web communications, i.e. a central server delivers code that is run by a browser on your phone. So, at the moment, the possibilities for viruses are very limited.

A virus could infect the server itself, but the chances for it to spread or to have an effect on users would be minimal.

First, there is nowhere on a WAP system that a virus can copy itself or survive. Unlike a PC, a WAP phone does not store applications. The phone downloads the code it needs and keeps no copy, except temporarily in the browser cache.

Second, a virus cannot yet spread from one user to another because there is no communication between client phones.

In theory, a 'virus' could distribute *links* to malicious WAP sites, tempting users to use harmful applications, but that still involves running code from the server.

Buzzwords

WAP	Wireless Application Protocol
WML	Wireless Markup Language
WML Script	A programming language resembling Java script
Cards	Pages in WML
Deck	A set of inter-related pages all available to a WAP browser without further downloads

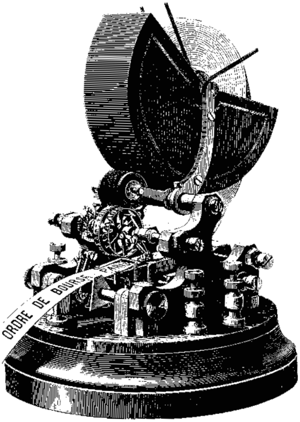
Viruses
Email
Internet
Mobile devices
Safety
Reference

Future risks for WAP

WAP uses a version of HTTP, the protocol for web pages, which could transmit more complex content than that processed by WAP browsers at present. A future generation of browsers might be able to download files, such as documents, that contain macro viruses.

Under WAP, the server will soon be able to push content to mobile phones. As well as alerting users to updated information (such as financial results or sports scores) or new email, 'push' technology could download the data to the cache – without the need for you to take any action. Malicious code could exploit this system to distribute itself.

There are other potential problems too. For instance, malicious WAP sites could pose as useful services. Such sites could crash the user's browser or fill its memory.



Buzzwords

XML	eXtensible Markup Language, recommended for use on the world wide web
WTLS	Wireless Transport Layer Security. Encryption method used on the mobile phone network

Mobile operating systems

Palmtop computers or personal digital assistants (PDAs) are likely to provide new opportunities for viruses in the very near future.

Palmtops or PDAs run specially written or scaled-down operating systems – such as EPOC, PalmOS and PocketPC (formerly Windows CE). Such systems will eventually be able to use versions of popular desktop applications, making them vulnerable to malicious code in the same way as desktop machines. In early 2001, there were already viruses that affect the Palm system.

Palmtops are also regularly connected to home or office PCs to synchronise the data on the two machines (e.g. address book information or calendars). Such data synchronisation could allow viruses to spread easily.

No-one yet knows which will be more successful in the future: mobile computers or smart mobile phones. Whichever it is, the security risks will increase as mobile computers become better at communicating.

Buzzwords

EPOC	An operating system for palmtops
PDA	Personal Digital Assistant
PalmOS	Operating system for Palm computers
PocketPC	Microsoft's operating system for palmtops, formerly Windows CE
UPNP	Universal Plug and Play, a Microsoft system for enabling connections between mobiles and other devices

Viruses
Email
Internet
Mobile devices
Safety
Reference

Viruses for your fridge?

More and more different devices will soon 'talk' to each other using infrared links or low-power radio, bringing new security risks.

Bluetooth is a standard for low-power radio data communication over very short ranges, e.g. 10 m. Computers, mobile phones, fax machines and even domestic appliances such as video recorders or fridges can use Bluetooth to discover what services are provided by other nearby devices and to establish links with them transparently.

Software that exploits Bluetooth is emerging. Sun's Jini technology, for example, allows devices to form connections, exchange Java code automatically and give remote control of services. The risk is that an unathorised user, or malicious code, could exploit Bluetooth to interfere with services.

Bluetooth and Jini are designed to ensure that only trusted code from known sources can carry out sensitive operations. These measures make it unlikely that there could be a virus outbreak but if a virus does bypass security, there may be little to stop it spreading.

Buzzwords

3G	'Third generation' mobile technology
Bluetooth	Short-range radio data communications
Jini	A technology to allow devices to exchange Java code
MExE	Mobile station application Execution Environment, a possible successor to WAP that would let service providers download Java code to a phone

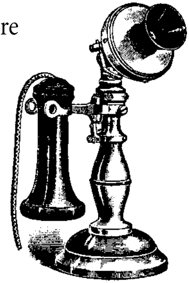
How to protect mobile devices

As mobile and PDA technology evolves, security measures will need to keep up. The main issue is where you use anti-virus measures.

