

a to z

of computer security threats



SOPHOS

a to z

of computer security threats

Whether you're a network administrator, use a computer at work, or just browse the internet, this book is for you. We tell you the facts about computer viruses, worms, spyware, spam – and more – in simple, easy-to-understand language.

Sophos is a world leader in integrated threat management solutions for business, education and government, protecting against known and unknown malware, spyware, intrusions, unwanted applications, spam, and policy abuse. Sophos's reliably engineered, easy-to-operate products protect more than 35 million users in more than 150 countries. Through 20 years' experience and a global network of threat analysis centers, the company responds rapidly to emerging threats – no matter how complex – and achieves the highest levels of customer satisfaction in the industry.

Contents

Introduction	4
A to Z of threats	6
Security software	75
Safety tips	83
Virus timeline	96

Copyright 2006 Sophos Group. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

ISBN 0-9553212-0-4

ISBN 978-0-9553212-0-7

Introduction

Everyone knows about computer viruses...or at least they think they do.

Just over twenty years ago, the first virus for PCs was written, apparently with the intention of protecting software on old-style floppy disks from bootleggers. Since then, hundreds of thousands of viruses and other “malware” – email viruses, Trojans, internet worms, keystroke loggers – have appeared, some spreading worldwide and making headlines. Many people have heard about viruses that fill your computer screen with garbage, or delete your files. In the popular imagination, malware still means pranks or sabotage. The nineties saw global panic about the **Michelangelo** virus, now long forgotten. Again, in the noughties, when millions of computers were infected with the **SoBig-F** virus and primed to download unknown programs from the web at a set time, anti-virus companies scrambled to persuade internet service providers to shut down servers to avoid a “doomsday scenario”. Movies like *Independence Day* and *The Net* reinforce this perception, with virus attacks signalled by flashing screens and alarms.

However, this is far from the truth today. The threats are no less real now, but they are low-profile, well-targeted, and more likely to be about making cash than creating chaos.

Today, malware is unlikely to delete your hard disk, corrupt your spreadsheet, or display a message. Such cyber-vandalism has given way to more lucrative exploits. Today’s virus might encrypt all your files and demand a ransom. Or a hacker might blackmail a large company by threatening to launch a “denial-of-service” attack, which prevents customers from accessing their website.

More commonly, though, viruses don’t cause any apparent damage or announce their presence at all. Instead, a virus might silently install a keystroke logger, which waits until the victim visits a banking website and then records the user’s account details and password, and forwards them to a hacker via the internet. The hacker can then

use these details to clone credit cards or plunder bank accounts. The victim isn’t even aware that the computer has been infected. Once the virus has done its job, it may delete itself altogether to avoid detection.

Another trend is that of blended threats – these combine different types of malware or hacking methods. A virus writer may use a spammer’s address list to email a Trojan horse program out, ensuring that large numbers of people receive and activate it in a short time. This type of technique can also help the spammers. Viruses and Trojans can turn computers into remote-controlled “zombies”, which the spammers use to distribute their profit-making spam mail.

Hackers may not even target large numbers of victims any more. Such high-visibility attacks bring unwanted attention, and anti-virus companies can soon neutralize malware that is widely reported. In addition, large-scale exploits can bring hackers more stolen data than they can handle. So threats are becoming more carefully focused. “Spear phishing” is an example. Originally, “phishing” involved sending out mass-mail messages that appeared to come from banks, asking customers to re-register confidential details, which could then be stolen. Spear phishing, by contrast, confines itself to a small number of people, usually within an organization. The mail appears to come from colleagues in trusted departments, asking for password information. The principle is the same, but the attack is more likely to succeed as the victim thinks that the message is internal, and his or her guard is down.

Stealthy, small-scale, well-targeted: for now, this seems to be the way that security threats are going.

What of the future, though? Predicting how security threats will develop is almost impossible. Some commentators assumed that there would never be more than a few hundred viruses, and Microsoft’s Bill Gates declared that spam would no longer be a problem by 2006. It’s not clear where future threats will come from, or how serious they will be. What is clear is that whenever there is an opportunity for financial gain, hackers and criminals will attempt to access and misuse data.

A



Z



Adware

Adware is software that displays advertisements on your computer.

Adware, or advertising-supported software, displays advertising banners or pop-ups on your computer when you use the application. This is not necessarily a bad thing. Such advertising can fund the development of useful software, which is then distributed free (for example, the Opera web browser).

However, adware becomes a problem if it:

- installs itself on your computer without your consent
- installs itself in applications other than the one it came with and displays advertising when you use those applications
- hijacks your web browser in order to display more ads (see **Browser hijackers**)
- gathers data on your web browsing without your consent and sends it to others via the internet (see **Spyware**)
- is designed to be difficult to uninstall.

Adware can slow down your PC. It can also slow down your internet connection by downloading advertisements. Sometimes programming flaws in the adware can make your computer unstable.

Advertising pop-ups can also distract you and waste your time if they have to be closed before you can continue using your PC.

Some anti-virus programs detect adware and report it as “potentially unwanted applications”. You can then either authorize the adware program or remove it from the computer. There are also dedicated programs for detecting adware.



Backdoor Trojans

A backdoor Trojan allows someone to take control of another user's computer via the internet without their permission.

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 – users may allow Trojans onto their computer by following a link in spam mail.

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. When the computer goes online, the person who sent the Trojan can perform many actions – for example, 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, more recently, **Graybird**, which was disguised as a fix for the notorious **Blaster** worm.

To avoid backdoor Trojans, you should keep your computers up to date with the latest patches (to close down vulnerabilities in the operating system), and run anti-spam and anti-virus software. You should also run a firewall, which can prevent Trojans from accessing the internet to make contact with the hacker.

Bluejacking

Bluejacking is sending anonymous, unwanted messages to other users with Bluetooth-enabled mobile phones or laptops.

Bluejacking depends on the ability of Bluetooth phones to detect and contact other Bluetooth devices nearby. The Bluejacker uses a feature originally intended for exchanging contact details or “electronic business cards”. He or she adds a new entry in the phone’s address book, types in a message, and chooses to send it via Bluetooth. The phone searches for other Bluetooth phones and, if it finds one, sends the message.

Despite its name, Bluejacking is essentially harmless. The Bluejacker does not steal personal information or take control of your phone.

Bluejacking can be a problem if it is used to send obscene or threatening messages or images, or to send advertising. If you want to avoid such messages, you can turn off Bluetooth, or set it to “undiscoverable”.

Bluetooth-enabled devices may also be at risk from the more serious Bluesnarfing.



Bluesnarfing

Bluesnarfing is the theft of data from a Bluetooth phone.

Like Bluejacking, Bluesnarfing depends on the ability of Bluetooth-enabled devices to detect and contact others nearby.

In theory, a Bluetooth user running the right software on their laptop can discover a nearby phone, connect to it without your confirmation, and download your phonebook, pictures of contacts and calendar.

Your mobile phone’s serial number can also be downloaded and used to clone the phone.

