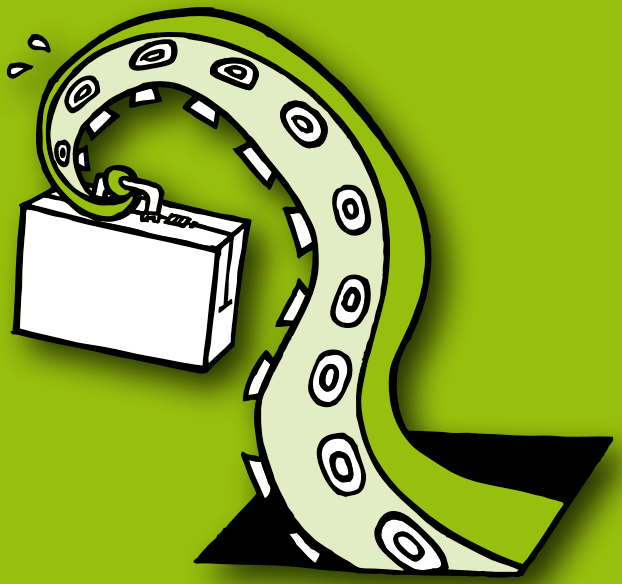
threatsaurus

the a-z of computer and data security threats



SOPHOS

the a-z

of computer and data security threats

Whether you're an IT professional, use a computer at work, or just browse the internet, this book is for you. We tell you the facts about the threats to your computers and to your data in simple, easy-to-understand language.

Sophos frees IT managers to focus on their businesses. The company provides endpoint, encryption, email, web, and NAC security solutions that are simple to deploy, manage and use. Over 100 million users trust Sophos as the best protection against today's complex threats and analysts endorse the company as a leader.

The company has more than two decades of experience and a global network of threat analysis centers that enable it to respond rapidly to emerging threats. As a result, Sophos achieves the highest levels of customer satisfaction in the industry. The company has headquarters in Boston, Mass., and Oxford, UK.

Contents

Introduction

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

Nearly 30 years ago, the first computer virus was written (*Elk Cloner*), apparently with the intention of displaying a short poem when a computer booted up for the 50th time. Since then, millions of viruses and other malware – email viruses, Trojans, internet worms, spyware, 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 early 1990s saw global panic about the Michelangelo virus. Again, in this decade, 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. Hollywood movies like “Independence Day” have reinforced this perception, with virus attacks signaled 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 is an identity thief – using 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 for malware to take over your computer, turning it into a remote-controlled "zombie," and use it without your knowledge to relay millions of profit-making spam messages or launch other malware attacks on unsuspecting computer users.

And as social networks like Facebook and Twitter have grown in popularity, hackers and cybercriminals are exploiting these systems to find new ways of infecting computer users and stealing identities.

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. Because of this, 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 because 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 however, is that whenever there is an opportunity for financial gain, hackers and criminals will attempt to access and misuse data.


Buy
me

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 an 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** p21)
- gathers data on your web browsing without your consent and sends it to others via the Internet (see **Spyware** p75)
- 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.

Anonymizing proxies

Anonymizing proxies allow the user to hide their web browsing activity. They are often used to bypass web security filters, for example to access blocked sites from a work computer.

Anonymizing proxies hold significant risks for organizations:

- **Security** – The anonymizing proxy bypasses web security and allows users to access infected web pages.
- **Liability** – Organizations can be legally liable if their computers are used to view pornography, hate material or to incite illegal behavior. There are also ramifications if users violate third-party licenses through illegal MP3, film and software downloads.
- **Productivity** – Anonymizing proxies can enable users to visit sites that, although safe, are often used for non-work purposes.

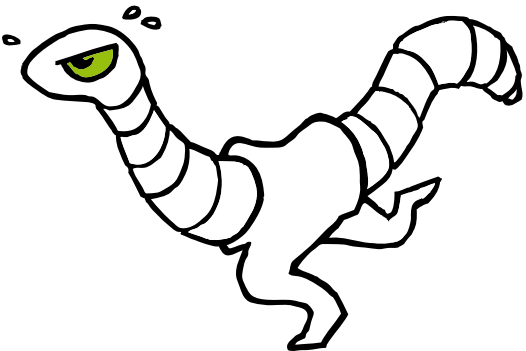
Autorun worms

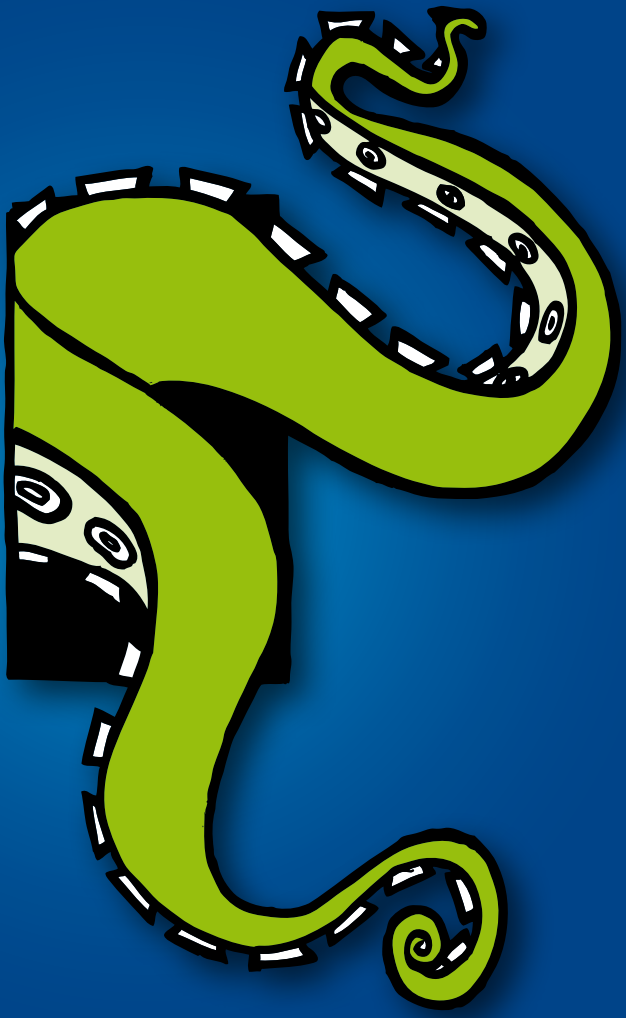
Autorun worms are malicious programs that take advantage of the Windows AutoRun feature. They execute automatically when the device on which they are stored is plugged into a computer.

Autorun worms are commonly distributed on USB drives.

Hairy-A is an example. It exploited the hype around the launch of the final Harry Potter novel. This worm, distributed on USB drives, was hidden in a file that posed as a copy of the novel and automatically infected computers as soon as the USB was plugged in.

AutoPlay is a similar technology to Autorun. It is initiated on removable media prompting users to choose to listen to music with the default media player, or to open the disk in Windows Explorer. Attackers have similarly exploited **AutoPlay**, most famously via the Conficker worm.





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 to fool users into running it. Alternatively – as is now increasingly common – users may allow Trojans onto their computer by following a link in spam mail or visiting a malicious web page.

Once the Trojan runs, 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 email.

Well-known backdoor Trojans include **Zapchast**, **Subseven**, **BackOrifice** and, more recently, **PcClient**.

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.

Blended threats

Blended threats use a combination of different malware techniques in an attack.

Virus and spyware writers, spammers and phishers often collaborate to create blended threats. These threats are increasingly surreptitious and low-profile, mutating in hours or even minutes in order to evade detection. They are also often financially motivated.

An example is the Storm worm (also known as Dorf and Dref). It started with a vast number of spammed-out malicious emails. Clicking on a link in the email took users to a webpage containing a malicious script that downloaded a Trojan, which took control of the computer. The computer could then be used to spam out more malware and junk mail, or to launch a distributed denial-of-service attack.

