Viruses and spam
what you need to know
Viruses and spam
what you need to know

Whether you’re a network administrator, use a computer at work, or just read email, this book is for you. We tell you the facts about computer viruses and spam in simple, easy-to-understand language.

Sophos is one of the world’s leading anti-virus and anti-spam companies, protecting over 25 million business users worldwide. To find out about Sophos’s complete range of solutions for protecting against spam and viruses, and for enforcing company email policy, visit our website at www.sophos.com
Contents

Viruses, Trojans and worms 5

Spam 27

Hoaxes and scams 41

Tips for safer computing 49

Glossary 53

Index 63
Viruses, Trojans and worms

In the mid-1980s two brothers in 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 minutes and can corrupt data, slow networks down, or harm your reputation.
What is a virus?

A virus or worm 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 effects. These can range from displaying irritating messages to stealing data or giving other users control over 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 file. Sometimes they can exploit security flaws in your computer’s operating system to run and to spread themselves automatically.

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

Trojan horses are programs that pretend to be legitimate software, but actually carry out hidden, harmful functions.

For example, DLoader-L arrives in an email attachment and claims to be an urgent update from Microsoft for Windows XP. If you run it, it downloads a program that uses your computer to connect to certain websites, in an attempt to overload them (this is called a denial of service attack).

Trojans cannot spread as fast as viruses because they do not make copies of themselves. However, they now often work hand-in-hand with viruses. Viruses may download Trojans which record keystrokes or steal information. On the other hand, some Trojans are used as a means of infecting a computer with a virus.

Worms

Worms are similar to viruses but do not need a carrier program or document.

Worms simply create exact copies of themselves and use communications between computers to spread (see the “Internet worms” section).

Many viruses, such as MyDoom or Bagle, behave like worms and use email to forward themselves.
What can viruses do?

Viruses used to play pranks or stop your computer working, but now they compromise security in more insidious ways. Here are the things that viruses can do.

■ Slow down email. Viruses that spread by email, such as Sobig, can generate so much email traffic that servers slow down or crash. Even if this doesn’t happen, companies may react to the risk by shutting down servers anyway.

■ Steal confidential data. The Bugbear-D worm records the user's keystrokes, including passwords, and gives the virus writer access to them.

■ Use your computer to attack websites. MyDoom used infected computers to flood the SCO software company’s website with data, making the site unusable (a denial of service attack).

■ Let other users hijack your computer. Some viruses place “backdoor Trojans” on the computer, allowing the virus writer to connect to your computer and use it for their own purposes.
■ **Corrupt data.** The *Compatable* virus makes changes to the data in Excel spreadsheets.

■ **Delete data.** The *Sircam* worm may attempt to delete or overwrite the hard disk on a certain day.

■ **Disable hardware.** *CIH*, also known as *Chernobyl*, attempts to overwrite the BIOS chip on April 26, making the computer unusable.

■ **Play pranks.** The *Netsky-D* worm made computers beep sporadically for several hours one morning.

■ **Display messages.** *Cone-F* displays a political message if the month is May.

■ **Damage your credibility.** If a virus forwards itself from your computer to your customers and business partners, they may refuse to do business with you, or demand compensation.

■ **Cause you embarrassment.** For example, *PolyPost* places your documents and your name on sex-related newsgroups.
Where are the virus risks?

Viruses can reach your computer via all the routes shown here. You can read more details on the pages that follow.

- **Programs and documents**
  
  Programs and documents can be infected with viruses. When you share them with other users, by putting them on your network or intranet, or by sending them out, the infection can spread.

- **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.

- **The internet**
  
  You may download programs or documents that are infected. Security vulnerabilities in your operating system can also allow viruses to infect your computer via the internet connection, without your having to do anything at all.

- **CDs and floppies**
  
  Floppy disks can have a virus in the boot sector. They can also hold infected programs or documents. CDs may also hold infected items.
Which files can viruses infect?

Viruses can attach themselves to any code that runs on your computer: programs, documents, or the files that start up the operating system.

**Programs**

Some viruses infect programs. When you start the infected program, the virus is launched first. This type of virus appeared early in virus history but still poses a threat, as the internet makes it easy to distribute programs.

**Documents**

Word processing or spreadsheet applications often use “macros” to automate tasks. Some viruses take the form of a macro that can spread from one document to another. If you open a document that contains the virus, it copies itself into the application’s startup files and infects other documents you open with that application.