Scanning at a gateway or during data transfer

In the near future, the best way to protect mobile devices may be to check data when you transfer it to or from them. For mobile phones, for example, the WAP gateway might be a good place to install virus protection. All communications pass through this gateway in unencrypted form, so there would be an ideal opportunity for virus scanning.

For palmtop computers, you could use virus protection when the palmtop is synchronising data with a conventional PC. The PC could run the major part of the virus checking software, so the palmtop's lack of power or memory wouldn't matter.

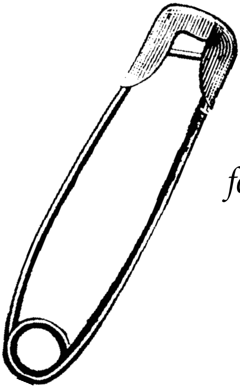


Virus scanning on the mobile device

As mobile devices become more interconnected, it will become difficult to police data transfer at a central point. The solution will be to put anti-virus software on each device – once they have sufficient processing power and memory.

Ten steps to safer computing

Apart from using anti-virus software, there are plenty of simple measures you can take to help protect yourself and your company from viruses. Here are our ten top tips for trouble-free computing.



Steps to safer computing

Don’t use documents in .doc and .xls format

Save your Word documents in RTF (Rich Text Format) and your Excel spreadsheets as CSV (Comma Separated Values) files. These formats don’t support macros, so they cannot spread macro viruses, which are by far the commonest virus threat. Tell other people to supply you with RTF and CSV files. Beware, though! Some macro viruses intercept FileSaveAs RTF and save the file with an RTF extension but DOC format. To be absolutely safe, use text-only files.

Don’t launch unsolicited programs or documents

If you don’t know that something is virus-free, assume it isn’t. Tell people in your organisation that they should not download unauthorised programs and documents, including screensavers or ‘joke’ programs, from the internet. Have a policy that all programs must be authorised by an IT manager and virus-checked before they are used.

Forward warnings to one authorised person only

Hoaxes are as big a problem as viruses themselves. Tell users not to forward virus warnings to their friends, colleagues or everyone in their address book. Have a company policy that all warnings go to one named person or department only.

Steps to safer computing

If you don’t need WSH, turn it off

Windows Scripting Host (WSH) automates some tasks on Windows computers but it also makes you vulnerable to email viruses like *Love Bug* and *Kakworm*. Unless it is needed disable it. For instructions, visit the FAQ page at www.sophos.com/support/faqs/wsh.html

Follow software companies’ security bulletins

Watch out for security news and download patches to protect against new virus threats. See the ‘Useful links’ chapter.

Block unwanted file types at the email gateway

Many viruses now use VBS (Visual Basic Script) and SHS (Windows scrap object) file types to spread. It is unlikely that you need to receive these file types from outside, so block them at the gateway.

Change your computer’s bootup sequence

Most computers try to boot from floppy disk (the A: drive) first. Your IT staff should change the CMOS settings so that the computer boots from the hard disk by default. Then, even if an infected floppy is left in the computer, it cannot be infected by a boot sector virus. If you need to boot from floppy at any time, you can have the settings changed back.

Viruses
Email
Internet
Mobile devices
Safety
Reference

Steps to safer computing

Write-protect floppies before giving to other users

A write-protected floppy cannot be infected.

Subscribe to an email alert service

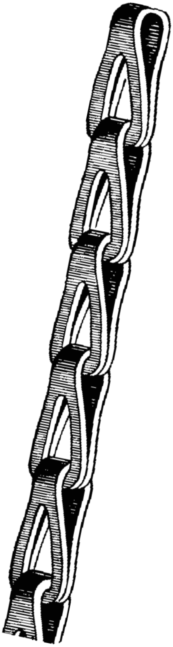
An alert service can warn you about new viruses and offer virus identities that will enable your anti-virus software to detect them. Sophos has a free alert service. For details, see http://www.sophos.com/virusinfo/notifications

Make regular backups of all programs and data

If you are infected with a virus, you will be able to restore any lost programs and data.