An integrated security approach that protects against spam, viruses and other malware is important to defend against blended threats. Because of their ability to change rapidly, it is also important to implement proactive detection and protection that identifies and stops threats before they launch.

See **Trojan Horse** p77, **Denial-of-service attack** p37, **Spam** p71 and **Zombie** p81.

Boot sector malware

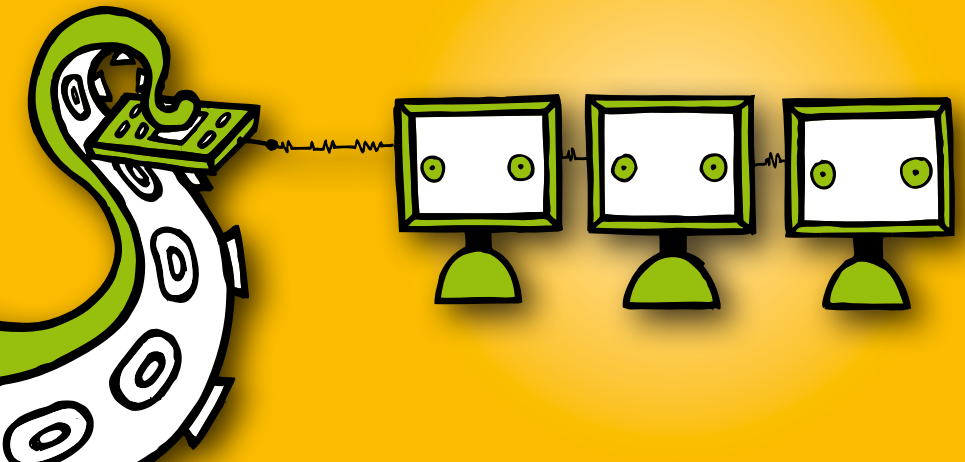
Boot sector malware spreads by modifying the program that enables your computer to start up.

When you turn 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.

Boot sector malware replaces the original boot sector with its own, modified version (and usually hides the original somewhere else on the hard disk). The next time you start up, the infected boot sector is used and the malware 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 malware is rare today, although more recent examples include **Mebroot**, also known as **Sinowal**, a password-stealing Trojan for the Windows platform.



Botnet

A botnet is a collection of infected computers that are remotely controlled by a hacker.

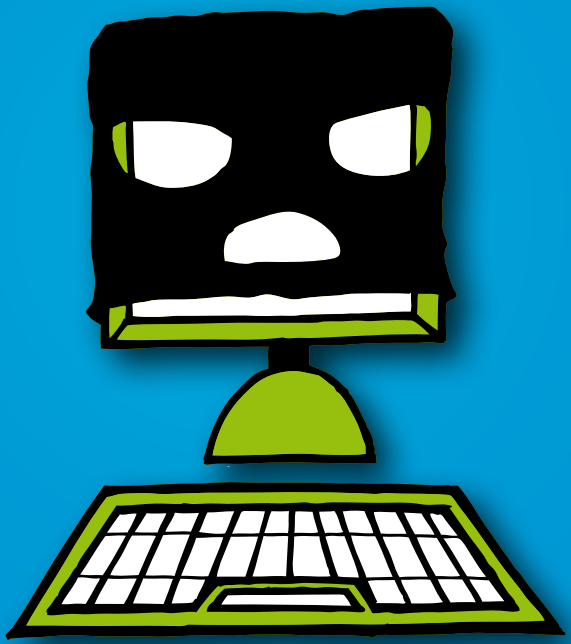
Once a computer is infected with a bot, the hacker can control the computer remotely via the internet. From then on, the computer is a “zombie,” doing the bidding of the hacker, although the user is completely unaware. Collectively, such computers are called a botnet.

The hacker can share or sell access to control the botnet, allowing others to use it for malicious purposes.

For example, a spammer can use a botnet to send out spam email. Up to 99% of all spam is now distributed in this way. This enables the spammers to avoid detection and to get around any blacklisting applied to their own servers. It can also reduce their costs because the computer’s owner is paying for the internet access.

Hackers can also use zombies to launch a distributed denial-of-service attack, also known as a DDoS. 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 **Zombies** p81, **Denial-of-service attack** p37, **Spam** p71, **Backdoor Trojans** p13, **Command and control center** p29.



Browser hijackers

Browser hijackers change the default home and search pages in your internet browser without your permission.

You may find that you cannot change your browser's homepage once it has been hijacked. 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.

Browser hijacking is used to boost advertising revenue and inflate a site's page ranking in search results.

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.

Brute force attack

A brute force attack is one in which hackers try a large number of possible key or password combinations to gain unauthorized access to a system or file.

Brute force attacks are often used to defeat a cryptographic scheme, such as those secured by passwords. Hackers use computer programs to try a very large number of passwords to decrypt the message or access the system.

To prevent brute force attacks, it is important to make your passwords as secure as possible.

See **How to choose secure passwords** p107.

Buffer overflow

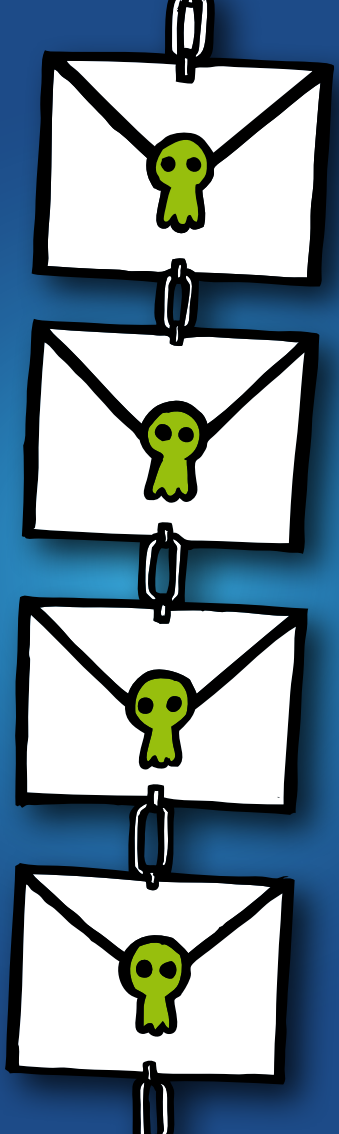
A buffer overflow occurs when a program stores excess data by overwriting other parts of the computer's memory, causing errors or crashes.

Buffer overflow attacks take advantage of this weakness by sending more data to a program than it expects. The program may then read in more data than it has reserved space for and overwrite parts of the memory that the operating system is using for other purposes.

Contrary to popular belief, buffer overflows don't just happen in Windows services or core programs. They can occur in any application.

Buffer overflow protection (BOP) looks for code that uses buffer overflow techniques to target security vulnerabilities.

See **Exploits** p45, **Drive-by download** p41.