**Boot sectors**

When you switch on your computer, it accesses a part of the disk called the “boot sector” and runs a program that starts the operating system. The earliest viruses replaced this boot sector with their own, modified version. If the user started up their computer from an infected disk, the virus became active.
Email viruses

Many of the most prolific viruses are email-aware: they distribute themselves automatically by email.

Typically, email-aware viruses depend on the user clicking on an attached document. This runs a script that can forward infected documents to other people. The Netsky virus, for example, searches the computer for files that may contain email addresses (e.g. EML or HTML files), and then uses the email program on your computer to send itself to those addresses. Some viruses, like Sobig-F, don’t even need to use your email browser; they include their own “SMTP engine” for sending mail.

Email viruses may compromise your computer’s security or steal data, but their most common effect is to create excessive email traffic and crash servers.

Email attachments

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

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 file may be a malicious VBS script with the real file type (.vbs) hidden from view.
Can I get a virus just by reading email?

You don’t have to open an attachment to become infected via email. Just viewing your mail is a risk.

Some viruses, such as Kakworm and Bubbleboy, can infect users as soon as 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 issue patches that eliminate this security weakness and others like it. To find out which patches you need, visit windowsupdate.microsoft.com. To keep informed about future patches, you can subscribe to a mailing list at www.microsoft.com/technet/security/bulletin/notify.asp
Internet worms

You may be at risk whenever you are connected to the internet, even if you don’t open suspicious email.

Internet worms can travel between connected computers by exploiting security “holes” in the computer’s operating system.

The Blaster worm, for example, takes advantage of a weakness in the Remote Procedure Call service that runs on Windows NT, 2000 and XP computers and uses it to send a copy of itself to another computer. As the worm spreads, it creates a lot of traffic on the internet, slowing down communications or causing computers to crash. This particular worm also later uses the computer to deluge a Microsoft website with data, with the aim of making the site inaccessible.

Microsoft (and other operating system vendors) issue patches to fix security loopholes in their software. You should update your computer regularly by visiting the vendor’s website.

Can I get a virus from a website?

Web pages are written in HTML (Hypertext Markup Language). This cannot carry a virus, although it can call up programs or files that do. You cannot be infected by visiting an HTML page unless there is a security vulnerability on your computer that allows a program to run and infect you.
Backdoor Trojans

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

A backdoor Trojan may pose as legitimate software, just as other Trojan horse programs do, so that users run it. Alternatively – as is now increasingly common – a virus may place a backdoor Trojan onto a computer. Once the Trojan is run, it adds itself to the computer’s startup routine. It can then monitor the computer until the user is connected to the internet. Once the computer is online, the person who sent the Trojan can run programs on the infected computer, access personal files, modify and upload files, track the user’s keystrokes, or send out spam mail. Well-known backdoor Trojans include Subseven, BackOrifice and Graybird, which was disguised as a fix for the notorious Blaster worm.
Spyware

Spyware is software that enables advertisers to gather information about a computer user’s habits.

Spyware programs are not viruses (you cannot spread them to other computers) but they can have undesirable effects.

You can get spyware on your computer when you visit certain websites. A pop-up message may prompt you to download a software utility that you “need”, or software may be downloaded automatically without your knowledge.

The spyware then runs on the computer, tracking your activity (for example, visits to websites) and reports it to others, such as advertisers. It can also change the home page displayed when you start your internet browser, and can use a dial-up modem to call 0900 (premium rate) phone numbers.

Spyware also uses memory and processing capacity, and can slow or crash the computer.

Software is available that detects known spyware programs and enables you to remove them.

Cookies

When you visit a website, it can place a small data packet called a “cookie” on the computer. This enables the site to remember your details and keep track of your visits.

Cookies do not pose a threat to your data. However, they do threaten your confidentiality. If you prefer to remain anonymous, use the security settings on your browser to disable cookies.
Can mobile phones get a virus?

Mobiles can be infected by worms that spread themselves via the mobile phone network, although at the time of writing the risks seem limited.

In 2004, the first mobile phone worm was written. The Cabir-A worm affects phones that use the Symbian operating system, and is transmitted as a telephone game file (an SIS file). If you launch the file, a message appears on the screen, and the worm is run each time you turn the phone on thereafter. Cabir-A searches for other mobile phones nearby using Bluetooth technology, and sends itself to the first it finds. This worm proves that infection is possible, but it was not released onto a public network.

There are also conventional viruses that send messages to mobile phones. For example, Timo-A uses computer modems to send text (SMS) messages to selected mobile numbers, but in cases like these the virus can’t infect or harm the mobile phone.