You should turn off Bluetooth or set it to “undiscoverable”. The undiscoverable setting allows you to continue using Bluetooth products like headsets, but means that your phone is not visible to others.



Boot sector viruses

Boot sector viruses spread by modifying the program that enables your computer to start up.

When you switch on a computer, the hardware looks for the boot sector program – which is usually on the hard disk, but can be on a floppy disk 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.

Boot sector viruses were the first type of virus to appear, and they are mostly quite old. They are rarely encountered today.



Browser hijackers

Browser hijackers change the default home and search pages in your internet browser.

Some websites run a script that changes the settings in your browser without your permission. This hijacker can add shortcuts to your “Favorites” folder or, more seriously, can change the page that is first displayed when you open the browser.

You may find that you cannot change your browser’s start page back to your chosen site. Some hijackers edit the Windows registry so that the hijacked settings are restored every time you restart your computer. Others remove options from the browser’s tools menu, so that you can’t reset the start page.

In every case, the intention is the same: to force you to visit a website. This inflates the number of “hits” and the site’s ranking with search engines, which boosts the advertising revenue that the site can earn.

Browser hijackers can be very tenacious. Some can be removed automatically by security software. Others may need to be removed manually. In some cases, it is easier to restore the computer to an earlier state or reinstall the operating system.



Chain letters

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

Chain letters, like virus hoaxes, depend on you, rather than on computer code, to propagate themselves. The main types are:

- Hoaxes about terrorist attacks, premium-rate phone line scams, thefts from ATMs and so forth.
- False claims that companies are offering free flights, free mobile phones, or cash rewards if you forward email.
- Messages, which purport to be from agencies like the CIA and FBI, warning about dangerous criminals in your area.
- Petitions. Even if genuine, they continue to circulate long after their expiry date.
- Jokes and pranks, e.g. the claim that the internet would be closed for maintenance on 1 April.

Chain letters don't threaten your security, but they can waste time, spread misinformation and distract users from genuine email.

They can also create unnecessary email traffic and slow down mail servers. In some cases the chain letter encourages people to send email to certain addresses, so that these are deluged with unsolicited mail.

The solution to the chain letter problem is simple: don't forward such mail.



Cookies

Cookies are files on your computer that enable websites to remember your details.

When you visit a website, it can place a file called a cookie on your computer. This enables the website to remember your details and track your visits. Cookies can be a threat to confidentiality, but not to your data.

Cookies were designed to be helpful. For example, if you submit your ID when you visit a website, a cookie can store this data, so that you don't have to re-enter it next time. Cookies also have benefits for webmasters, as they show which web pages are well-used, providing useful input when planning a redesign of the site.

Cookies are small text files and cannot harm your data. However, they can compromise your confidentiality. Cookies can be stored on your computer without your knowledge or consent, and they contain information about you in a form you can't access easily. And when you revisit the same website, this data is passed back to the web server, again without your consent.

Websites gradually build up a profile of your browsing behavior and interests. This information can be sold or shared with other sites, allowing advertisers to match ads to your interests, ensure that consecutive ads are displayed as you visit different sites, and track the number of times you have seen an ad.

If you prefer to remain anonymous, use the security settings on your internet browser to disable cookies.



Denial-of-service attack

A denial-of-service (DoS) attack prevents users from accessing a computer or website.

In a DoS attack, a hacker attempts to overload or shut down a computer, so that legitimate users can no longer access it. Typical DoS attacks target web servers and aim to make websites unavailable. No data is stolen or compromised, but the interruption to the service can be costly for a company.

The most common type of DoS attack involves sending more traffic to a computer than it can handle. Rudimentary methods include sending oversized data packets or sending email attachments with names that are longer than permitted by the mail programs.

An attack can also exploit the way that a “session” of communications is established when a user first contacts the computer. If the hacker sends many requests for a connection rapidly and then fails to respond to the reply, the bogus requests are left in a buffer for a while. Genuine users’ requests cannot be processed, so that they can’t contact the computer.

Another method is to send an “IP ping” message (message requiring a response from other computers) that appears to come from the victim’s computer. The message goes out to a large number of computers, which all try to respond. The victim is flooded with replies and the computer can no longer handle genuine traffic.

A **distributed denial-of-service attack** uses numerous computers to launch the attack. Typically, hackers use a virus or Trojan to open a “back door” on other people’s computers and take control of them. These “zombie” computers can be used to launch a coordinated denial-of-service attack.

See [Backdoor Trojans, Zombies](#).

Dialers

Dialers change the number used for dial-up internet access to a premium-rate number.

Dialers are not always malicious. Legitimate companies that offer downloads or games may expect you to use a premium-rate line to access their services. A pop-up prompts you to download the dialer and tells you how much calls will cost.

Other dialers may install themselves without your knowledge when you click on a pop-up message (for example, a message warning you about a virus on your computer and offering a solution). These do not offer access to any special services – they simply divert your connection so that you access the internet via a premium-rate number.

Broadband users are usually safe, even if a dialer installs itself. This is because broadband doesn't use regular phone numbers, and because broadband users don't usually have a dial-up modem connected.

Anti-virus software can detect and eliminate Trojan horse programs that install dialers.

Document viruses

Document or “macro” viruses take advantage of macros – commands that are embedded in files and run automatically.

Many applications, such as word processing and 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 and Excel files. They can also spread to any platform on which their host application runs.

Macro viruses first appeared in the mid-1990s and rapidly became the most serious virus threat of that time. Few viruses of this type are seen now.



Email viruses

Many of the most prolific viruses distribute themselves automatically by email.

Typically, email-aware viruses depend on the user double-clicking on an attachment. This runs the malicious code, which will then mail itself to other people from that computer. The **Netsky** virus, for example, searches the computer for files that may contain email addresses, and then uses the email client on your computer to send itself to those addresses. Some viruses, like **Sobig-F**, don't even need to use your email client; they include their own "SMTP engine" for constructing and sending the email messages.