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:

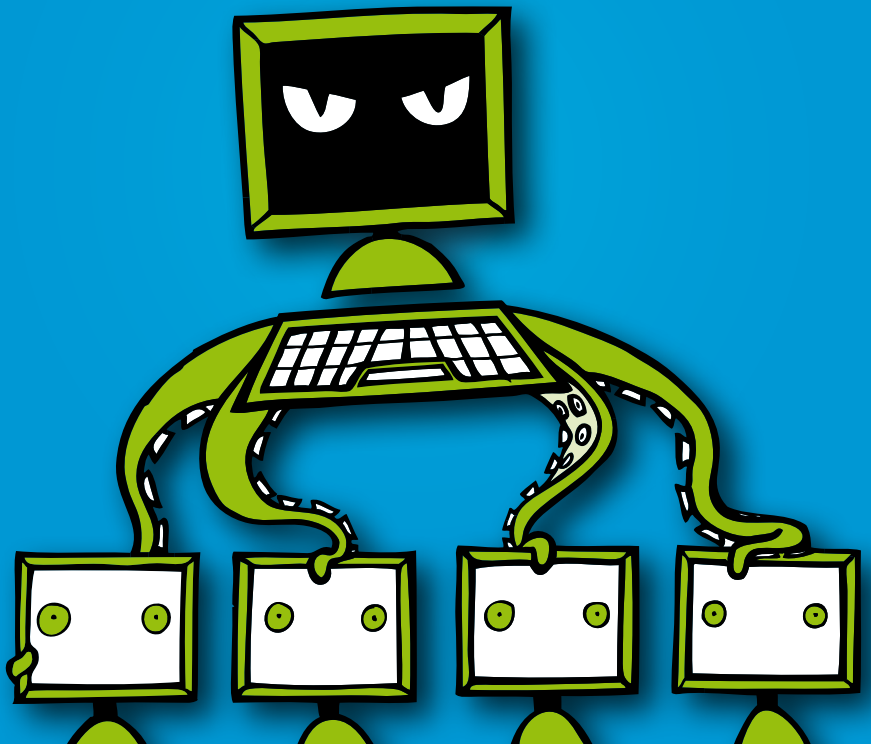
- Hoaxes about terrorist attacks, premium-rate phone line scams, thefts from ATMs and so forth
- False claims that companies are offering free flights, free mobile phones or cash rewards if you forward the email
- Messages that purport to be from agencies like the CIA and FBI, warning about dangerous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

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 they are deluged with unsolicited mail.

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

See **Hoaxes** p49.



Command and control center

A command and control center (C&C) is a computer that controls a botnet (i.e., a network of compromised or zombie computers). Some botnets use distributed command and control systems, making them more resilient.

From the command and control center, hackers can instruct multiple computers to perform their desired activities.

Command and control centers are often used to launch distributed denial-of-service attacks because they can instruct a vast number of computers to perform the same action at the same time.

See **Botnet** p19, **Zombies** p81, **Denial-of-service attack** p37.

Cookies

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

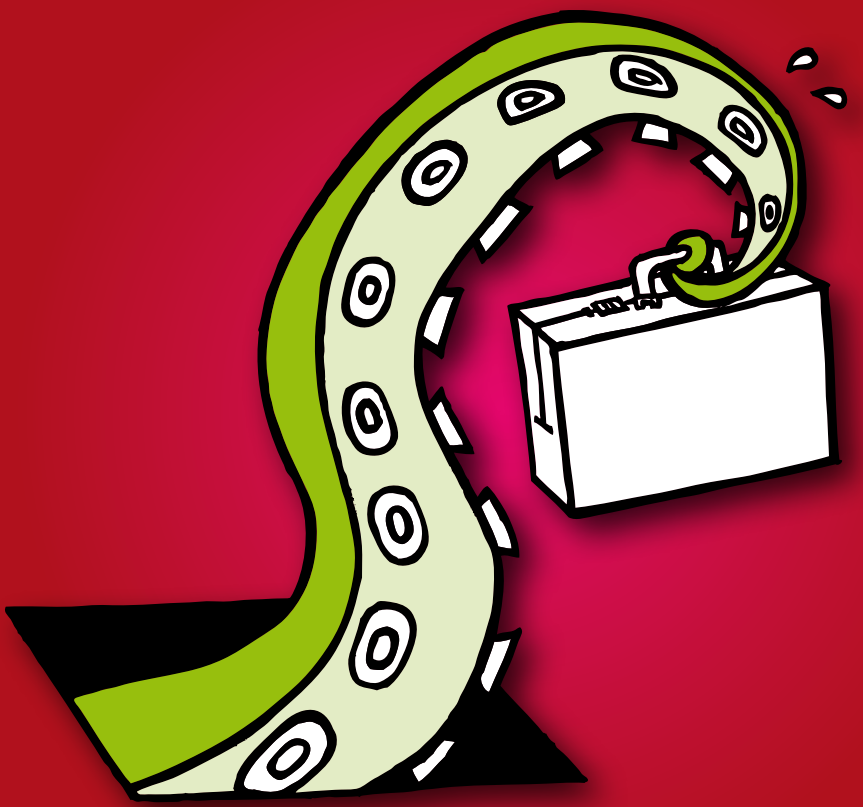
When you visit a website, it can place a file called a cookie on your computer. This enables the website to remember your details and track your visits. Cookies can be a threat to confidentiality, but not to your data.

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 you don't have to re-enter it the next time. Cookies also have benefits for webmasters, as they show which webpages 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.



Data leakage

Data leakage is the unauthorized movement of information, usually outside an organization. It can be deliberate (data theft) or accidental (data loss).

Data leakage prevention is a top concern for organizations, with scandals frequently dominating the headlines. Many corporate and government organizations have failed to protect their confidential information, including the identities of their workforce, their customers and the general public.

Users routinely use and share data without giving sufficient thought to confidentiality and regulatory requirements.

A variety of techniques can be used to prevent data leakage. These include anti-virus software, encryption, firewalls, access control, written policies and improved employee training.

See **Data loss** p34, **Data theft** p35, **How to secure your data** p100.

Data loss

Data loss is the result of the accidental misplacement of data, rather than its deliberate theft.

Data loss frequently occurs through the loss of a device containing data, such as a laptop, CD-ROM, mobile phone or USB stick. When these are lost, the data is at risk of falling into the wrong hands unless an effective data security technique is used.

See **Data leakage** p33, **Data theft** p35, **How to secure your data** p100.

Data theft

Data theft is the deliberate theft of information, rather than its accidental loss.

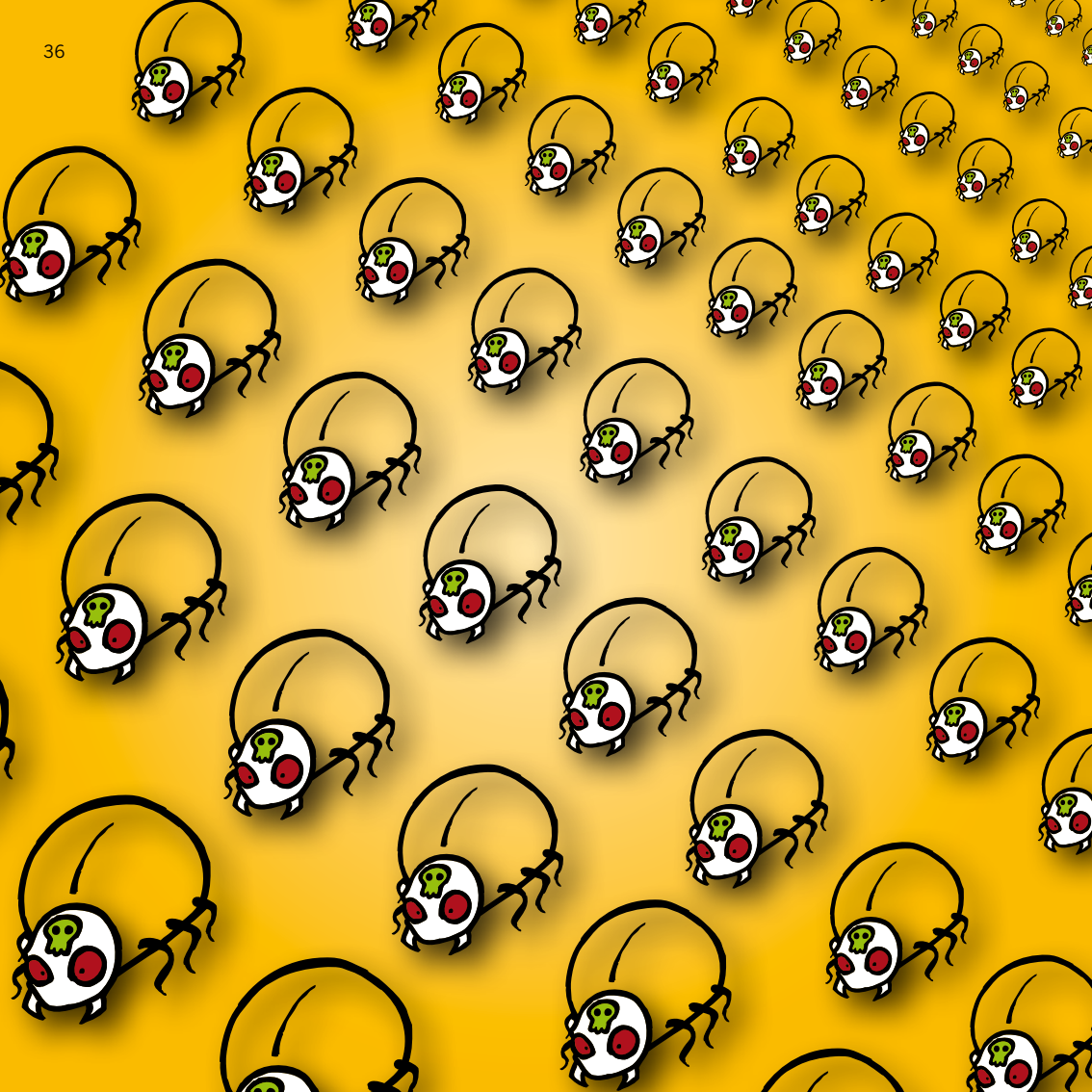
Data theft can take place both inside an organization (e.g., by a disgruntled employee), or by criminals outside the organization.