Until now, the risks for mobile phones have been few. This could be because they use many different operating systems, and because the software and device characteristics change so rapidly.
Does Bluetooth carry risks?

*Bluetooth technology for mobiles, computers and other devices could open the way for viruses, breaches of security or pranks.*

Bluetooth technology allows computers, mobile phones and even video recorders or fridges to locate nearby devices and to establish links with them transparently.

Bluetooth has already been exploited by a mobile phone worm, which uses it to find nearby phones to which it can forward itself.

Technologies based on Bluetooth, e.g. Jini, also enable remote control of services. Bluetooth and Jini are designed so that only trusted code can carry out sensitive operations – but such technologies open up the possibility that malicious code could interfere with services.

Bluetooth-enabled phones can also be used to locate other phone users nearby and send them unexpected – and sometimes offensive – messages.

You can protect yourself against all sorts of Bluetooth threats – whether from malicious programs or from unwanted messages by turning off the “visible to others” Bluetooth setting in your phone.
Can palmtops get a virus?

*Palmtops or PDAs provide new opportunities for viruses, but so far virus writers have shown little interest.*

Palmtops or PDAs run special operating systems – such as Palm and Microsoft PocketPC. These are vulnerable to malicious code, but so far the risks seem low.

There is only one virus written for Palm, and one Trojan horse, but neither seems to have been released.

Virus writers prefer to target desktop systems, perhaps because they are more popular and allow viruses to spread rapidly via email and the internet.

The real risk at present is that your palmtop will act as a carrier. When you connect it to a home or office PC to synchronise data, a virus that is harmless on the palmtop could spread to the PC, where it can do harm. To avoid this risk, follow our “Tips for safer computing” and always run anti-virus software on your desktop computer.
Anti-virus software

Anti-virus software can detect viruses, prevent access to infected files and often eliminate the infection.

Virus scanners

Virus scanners detect, and often disinfect, the viruses known to the scanner. 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-access and on-demand scanners. Many packages offer both.

On-access scanners stay active on your machine whenever you are using it. They automatically check files as you try to open or run them, and can prevent you from using infected files.

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

Heuristics

Heuristic software tries to detect viruses – both known and unknown – by using general rules about what viruses look like.

This software doesn’t rely on frequent updates. However, heuristics can also be prone to false alarms.
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?”*

Virus writers sometimes want to spread a political message, or to disrupt companies of which they disapprove (many viruses and worms have criticised or targeted Microsoft, for example). They can also break into other users’ computers, or gather email addresses, and then sell that information to spammers.

However, virus writers are more often motivated by the notoriety that their exploits can gain them.

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, like graffiti art, is 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.
A brief history of viruses

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


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.

1992  There is worldwide panic about the *Michelangelo* virus, although very few computers are infected.
1994  *Good Times*, the first major virus hoax, appears.


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.

2001  A virus claiming to contain pictures of tennis player Anna Kournikova infects hundreds of thousands of computers worldwide.

2002  David L Smith, the author of *Melissa*, is sentenced to 20 months in prison by US courts.

2003  The *Blaster* worm spreads itself across the internet via a security weakness in Microsoft software. Together with the *Sobig* email virus, it makes August 2003 the worst month ever for virus incidents.

2004  The creators of the *Netsky* and *Bagle* series of worms compete to see which can have the greater impact.
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. 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. A badly written virus can cause unforeseen problems. Even if it’s harmless on one system, it may be harmful on others.

Thirdly, viruses spread indiscriminately: the writer has no control over who receives them.

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 don’t usually have any effects and shouldn’t be released onto other users’ computers.

Virus 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.
Preventing viruses

There are simple measures you can take to avoid being infected or to deal with viruses if you are infected. For more details, see the “Tips for safer computing” chapter.

Make users aware of the risks

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

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.

Use software patches to close security loopholes

Watch out for “patches” for your operating system. These often close loopholes that make you vulnerable to viruses.

Use firewalls

A firewall can prevent unauthorised access to your network and also prevent viruses sending out information.

Keep backups of all your data

Keep 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.
Spam

The chances are that you have had emails offering you drugs without a prescription, or loans, or get-rich-quick schemes – sometimes cleverly disguised to look like personal email. This “spam” mail accounts for more than half of all the email sent worldwide, cluttering up inboxes and distracting users from more important messages.
What is spam?

Spam is unsolicited commercial email, the electronic equivalent of the junk mail that comes through your letterbox.