Useful links

Visit these sites for more information



Information on viruses

http://www.sophos.com/virusinfo/analyses

Virus hoaxes and scares

http://www.sophos.com/virusinfo/hoaxes

http://www.vmyths.com

Automatic notification of new viruses

http://www.sophos.com/virusinfo/notifications

Microsoft Security Bulletins

http://www.microsoft.com/security

Netscape Security Center

http://home.netscape.com/security

Java security information

http://java.sun.com/security

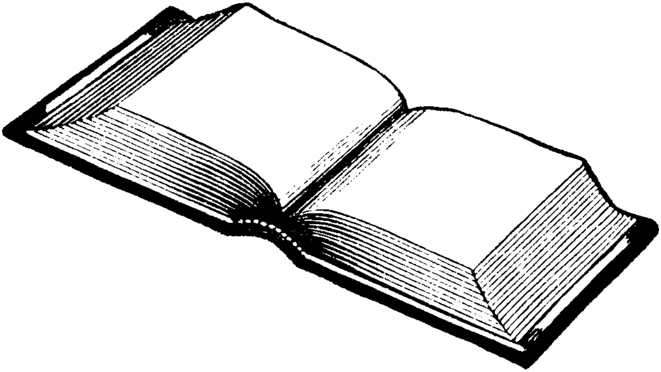
The WildList Organization

http://www.wildlist.org

Virus Bulletin

http://www.virusbtn.com

Glossary



Viruses
Email
Internet
Mobile devices
Safety
Reference

ActiveX: A Microsoft technology that extends the capabilities of a web browser.

Applet: A small application. Usually refers to Java applets (q.v.).

ASCII: American Standard Code for Information Interchange. The standard system for representing letters and symbols.

Attachment: A document, spreadsheet, graphic, program or any other kind of file attached to an email message.

Back door: An undocumented means of bypassing the normal access control system of a computer. See Backdoor Trojan.

Backdoor Trojan: A Trojan horse (q.v.) program that gives a remote user unauthorised access to and control over a computer.

Backup: A copy of computer data that is used to recreate data that has been lost, mislaid, corrupted or erased.

BIOS: The Basic Input/Output System. The lowest level of software which interfaces directly with hardware.

Boot sector: The part of the operating system which is read into memory from disk first when a PC is switched on. The program stored in the boot sector is then run, which in turn loads the rest of the operating system.

Boot sector virus: A type of virus which subverts the booting process.

Booting: A process carried out when a computer is first switched on, in which the operating system is loaded from disk.

CGI: Common Gateway Interface. A mechanism that allows a web server to run programs or scripts and send the output to a user's web browser.

Checksum: A value calculated from item(s) of data which can be used to verify that the data has not been altered.

Companion virus: A virus that exploits the fact that when there are two programs with the same name, the operating system uses the file extension to decide which one to run. For example, DOS computers will run a .com file in preference to an .exe file. The virus creates a .com file containing the virus code and gives it the same name as an existing .exe file.

Cookie: A small packet of data that stores information on a user’s computer. Cookies are usually used to enable a website to track visits and remember visitors’ details.

CSV: Comma Separated Values. A file format in which values (e.g. the values from an Excel spreadsheet) are shown separated by commas. The format does not support macros, so that it cannot spread macro viruses.

Digital signature: A means of ensuring that a message has not been tampered with and that it originates from the claimed sender.

DOS boot sector: The boot sector which loads DOS into PC RAM. Common point of attack by boot sector viruses.

Downloading: The transfer of data from one computer, typically a server, to another computer.

File server: A computer which provides central data storage and often other services for the workstations on the network.

File virus: See parastic virus.

Viruses
Email
Internet
Mobile devices
Safety
Reference

Firewall: A security system that sits between the internet and an organisation's network, and only passes authorised network traffic.

Floppy disk: Removable magnetic disk used to store data.

FTP: File Transfer Protocol. A system that allows internet users to connect to remote sites and upload or download files.

Gateway: Either a computer that serves for the transfer of data (e.g. a mail gateway that handles all the mail coming into an organisation), or a computer that converts data from one protocol to another.

Hacker: A computer user who attempts to gain unauthorised access to other users' computer systems.

Hard disk: A sealed magnetic disk, generally inside a computer, which is used to store data.

Heuristic scanner: A program that detects viruses by using general rules about what viruses are like or how they behave.

Hoax: A report about a non-existent virus.

HTML: Hypertext Markup Language. The format for most documents on the web.