In one example, hackers broke into a Virginia government website, stealing the details of almost 8.3 million patients, and threatened to auction them to the highest bidder. In another, a former Goldman Sachs employee uploaded the company's secret source code to an FTP server in Germany.

Criminals often use malware to access a computer and steal data. A common approach is to use a Trojan to install keylogging software that tracks everything the user types, including usernames and passwords, before using this information to access the user's bank account.

Data theft also occurs when devices containing data, such as laptops or USB drives, are stolen.

See **Data leakage** p33**, Data loss** p34**, How to secure your data** p100.



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 service 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. There are a variety of methods for DoS attacks, but the simplest and most common is to have a **botnet** flood a web server with requests. This is called a **distributed denial-of-service attack (DDoS)**.

See **Backdoor Trojans** p13, **Zombies** p81.

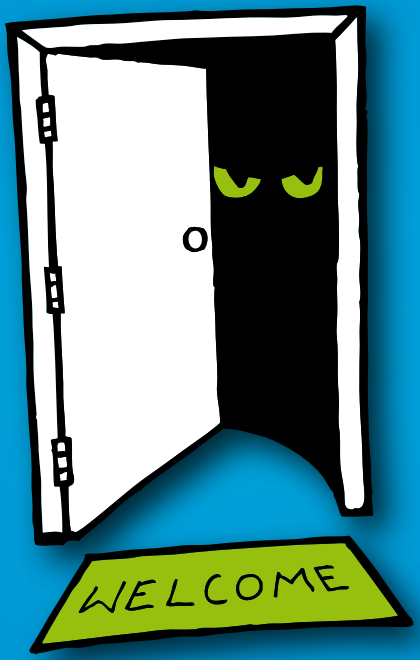
Document malware

Document malware takes advantage of embedded script or macro content in document files.

Macro viruses infecting Microsoft Office documents first appeared in the mid-1990s and rapidly became the most serious threat of that time. More recently there has been a resurgence in document malware, with cybercriminals turning their attention to other widespread and trusted document formats such as PDFs, and even AutoCAD.

By embedding malicious content within documents, hackers can exploit vulnerabilities in the host applications used for opening the documents.

See **Exploits** p45.


WELCOME

Drive-by download

A drive-by download is the infection of a computer with malware when a user visits a malicious website.

Drive-by downloads occur without the knowledge of the user. Simply visiting an infected website may be sufficient for the malware to be downloaded and run on a computer. Vulnerabilities in a user's browser (and browser plug-ins) are exploited in order to infect them.

Hackers continually attack legitimate websites in order to compromise them, injecting malicious code into their pages. Then, when a user browses that legitimate (but compromised) site, the injected code is loaded by his/her browser, which initiates the drive-by attack. In this manner, the hacker can infect users without having to trick them into browsing a specific site.

To defend against drive-by downloads, you should have effective endpoint security software coupled with web security filtering.

See **Exploits** p45.

Email malware

Email malware refers to malware that is distributed via email.

Historically, some of the most prolific virus families (e.g., **Netsky** or **SoBig**) distributed themselves as file attachments in email. These families relied on users double-clicking an attachment, which would run the malicious code, infect their machine and send itself to more email addresses from that computer.

Nowadays, hackers have changed their focus and predominantly use the web for malware distribution. Email messages are still used, but mostly as a way of distributing links to malicious sites, not for carrying malicious file attachments.

A lot of the spam sent from a botnet is for the purpose of increasing the size of that botnet.

Effective anti-spam security in conjunction with endpoint security software should be used to defend against email malware. In addition, user education can raise awareness of email scams and seemingly innocent attachments from strangers.

See **Exploits** p45, **Botnet** p19.

Exploits

An exploit takes advantage of a vulnerability in order to access or infect a computer.

Usually an exploit takes advantage of a specific vulnerability in an application and so becomes obsolete when that vulnerability is patched. **Zero-day exploits** are those that are used or shared by hackers before the software vendor knows about the vulnerability (and so before there is any patch available).

To secure against exploits, you should ensure your anti-virus or endpoint security software is active and your computers are fully patched. Buffer overflow protection (BOP) technology can provide effective protection against many exploits. Client firewalls are a first defense against many exploits and should be deployed throughout an organization, not simply on mobile assets.

See **Vulnerabilities** p80, **Drive-by download** p41, **Buffer overflow** p25.

Fake anti-virus malware

Fake anti-virus malware reports non-existent threats in order to scare the user into paying for unnecessary product registration and cleanup.

Fake anti-virus malware is commonly known as scareware. Typically it is installed through malicious websites and takes the form of fake online scans. Cybercriminals attract traffic to these sites by sending out spam messages containing links or by compromising legitimate websites. Frequently they also attempt to poison the results of popular search engines so that users access the malicious distribution sites when conducting a search.

Fake anti-virus malware is financially motivated and is a big earner for cybercriminals. The large profits enable significant resources to be invested into its creation and distribution. Hacking gangs are proficient at rapidly producing professional-looking bogus websites that pose as legitimate security vendors.

Using up-to-date, legitimate anti-virus or endpoint security software will protect you against fake anti-virus software.

Hoaxes

Hoaxes are reports of non-existent viruses or threats.

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 piece of malware
- 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 the new malware 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 malware effects (e.g., **Sector Zero** claims that the malware can “destroy sector zero of the hard drive”)
- Urge you to forward the warning

Many users forwarding such hoax emails can result in a deluge of email, which may overload mail servers. Hoax messages may also distract from efforts to deal with real malware threats.

Since hoaxes aren’t malware, your anti-virus and endpoint security software can’t detect or disable them.

Honeypot

A honeypot is a form of trap that is used to detect hacking attacks or collect malware samples.

There are many different types of honeypots. Some consist of machines connected to the network that are used to capture network worms. Others provide fake network services (e.g., a web server) in order to log incoming attacks.

Honeypots are frequently used by security specialists in order to gather information about current threats and attacks.

Internet worms

Worms are viruses that create copies of themselves across the internet.

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.

The Conficker worm is an example of an internet worm that exploits a system vulnerability in order to infect machines over the network. Such worms are capable of spreading very rapidly, infecting large numbers of machines.

Some 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 **Zombies** p81).

Operating system vendors regularly issue patches to fix security loopholes in their software. You should update your computer regularly by using Windows Update or selecting the Apple logo and choosing Software Updates.

In-the-cloud detection

In-the-cloud detection uses real-time online checking of data in order to detect threats.

The goal of in-the-cloud detection is to reduce the time taken for a security product to use a new malware signature. By querying data published online (i.e., “in the cloud”), security products avoid having to send out signatures to computers.