The commonest types of spam concern

- prescription drugs, drugs that enlarge or enhance body parts, herbal remedies, or weight loss drugs
- get-rich-quick schemes
- financial services, e.g. mortgage offers or schemes for reducing debts
- qualifications, e.g. university degrees, or professional titles available for purchase
- on-line gambling
- cut-price or pirated software.

Spam sometimes comes in disguise, with a subject line that reads like a personal message, e.g. “Sorry about yesterday”, a business message, e.g. “Your account renewal now due”, or a non-delivery message.

Why do people send spam?

People send spam because it is profitable. Spammers can send millions of emails in a single campaign for a negligible cost (and if they can hijack other people’s computers to send the mail, the cost is even less). If even one recipient out of ten thousand makes a purchase, the spammer can turn a profit.
Is spam really a problem?

*Spam doesn’t threaten your data in the way that viruses do, but it does harm your business.*

- Spam wastes staff time. Users without anti-spam protection have to check which email is spam and then delete it.
- Users can easily overlook or delete important email, confusing it with spam.
- Spam, like hoaxes or email viruses, uses bandwidth and fills up databases.
- Some spam offends users. Employers may be held responsible, as they are expected to provide a safe working environment.
- Spammers often use other people’s computers to send spam (“hijacking”).

**Hijacking**

Spammers often hijack other users’ computers and use them to forward spam. The victims of hijacking are unwittingly bombarding other users with spam. Spammers are careful to ensure that they cannot be traced, so it is the company with the hijacked computer that receives complaints and has its reputation harmed.
Spammers know when you’re reading

*Spammers want to know who is receiving their messages and who isn’t, so that they can target the next campaign.*

Even if you don’t reply to spam, the spammer has ways of finding out that you have received it.

- If you have your email program set to preview messages (i.e. to show you the contents of the message in a window below the list of email), the spammer may be able to see that the email has been received.

- If you click on a link that lets you unsubscribe from a mailing list, you confirm that your email address is active. The spammer can then sell your address to others.

- Spammers can include a “web bug” in an email. This is a link that connects to the spammer’s website as soon as the email is read or previewed.

If you want to avoid letting spammers know that their mail got through, follow the advice in the “How to avoid spam” section.
Anti-spam software

*Anti-spam programs can detect unwanted email and prevent it from reaching users’ inboxes.*

These programs use a combination of methods to decide whether an email is likely to be spam. They can:

- Block email that comes from addresses on a blacklist. This can be a commercially available list or a “local” list of addresses that have sent spam to your company before.

- Check whether email comes from a genuine domain name or web address. Spammers often use fake addresses to try to avoid anti-spam programs.

- Look for keywords or phrases that occur in spam (e.g. “credit card”, “lose weight”).

- Look for patterns that suggest the email’s sender is trying to disguise their words (e.g. putting “hardc*re p0rn”).

- Look for unnecessary HTML code (the code used for writing web pages) used in email, as spammers often use this to try to conceal their messages and confuse anti-spam programs.

The program combines all the information it finds to decide the probability of an email being spam. If the probability is high enough, it can block the email or delete it, depending on the settings you choose.
Software that learns which email you want

Some anti-spam software is “adaptive”: it learns which subjects you find acceptable and which ones you don’t.

Suppose that a pharmaceutical company installs anti-spam software. At first, the software tries to spot spam by looking for words like the following: credit, free, consolidate, debt, mortgage, drugs, prescription, medication, doctor. It blocks email with too many of these keywords, but allows individual users to retrieve mail that they want to read.

Someone in the research department finds that genuine mail about new drugs has been blocked, and asks for it to be released. The software learns that that user frequently receives email about drugs – and so gives less weight to drug-related words when checking for spam.

In the finance department, users reclaim email with financial terms in it, so the software learns to give less weight to these words – but still blocks drug-related email for that user.
Won’t anti-spam programs block real email?

*Many users worry that anti-spam software will delete personal or useful email. In fact, your email is safe, and you can even see selected spam if you wish.*

Anti-spam programs can be very accurate. Typically, they may block less than one genuine email in ten thousand, or even a hundred thousand.

Even if the program does incorrectly identify an email as spam, it can be configured to place it in a “quarantine” area, rather than deleting it. An administrator can then decide whether to let the mail be delivered or to delete it. Some programs let each user reclaim any quarantined mail that they want.

**But I want spam!**

One man’s spam might be another’s essential reading.

Someone who works for a finance company might want to see interest rates offered by other companies. Or a software company might want to know if spammers are selling pirated products. Fortunately, you can customise some anti-spam software to accept the spam that interests you.
The tricks spammers use

Spammers are constantly trying to find ways to disguise their messages and fool anti-spam software. Here are some of the tricks they use.