HTTP: Hypertext Transport Protocol. A protocol used by web servers to make documents available to web browsers.

Hypertext: Computer-readable text which allows extensive linking of files.

Internet: A network consisting of many connected networks. '*The* internet' is by far the largest of these.

Java: Platform-independent programming language for the web, developed by Sun Microsystems. Programs written in Java are either applications or applets (small applications).

Java applet: Small application generally used to create effects on web pages. Applets are run by the browser in a safe environment (see Sandbox) and cannot make changes to your system.

Java application: Java-based program that can carry out the full functions that might be expected, e.g. saving files to disk.

Laptop: A portable computer small enough to be used on your lap.

Link virus: A virus which subverts directory entries so that they point to the virus code, allowing it to run.

Macro: Sets of instructions inside data files that can carry out program commands automatically, e.g. opening and closing files.

Macro virus: A virus which uses macros in a data file to become active and attach itself to other data files.

Master boot record: Also known as the partition sector.The first physical sector on the hard disk which is loaded and executed when the PC is booted. The most critical part of the startup code.

Modem: A MOdulator/DEModulator converts computer data into a form suitable for transmission via telephone line, radio or satellite link.

Multipartite virus: A virus which infects both boot sectors and program files.

Notebook: A computer even smaller than a laptop computer.

Operating system: The program which controls the use of the computer's hardware resources and performs basic functions such as maintaining lists of files and running programs.

Palmtop: A computer small enough to be held in the palm of the hand.

Parasitic virus: A computer virus which attaches itself to another computer program, and is activated when that program is run.

Password: Sequence of characters which gives access to a system.

PC: Personal Computer. A desktop or portable single-user computer.

PDA: Personal Digital Assistant. A small, mobile computing device used mostly for managing data such as address books and calendars.

Polymorphic virus: Self-modifying virus. By changing its code, the virus tries to make itself harder to detect.

Proxy server: A server that makes requests to the internet on behalf of another machine. It sits between a company and the internet and can be used for security purposes.

Program: A set of instructions that specifies actions a computer should perform.

RAM: Random Access Memory. A form of temporary memory in a computer. RAM acts as the computer's workspace, but data stored there is lost once the computer is switched off.

ROM: Read Only Memory. A form of permanent memory in a computer. A ROM is usually used to store a computer's startup software.

RTF: Rich Text Format. A document format that does not support macros, so that it cannot spread macro viruses.

Sandbox: A mechanism for running programs in a controlled environment, particularly used with Java applets.

SHS: File extension for Windows 'scrap object' files. SHS files can include almost any code and run automatically if you click on them. The extension may be hidden.

SMTP: Simple Mail Transport Protocol. The delivery system for internet email.

Spam: Unsolicited email.

Spoofing: Pretending to be someone or something else (e.g. by forging the sender's address in email).

Stealth virus: A virus which hides its presence from the computer user and anti-virus programs, usually by trapping interrupt services.

TCP/IP: Transmission Control Protocol/Internet Protocol. The collective name for the standard internet protocols.

Trojan horse: A computer program with (undesirable) effects that are not described in its specification.

URL: Uniform Resource Locator. A web 'address'.

VBS: Visual Basic Script. Code embedded in an application, document, or web page that can run as soon as the page is viewed.

Virus: A program which can spread across computers and networks by attaching itself to another program and making copies of itself.

Virus identity: A description of virus characteristics used for virus recognition.

Virus scanner: A program that detects viruses. Most scanners are virus-specific, i.e. they identify those viruses that are already known. See also Heuristic scanner.

WAP: Wireless Application Protocol. Internet-type protocol that provides information to mobile phones and organisers.

Web: See World wide web.

Web browser: A program used to access information on the web, i.e. the 'client' side of the web.

Web server: A computer connected to the internet that makes Web documents available, generally using HTTP.

WSH: Windows Scripting Host. A utility that automates certain actions, e.g. the running of VBS or Java Script, on Windows computers.

Workstation: A single-user computer, often connected to a network.

World wide web: A distributed hypertext system for the reading of documents across the internet.

Worm: A program that distributes multiple copies of itself. Unlike a virus, a worm does not need a 'host' program.

WWW: See World wide web.

Index

Viruses
Email
Internet
Mobile devices
Safety
Reference

Index of viruses

Edited and designed by Paul Oldfield.

ISBN 0-9538336-0-7

Enquiries: enquiries@sophos.com
Website: www.sophos.com