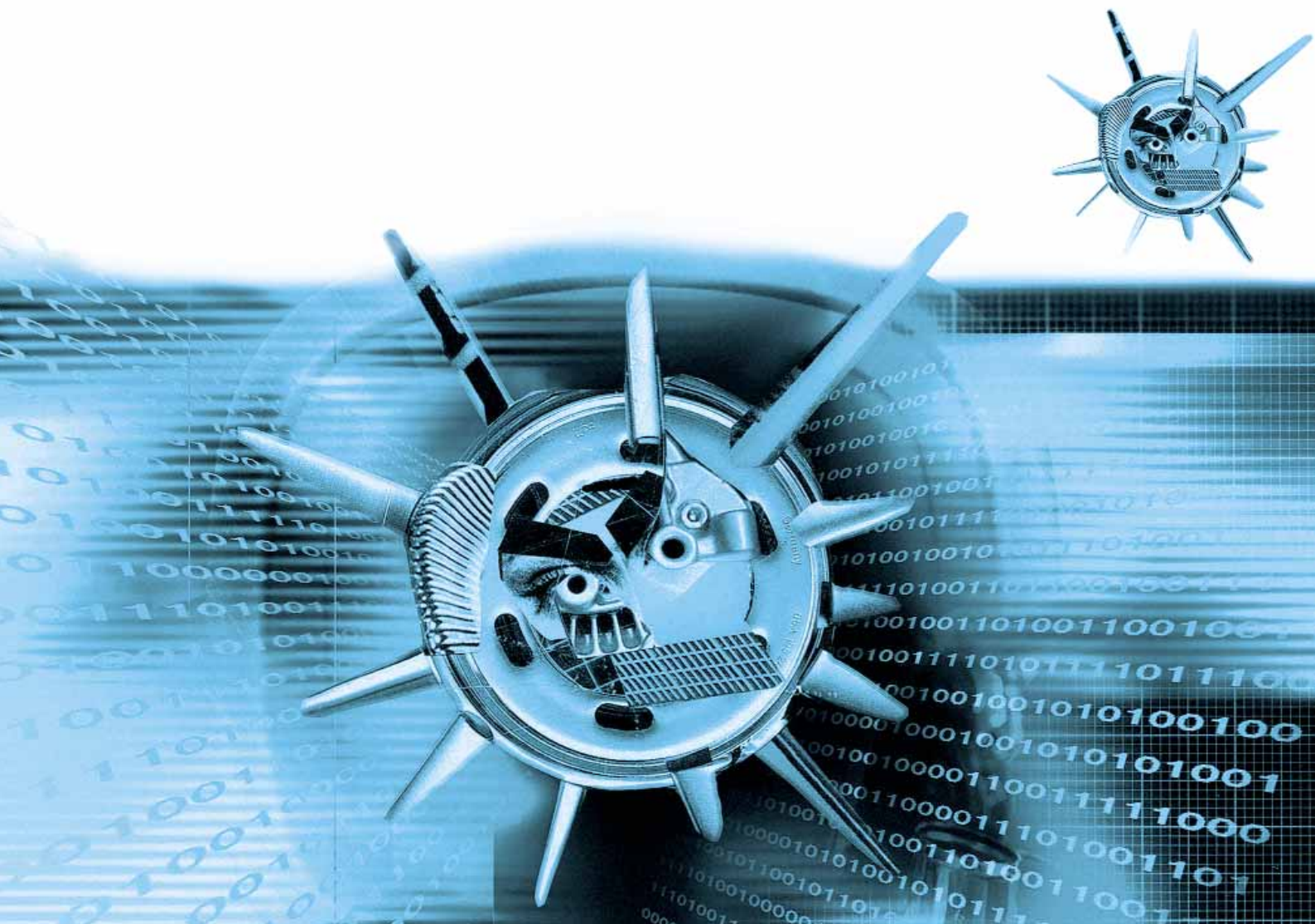
User guide: Kaspersky Lab (internet security)

Brief:
Kaspersky Lab wanted to warn consumers about the emergence of crimeware – computer viruses designed to steal money surreptitiously – by issuing a guide containing practical tips on how to protect themselves from this growing threat.