In-the-cloud detection offers a very rapid response to new threats as they are discovered, but it has the drawback that it requires an internet connection in order to do the checking.

Keylogging

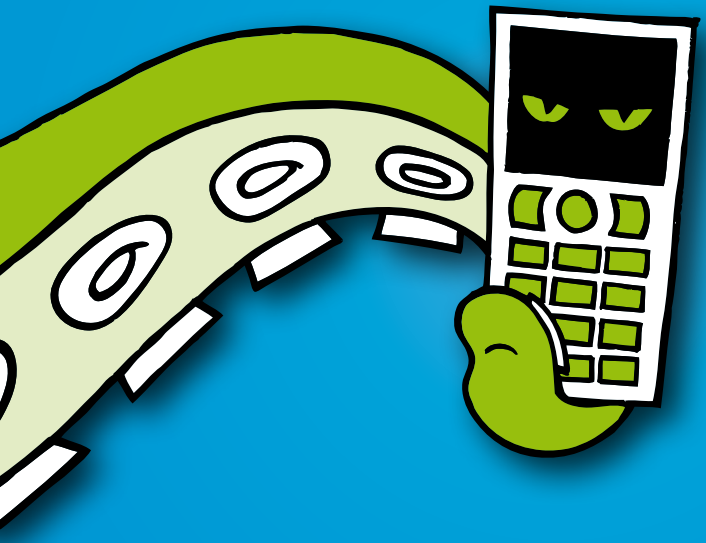
Keylogging is when keystrokes are surreptitiously recorded by an unauthorized third party.

This is a common payload in malware because it is an effective way to steal usernames, passwords, credit card details and other sensitive data.

Malware

Malware is a general term for malicious software including viruses, worms, Trojan horses and spyware. Many people use the terms malware and viruses interchangeably.

Anti-virus software usually detects a wider range of threats than just viruses.



Mobile phone malware

Mobile phone malware is malware intended to run on mobile devices, such as smartphones or PDAs.

The first mobile phone worm was written in 2004. 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 on the phone thereafter. **Cabir-A** searches for other mobile phones nearby using Bluetooth technology and sends itself to the first one it finds.

Since then, a handful of malware on mobile devices has emerged. In 2009, Research In Motion (RIM) learned of a BlackBerry PDF vulnerability that could be exploited by hackers. If a BlackBerry user tried to open a maliciously crafted PDF file, malicious code could be executed on a computer hosting the BlackBerry Attachment Service. To date, we have only seen a small number of threats impacting mobile devices. This is most likely due to a heterogeneous market, with many operating systems still competing to be the market leader.

Non-compliance

Non-compliance is the failure to comply with local, federal or industry regulations regarding data privacy and security.

Non-compliance can be costly. Organizations may incur fines, suffer a loss of reputation or even face legal action.

A 2008 study by the Ponemon Institute shows that the average cost of a data breach is $6.3 million, with the average cost per customer record increasing by 43% between 2005 and 2007.

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 and then became quite rare. However, they are now becoming more common again with recent examples including **Sality**, **Virut** and **Vetor**.

Patches

Patches are software add-ons designed to fix software bugs, including security, in operating systems or applications.

Patching against new security vulnerabilities is critical to protect against malware. Many high-profile threats take advantage of security vulnerabilities, such as Conficker. If your patches are not applied or not up to date, you risk leaving your computer open to hackers.

Many software suppliers routinely release new patches, with Microsoft issuing fixes on the second Tuesday of each month ("Patch Tuesday"), and Adobe issuing quarterly updates to Adobe Reader and Acrobat on the second Tuesday after a quarter begins.

To stay abreast of the latest vulnerabilities and patches, subscribe to vulnerability mailing lists. Most reputable vendors offer such a service. For example, Microsoft security information is available at **www.microsoft.com/technet/security/bulletin/notify.mspx**.

Microsoft Windows home users can visit **http://update.microsoft.com** to check their computers for available updates. Apple OS X users can click the Apple logo in the upper-left corner of their desktop and select Software Updates.

Organizations should ensure that all computers connecting to their network abide by a defined security policy that includes having the latest security patches in place.

See **Exploits** p45, **Vulnerabilities** p80.

Phishing

Phishing refers to the process of tricking recipients into sharing sensitive information with an unknown third party.

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.

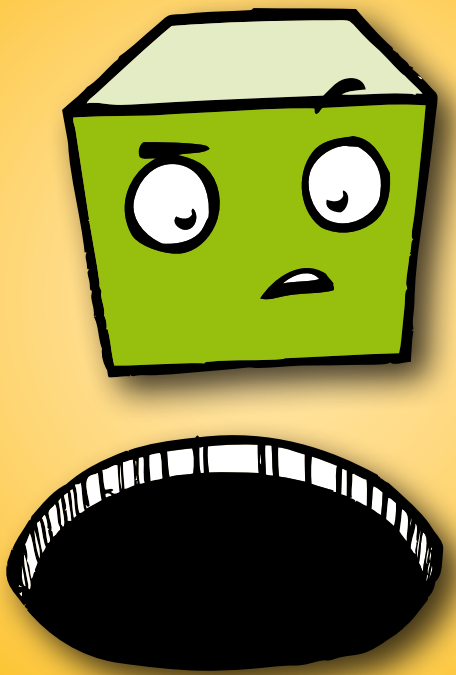
Sometimes the link displays the genuine website but superimposes a bogus pop-up window. You can see the address of the real website in the background, but the details you enter in the pop-up window can be stolen.

Phishing originated 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 hacked into the telephone network.

To better protect against phishing attacks, it is good practice not to click on links in email messages. Instead, you should enter the website address in the address field and then navigate to the correct page, or use a bookmark or a Favorite link.

Phishing attacks via email are beginning to include an offline aspect to convince users who are well trained to still leak information; we have seen phishing schemes use phone numbers and fax numbers in addition to websites.

Anti-spam software can block many phishing-related emails and web security software can block access to phishing-related websites.

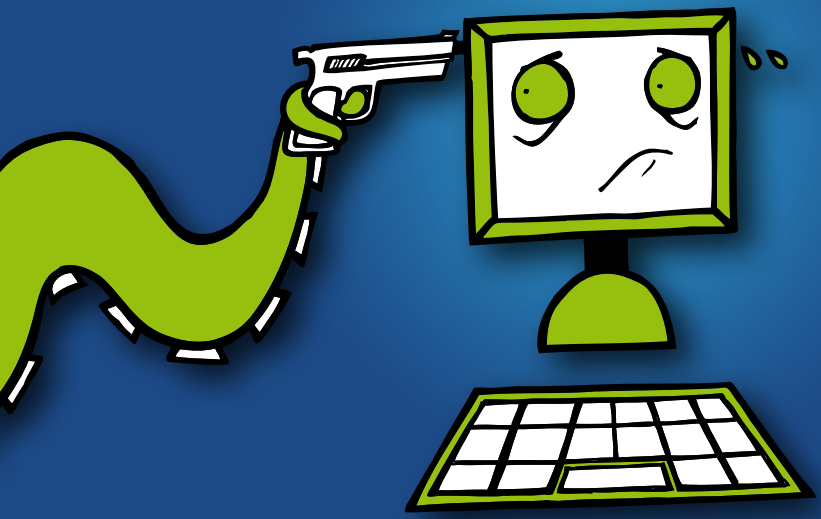


Potentially unwanted applications (PUAs)

Potentially unwanted applications are programs that are not malicious but may be unsuitable for use in a business environment.

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 and endpoint security 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.



