

About Kaspersky Lab

Kaspersky Lab delivers the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam. Kaspersky Lab products provide superior detection rates and the industry's fastest outbreak response time for home users, SMBs, large enterprises and the mobile computing environment. Kaspersky® technology is also used worldwide inside the products and services of the industry's leading IT security solution providers.

Learn more at www.kaspersky.co.uk. For the latest on antivirus, anti-spyware, anti-spam and other IT security issues and trends, visit www.securelist.com.

Kaspersky Lab UK Ltd

97 Milton Park

Abingdon

Oxfordshire

OX14 4RY

United Kingdom

Tel UK: +44 (0)871 789 1631

Tel Ireland: +44 (0)870 011 3461

Fax: +44 (0)871 789 1633

E-mail: info@kasperskylab.co.uk

www.kaspersky.co.uk



Your Guide To Stopping Cybercrime

Why have we produced this guide?	1
What's the risk?	1
What do malicious programs do?	2
Hacker attacks	4
How can I protect myself from malicious code and hacker attacks?	5
What is phishing?	6
How can I protect myself from phishing attacks?	7
Can my data be damaged by a malicious program?	8
How can I protect myself from ransomware?	8
What is a rogue dialer?	8
How can I protect myself from rogue dialers?	9
How do I secure my wireless network?	10
What is spam?	10
How can I protect myself from spam?	11
Why are passwords important?	12
Does it matter what password I use?	13
How can I help my children stay safe online?	14
What should I do if my computer has been compromised?	16
A final note about identity theft	17
Useful web sites	17
About Kaspersky Lab	18

Why have we produced this guide?

The aim of this guide is to help you protect yourself from cyber attacks. Cyber attacks include viruses, worms, Trojans, hacker attacks, phishing attacks and more. They are more sophisticated than ever before. There are more of them than ever before. Many of them are designed to steal your identity, gather your personal data and defraud you of your money.

However, while the risk from online attacks continues to grow, if you follow 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's the risk?

The moment you connect your PC to the Internet it becomes a potential target for cybercriminals. Just as an unprotected home offers easy pickings for burglars, an unprotected PC is an open invitation to the writers of malware (short for malicious software) and the cybercriminals who sponsor them.

Until a few years ago, malicious programs were just cyber vandalism, anti-social form of self-expression exploiting computer technology. Few of them were deliberately written to cause harm, although a small number caused damage to data or made the computer unusable (quite often as a side-effect, rather than by design). The bulk of malicious programs in circulation at this stage were viruses and worms.

Today, by contrast, the greatest threat comes from cybercrime. The criminal underground has realised that malicious code can be used to make money in our constantly connected world and they use it to steal confidential data (logins, passwords, PINs, etc.).

Most malicious programs today are Trojans. There are many different types of Trojan. Some record which keys you press, some take a picture of your screen when you visit a banking web site, some download additional malicious code, and some provide a remote hacker with access to your computer. However, they all have one thing in common: they allow cybercriminals to harvest your confidential information and use it to steal your money.

Cyber threats are not just getting more sophisticated, the volume is growing: our virus lab currently sees over 30,000 new Internet threats every day.

Kaspersky Lab sees over 30,000 new Internet threats every day.

Most malicious programs are Trojans, designed to steal confidential information and use it to steal your money.

What do malicious programs do?

Just like other software, malicious programs are designed to behave in a particular way and carry out certain specific functions. They have exactly the same limitations as any other program. What they do depends on what the malware author has coded them to do.

Many older viruses had no payload: they were simply designed to spread. Some caused unintended side-effects (as a result of poor programming). A relatively small number were deleted files or corrupted data. They could be a nuisance, or they could cause loss of data, but they seldom tried to gather data for later use.

Things are different now. Today, malicious programs are typically to steal information. This is why many Trojans are referred to as spyware: they're installed stealthily, without your knowledge or consent, and they are designed to monitor your actions day after day. They carefully hide their tracks using programs called rootkits. So everything runs normally and you have no reason to suspect that there's a problem.

Today, spyware programs install stealthily, without your knowledge or consent, and silently gather your personal information.



Hacker attacks

Today's applications are very complex, compiled from thousands of lines of code. And they're written by humans, who are fallible. So it's hardly surprising that they contain programming mistakes known as vulnerabilities. These loopholes are used by hackers to break into systems; they are also used by authors of malicious code to launch their programs automatically on your computer.