Staying Safe Online

Produced in association with

KASPERSKY lab



Staying Safe Online

Contents

Introduction

Why are we producing this guide?

The purpose of this guide is to arm you, the home PC user, with all the information you need to protect yourself from online attacks.

As you read on, you will see that attacks on home PCs are not only increasing in frequency, they are also becoming ever more sophisticated and destructive – particularly with the advent of 'crimeware'.

However, while it is true that the risk to home PC users from online attacks has never been greater, it is also true that by following the simple precautions outlined in this guide, there is no reason why surfing the Internet should not continue to be an enjoyable, productive and worry-free experience.

What is the risk of having a PC at home?

Unfortunately, the moment a home PC connects to the Internet it becomes a potential target for cyber criminals. Rather like an unlocked home is an invitation to burglars, an unprotected PC extends a similar invitation to cyber criminals, the writers of 'malware' (an abbreviation of **mal**icious soft**ware**).

Traditional viruses and worms versus contemporary crimeware

In the past, PCs were mainly under threat from viruses and worms. These programs are purpose-built to spread and some of them cause damage to files and PCs. Until a few years ago malware could be described as 'cyber vandalism': an anti-social form of self-expression, written for the challenge, to cause irritation or, at worst, designed to damage data on your computer.

Today, the greatest threat to PC users comes from crimeware. Quite simply, crimeware is malicious code that is distributed for the ultimate purpose of making money illegally. Crimeware is a general term used to highlight the purpose of malicious code today and may take the form of viruses, worms, Trojans or other malicious programs.

Why crimeware is becoming more prevalent

Crimeware has largely replaced the traditional threat from viruses and worms because the criminal underground has realised the potential for making money from malicious code in a 'wired' world.

What happens when a PC is infected?

Different malware affects PCs in different ways. It's software and so it can potentially do anything that software can be programmed to do.

A virus or worm may result in:

- Data loss – to documents, photographs, music files, etc.
- Emotional loss – resulting from damage or loss of personal documents, emails, etc.

Crimeware is likely to cause:

- Financial loss – theft of personal data leading to money siphoned from bank accounts.

The threats to home PC users

What is a virus?

A virus is a program that replicates. In other words, it spreads from file to file on your system and from PC to PC. In addition, it may be programmed to erase or damage data.

What is a worm?

Like a virus, a worm is designed to spread. However, instead of infecting objects on the PC and trying to infect more and more of them, it installs itself once and then looks for other PCs to infect.

What is a Trojan?

Think Greek myth. The Greeks tried to sneak into the city of Troy and catch their enemies off-guard using a wooden horse delivered as a 'gift'. A Trojan program is a program that masquerades as something good but does something bad. These days, however, Trojans tend not to masquerade as anything: they're a silent menace designed to be as unobtrusive as possible so as not to raise suspicion. Much of today's crimeware is made up of Trojan programs.

How can I protect myself from malicious code?

In excess of 200 new viruses, worms and Trojans are released every day, which is why the golden rule is to regularly update your anti-virus software (at least once a day is recommended) and run weekly virus scans. This way you won't get caught cold.

What is crimeware?

Crimeware is malicious software that is planted surreptitiously on PCs. Most crimeware progams are in fact Trojans. There are many types of Trojans designed to do different things. For example, some are used to log every key you type, some capture screenshots when you are using banking websites, some download other malicious code, others let a remote hacker access your system. What they each have in common is the ability to 'steal' your confidential information – such as passwords and PINs – and feed it back to the criminal. Armed with this information, the criminal can then set about stealing your money.

How can I protect myself from crimeware?

Above all, ensure your software regularly updates and that you run weekly scans.