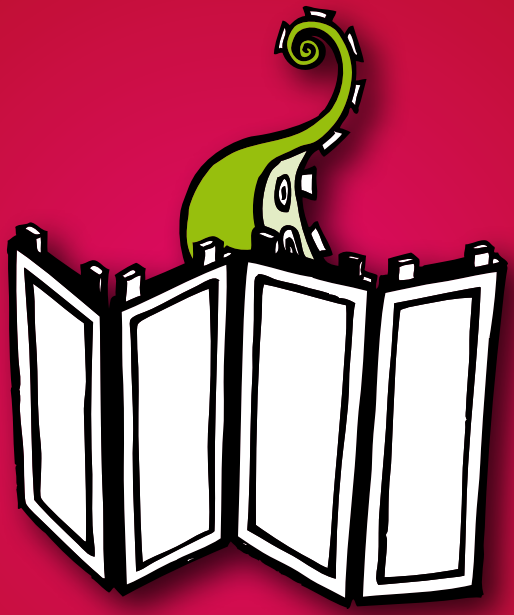
Ransomware

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

In the past, malicious software typically corrupted or deleted data, but now it can hold your data hostage instead. For example, the **Archiveus** Trojan copies the contents of the My Documents folder 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 malware 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 computer misuse or data theft.

A significant proportion of current malware installs rootkits upon infection to hide its activity.

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 email) without the user's knowledge.

Endpoint security products now often detect and remove rootkits as part of their standard anti-malware routines, although some rootkits require a standalone removal tool to effectively remove them.

Social engineering

Social engineering refers to the tricks attackers use to fool victims into performing an action. Typically, these actions are opening a malicious webpage or running an unwanted file attachment.

Many social engineering efforts are focused on tricking users into disclosing usernames or passwords, enabling attackers to send messages as an internal user to further their data acquisition attempts.

In March 2009, hackers distributed personalized emails posing as breaking news from a Reuters-related website of a bomb blast in the recipients' city. Clicking on the link in the email took users to a webpage that installed malicious code and video footage, which then downloaded the **Waled** malware.

Social networking

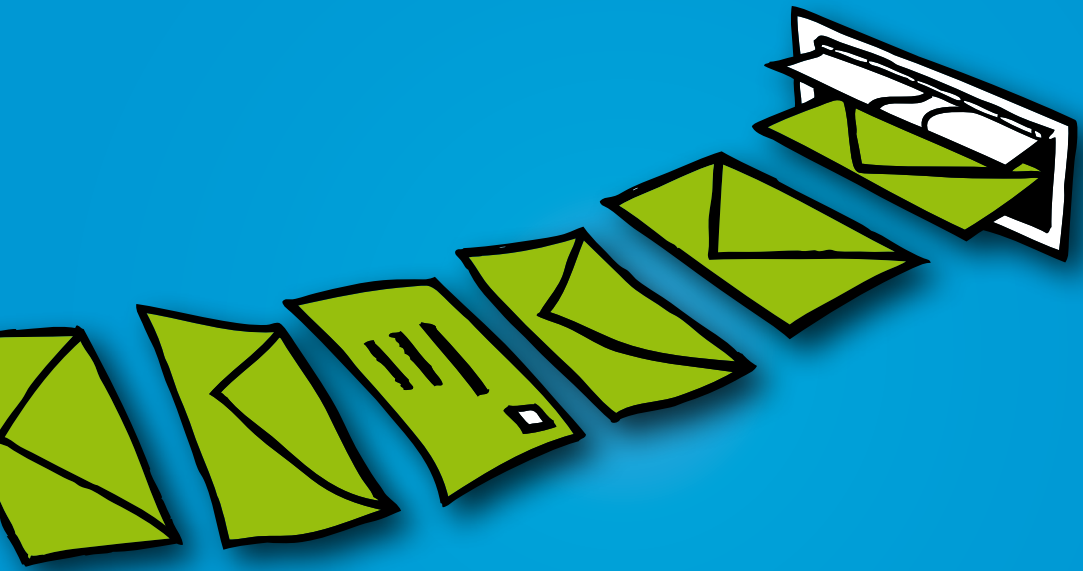
Social networking websites allow you to communicate and share information. But they can also be used to spread malware and to steal personal information.

Such sites sometimes have lax security, which enables criminals to access personal information that can be used to hack into computers, bank accounts and other secure sites.

These sites can also be used for phishing exploits. For example, in 2009 Twitter users received messages from their online followers encouraging them to visit a website that attempted to steal their username and password. The same year, hackers accessed a British politician's Facebook account and used it to send messages to contacts, directing them to a malicious webpage.

To prevent social networking threats, you should run web security solutions that check every link and webpage as it is clicked to see if it contains malware or suspicious activity. You should also ensure that your anti-virus or endpoint security is active.

See **How to be safe on the internet** p105.



Spam

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

Spammers often disguise their email in an attempt to evade anti-spam software.

More than 99% of all spam comes from compromised computers, infected machines that are part of a botnet. Spam is often profitable: Spammers can send millions of emails in a single campaign at a negligible cost. If even one recipient out of 10,000 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).
- Spam is frequently used to distribute malware (see Email malware).

Spammers are now also exploiting the popularity of instant messaging and social networking sites such as Facebook and Twitter to avoid spam filters and to trick users into revealing sensitive and financial information.

Spear phishing

Spear phishing is targeted phishing, the use of spoof emails to persuade people within a company to reveal sensitive information or credentials.

Unlike **phishing**, which involves mass-emailing, spear phishing is small-scale and well-targeted. The spear phisher emails users in a single business. The emails may appear to come from another staff member 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.

Spoofing

Email spoofing is when the sender address of an email is forged for the purposes of social engineering.

Spoofing can be put to a number of malicious uses.

Phishers (criminals who trick users into revealing confidential information) use spoofed 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 spoofed addresses to cover their tracks and avoid detection.

Spammers can use a spoofed 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.

See **Email malware** p43.

Spyware

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

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 it says you need, or software may be downloaded automatically without your knowledge.

When spyware runs on the computer, it may track your activity (e.g., visits to websites) and report it to unauthorized third parties, such as advertisers. Spyware consumes memory and processing capacity, which may slow or crash the computer.

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

Suspicious files and behavior

When a file is scanned, it is labeled as clean or malicious. If a file has a number of questionable characteristics, it is labeled as suspicious.

Suspicious behavior refers to files exhibiting questionable behavior, such as copying themselves to a system folder, when they are run on a computer.

Runtime protection helps protect against suspicious files by analyzing the behavior of all the programs running on your computer and blocking any activity that looks as if it could be malicious.

See **Buffer overflow** p25.

Trojan horses (aka Trojans)

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

Trojan horse is an umbrella term under which many types of malware sits: **bots**, **backdoor Trojans** and **downloader Trojans**.

A significant percentage of today's malware is Trojans.

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. Trojans are often distributed with pirated software applications and keygens that create illegal license codes for downloadable software.

See **Backdoor Trojans** p13.

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.

Viruses can attach themselves to other programs or hide in code that is run automatically when you open certain types of files. Sometimes they can exploit security flaws in your computer's operating system to run and spread 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.

See **Parasitic viruses** p57, **Email malware** p43, **Internet worms** p51, **Malware** p53.

Vulnerabilities

Vulnerabilities are bugs in software programs that hackers exploit to infect computers.

Security vulnerabilities leave users susceptible to attacks and can be present in any software product. Responsible software vendors, when aware of the problem, create and issue patches, which address the problem.

There are companies that pay researchers or ethical hackers for new vulnerabilities. There are also hackers that sell new vulnerabilities on the black market. These zero-day attacks refer to vulnerabilities being exploited before a patch is available.

To avoid vulnerabilities, your operating system and any installed applications need to be running the latest available patches.

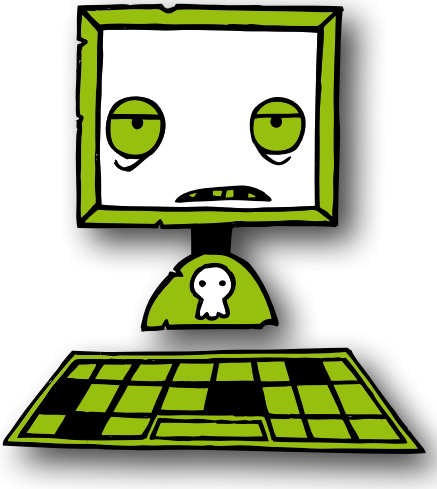
See **Exploits** p45, **Patches** p59.