The term hacker was once used to describe a clever programmer. Today, it's applied to those who exploit security vulnerabilities to break into a computer system. You can think of it as electronic burglary. Hackers regularly break into both individual computers and large networks. Once they have access, they install malicious programs, steal confidential data or use compromised computers to distribute spam. They may also flood another company's web servers with network traffic: such Denial-of-Service (DoS) attacks are designed to make the site inaccessible and damage the company's business.

Cybercriminals, of course, want to maximise the return on the time and effort they've put in, so they target the most widely used systems. That's why, for example, hackers focus so much attention on Microsoft® Windows®: it's the operating system used by the vast majority of people.

Hackers are like electronic burglars who use loopholes in your programs, called vulnerabilities, to break into your computer.



How can I protect myself from malicious code and hacker attacks?

There are several steps you can take to protect your computer from today's cyber threats. Following the simple guidelines below will help minimise the risk of attack.

- Protect your computer by installing Internet security software.
- Update it regularly (i.e. at least once a day).
- Install security patches for your operating system and applications. If you use Windows® simply switch on Automatic Updates. And don't forget to update Microsoft® Office
- Update your other applications
- If you receive an e-mail with an attached file (Word documents, Excel spreadsheets, EXE files, etc.) don't open it unless you know who sent it and only then if you're expecting it. NEVER open an attachment sent in an unsolicited (spam) e-mail. The same is true for e-mail messages or IM (Instant Messaging) messages that contain links.
- Only use your computer's Administrator account if you need to install software or make system changes. For everyday use, create a separate account with only limited access rights (this can be done using User Accounts in Control Panel). By doing this, you limit a malicious program's access to valuable system data.
- Backup your data regularly to a CD, DVD, or external USB drive. If your files have been damaged or encrypted by a malicious program you can then copy them back from your backup.

To protect against malicious code and hacker attacks:

- ✓ Install Internet security software.
- ✓ Install security patches.
- ✓ Be wary of unsolicited e-mail or IM messages.
- ✓ Be careful about logging in with Administrator rights.
- ✓ Backup your data.

What is phishing?

Phishing is designed to steal your identity, gather your personal data and defraud you of your money.

Cybercriminals send you an e-mail containing a link. When you click on the link it takes you to a fake site that looks just like your bank's web site. They then try to trick you into typing in your login, password or PIN. They capture this information and use it to take money from your bank account.

Typically, cybercriminals send out large numbers of e-mails that appear to come from a specific bank or financial institution. Of course, many people who receive the e-mail are not customers of the bank in question. But it only takes a small percentage of the people who get the e-mail to fall for the scam for the cybercriminals to make money.

Phishing e-mails often try to put you off your guard by using the real bank's style and logo, by using a link that resembles the real bank's URL or by including your name to make it seem as though the e-mail is addressed to you personally. They usually provide a fake reason for sending you the e-mail and asking you for your personal details: the bank is conducting random security checks, or the bank has made changes to its infrastructure and needs everyone to re-confirm their details.

Often cybercriminals withdraw a relatively small amount, so as not to arouse suspicion. Of course, there are lots of potential victims, so a small amount from each victim means big profits for the cybercriminals.

Phishing e-mails pretend to be a message from a bank or other financial body. They normally include a link that directs you to a fake web site where cybercriminals try to persuade you to type in confidential data that they use to take money from your bank account.

Susan's protected.

Susan organises her life on the Internet. Shopping, browsing, banking and catching up with old friends. She's far too busy to worry about cybercrime. She doesn't care that cybercriminals are creating 30,000 new Internet threats daily aimed at making money from people just like her.

Online fraud, ID theft, banking scams, phishing – none of these worry Susan. Like 300 million others worldwide, she's protected by Kaspersky Lab.



How can I protect myself from phishing attacks?

You should follow the advice given above about protecting yourself from malicious code and hacker attacks. In addition, the following guidelines will help you minimise the risk of becoming the victim of a phishing attack.

- Don't disclose personal information in response to an e-mail message. It's highly unlikely that your bank will ask for such information by e-mail. If an email message claims to be from your bank, call them to check.
- Don't click on links in HTML e-mails to get to a web site. Cybercriminals can hide the URL of a fake web site behind a link that looks legitimate. Instead, type the URL into your web browser yourself. Or configure your e-mail reader to use plain text only, since this trick doesn't work in plain text.
- Don't complete a form asking for personal information in an e-mail. Only enter such data using a secure web site. Check that the URL starts with 'https://' and look for the padlock symbol in the lower right-hand corner of your web browser. You should double-click the padlock and check that the address in the security certificate matches the one shown in the web browser address bar. If you're in any doubt, use the telephone to transact your business.
- Check your bank accounts regularly (including debit and credit cards, bank statements, etc.), to make sure you can account for all the transactions. Report anything suspicious to your bank immediately.
- Be suspicious of any e-mail that is not addressed to you personally: for example, if it begins 'Dear Valued Customer', or something similar.
- Be suspicious if you're not the only recipient. In the very unlikely event that your bank does communicate with you by email about your personal account, it will not send the e-mail to other people.
- Be suspicious of spelling mistakes, poor grammar or syntax and other clumsy use of language.