In addition, there are a number of tips that will prevent you from falling victim to an attack:

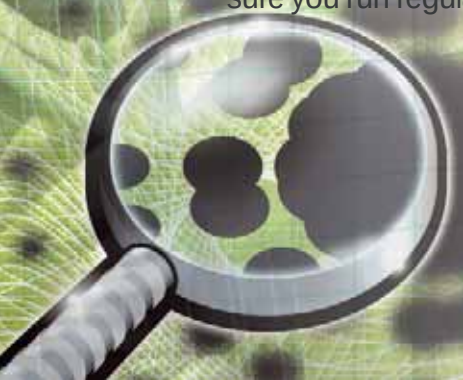
- Only open email attachments that come from a reputable source, and even then only if you're expecting to receive something. NEVER open an attachment sent in an unsolicited (spam) email.
- Protect your computer system, and any online accounts, with a password.
- Do not use obvious passwords, for example your name or date of birth. Try to avoid using real words that an attacker could find in a dictionary. Instead, use made-up words and include at least one numeric character, at least one non-alphanumeric character and a mix of upper and lower case letters.
- Don't log in to your computer for regular use as a user with administrator rights. For everyday use, create an account for yourself that has only limited rights to the system.
- Do not reply to spam email, or click 'unsubscribe' in a spam email as this just confirms that your email address is genuine.
- Don't complete a form in an email message asking for personal information. Only enter such information using a secure website – check that the URL (i.e. the web address) starts with 'https://', rather than just 'http://'. Look for the padlock symbol in the lower right-hand corner of the web browser and double-click on it to check its validity.
- Avoid clicking on links in email messages. It's safer to manually type the URL into the web browser.
- NEVER divulge passwords or PINs via email, or by any other method, to someone you don't know. If any organisation contacts you, even by phone, don't be afraid to refuse to tell them personal details. After all, you don't know who is at the other end of the line.

What is spyware?

'Spyware' is a general term used to describe programs that collect and transmit information about a PC without the consent of the PC's owner. Spyware includes all varieties of Trojans, such as keystroke loggers and screenshot grabbers. It also includes malware-related programs like adware or dialers.

How can I protect myself from spyware?

Make sure your anti-virus software includes protection from spyware. And, again, make sure you run regular updates and scans to make sure you're protected at all times.



What is a phishing attack?

A phishing attack is a specific form of cyber crime. The criminal creates an almost 100 percent perfect replica of a chosen financial institution's website, then attempts to trick the user in to disclosing their personal details – username, password, PIN etc – via a form on the fake website, allowing the criminal to use the details to obtain money.

Phishers use various techniques to trick users in to accessing the fake website, such as sending emails that pretend to be from a bank. These emails often use legitimate logos, a good business style and often spoof the header of the email to make it look like it came from a legitimate bank. In general, these letters inform recipients that the bank has changed its IT infrastructure and asks all customers to re-confirm their user information. When the recipient clicks on the link in the email, they are directed to the fake website, where they are prompted to divulge their personal information.

How can I protect myself from a phishing attack?

- Be very wary of any email messages asking for personal information. It's highly unlikely that your bank will request such information by email. If in doubt, call them to check!
- Don't use links in an email message to load a web page. Instead, type the URL into your web browser.
- Don't complete a form in an email message asking for personal information. Only enter such information using a secure website. Check that the URL starts with 'https://', rather than just 'http://'. Look for the lock symbol on the lower right-hand corner of the web browser and double-click it to check the validity of the digital certificate. Or, alternatively, use the telephone to conduct your banking.
- Check if your anti-virus program blocks phishing sites, or consider installing a web browser tool bar that alerts you to known phishing attacks.
- Check your bank accounts regularly (including debit and credit cards, bank statements, etc.), to make sure that listed transactions are legitimate.
- Make sure that you use the latest version of your web browser and that any security patches have been applied.
- Report anything suspicious to your bank immediately.

What is a rogue dialer?