Lost in space

The spammer puts spaces between the letters of words that he wants to hide, for example “d r u g s”, hoping that the anti-spam software will not read the letters as one word. This trick is easy to detect.

The black hole

The spammer uses HTML code (the code used for writing web pages) to insert a space between letters, but also sets the size of the space to zero.

What the anti-spam program sees

\[ <\text{V} \text{ i} \text{a} \text{g} > \text{r} \text{a} > \text{a} \]

What you see

Viagra
The tricks spammers use

**Invisible ink**

Spammers sometimes want the reader to see one message while the anti-spam program sees another, more innocent one. They use HTML code to insert an innocent-looking message, but in the same colour as the background.

*What the anti-spam program sees*

```html
<body bgcolor=white> Viagra
<font color=white>Hi, Johnny! It was really nice to have dinner with you.
See you soon, love Mom</font></body>
```

*What you see*

Viagra

**The microdot**

The spammer inserts an extra letter into the middle of a word he wants to disguise, but uses a very small type size. The anti-spam program sees the letter and misreads the word, but the recipient of the email doesn’t.

**Return to sender**

The spammer deliberately sends his email to an invalid address, but puts your address in the “From” field. The email can’t be delivered, so the service provider’s server may send it back to … you.
The tricks spammers use

The numbers game

A spammer can write a word by using the special HTML codes for each letter, instead of ordinary letters. For example the letter “a” can be written by typing &#97.

What the anti-spam program sees

&amp;86;&lt;font size=0&gt;&amp;nbsp;&lt;/font&gt;&amp;105;&lt;font size=0&gt;&amp;nbsp;&lt;/font&gt;&amp;97;&lt;font size=0&gt;&amp;nbsp;&lt;/font&gt;&amp;103;&lt;font size=0&gt;&amp;nbsp;&lt;/font&gt;&amp;114;&lt;font size=0&gt;&amp;nbsp;&lt;/font&gt;&amp;97

What you see

Viagra

Slice and dice

Spammers use HTML tables to “shred” text into thin vertical columns, as if the message had been put through a shredder.

What the anti-spam program sees

Viagra
samples
free
Spam and viruses together

Spammers and virus writers can team up to create even more problems for email users.

Viruses can open up new opportunities for spam. A virus writer can write a virus that enables other users to take control of a computer without the legitimate user realising. If that virus succeeds in infecting a computer, it sends a message to the virus writer, who can sell his list of infected computers to a spammer. The spammer then uses these computers to send out spam.

More than 30% of spam is now sent via such compromised computers. By sending out spam this way, the spammers distance themselves from the activity and make themselves harder to trace.

Spammers may have returned the compliment by helping to spread email viruses. A virus writer could kick-start a virus by emailing it to large numbers of users, using a spammer’s address list. With so many recipients, a substantial number would activate the virus, ensuring that it could forward itself and spread rapidly.

There seems to be some evidence of collusion between spammers and virus writers. The Mimail-L virus, for example, attempted to launch a denial of service attack on several anti-spam websites.
How to avoid spam

**Use anti-spam software**

Anti-spam software can reduce unwanted email, especially if it uses your feedback to “learn” which mails are spam.

**Never make a purchase from unsolicited email**

By making a purchase, you are funding future spam. Your email address may also be added to lists that are sold to other spammers, so that you receive even more junk email. Worse still, you could be the victim of a fraud.

**If you don’t know the sender, delete the email**

Most spam is just a nuisance, but sometimes it can contain a virus that damages the computer when the email is opened.

**Never respond to spam or click on links in it**

If you reply to spam – even to unsubscribe from the mailing list – you confirm that your email address is a valid one, so encouraging more spam.

**Opt out of further information or offers**

When you fill out forms on websites, look for the checkbox that lets you choose whether to accept further information or offers. Tick or un-tick the box as appropriate.
How to avoid spam

Don’t use the “preview” mode in your email viewer

Many spammers can track when a message is viewed, even if you don’t click on the email. The preview setting effectively opens the email and lets spammers know that you receive their messages. When you check your email, try to decide whether it is spam on the basis of the subject line only.

Use the “bcc” field if you email many people at once

The “bcc” or blind copy field hides the list of recipients from other users. If you put the addresses in the “To” field, spammers may harvest them and add them to mailing lists.

Never provide your email address on the internet

Don’t publish your email address on websites, newsgroup lists or other online public forums. Spammers use programs that surf the internet to find addresses in such places.