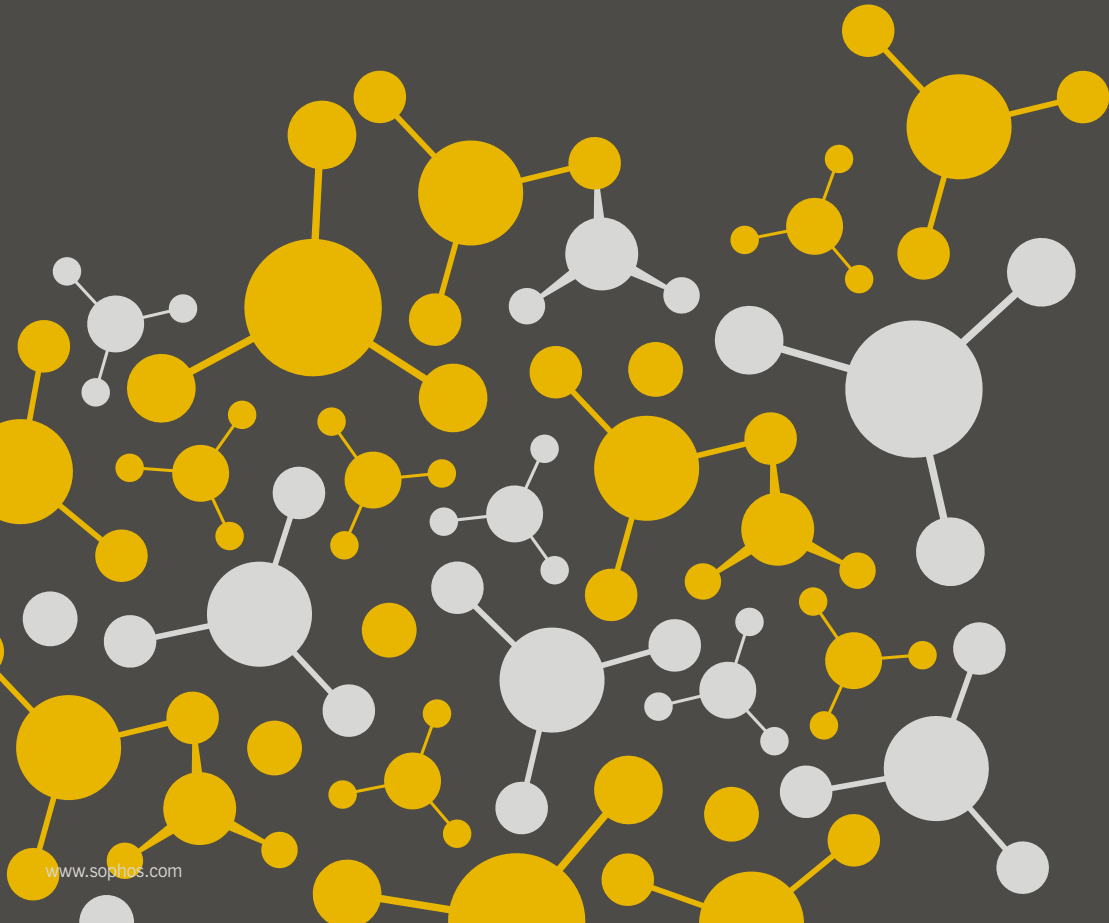
Any attachment that you receive by email could carry a virus; and launching such an attachment can infect your computer.

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.

Some viruses, such as **Kakworm** and **Bubbleboy**, can infect users as soon as they read email, exploiting a vulnerability in the operating system or mail program. 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.

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.

To avoid email viruses, you should run anti-virus software and avoid clicking on unexpected attachments. You should also install the patches issued by software vendors, as these can close down the vulnerabilities exploited by email viruses.



Internet worms

Worms are programs that create copies of themselves and spread via internet connections.

Worms differ from computer viruses because they can propagate themselves, rather than using a carrier program or file. They simply create exact copies of themselves and use communication between computers to spread.

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 unpatched Windows NT, 2000 and XP computers and uses it to send a copy of itself to another computer.

Many viruses, such as **MyDoom** or **Bagle**, now behave like worms and use email to forward themselves.

A worm can have malicious effects. For example, it may use affected computers to deluge websites with requests or data, causing them to crash (a “denial-of-service” attack). Alternatively, it can encrypt a user’s files and make them unusable. In either case, companies can be blackmailed.

Many worms open a “back door” on the computer, allowing hackers to take control of it. Such computers can then be used to send spam mail (see **Zombie**).

Quite apart from such effects, the network traffic generated by a fast-spreading worm can slow down communications. The **Blaster** worm, for example, creates a lot of traffic on the internet as it spreads, slowing down communications or causing computers to crash. Later it uses the affected computer to bombard a Microsoft website with data, with the aim of making it 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.



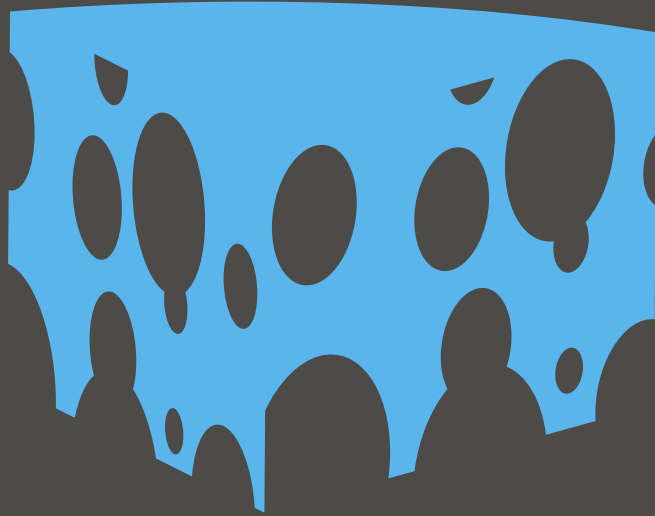
Mobile phone viruses

Mobiles can be infected by worms that spread themselves via the mobile phone network.

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.

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. The reason could be that they use many different operating systems, and that the software and device characteristics change so rapidly.



Mousetrapping

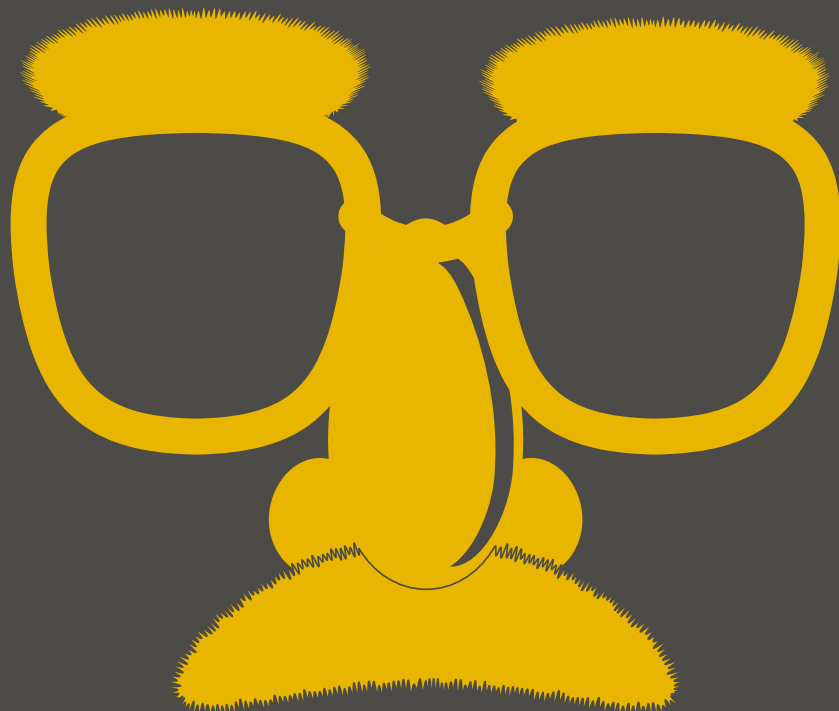
Mousetrapping prevents you from leaving a website.