A rogue dialer diverts your modem to a premium rate phone number, instead of the number of your ISP (Internet Service Provider) without you knowing it has done so. You'll only know that you've been snared by a rogue dialer when your phone bill is far higher than normal, and there will be premium rate telephone numbers on your bill that you won't recognise. These threats apply only to users who have a dial-up account.

How can I protect myself from rogue dialers?

The simplest and most effective measure is to contact your telephone service provider and put a ban on all telephone numbers beginning with '09'.

You should also report all suspect numbers to ICSTIS, the regulatory body for premium rate telephone services. ICSTIS can be contacted at www.icstis.org.uk.

What is spam?

Spam is anonymous, unsolicited bulk email – it is effectively the email equivalent of physical junk mail delivered through the post. It is sent out in mass quantities by spammers who make money from the small percentage of recipients that actually respond.

Time-consuming and frustrating to wade through, it clogs up your mailbox and absorbs bandwidth and storage space that you've paid for.

Today, however, it is also being used for a more sinister reason – to spread malicious code.

How can I protect myself from spam?

- Maintain at least two email addresses. Use your private address only for personal correspondence, and the other address for registering on public forums, in chat rooms, to subscribe to mailing lists etc.
- Never publish your private address on publicly accessible resources.
- Your private address should be difficult to guess. Spammers use combinations of obvious names, words and numbers to build possible addresses. Your private address should not simply be your first and last name. Be creative and personalise your email address.
- If you must publish your private address electronically, mask it to avoid having it picked up by spammers. 'Joe.Smith@yahoo.com' is easy to guess, as is 'J.Smith@yahoo.com.' Try writing 'Joe-dot-Smith-at-yahoo.com' instead. If you need to publish your private address on a website, do this as a graphics file rather than as a link.
- Treat your public address as a temporary one. Chances are high that spammers will guess your public address fairly quickly. Don't be afraid to change it often.
- Consider using a number of public addresses in order to trace which services are selling your address to spammers.
- Never respond to spam. Most spammers verify receipt and log responses. The more you respond, the more spam you will receive.
- Do not click on 'unsubscribe' links from questionable sources. Spammers send fake unsubscribe letters in an attempt to collect active email addresses. If you click 'unsubscribe' in one of these letters, it will just increase the amount of spam you receive.
- If your private address is discovered by spammers - change it. This can be inconvenient, but changing your email address does help you avoid spam - at least for a while!
- Use an anti-spam solution and only open email accounts with providers who provide spam filtering.

What is hacking?

A hacker is someone who electronically gains illegal access to data. Hackers regularly breach both individual computers and large networks.

Once they have gained access, hackers use the victim machines for a variety of goals. Many hackers use their skills for financial gain, while some use their knowledge to spread viruses or launch attacks on the Internet or specific web sites.

How do I protect myself from hackers?

By using anti-hacking technology, such as a personal firewall. A personal firewall protects PCs from potentially damaging data sent via the Internet by detecting potential intruders and making the PC invisible to hackers.

Inherent weaknesses in home PC systems and how to protect against them

All sufficiently complex software contains flaws, weaknesses or limitations. And many of today's applications are very complex. So it's not surprising that there are many flaws in common operating systems, such as Microsoft® Windows®. And, unfortunately, common operating systems inevitably become the targets of malware writers, as attacking the most common systems will cause maximum damage.

Therefore it is highly recommended that users enable Automatic Updates in Windows®. This can be done by clicking the 'Control Panel', selecting 'Settings' and then clicking on 'Security Center'.

Required protection to remain safe online

Below is an at-a-glance list of components that should be installed on your PC to ensure your online safety:

- Anti-virus software
- Personal firewall software
- Anti-spam software
- Anti-spyware software (look for anti-virus programs that include this)

When choosing the above, make sure you buy from a reputable provider – security is something on which you cannot afford to compromise. Many providers offer all of these in one bundle.

Also, contact your telephone provider and ban premium rate numbers to remove the threat of rogue diallers.

Diagnosing common problems

If you experience any of the following, it's quite likely that your PC is infected and you should contact your anti-virus helpdesk or a reputable PC repair outlet ASAP.