Only give your main address to people you trust

Give your main email address only to friends and colleagues.

Use one or two “secondary” email addresses

If you fill out web registration forms or surveys on sites from which you don’t want further information, use a secondary email address. This protects your main address from spam.
Hoaxes and scams

If you have had an email that warns you about an unlikely-sounding new virus, offers you a free mobile phone, or asks you to update your bank account details, you have been the victim of a hoax. Hoax mail can interrupt work, overload mail systems, or even trick you into giving personal credentials and passwords to criminals.
Virus hoaxes

Virus hoaxes are reports of non-existent viruses. Usually 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, e.g. The A moment of silence hoax 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.

Hoax or not?

On April 1, 2000 an email headed Rush-Killer virus alert began circulating. It warned of viruses that dial 911 (the US emergency number), and urged you to forward the warning. The email had the hallmarks of a hoax, but the virus was real. It’s difficult to tell a hoax from a real warning; follow the advice in the “How to avoid hoaxes” section.
Why virus hoaxes matter

*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 Sobig virus, but the hoaxter 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.

Can hoaxes inspire viruses?

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

Page-jacking is the use of replicas of reputable webpages to catch users and redirect them to other websites.

Page-jackers copy pages from an established website and put them on a new site that appears to be legitimate. They register this new site with major search engines, so that users doing a search find and follow links to it. When the user arrives at the website, they are automatically redirected to a different site that displays advertising or offers of different services.

Page-jacking annoys users and can confront them with offensive material. It also reduces revenue for legitimate websites, and makes search engines less useful.

In some cases, page-jacking can be used for “phishing” (see next page).

You cannot be affected by page-jacking if you use a bookmark or “favourite”, or type the website address (the URL) in directly.

Mouse-trapping

If you are redirected to a bogus website, you may find that you cannot quit with the back or close buttons. This is called mouse-trapping.

To escape, type an address in the “Address” field, use a bookmark, or open the list of recently-visited addresses and select the next-to-last. To regain use of the back or close buttons, close the browser or restart the computer.
Phishing

Phishing is the use of bogus emails and websites to trick you into supplying confidential or personal information.

Typically, you receive an email that appears to come from a reputable organisation, such as a bank. The email includes what appears to be a link to the organisation’s website. However, if you follow the link, you are connected to a replica of the website. Any details you enter, such as account numbers, PINs or passwords, can be stolen and used by the hackers who created the bogus site.

You should always be wary about following links sent to you in emails. Instead, enter the website address in the “Address” field, or use a bookmark or a “favourite” link, to make sure that you are connecting to the genuine site.

Anti-spam software will also help to block phishing email.
Chain letters

An electronic chain letter is an email that urges you to forward copies to other people.

The main types of chain letter are:

- **Hoaxes.** Chain letters have warned of terrorist attacks, scams involving premium-rate phone lines, and thefts from ATMs. All were either deliberate hoaxes or urban myths.

- **Fake freebies.** Some letters falsely claim that companies are offering free flights, free mobile phones, or cash rewards if you forward email.

- **Petitions.** These are usually petitions against proposed legislation. Even if genuine, they continue to circulate long after their expiry date.

- **Jokes and pranks.** The “Internet cleaning” letter claimed that the internet would be closed for maintenance on 1 April.

---

**Are chain letters really a problem?**

Chain letters don’t threaten your security, but they can:

- Waste time and distract users from genuine email.

- Create unnecessary email traffic and slow down mail servers.

- Spread misinformation.

- Encourage people to send email to certain addresses, so that these are deluged with unsolicited mail.
How to avoid hoaxes

**Have a company policy on virus warnings**

Set up a company policy on virus warnings, for 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.”

**Keep informed about hoaxes**

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

**Don’t forward chain mail**

Don’t forward chain mail, even if it offers you rewards for doing so, or claims to be distributing useful information.

**Don’t trust links in unsolicited email**

If you want to visit your bank’s website, or any site where you enter passwords or confidential information, don’t follow links in unsolicited email or newsgroups. Enter the address yourself, or use a bookmark or “favourites” link.
Tips for safer computing

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

**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.

**Don’t use documents in .doc and .xls format**
Save Word documents as RTF files and Excel spreadsheets as CSV files. These formats don’t support macros, so they can’t spread document viruses. Tell other people to send you RTF and CSV files. Beware, though! Some document viruses disguise the format. To be absolutely safe, use text-only files.