If you are redirected to a bogus website, you may find that you cannot quit with the back or close buttons. In some cases, entering a new web address does not enable you to escape either.

The site that mousetraps you will either not allow you to visit another address, or will open another browser window displaying the same site. Some mousetraps let you quit after a number of attempts, but others do not.

To escape, use a bookmark or “Favorite”, or open the list of recently-visited addresses and select the next-to-last. You can also press Ctrl+Alt+Del and use the Task Manager to shut down the browser or, if that fails, restart the computer.

To reduce the risk of mousetrapping, you can disable Java script in your internet browser. This prevents you from being trapped at sites that use this script, but it also affects the look and feel of websites.



Obfuscated spam

Obfuscated spam is email that has been disguised in an attempt to fool anti-spam software.

Spammers are constantly trying to find ways to modify or conceal their messages so that your anti-spam software can't read them, but you can.

The simplest example of this "obfuscation" is putting spaces between the letters of words, hoping that anti-spam software will not read the letters as one word, for example

V I A G R A

Another common technique is to use misspellings or non-standard characters, for example

V!agra

These tricks are easily detected.

More advanced techniques exploit the use of HTML code (normally used for writing web pages) in email. This allows the spammer to write messages that anti-spam software "sees" quite differently from the way you see them.

For example, words can be written using special numerical HTML codes for each letter, e.g. instead of "Viagra", you can write

Viagra

HTML can also allow the reader to see one message, while the anti-spam software sees another, more innocent one. The more innocent message is in the same color as the background.

<body bgcolor=white> Viagra

Hi, Johnny! It was nice to have dinner with you. </body>

Spammers often include large amounts of hidden text, often cut from online reference books, to try to fool anti-spam software that assesses mail according to the frequency of certain key words.



Page-jacking

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

Scammers 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. They may also find that they cannot escape from the site without restarting their computer (see **Mousetrapping**).

Scammers use page-jacking to increase the number of visitors to a website. That means that their site commands more advertising revenue and is also more valuable if they decide to sell it. Alternatively, the scammer can redirect users to another site and claim a fee for “referring” visitors to that site.

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 is used in **phishing** attacks.

To avoid page-jacking, use a bookmark or “Favorite” (but you must be sure that you did not set up the favorite at a page-jacked site), or type the desired website address (the URL) in directly.



Palmtop viruses

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 are low.

There are currently only a few items of known malware written for Palm.

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 synchronize 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 on [How to avoid viruses, Trojans, worms and spyware](#) and always run anti-virus software on your desktop computer.



Parasitic viruses

Parasitic viruses, also known as file viruses, spread by attaching themselves to programs.

When you start a program infected with a parasitic virus, the virus code is run. To hide itself, the virus then passes control back to 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 make changes on your computer.

Parasitic viruses appeared early in virus history but they can still pose a threat.



Pharming

Pharming redirects you from a legitimate website to a bogus copy, allowing criminals to steal the information you enter.

Pharming exploits the way that website addresses are composed.

Each computer on the internet has a numerical “IP address”, e.g. 127.0.0.1. However, these are not easy to remember, so web addresses also have a domain name, like sophos.com. Every time you type in an address, the domain name has to be turned back into the IP address. A DNS or Domain Name Server on the internet handles this, unless a “local host file” on your computer has already done it.

Hackers can subvert this process in two ways. They can send out a Trojan horse that rewrites the local host file on your PC, so that it associates the domain name with a bogus website. You are then directed to that site, even though you enter the correct address. Alternatively, they can “poison” the DNS directory, i.e. alter it so that anyone who tries to visit that address is directed to the bogus site.

To avoid pharming, make sure that you use secure web connections when you access sensitive sites. Just look for the https:// prefix in the web address. If a hacker tries to mimic a secure site, a message will warn you that the site’s certificate does not match the address being visited.

If you see a warning that a site’s certificate is not valid or not issued by a trusted authority, you should not enter the site.

There are also software solutions. Some software can display a warning if you enter personal information in reply to an unknown email address. Other utilities can check to see if websites or IP addresses are blacklisted.

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 organization, such as a bank. The email includes what appears to be a link to the organization'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.

Sometimes the link displays the genuine web site, but superimposes a bogus pop-up window. You can see the address of the real website in the background, but details you enter in the pop-up window can be stolen.

Sometimes the hacker uses a technique called "cross-site scripting": the link takes you to the correct website, but subverts it by pulling in content from elsewhere. Once again, the part of the site where you enter information is controlled by the hacker.

Phishing had its origins in the 1990s, when scammers used the technique to collect AOL account details so that they could gain free internet access. The details were called "phish" because they were gathered by "fishing" for users. The "ph" imitates the spelling of "phreaker", the term for those who used to hack into the telephone network.

You should always be wary about emails that use generic salutations, e.g. "Dear Customer", and about following links sent to you in emails. Instead, you should enter the website address in the address field and then navigate to the right page, or use a bookmark or a "Favorite" link. Even if you enter the address, there is a risk of being redirected to a bogus site (see [Pharming](#)), so you should always exercise caution.

Anti-spam software can block many phishing-related emails. Some software can detect phishing content on web pages or in email, and can provide a toolbar that shows the real domain for the website you are following a link to.





Potentially unwanted applications (PUAs)

Potentially unwanted applications are programs that are not malicious but may be unsuitable on company networks.

Some applications are non-malicious and possibly useful in the right context, but are not suitable for company networks. Examples are adware, dialers, non-malicious spyware, tools for administering PCs remotely, and hacking tools.

Certain anti-virus programs can detect such applications on users' computers and report them. The administrator can then either authorize the applications for use or remove them from the computers.