To protect against phishing attacks:

- ✓ Don't click on links in e-mail messages.
- ✓ Only type in confidential data on a secure web site.
- ✓ Check your bank account(s) regularly and report anything suspicious to your bank.
- ✓ Look for giveaway signs of phishing e-mails:
 - If it's not addressed to you personally.
 - If you're not the only recipient.
 - If there are spelling mistakes, poor grammar or syntax or other clumsy use of language.
- ✓ Follow the advice above on how to protect from malicious code and hacker attacks.

Can my data be damaged by a malicious program?

Yes, some cybercriminals try to extort money from their victims using ransomware programs. These programs encrypt your data and create a 'readme' file on your hard disk that tells you how to contact the cybercriminals. They promise to tell you how to get your data back, but only if you pay them some money, using an online payment system like e-gold or WebMoney.

Some cybercriminals use ransomware programs to encrypt your data. They try to extort money in return for instructions on how to get your data back.

How can I protect myself from ransomware?

You should follow the advice given above about protecting yourself from malicious code and hacker attacks. In addition, the following guidelines will help you minimise the risk of becoming the victim of ransomware.

- Backup your data regularly. So far Kaspersky Lab has been able to recover data encrypted by ransomware programs. However, since cybercriminals are using more and more sophisticated levels of encryption, we may not be able to do so in the future. However, if you have a backup, you will not lose any data.
- NEVER pay money to a cybercriminal. If you do not have a backup, contact your anti-virus vendor as they may be able to help you recover the data.

To protect against ransomware:

- ✓ Backup your data.
- ✓ NEVER pay money to a cybercriminal.
- ✓ Follow the advice above on how to protect from malicious code and hacker attacks.

What is a rogue dialer?

Rogue dialers are programs that divert your computer's modem to a premium rate phone number, instead of the normal number you use to connect to your Internet Service Provider [ISP].

These programs are installed without your knowledge or consent and operate secretly. So the first indication that you have become a victim may be when the phone bill arrives and it's substantially larger than normal. There will also be premium rate telephone numbers listed on your bill that you know you haven't called.

Rogue dialers only target people with a dial-up connection. If you have a broadband Internet connection, rogue dialers will not work. However, when you switch from dial-up to broadband, be sure to disconnect your modem cable from the telephone socket and remove any dial-up icon from your desktop. This will ensure you don't accidentally use your dial-up connection.

Don't worry, if you ever need a dial-up connection again (for example, if your broadband connection is interrupted temporarily), you can reconnect the modem cable to the telephone socket and re-activate your dial-up connection.

Rogue dialers hijack the computer's modem and silently dial a premium rate number, significantly increasing the size of your telephone bill.

How can I protect myself from rogue dialers?

You should follow the advice given above about protecting yourself from malicious code and hacker attacks. In addition, consider asking your telephone service provider and put a ban on all telephone numbers beginning with '09'.

UK only - If you think you have already fallen victim to a rogue dialer, report the suspect number(s) to PhonepayPlus (www.phonepayplus.org.uk), formerly known as ICSTIS, the regulatory body for phone-paid services in the UK.

To protect against rogue dialers:

- ✓ Ban telephone numbers beginning with '09'.
- ✓ Disconnect your modem if you upgrade to broadband.



Jason's protected.

Jason can't imagine life without the Internet: surfing; social networking; e-mailing; downloading files; gaming. He doesn't care that cybercriminals are creating over 30,000 new Internet threats daily aimed at making money from people just like him.

Online fraud, ID theft, banking scams, phishing – none of these worry Jason. Like 300 million others worldwide, he's protected by Kaspersky Lab.

How do I secure my wireless network?

Most computers are wireless-enabled: they let you connect to the Internet without a physical network cable. The major benefit, of course, is that you can use your computer anywhere in the house or office (as long as it's within range of your wireless router). However, there are potential risks unless you secure your wireless network.

1. A hacker could intercept any data you send and receive.
2. A hacker could get access to your wireless network.
3. Another person could hijack your Internet access.

If your wireless network is not secure, a hacker could intercept the data you send, access your network and use your connection to access the Internet.