**Use software patches to close security loopholes**
Watch out for security news and download patches. Such patches often close loopholes that can make you vulnerable to viruses or internet worms. IT managers should subscribe to software vendors’ mailing lists such as that at www.microsoft.com/technet/security/bulletin/notify.asp. Home users who have Windows computers can visit windowsupdate.microsoft.com, where you can scan your PC for security loopholes and find out which patches to install.
Tips for safer computing

Block files with double extensions at the gateway

Some viruses disguise the fact that they are programs by using a double extension, such as .TXT.VBS, after their filename. At first glance a file like LOVE-LETTER-FOR-YOU.TXT.VBS looks like a harmless text file or a graphic. Block any file with double extensions at the email gateway.

Block unwanted file types at the email gateway

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

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 www.sophos.com/virusinfo/notifications

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.
Tips for safer computing

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.

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.

Change your computer’s bootup sequence
Most computers try to boot from floppy disk (the A: drive) first. IT staff should change the settings so that the computer boots from the hard disk first. Then, even if an infected floppy disk is left in the computer, it cannot be infected by a boot sector virus.

Write-protect floppies before giving to other users
A write-protected floppy cannot be infected.
Glossary
ActiveX: A Microsoft technology that extends the capabilities of a web browser.

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


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.

Bayesian filtering: A statistical approach to determining whether email is spam (based on Bayesian probability theory).

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

Blackhole list: A published list, usually commercial, of addresses known to be sources of spam. See also Real-time blackhole list.

Blacklist: A list of email addresses and domains from which no mail will be accepted.

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.

**Complex dictionary checking:**  A feature of anti-spam software that finds words often used in spam, even if letters are replaced with lookalike numerals or characters (such as “1nterest r@te”).

**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.

**Denial of service attack:**  An attempt to prevent the use of an email system or web server by sending unusual or excessive messages or attachments.

**Dictionary attack:**  A program that bombards a mail server with alphabetically-generated email addresses in the hope that some addresses will be guessed correctly. The same method can be used to guess passwords.
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.

False positive: A report that a virus has been found (or that an email is spam) when this is not the case.

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

Firewall: A security system that is placed between the internet and an organisation’s network, or within a 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.

Greylist: Email senders who are not blacklisted (excluded) or whitelisted (accepted) can be placed on a greylist and requested to prove that they are sending legitimate mail.

Hacker: Someone who intentionally breaches computer security, usually to cause disruption or gain confidential information such as financial details. Originally the word “hacker” referred to any person who was interested in computer technology, but is now commonly used by the public and media to refer to those who have malicious intentions.
Ham: Email that a recipient does not consider to be spam (q.v.).

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

Harvesting: Scanning the internet for email addresses that can be put on spammers’ mailing lists.

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

Hoax: A communication, often by email, which is intended to deceive.

Honeypot: A computer system on the internet set up to attract and trap spammers and hackers.

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.

HTTP scanning: Real-time scanning of HTTP traffic to ensure web pages you are viewing or downloading are free from viruses.