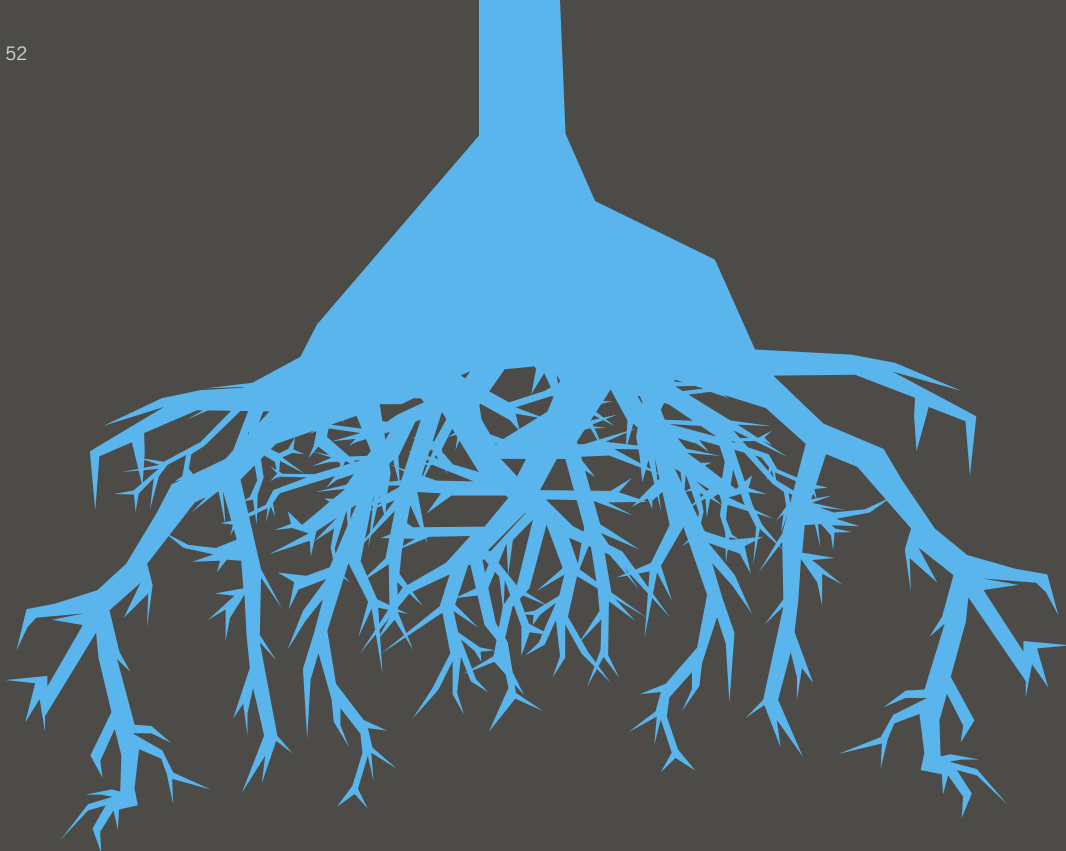
Ransomware

Ransomware is software that denies you access to your files until you pay a ransom.

In the past, malicious software typically used to corrupt or delete data, but now it can hold your data hostage instead. For example, the **Archiveus** Trojan copies the contents of “My Documents” into a password-protected file and then deletes the original files. It leaves a message telling you that you require a 30-character password to access the folder, and that you will be sent the password if you make purchases from an online pharmacy.

In that case, as in most ransomware so far, the password or key is concealed inside the Trojan’s code and can be retrieved by virus analysts. However, in the future hackers could use asymmetric or public-key encryption, which uses one key to encrypt the data, but another to decrypt it, so that the password would not be stored on your computer.

In some cases, the threat to deny access is sufficient. For example, the **Ransom-A** Trojan threatens to delete a file every 30 minutes until you pay for an “unlock code” via Western Union. If you enter an incorrect unlock code, the Trojan warns that the computer will crash after three days. However, the threats are a bluff, as **Ransom-A** is not capable of doing these things.



Rootkit

A rootkit is a piece of software that hides programs or processes running on a computer. It is often used to conceal misuse of the computer or data theft.

When malicious software, such as an internet worm, gains access to your computer, it sometimes installs a rootkit. This is often used to hide the presence of utilities that allow a hacker to open a “back door” that gives continuing access to the computer. The hidden utilities may also give the hacker rights to carry out functions that can usually only be performed by a user with special privileges. (On UNIX and Linux computers, such users are called “root”, and hence the name rootkit).

A rootkit can hide keystroke loggers or password sniffers, which capture confidential information and send it to hackers via the internet. It can also allow hackers to use the computer for illicit purposes, e.g. launching a “denial-of-service” attack against other computers, or sending out spam mail, without the user’s knowledge.

Even if a rootkit is not installed with malicious intent (as in the case of Sony’s Digital Rights Management, used to prevent pirating of music CDs), it can make the computer vulnerable to hackers.

Detecting rootkits is difficult. Once a rootkit is running on the computer, you cannot reliably identify all the processes running on that computer, or all the files in a directory – so traditional anti-virus software may not find evidence of the rootkit’s presence. A rootkit may also suspend its activity until the software has finished its scanning. A sure method of finding the rootkit is to turn off the computer, restart it from a rescue CD and then use anti-virus software to scan the computer. As the rootkit is not running, it cannot hide itself.

Anti-virus programs can detect the Trojans or worms that typically install the rootkit, of course, and some programs can now detect the rootkit itself while it is running.



Share price scams

Spammers now send out tips to push up the price of shares that can then be sold at a profit.

Share price scams, also known as “pump-and-dump” schemes, involve mass-mailing misleading tips about “high-performing” companies. Victims are encouraged to invest in a company’s shares, pushing up the price artificially; the scammer then sells their own shares at a profit, before the price collapses.

Pump-and-dump mail has all the characteristics of spam. It is unsolicited commercial mail, usually distributed from “zombie” PCs that have been taken over by hackers, and it uses obfuscation techniques to avoid anti-spam software (e.g. the subject line may use “st0ck” instead of “stock”). These emails also make inaccurate claims, although they may include some genuine information from the featured company to appear more plausible.

These scams harm both investors and small companies. When the bubble bursts and share prices plummet, investors lose their money. The collapse in value can also be devastating for companies that have limited assets.

The advice for dealing with these scams is the same as for any other spam: don’t buy, don’t try, don’t reply.

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
- online 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.

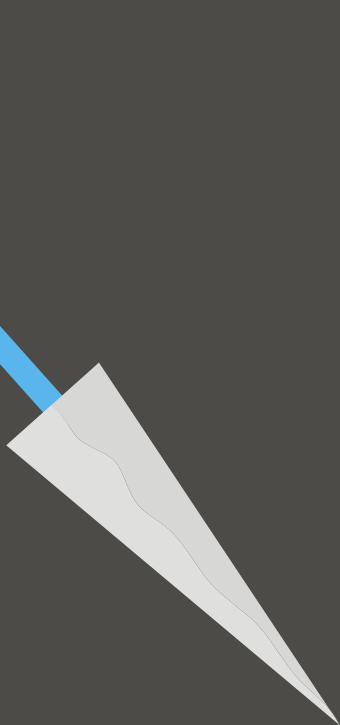
Spammers often disguise their email in an attempt to evade anti-spam software (see **Obfuscated spam**).

People send spam because it is profitable. Spammers can send millions of emails in a single campaign at 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.

Does spam matter?

- 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 (see **Zombies**).





Spear phishing

Spear phishing is the use of spoof emails to persuade people within a company to reveal their usernames and passwords.

Unlike **phishing**, which involves mass-mailing, spear phishing is small-scale and well-targeted. The spear phisher mails users in a single business. The emails appear to come from another member of staff at the same company and ask you to confirm a username and password. A common tactic is to pretend to be from a trusted department that might plausibly need such details, such as IT or Human Resources. Sometimes you are redirected to a bogus version of the company website or intranet. When you reply, the phisher takes the details and misuses them.

The spear phisher can easily generate the victims' addresses by using spammers' software that combines given names and family names, for example. He or she also needs to send emails to only a single domain, which makes it less likely that the email will be detected as spam.

Spoofting

Spoofting is sending email that appears to come from one sender but has actually been sent by another.