There are some simple steps you can take to secure your wireless router and minimise these risks:

- Change the administrator password for your wireless router. It's easy for a hacker to find out the manufacturer's default password and use this to access your wireless network. And avoid using a password that can be guessed easily: follow the guidelines provided in the section below on choosing a password.
- Enable encryption: WPA encryption is best, if your device supports it (if not, use WEP).
- Switch off SSID (Service Set Identifier) broadcasting, to prevent your wireless device announcing its presence to the world.
- Change the default SSID name of your device. It's easy for a hacker to find out the manufacturer's default name and use this to locate your wireless network. Avoid using a name that can be guessed easily: follow the guidelines provided in the section below on choosing a password.
- When buying a router, choose one that supports NAT [Network Address Translation]. This will hide your computer(s) from outside attackers, who will only be able to see the router itself.

To secure your wireless network:

- ✓ Change the administrator password.
- ✓ Enable encryption.
- ✓ Switch off SSID and change the default name of your wireless router.
- ✓ Follow the advice above on how to protect from malicious code and hacker attacks.

What is spam?

Spam is anonymous, unsolicited bulk e-mail, the electronic equivalent of junk mail delivered through the post. Spam makes up approximately 70% - 80% of all e-mail sent.

Spam is used to advertise goods and services. Spammers send out large volumes of e-mail and make money by selling goods to those who respond. Typically only a very small number of recipients respond, but this is enough for spammers to make a profit.

It's time-consuming and frustrating to have to wade through junk e-mail. It also clogs up your mailbox and absorbs bandwidth and storage space. However, there's another important point: spam can carry malicious programs. Spam e-mails may come with an infected attachment. Or they may contain a link to a web site that contains a malicious program (this code may download automatically when you visit the site and install on your computer if you have missed any security patches).

Spammers use botnets to distribute their e-mails. Botnets are networks of computers that have been taken over by cybercriminals using Trojans or other malicious code. The victim doesn't realise that the spammer can control their computer remotely, but the infected machines automatically send junk e-mail to others. Of course, if you protect your computer with Internet security software this will minimise the risk of your computer being taken over in this way.

Spam e-mail, electronic junk-mail, wastes time, clogs up your mailbox and absorbs your bandwidth and storage space. It's also used to distribute malicious code.

How can I protect myself from spam?

You should follow the advice given above about protecting yourself from malicious code and hacker attacks. In addition, the following guidelines will help you minimise the amount of spam you receive.

- Don't respond to spam e-mails. Spammers often verify receipt and log responses, so responding just increases the risk of receiving more spam in the future.
- Don't click on 'Unsubscribe' links in spam e-mails. This will confirm that your e-mail address is active, and spammers will target you in the future.
- Use multiple e-mail addresses. Keep one for personal correspondence and at least one other for public forums, chat rooms, mailing-lists and other public web sites or services. Then, if you start receiving lots of spam, you can simply delete your public address and create a new one.
- Make your private e-mail address difficult to guess. Spammers use combinations of obvious names, words and numbers to build possible addresses. So be creative and avoid using just your first name and last name.
- Avoid publishing your private address anywhere public. If you have no choice, mask the address so it can be picked up by automated tools used by spammers to gather e-mail addresses from the Internet. For example, write 'joe-dot-Smith-at -mydomain-dot-com', instead of 'joe.smith@mydomain.com'.

To reduce the amount of spam you receive:

- ✓ Don't respond to spam e-mails.
- ✓ Don't click on 'Unsubscribe' links in spam e-mails.
- ✓ Use multiple e-mail addresses; one for private use, one for public use.
- ✓ Don't publish your private e-mail address and make it hard for spammers to guess.
- ✓ Follow the advice above on how to protect from malicious code and hacker attacks.

Why are passwords important?

One important way to safeguard confidential information is to use a password to prevent other people from accessing your personal data.

This has become more important as Internet use has increased. There are more Internet users than ever before, and we're using it for a far wider range of activities, including online banking, online shopping and online research. Increasingly, we're also using the Internet to socialise. In the last few years there's been a massive growth in the number of social networking sites such as Facebook, MySpace, etc. We share all kinds of personal details as well as music, pictures, and videos.

Unfortunately, the more personal details we make available, the more exposed we are to online identity theft. Identity theft is when a criminal steals confidential personal data that lets them fraudulently obtain goods and services in your name. A cybercriminal could, for example, open a bank account, obtain a credit card or apply for a driving licence or passport. Or they could simply steal money directly from your bank account.

Given that passwords protect such valuable data, they're clearly very important. You should protect all your online accounts with a password. But you have to be careful when choosing passwords.