Zombies

A zombie is an infected computer that is remotely controlled by a hacker. It is often part of a botnet, which is a network of many zombie, or bot, computers.

Once a hacker can control the computer remotely via the internet, the computer is a zombie.

See **Botnet** p19.



Security software

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 his or her words (e.g., "hardc*re p0rn").
- Look for unnecessary HTML code (the code used for writing webpages) 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.

Anti-virus software

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

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 considered undesirable, the scanner warns that it may be a virus.

Detection of known viruses depends on frequent updates about the latest virus identities.

There are on-access and on-demand scanners, and 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.

Appliances

Appliances are hardware and software security elements that are combined in one solution. This lets you plug them in rather than installing the software separately.

The most common types of appliances are **Email appliances** and **Web appliances**. They sit at the gateway between an organization's IT systems and the internet, and filter traffic to block malware, spam and data loss.

Email appliances block spam, phishing, viruses, spyware and other malware, and—depending on the solution—also employ content filtering and encryption to prevent the loss of confidential or sensitive information via email.

Web appliances block malware, spyware, phishing, anonymizing proxies and other unwanted applications at the web gateway. They may also offer tools to enforce internet use policies.

Application control

Application control enables you to control the use of applications that may be inappropriate for use on business computers or networks.

The main goal is to control those applications that have the potential to spread malware and can adversely impact network and user productivity. This includes many consumer-based applications such as peer-to-peer file sharing software, games or media players.

Application control can be used to enforce the use of chosen business applications. For example, a policy could be set to only allow the use of Internet Explorer and block all other internet browsers. Categories of applications that businesses may wish to control include Voice Over Internet Protocol (VoIP), remote management tools and instant messaging clients.

Device control

Device control helps you control the use of removable storage, optical media drives and wireless networking protocols.

Device control is a central element of data leakage prevention strategies, and also helps prevent malware that spreads through USB drives.

Many organizations use device control to enforce policies relating to the use of removable storage devices. Depending on the solution used, device control can enable organizations to decide which devices can connect to the computers through a central policy.

Encryption software

Encryption solutions secure your data by encrypting your desktops, laptops, removable media, CDs, email, files and other devices. Information can only be accessed by entering an encryption key or password.

Some encryption solutions can be configured so that data is automatically decrypted for authorized users so they do not need to enter an encryption key or password to access the information.

Depending on the product, encryption solutions often include key management (facilitating the storage, exchange and recovery of encryption keys), encryption policy enforcement, and centralized management and reporting features.

Encryption solutions enable you to protect your confidential information and comply with regulatory mandates for data security.

Endpoint security software

Endpoint security software protects computers or devices against a wide range of security, productivity and compliance threats, and enables you to manage centrally the security of multiple endpoints.

Endpoint security products bring together individual point products required to protect against modern threats in one solution. They often integrate the protection for multiple features into one agent or central console, facilitating management and reporting. They can include:

- Anti-virus software
- Firewalls
- Device control
- Network access control
- Application control
- Runtime protection
- Encryption technology
- Data leakage prevention

Firewall

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

As its 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. This is usually located 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.

Network access control (NAC)

A network access control solution protects your network and the information on it from the threats posed by users or devices accessing your network.

There are three main aspects to network access control:

- **Authentication** of users and devices – to check that they are who they say they are
- **Assessment** of computers attempting to access the network – to make sure they are virus-free and meet your security criteria
- **Enforcement** of policy based on the role of the user – so each person can access information appropriate to his or her role, while preventing inappropriate access to other information

Runtime protection

Runtime protection protects against attempts to access vulnerable parts of your computer.

Runtime protection 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.

Runtime protection solutions include host intrusion prevention systems (HIPS) and buffer overflow prevention systems (BOPS), which guard against unknown threats by analyzing behavior before code executes.

Safety tips

How to:
avoid viruses, Trojans, worms and spyware

Use anti-virus or endpoint security software

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

To protect your business from the threats of email-borne viruses, spam and spyware, run email filtering software at your email gateway as well.

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 malware

Block executable file types; it is unlikely that your organization will ever need to receive these types of files from the outside world.

Block files with more than one file-type extension

Some threats 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.

Subscribe to an email alert service

An alert service can warn you about new malware and offer malware identities that will enable your endpoint security software to detect them. Sophos has a free alert service. For details, see www.sophos.com/security/notifications. Consider adding a live malware information feed to your website or intranet to ensure your users know about the very latest computer threats.

Use a firewall on all computers

You should use a firewall to protect computers that are connected to a network. Many worms can be accidentally introduced even into closed network environments by USB sticks, CDs and mobile devices. Laptops and home workers will also need firewall protection.

Stay up to date with software patches

Watch for security news and make sure you have up-to-date patches for both your operating system and your applications. Such patches often close loopholes that can make you vulnerable to malware threats. IT managers should subscribe to software vendors' mailing lists such as that at www.microsoft.com/technet/security/bulletin/notify.mspx. Home users who have Windows computers can visit http://windowsupdate.microsoft.com, where they can scan their 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 your computer is infected with malware, you will be able to restore any lost programs and data. Any sensitive backup information should be encrypted and physically secured.

Introduce a computer security 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 that did not come with the operating system.
- Submit email attachments to the IT department for review.
- 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.
- Disconnect from the network and inform IT immediately if you think your computer may have been infected with malware.

Implement device control

Prevent unauthorized devices from connecting to your computers. Unauthorized devices such as USB sticks, music players and mobile phones can harbor malware that will infect a computer when plugged in.

Disable Autorun functionality

Autorun functionality is often used by malware to copy itself from devices such as USB drives to host computers and even shared network drives.

Microsoft and other operating system vendors offer instructions on how to disable autorun functionality (see http://support.microsoft.com/kb/967715).

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 that comes from any other source should be ignored."

Keep informed about hoaxes

Keep informed about hoaxes by visiting the Hoaxes pages on our website at **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 distribute useful information.

How to:
secure your data

Encrypt your computers, emails and other devices

By encrypting your data, you can ensure that only authorized users with the appropriate encryption key or password can access the information. With encryption you can ensure that your data remains secure at all times, even if the laptop, CD or other device on which it is stored is lost or stolen, or if the email in which it is contained is intercepted.

Use device and application control

Prevent users from accessing peer-to-peer file sharing and USB drives, both common routes by which data is lost.

Only allow compliant computers to access your network

Only allow computers that comply with your security policy to access your network. This could include requirements for encryption, or device or application control technologies.

Implement outbound content controls

Identify the sensitive data you want to control (e.g., any files containing the term “confidential” or credit card details) and then decide how these files can be used. For example, you may wish to present the user with a warning about potential data loss or prevent distribution of the data by email, blogs or forums.

Many endpoint security solutions and email and web appliances offer content filtering as part of their solution.

How to:
avoid spam

Use email filtering software at your email gateway

You should run email filtering software at the email gateway because 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 and consequently encourage 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 ecommerce 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 in to your online accounts and check your statements. If you see any suspicious transactions, report them to your bank or credit card provider.

Ensure that 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” stands for secure) rather than the usual “http://”. Also look for a small padlock icon on the browser’s status bar. These signs tell you that the website is using encryption.

However, even if a site is secure there is no guarantee that it is safe because hackers can create websites that use encryption but are designed to steal personal information.

Be cautious with emails and personal data

Look at your bank’s advice on conducting 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 safely using email and the web. You should also see our tips on **How to avoid being phished** p103 and **How to avoid viruses, Trojans, worms and spyware** p96.