If a company's mail server allows connections to the SMTP port, anyone can connect to that port and send email that appears to be from an address on that site; the address can be a genuine email address or a fictitious address. This is called "spoofting".

Spoofting can be put to a number of malicious uses.

Phishers, criminals who trick users into revealing confidential information, use spoof sender addresses to make it appear that their email comes from a trusted source, such as your bank. The email can redirect you to a bogus website (e.g. an imitation of an online banking site), where your account details and password can be stolen.

Phishers can also send email that appears to come from inside your own organization, e.g. from a system administrator, asking you to change your password or confirm your details.

Criminals who use email for scams or frauds can use spoof addresses to cover their tracks and avoid detection.

Spammers can use a spoof sender address to make it appear that an innocent individual or company is sending out spam. Another advantage for them is that they are not inundated with non-delivery messages to their own email address.

You can avoid spoofing in various ways.

You can configure your mail system to prevent anyone from connecting to your SMTP port.

You can also use encryption to send authenticated email. This ensures that messages come from the senders they appear to be from, and that the message has not been modified.

Ensure that your mail delivery system allows logging and is configured to provide sufficient logging to assist you in tracking the origin of spoofed email.

Consider a single point of entry for email to your site. You can implement this by configuring your firewall so that SMTP connections from outside your firewall must go through a central mail hub. This will provide you with centralized logging, which may assist in detecting the origin of mail spoofing attempts to your site.





Spyware

Spyware is software that enables advertisers or hackers to gather information without your permission.

Spyware programs are not viruses (they do not spread 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 may also change the home page displayed when you start your internet browser, or use a dial-up modem to call premium-rate phone numbers. Spyware also consumes memory and processing capacity, which may slow or crash the computer.

Good anti-virus programs can detect and remove spyware programs, which are treated as a type of Trojan.



Trojan horses

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

A Trojan program claims to have one function (and may even appear to carry it out), but actually does something different, usually without your knowledge. 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 that record keystrokes or steal information – and some Trojans are used as a means of infecting a computer with a virus.

See also [Backdoor Trojans](#).



Viruses

Viruses are computer programs that can spread by making copies of themselves.

Computer viruses spread from one computer to another, and from one network to another, by making copies of themselves, usually without your knowledge.

Viruses can have harmful effects, ranging from displaying irritating messages to stealing data or giving other users control over your computer.

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 spread themselves automatically.

You might receive an infected file in a variety of ways, including via 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.



Virus hoaxes

Virus hoaxes are reports of non-existent viruses.

Hoaxes are usually in the form of emails that 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. 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.

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 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.



Voice phishing

Voice phishing is the use of bogus phone numbers to trick people into revealing confidential information.

Phishing originally involved sending out emails that include links to bogus websites, where victims are asked to enter account details or other confidential information. Voice phishing (also known as vishing, v-phishing or phone phishing) asks the victim to call a phone number, rather than visit a website, but the intention is the same: to steal details for financial gain.

An example is the **PayPal** voice phishing email. The email appears to come from PayPal, the electronic payment service, and claims that the user's account may have been used fraudulently. It warns that the account will be suspended unless the user calls a phone number to "verify" their details. When the user calls, an automated message asks for their card number. Criminals can then misuse the number for their own gain.

Users may be wary of following links in unexpected email, and they can ensure that they enter the correct web address when they visit a financial services site. They are less likely to know the company's phone number, though.

To protect against phone phishing, you should use anti-spam software, which can detect phishing mails, and always treat unsolicited email cautiously.



Zombies

A zombie is a computer that is remotely controlled and used for malicious purposes, without the legitimate user's knowledge.

A virus or Trojan can infect a computer and open a "back door" that gives other users access. As soon as this happens, the virus sends a message back to the virus writer, who can now control the computer remotely via the internet. From now on, the computer is a "zombie", doing the bidding of others, although the user is unaware. Collectively, such computers are called a "botnet".

The virus writer can share or sell access to control his or her list of compromised computers, allowing others to use them for malicious purposes.

For example, a spammer can use zombie computers to send out spam mail. Up to 80% of all spam is now distributed in this way. This enables the spammers to avoid detection and to get around any blocklisting applied to their own servers. It can also reduce their costs, as the computer's owner is paying for the internet access.

Hackers can also use zombies to launch a "denial-of-service" attack. They arrange for thousands of computers to attempt to access the same website simultaneously, so that the web server is unable to handle all the requests reaching it. The website thus becomes inaccessible.

See also [Denial-of-service attack](#), [Spam](#), [Backdoor Trojan](#).

Security software

Anti-virus software

Anti-virus software can defend you against viruses, Trojans, worms and – depending on the product – spyware and other types of malware.

Anti-virus software uses a scanner to identify programs that are, or may be, malicious. Scanners can detect:

- **Known viruses** – The scanner compares files on your computer against a library of “identities” for known viruses. If it finds a match, it issues an alert and blocks access to the file.
- **Previously unknown viruses** – The scanner analyzes the likely behavior of a program. If it has all the characteristics of a virus, access is blocked, even though the file does not match known viruses.
- **Suspicious files** – The scanner analyzes the likely behavior of a program. If that behavior is of a kind usually considered undesirable, the scanner warns that it may be a virus.

Detection of known viruses depends on frequent updating with the latest virus identities.

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

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

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

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 computers on a blocklist. This can be a commercially available list or a local list of computer addresses that have sent spam to your company before.
- Block email that includes certain web addresses.
- 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.

Anti-spam software needs frequent updating with new "rules" that enable it to recognize the latest techniques used by spammers.

How software protects mail you DO want

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.

How software adapts to your needs

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.

Firewall

A firewall prevents unauthorized access to a computer or a network.

As the name suggests, a firewall acts as a barrier between networks or parts of a network, blocking malicious traffic or preventing hacking attempts.

A **network firewall** is installed on the boundary between two networks. Usually this is between the internet and a company network. It can be a piece of hardware, or software running on a computer that acts as a gateway to the company network.

A **client firewall** is software that runs on an end user's computer, protecting only that computer.

In either case, the firewall inspects all traffic, both inbound and outbound, to see if it meets certain criteria. If it does, it is allowed; if not, the firewall blocks it. Firewalls can filter traffic on the basis of

- the source and destination addresses and port numbers (address filtering)
- the type of network traffic, e.g. HTTP or FTP (protocol filtering)
- the attributes or state of the packets of information sent.

A client firewall can also warn the user each time a program attempts to make a connection, and ask whether the connection should be allowed or blocked. It can gradually learn from the user's responses, so that it knows which types of traffic the user allows.

Resource shielding

Resource shielding protects you against attempts to access vulnerable parts of your computer.

Resource shielding analyzes the behavior of all the programs already running on your computer and blocks any activity that looks as if it could be malicious. For example, it checks any changes being made to the Windows registry, which may indicate that malware is installing itself so that it starts automatically whenever you restart the computer.

Resource-shielding products usually allow you to set up your own rules about which resources should be protected.