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.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link virus:</td>
<td>A virus which subverts directory entries so that they point to the virus code, allowing it to run.</td>
</tr>
<tr>
<td>Macro:</td>
<td>Sets of instructions inside data files that can carry out program commands automatically, e.g. opening and closing files.</td>
</tr>
<tr>
<td>Macro virus:</td>
<td>A virus which uses macros in a data file to become active and attach itself to other data files.</td>
</tr>
<tr>
<td>Mail drop:</td>
<td>An email address set up to receive replies to spam. The spammer then cancels the account from which the spam was sent in an attempt to avoid detection.</td>
</tr>
<tr>
<td>Master boot record:</td>
<td>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.</td>
</tr>
<tr>
<td>Memory-resident virus:</td>
<td>A virus that stays in memory after it becomes active and after its host program is closed (unlike other viruses that are activated only when an infected application runs).</td>
</tr>
<tr>
<td>Modem:</td>
<td>A MOdulator/DEModulator converts computer data into a form suitable for transmission via telephone line, radio or satellite link.</td>
</tr>
<tr>
<td>Multipartite virus:</td>
<td>A virus which infects both boot sectors and program files.</td>
</tr>
<tr>
<td>Munging:</td>
<td>Disguising email addresses so that they cannot be harvested. Recipients are told how to decode the address.</td>
</tr>
<tr>
<td>Newsgroup:</td>
<td>An electronic forum where readers post articles and follow-up messages on specified topics.</td>
</tr>
<tr>
<td>Notebook:</td>
<td>A computer even smaller than a laptop computer.</td>
</tr>
<tr>
<td>Obfuscation:</td>
<td>Spammers’ attempts to hide messages so that they will not be detected. Sometimes used to refer to disguising email addresses so that spammers cannot harvest them.</td>
</tr>
<tr>
<td>Open relay:</td>
<td>An SMTP email server that allows the third-party relay of email messages. Spammers can hijack such servers and use them to send spam.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Operating system:</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Palmtop:</strong></td>
<td>A computer small enough to be held in the palm of the hand.</td>
</tr>
<tr>
<td><strong>Parasitic virus:</strong></td>
<td>See Program virus.</td>
</tr>
<tr>
<td><strong>Password:</strong></td>
<td>Sequence of characters which gives access to a system.</td>
</tr>
<tr>
<td><strong>PC:</strong></td>
<td>Personal Computer. A desktop or portable single-user computer.</td>
</tr>
<tr>
<td><strong>PDA:</strong></td>
<td>Personal Digital Assistant. A small, mobile computing device used mostly for managing data such as address books and calendars.</td>
</tr>
<tr>
<td><strong>Phishing:</strong></td>
<td>Tricking users into submitting confidential information or passwords by creating a replica of a legitimate website.</td>
</tr>
<tr>
<td><strong>Polymorphic virus:</strong></td>
<td>Self-modifying virus. By changing its code, the virus tries to make itself harder to detect.</td>
</tr>
<tr>
<td><strong>Program:</strong></td>
<td>A set of instructions that specifies actions a computer should perform.</td>
</tr>
<tr>
<td><strong>Program virus:</strong></td>
<td>A computer virus which attaches itself to another computer program, and is activated when that program is run.</td>
</tr>
<tr>
<td><strong>Proxy server:</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>RAM:</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Real-time blackhole list (RBL):</strong></td>
<td>A list that rejects all mail, valid or not, from addresses known to send spam or host spammers. This can induce internet service providers to take anti-spam measures.</td>
</tr>
</tbody>
</table>
Reverse DNS check: Checking an email’s sender address against a Domain Name System database to ensure that it originated from a valid domain name or web address.

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.


Spam: Unsolicited commercial email (UCE) and unsolicited bulk email (UBE) that a recipient does not want.

Spambot: A program that spammers use to harvest email addresses from the internet.

Spoofing: Forging the sender’s address in email. Spoofing can be used to hide the origin of spam, or to convince recipients that unsafe email is from a reliable source.

Spyware: Software that tracks user activity and reports information to others, such as advertisers. Usually, the tracking is concealed from the software user.

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

Tarpitting: Monitoring email traffic to identify addresses sending a suspiciously large volume of email, which may be spam.
Tarpit: An intentionally slow email server that aims to trap spammers using harvesting programs.


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 bug: A small graphic inserted in an email or web page that alerts a spammer when a message is read or previewed.

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

Whitelist: A list of external email addresses, IP addresses and domains from which email is accepted without being checked for spam and/or viruses.
**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.

**Zombie:** An insecure computer that is hijacked and used to send spam or launch a denial of service attack (q.v).
Index

A

adaptive software 32
anti-spam software 31
adaptive 32
anti-virus software 20
heuristic 20

B

backdoor Trojan 15
boot sector virus 11

C

chain letters 46
cookies 16

D

denial of service 8
document virus 11

E

email attachments 12
e-mail virus 12, 13

H

"harmless" virus 24
heuristic software 20
hoax virus 42
side-effects 43
hoaxes 41
avoiding 47
chain letters 46
page-jacking 44
phishing 45
virus hoaxes 42, 43

I

internet worm 14

J

Jini 18

M

macro virus, see document virus
mobile phones 17
mouse-trapping 44
P
page-jacking 44
palmtop 19
phishing 45
PocketPC 19
program virus 11
proof-of-concept virus 24
S
spam
    and viruses 37
    avoiding 38–39
    defined 28
    side-effects 29
    tricks for disguising 34–36
spam filter 31
    adaptive 32
spyware 16
T
Trojan horse 7
    backdoor 15
V
virus
    and spam 37
    boot sector 11
    defined 6
    "harmless" 24
    history 23
    in attachments 12
    in program 11
    on a mobile phone 17
    on a palmtop 19
    prevention 20, 25
    proof-of-concept 24
    side-effects 8–9
    spread by email 12, 13
virus hoax 42
    side-effects 43
virus writers 20
W
web bug 30
websites
    bogus 44, 45
    page-jacking 44
worm 7
    internet 14