Keep up to date with security patches

Hackers frequently exploit vulnerabilities in operating systems and programs in an attempt to infect computers. Be aware of security updates for your computer's operating system, browser, plug-ins and other code that could be the target of hackers. If you can, set up your computer to automatically download security patches.

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.

Don't follow links in unexpected emails

Links in unexpected emails can take you to bogus websites, where any confidential information you enter, such as account details and passwords, can be stolen and misused.

In addition, hackers often try to direct you to malicious webpages by spamming out links via email.

Use different passwords for every site

You should use a different password for each site where you have a user account. That way, if a password is compromised, only one account will be affected. In addition, make sure that your passwords are hard to guess and never use a dictionary word as your password.

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 (e.g., by installing spyware on computers) or offend someone. You can do this with web filtering software or a hardware appliance. Even if users are allowed to visit websites, you should ensure that all webpages that are visited are scanned for security threats.

Scan email for malware and spam

Anti-spam programs can detect unwanted email and prevent it from reaching users' inboxes, as well as scan for malware contained within the email itself.

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 code such as fake anti-virus software.

Use routers

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

How to:
choose secure 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 a password is, the harder it is to guess or to find by trying all possible combinations (i.e., a brute force attack). Passwords of 14 characters or more are vastly more difficult to crack.

Use different types of characters

Include numbers, punctuation marks, symbols, and uppercase and lowercase 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. There are good free programs available that will help you manage your passwords.

Reputed password management programs can help you choose unique passwords, encrypt them and store them securely on your computer. Examples include KeePass, RoboForm and 1Password.

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 cracks 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** p61).

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.

How to:
use removable media securely

Educate users

Many users are not aware of the potential dangers that removable media such as USBs and CDs present, such as spreading malware and data loss. Educating users helps reduce the risks significantly.

Identify device types

Computers interact with a growing variety of removable media including USB thumb drives, MP3 players and smartphones. Having visibility of what removable media is attempting to connect to your network can help you set appropriate restrictions or permissions.

Implement device control

Controlling the type of removable media that is permitted and what data is allowed to be exchanged is a vital component of network security. Choose solutions that can set permissions (or restrictions) for individual devices as well as entire classes of devices.

Encrypt your data

Data encryption prevents the loss of data. This is particularly useful for removable media that can be easily misplaced or stolen because the data cannot be viewed or copied by unauthorized third parties.

How to:
buy online safely

Can you trust your common sense and intuition?

Unfortunately, it isn't practical for users to determine if a website is safe or not with the naked eye.

Although invisible to the visiting online customer, hackers often target improperly secured legitimate websites. Being a large, well-established company is no guarantee that the site is safe.

Purchasing from a secure computer or device running the latest anti-virus software, firewalls and security patches will significantly decrease your chances of becoming a victim.

Never follow links from unsolicited online communications, such as email, Twitter or Facebook. Spammers and hackers use social engineering techniques as lures to fraudulent or infected websites.

Only part with sensitive information like your personal or financial details when you are fully satisfied with the legitimacy of the company.

Familiarize yourself with the Terms of Use and the Data Protection Policy

Read the fine print. Terms can sometimes detail hidden and unexpected costs or obligations.

Only purchase through websites using encryption

URLs that start with "https://" rather than "http://" (the "s" stands for secure) are encrypting information during transfer. Another indicator of a website using encryption is a small padlock icon displayed in the internet browser.

However, there is no guarantee that these sites are safe, as hackers can create websites that use encryption but are designed to steal personal information.

Provide the minimum amount of personal information

Leave optional fields blank. Middle name, date of birth, mobile phone number, hobbies … many website operators request optional information alongside required information to process a business transaction. Compulsory fields are often identifiable by an asterisk.

Never share your password

Even if someone else is making the purchase for you, you should enter the password yourself and never share it with others.

To stop subsequent users from accessing your account without authorization, never select the “remember my password” option on a shared computer.

Buy local where possible

When the seller is based in a different country, it can be much more difficult and expensive to resolve any issues and to enforce consumer rights legislation.

Check your bank statements

Check your bank account transactions regularly, particularly after making purchases over the internet, to ensure that all payments are legitimate. If you discover payments that you cannot identify, inform your bank immediately.

Keep your order confirmations and receipts

Always retain important information relating to a purchase in either printed or electronic format. This information will be very useful in resolving any issues relating to the purchase.

How to:
stay safe on the move

Educate users

The risks of data loss from unsecured laptops or removable media should not be underestimated. Organizations should develop clear policies concerning the use of mobile devices.

Use secure passwords

Passwords are the very first walls of defense and should always be as strong as possible.

See **How to choose secure passwords** p107.

Implement additional security checks

Smartcards or tokens require you to enter additional information (e.g., a token code together with your password) in order to access your computer. With fingerprint readers, you need to confirm your identity using your fingerprint when booting up or logging in.

Encrypt all important data

If your data is encrypted, it will remain safe even if your laptop or removable media is lost or stolen. If you don't want to encrypt your entire hard drive, you can create a virtual disk to store confidential information securely.

Restrict Plug and Play

Plug and Play allows USB drives, MP3 players or external hard drives to connect to laptops automatically, making it easy for data to be copied. Instead, lock the computer so only authorized devices are allowed to connect.

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 Vysottsky, 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.

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.

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.

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.

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.

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".

1995 The first document virus

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

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.

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.

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.

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.

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.

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.

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.

2008 Fake anti-virus software

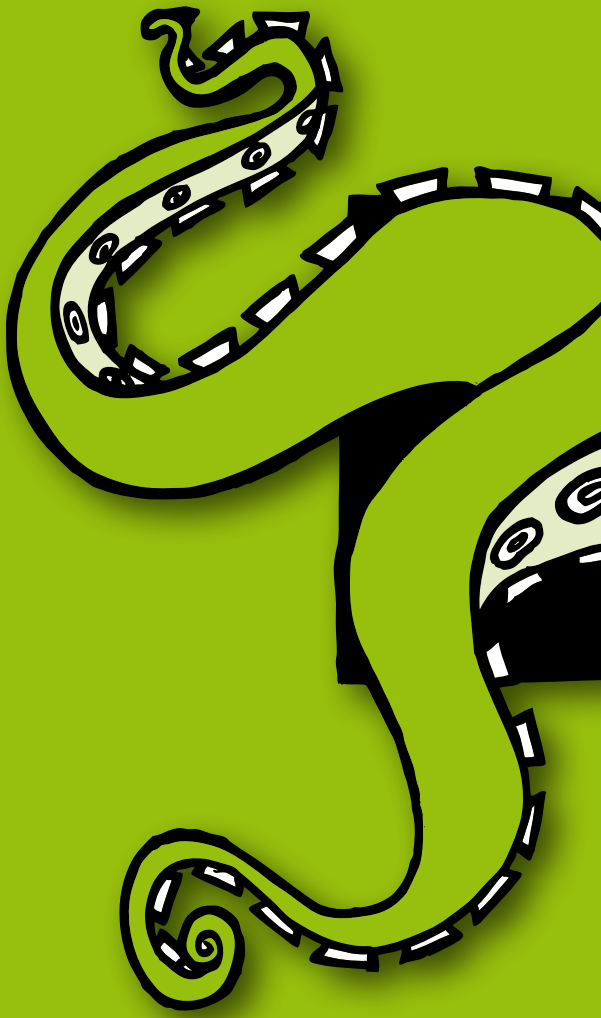
Scaremongering tactics encourage people to hand over credit card details for fake anti-virus products like **AntiVirus 2008**.

2009 Conficker hits the headlines

Conficker, a worm that initially infects via unpatched machines, creates a media storm across the world.

2009 Polymorphic viruses rise again

Complex viruses return with avengance, including **Scribble**, a virus which mutates its appearance on each infection and used multiple vectors of attack.



www.sophos.com

Whether you're an IT professional, use a computer at work, or just browse the internet, this book is for you. We tell you the facts about the threats to your computers and to your data in simple, easy-to-understand language.

SOPHOS
WWW.SOPHOS.COM