Safety tips

How to: avoid viruses, Trojans, worms and spyware

Use anti-virus software

Install anti-virus software on all your desktops and servers, and ensure they are kept up to date. New viruses can spread extremely quickly, so have an updating infrastructure in place that can update all the computers in your company seamlessly, frequently, and at short notice.

Run email filtering software at your email gateway as well, in order to protect your business from the threats of email-borne viruses, spam and spyware.

And don't forget to protect your laptop computers and desktop computers used by home workers. Viruses, worms and spyware can easily use these devices to enter your business.

Block file types that often carry viruses

These include EXE, COM, PIF, SCR, VBS, SHS, CHM and BAT file types. It is unlikely that your organization will ever need to receive files of these types from the outside world.

Block files with more than one file-type extension

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 or ANNAKOURNIKOVA.JPG.VBS looks like a harmless text file or a graphic. Block any file with double extensions at the email gateway.

Ensure all programs are checked by the IT department

Ensure that all programs received from the outside world via email go directly to your IT department or, in the case of small businesses, your IT person, for checking and approval. They can confirm that it is virus-free, properly licensed, unlikely to conflict with existing software, and is suitable.

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/security/notifications. Consider adding a live virus information feed to your website or intranet to ensure your users know about the very latest computer viruses.

Use a firewall on computers connected to the internet

You should use a firewall to protect computers that are connected to the outside world. Laptops and home workers will also need firewall protection.

Stay up to date with software patches

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.msp. 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.

Back up your data regularly

Make regular backups of important work and data, and check that the backups were successful. You should also find a safe place to store your backups, perhaps even off-site in case of fire. If you are infected with a virus, you will be able to restore any lost programs and data.

Disable booting from floppy disks

Boot sector viruses are rarely seen now, but you may want to protect yourself from them. Change the bootup sequence on PCs so that they always boot from the hard disk first, rather than trying to boot from floppy disk (drive A:). Then, even if an infected floppy disk is left in the computer, it cannot be infected by a boot sector virus. Should you need to boot from a floppy disk, the setting can easily be switched back.

Introduce an anti-virus policy

Produce a policy for safe computing in the workplace and distribute it to all staff. Such a policy could include:

- Don't download executables and documents directly from the internet.
- Don't open unsolicited programs, documents or spreadsheets.
- Don't play computer games or use screensavers which did not come with the operating system.
- Submit email attachments to the IT department for checking.
- Save all Word documents as RTF (Rich Text Format) files, since DOC files can harbor macro viruses.
- Treat any unexpected email with suspicion.
- Forward virus warnings or hoaxes directly to IT (and no-one else) to confirm whether they are genuine or not.
- Inform IT immediately if you think your computer may have been infected with a virus.

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/security/hoaxes/

Don't forward chain letters

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

How to: avoid spam

Use email filtering software at your email gateway

You should run email filtering software at the email gateway, as this will protect your business from spam, as well as email-borne spyware, viruses and worms.

Never make a purchase from an 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 do not know the sender of an unsolicited email, delete it

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

Never respond to any spam messages or click on any links in the message

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.

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 a message 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.

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. Check or uncheck the box as appropriate.

How to: avoid being phished

Never respond to emails that request personal financial information

You should be suspicious of any email that asks for your password or account details or includes links for that purpose. Banks or e-commerce companies do not usually send such emails.

Look for signs that an email is “phishy”

Phishing mails usually use a generic greeting, such as “Dear valued customer”, because the email is spam and the phisher does not have your name. They may also make alarming claims, e.g. that your account details have been stolen or lost. The email often includes misspellings or substitute characters, e.g. “1nformati0n”, in an attempt to bypass anti-spam software.

Visit banks' websites by typing the address into the address bar

Don't follow links embedded in an unsolicited email. Phishers often use these to direct you to a bogus site. Instead, you should type the full address into the address bar in your browser.

Keep a regular check on your accounts

Regularly log into your online accounts and check your statements. If you see any suspicious transactions, report them to your bank or credit card provider.

Check the website you are visiting is secure

Check the web address in the address bar. If the website you are visiting is on a secure server, it should start with “https://” (“s” for secure) rather than the usual “http://”. Also look for a lock icon on the browser's status bar. This tells you that the website is using encryption, but doesn't necessarily mean that the website is legitimate.

Be cautious with emails and personal data

Look at your bank's advice on carrying out safe transactions. Don't let anyone know your PINs or passwords, do not write them down, and do not use the same password for all your online accounts. Don't open or reply to spam emails as this lets the sender know that your address is valid and can be used for future scams.

Keep your computer secure

Anti-spam software will prevent many phishing emails from reaching you. A firewall also helps to keep your personal information secure and block unauthorized communications. You should also run anti-virus software to detect and disable malicious programs, such as spyware or backdoor Trojans, which may be included in phishing emails. Keep your internet browser up to date with the latest security patches.

Always report suspicious activity

If you receive an email you suspect isn't genuine, forward it to the spoofed organization. (Many companies have a dedicated email address for reporting such abuse.)

How to: be safe on the internet

This section gives general advice on making safe use of email and the web.

You should also see our tips on [How to avoid being phished](#).

Don't click on pop-up messages

If you see unsolicited pop-ups, such as a message warning that a computer is infected and offering virus removal, don't follow links or click to accept software downloads. Doing so could result in you downloading malicious software.

Don't follow links in unexpected emails

Such links can take you to bogus websites, where any confidential information you enter, such as account details and passwords, can be stolen and misused. Always enter the website address you want to visit in the address bar in your browser.

Use different passwords for every site

You should use a different password for each site where you have a user account. If a password is compromised, only one account will be affected.

Configure your internet browser for security

You can disable Java or ActiveX applets, 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 settings you want.

Consider blocking access to certain websites or types of web content

In a company environment, you may want to prevent users from accessing sites that are inappropriate for workplace use, or that may pose a security threat (for example, by installing spyware on computers), or that may give offense. You can do this with web filtering software or a hardware "appliance".

Use reputation filtering

Reputation filtering software can check the sender addresses in email against a database that shows how often mail from that address is spam, or contains viruses, worms, etc. The software then assigns the email a "reputation" score that is used to decide whether to block the email or to slow down its delivery (giving priority to email with a better reputation).

Use firewalls

A network firewall is installed at your company boundary and admits only authorized types of traffic. A client firewall is installed on each computer on your network, and also allows only authorized traffic, thereby blocking hackers and internet worms. In addition, it prevents the computer from communicating with the internet via unauthorized programs.

Use routers

You can use a router to limit connection between the internet and specific computers. Many routers also incorporate a network firewall.

How to: choose passwords

Passwords are your protection against fraud and loss of confidential information, but few people choose passwords that are truly secure.

Make your password as long as possible

The longer it is, the harder it is to guess or to find by trying all possible combinations (a “brute-force attack”). Use eight characters or more.

Use different types of characters

Include numbers, punctuation marks, upper-case and lower-case letters.

Don't use words that are in dictionaries

Don't use words, names or place-names that are usually found in dictionaries. Hackers can use a “dictionary attack” (i.e. trying all the words in the dictionary automatically) to crack these passwords.