- Unexpected messages or images are suddenly displayed
- Programs suddenly start on your computer
- Files and folders have been deleted or their content has changed
- Telephone bill is unusually high and shows premium rate numbers

For more information on what to do if you suspect your PC is infected, visit http://www.viruslist.com/en/viruses/encyclopedia?chapter=153280800

Glossary of terms

Personal firewall:
synonym – firewall
A personal firewall is a barrier between a PC and external computer systems that protects a PC from potentially damaging data sent via the Internet.

Hacker:
An individual who electronically gains illegal access to data. Hackers regularly breach both individual computers and large networks.

Malware:
synonyms – malicious code, malicious software
Malware (short for **mal**icious soft**ware**) refers to any program that is deliberately created to perform an unauthorised, often harmful, action.

Phishing:
Phishing is a form of cyber crime based on social engineering techniques. The name 'phishing' is a conscious misspelling of the word 'fishing' and involves stealing confidential data from a user's computer and subsequently using the data to steal the user's money.

The cyber criminal creates an almost 100 percent perfect replica of a financial institution or online commerce web site. He then tries to lure unsuspecting users to the site to enter their login, password, credit card number, PIN, etc. into a fake form. This data is collected by the phisher who later uses it to access users' accounts fraudulently.

Some financial institutions now make use of a graphical keyboard, where the user selects characters using a mouse, instead of using a physical keyboard. This prevents collection of confidential data by phishers who trap keyboard input, but is of no avail against so-called 'screenscraper' techniques: where a Trojan that takes a snapshot of the user's screen and forwards it to the server controlled by the Trojan author or 'master'.

Rogue dialer:
A program that diverts a modem to a premium rate phone number, instead of the number of the ISP (Internet Service Provider) without the PC user's knowledge or consent.

Spam:
synonyms – UCE (Unsolicited Commercial Email), junk email
Spam is the name commonly given to unsolicited email. It is effectively unwanted advertising, the email equivalent of physical junk mail delivered through the post or from unsolicited telemarketing calls.

Trojan:
synonym – Trojan horse
The term Trojan is taken from the wooden horse used by the Greeks to sneak inside the city of Troy and capture it. The first Trojans, which appeared in the late 1980s, masqueraded as innocent programs. Once the unsuspecting user ran the program, the Trojan would deliver its harmful payload. Hence the copy-book definition of a

Trojan as a non-replicating program that appears to be legitimate but is designed to carry out some harmful action on the victim computer.