Don't use personal information

Others are likely to know information such as your birthday, the name of your partner or child, or your phone number, and they might guess that you have used them as a password.

Don't use your username

Don't use a password that is the same as your username or account number.

Use passwords that are difficult to identify as you type them in

Make sure that you don't use repeated characters or keys close together on the keyboard.

Consider using a passphrase

A passphrase is a string of words, rather than a single word. Unlikely combinations of words can be hard to guess.

Try to memorize your password

Memorize your password rather than writing it down. Use a string of characters that is meaningful to you, or use mnemonic devices to help you recall the password.

Don't store your passwords on your computer or online

Hackers may be able to access your computer and find the passwords.

If you write down your password, keep it in a secure place

Don't keep passwords attached to your computer or in any easily accessible place.

Use different passwords for each account

If a hacker breaks one of your passwords, at least only one account has been compromised.

Don't tell anyone else your password

If you receive a request to “confirm” your password, even if it appears to be from a trustworthy institution or someone within your organization, you should never disclose your password. (See **Phishing**).

Don't use your password on a public computer

Don't enter your password on a publicly available computer, e.g. in a hotel or internet café. Such computers may not be secure and may have keystroke loggers installed.

Change your passwords regularly

The shorter or simpler your password is, the more often you should replace it.

Virus timeline

When did viruses, Trojans and worms begin to pose a threat? Most histories of viruses start with the Brain virus, written in 1986. That was just the first virus for a Microsoft PC, though. Programs with all the characteristics of viruses date back much further. Here's a timeline showing key moments in virus history.

1949 Self-reproducing “cellular automata”

John von Neumann, the father of cybernetics, published a paper suggesting that a computer program could reproduce itself.

1959 Core Wars

H Douglas McIlroy, Victor Vysotsky, and Robert P Morris of Bell Labs developed a computer game called Core Wars, in which programs called organisms competed for computer processing time.

1960 “Rabbit” programs

Programmers began to write placeholders for mainframe computers. If no jobs were waiting, these programs added a copy of themselves to the end of the queue. They were nicknamed “rabbits” because they multiplied, using up system resources.

1978 The Vampire worm

John Shoch and Jon Hupp at Xerox PARC began experimenting with worms designed to perform helpful tasks. The **Vampire** worm was idle during the day, but at night it assigned tasks to under-used computers.

1975 Replicating code

A K Dewdney wrote **Pervade** as a sub-routine for a game run on computers using the UNIVAC 1100 system. When any user played the game, it silently copied the latest version of itself into every accessible directory, including shared directories, consequently spreading throughout the network.

1971 The first worm

Bob Thomas, a developer working on ARPANET, a precursor to the internet, wrote a program called **Creeper** that passed from computer to computer, displaying a message.

1981 Apple virus

Joe Dellinger, a student at Texas A&M University, modified the operating system on Apple II diskettes so that it would behave as a virus. As the virus had unintended side-effects, it was never released, but further versions were written and allowed to spread.

1982 Apple virus with side effects

Rich Skrenta, a 15-year-old, wrote **Elk Cloner** for the Apple II operating system. **Elk Cloner** ran whenever a computer was started from an infected floppy disk, and would infect any other floppy put into the disk drive. It displayed a message every 50 times the computer was started.

1985 Mail Trojan

The **EGABTR** Trojan horse was distributed via mailboxes, posing as a program designed to improve graphics display. However, once run, it deleted all files on the hard disk and displayed a message.

1986 The first virus for PCs

The first virus for IBM PCs, **Brain**, was allegedly written by two brothers in Pakistan, when they noticed that people were copying their software. The virus put a copy of itself and a copyright message on any floppy disk copies their customers made.

1987 The Christmas tree worm

This was an email Christmas card that included program code. If the user ran it, it drew a Christmas tree as promised, but also forwarded itself to everyone in the user's address book. The traffic paralyzed the IBM worldwide network.

1988 The Internet Worm

Robert Morris, a 23-year-old student, released a worm on the US DARPA internet. It spread to thousands of computers and, due to an error, kept re-infecting computers many times, causing them to crash.

1989 Trojan demands ransom

The **AIDS** Trojan horse came on a floppy disk that offered information about AIDS and HIV. The Trojan encrypted the computer's hard disk and demanded payment in exchange for the password.

1991 The first polymorphic virus

Tequila was the first widespread polymorphic virus. Polymorphic viruses make detection difficult for virus scanners by changing their appearance with each new infection.

1992 The Michelangelo panic

The **Michelangelo** virus was designed to erase computer hard disks each year on March 6 (Michelangelo's birthday). After two companies accidentally distributed infected disks and PCs, there was worldwide panic, but few computers were infected.

2000 Denial-of-service attacks

"Distributed denial-of-service" attacks by hackers put Yahoo, eBay, Amazon, and other high profile websites offline for several hours.

Love Bug became the most successful email virus yet.

2000 Palm virus

The first virus appeared for the Palm operating system, although no users were infected.

1999 Email viruses

Melissa, a virus that forwards itself by email, spread worldwide.

Bubbleboy, the first virus to infect a computer when email is viewed, appeared.

1998 The first virus to affect hardware

CIH or **Chernobyl** became the first virus to paralyze computer hardware. The virus attacked the BIOS, which is needed to boot up the computer.

1995 The first document virus

The first document or "macro" virus, **Concept**, appeared. It spread by exploiting the macros in Microsoft Word.

1994 The first email virus hoax

The first email hoax warned of a malicious virus that would erase an entire hard drive just by opening an email with the subject line "Good Times".

2001 Viruses spread via websites or network shares

Malicious programs began to exploit vulnerabilities in software, so that they could spread without user intervention. **Nimda** infected users who simply browsed a website. **Sircam** used its own email program to spread, and also spread via network shares.

2003 Zombie, Phishing

The **Sobig** worm gave control of the PC to hackers, so that it became a "zombie", which could be used to send spam.

The **Mimail** worm posed as an email from Paypal, asking users to confirm credit card information.

2004 IRC bots

Malicious IRC (Internet Relay Chat) bots were developed. Trojans could place the bot on a computer, where it would connect to an IRC channel without the user's knowledge and give control of the computer to hackers.

2005 Rootkits

Sony's DRM copy protection system, included on music CDs, installed a "rootkit" on users' PCs, hiding files so that they could not be duplicated. Hackers wrote Trojans to exploit this security weakness and install a hidden "back door".

2006 Share price scams

Spam mail hyping shares in small companies ("pump-and-dump" spam) became common.

2006 Ransomware

The **Zippo** and **Archiveus** Trojan horse programs, which encrypted users' files and demanded payment in exchange for the password, were early examples of ransomware.

Whether you're a network administrator, use a computer at work, or just browse the internet at home, this book is for you. We describe the security threats you're facing and explain practical measures you can take to protect your computer.

£5.00 / \$7.50 / €7.60

ISBN 0-9553212-0-4



9 780955 321207 >

SOPHOS
secured.