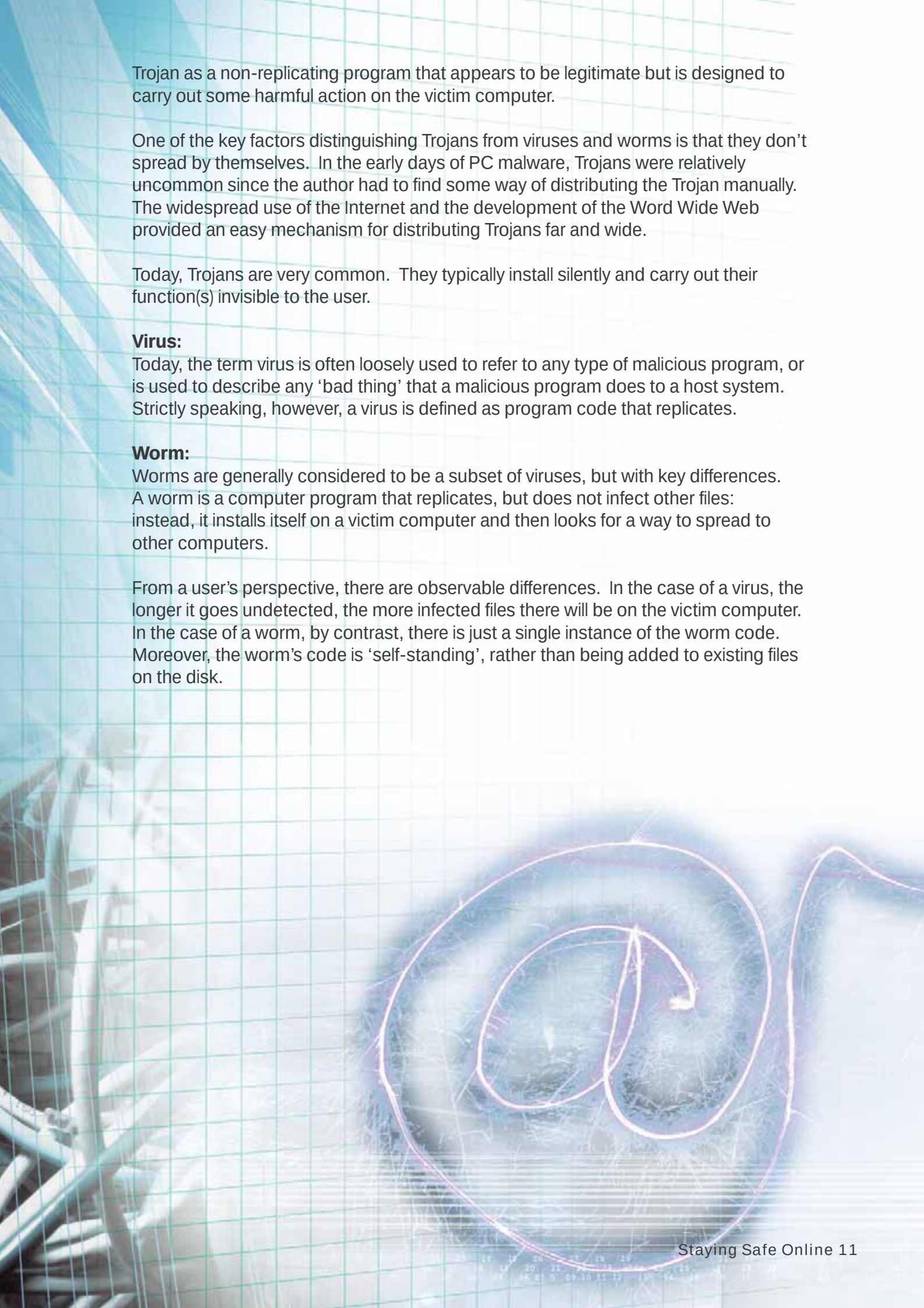
One of the key factors distinguishing Trojans from viruses and worms is that they don't spread by themselves. In the early days of PC malware, Trojans were relatively uncommon since the author had to find some way of distributing the Trojan manually. The widespread use of the Internet and the development of the Word Wide Web provided an easy mechanism for distributing Trojans far and wide.

Today, Trojans are very common. They typically install silently and carry out their function(s) invisible to the user.

Virus:
Today, the term virus is often loosely used to refer to any type of malicious program, or is used to describe any 'bad thing' that a malicious program does to a host system. Strictly speaking, however, a virus is defined as program code that replicates.

Worm:
Worms are generally considered to be a subset of viruses, but with key differences. A worm is a computer program that replicates, but does not infect other files: instead, it installs itself on a victim computer and then looks for a way to spread to other computers.

From a user's perspective, there are observable differences. In the case of a virus, the longer it goes undetected, the more infected files there will be on the victim computer. In the case of a worm, by contrast, there is just a single instance of the worm code. Moreover, the worm's code is 'self-standing', rather than being added to existing files on the disk.



About Kaspersky Lab

Kaspersky Lab provides products that protect home users from viruses, worms, Trojans, phishing attacks, spyware, spam and hackers.

The latest version of its software, Kaspersky Internet Security 6.0, is available now.

For more information, please contact Kaspersky Lab on 0870 011 3461 or info@kasperskylab.co.uk

Useful websites
www.viruslist.com
www.banksafeonline.org.uk
www.kaspersky.co.uk