Passwords help safeguard you against identity theft. They make it harder for cybercriminals to profile you, access your bank account (or other online accounts) and steal your money.

Anna's protected.

Anna e-mails her grandchildren, shops online and surfs the Internet. She doesn't worry about cybercrime. She has no idea that cybercriminals are creating over 30,000 new Internet threats daily aimed at making money from people just like her.

Online fraud, ID theft, banking scams, phishing – none of it worries Anna. Like 300 million others worldwide, she's protected by Kaspersky Lab.



Does it matter what password I use?

Yes, it's very important. If you choose a weak password, you increase the risk of becoming a victim of cybercrime. You should follow the advice given above about protecting yourself from malicious code and hacker attacks. The following guidelines will help you when choosing a password for an online account.

- Make your passwords memorable, so you don't have to write them down or store them in a file on your computer (remember, this file could be stolen by cybercriminals).
- Don't tell anyone your password. If an organisation contacts you and asks for your password, even by phone, don't give them any of your personal details. Remember, you don't know who's at the other end of the telephone line.
- If an online store, or any web site, sends you an e-mail confirmation that contains a new password, login again and change your password immediately.
- Don't use obvious passwords that can be easily guessed, such as spouse's name, child's name, pet's name, car registration, postcode etc.
- Don't use real words that a hacker or cybercriminal can find in a dictionary.
- Use a mixture of uppercase and lowercase, numbers and non-alpha-numeric characters such as punctuation marks.
- If possible, use a passphrase, rather than a single word.
- Don't use the same password for multiple accounts. If a cybercriminal finds the password to one account, they can use to access other accounts.
- Don't recycle passwords, e.g. don't use 'password1', 'password2', 'password3', etc. for different accounts.
- Check that your Internet security software blocks attempts by cybercriminals to intercept or steal passwords.

When choosing passwords:

- ✓ Make them memorable.
- ✓ Keep them secret.
- ✓ Don't be fooled into disclosing them to seemingly legitimate organisations.
- ✓ Mix uppercase and lowercase letters, numbers and non-alpha-numeric characters.
- ✓ Don't use the same password for multiple accounts.
- ✓ Don't recycle passwords ('password1', 'password2', etc.).
- ✓ Follow the advice above on how to protect from malicious code and hacker attacks.

How can I help my children stay safe online?

First think about the possible dangers they face. These include the following:

1. So-called 'drive-by downloads' (i.e. malicious programs that install on your computer automatically when you view a web page).
2. The risk of infection through peer-to-peer (P2P) file-sharing programs that give others access to your computer.
3. Unwanted advertising, including pop-ups and adware programs: these are sometimes installed automatically with freeware programs that are available for download on the Internet.
4. Sexually explicit (or other inappropriate) content.
5. Children may be tricked into disclosing personal information (about them or you).
6. Children may download pirated material (e.g. music or video files).
7. Children may be targeted by online bullies.
8. Children may be approached (in Internet chat rooms, for example) by paedophiles.

Children can be just as vulnerable online as they are in the real world and it's important that you understand the potential dangers.



There are things you can do to minimise the chance of them being exposed to these dangers:

- Talk to your children about the potential dangers they face online.
- If possible, locate your computer in a family room and try to make the computer a shared family experience.
- Encourage your children to talk to you about anything they experience online that upsets them or makes them feel uncomfortable.
- Provide guidelines for them on what they may, or may not, do. Here are some of the things you should think about (remember that the answers may change as your children get older):
 - Is it OK to register on social networking or other web sites?
 - Is it OK to make online purchases?
 - Is it OK to use instant messaging programs? If the answer to this is 'yes', make sure your children understand they should not chat to unknown users.
 - Is it OK to visit Internet chat rooms?
 - Is it OK to download music, video or program files?
- Restrict the content that can be accessed from your computer. Many Internet security solutions let you do this. In addition, Internet Explorer includes a Content Advisor that can help you do this (this can be found under Tools | Internet Options | Content).
- Follow the guidelines above for protecting your computer from malicious programs and hackers and explain to your children how this helps protect them.

To protect your children online:

- ✓ Talk to them about the potential dangers.
- ✓ Keep the computer in a family room.
- ✓ Encourage your children to talk to you about their online experience.
- ✓ Provide them with guidelines for online activity.
- ✓ Restrict content that your children can access online.
- ✓ Follow the advice above on how to protect from malicious code and hacker attacks.

Emily's protected.

Emily e-mails, surfs and plays games online. Her parents don't worry about chat room predators or cyber bullying. Like 300 million others worldwide, they rely on Kaspersky Lab to provide online protection for the whole family.

With parental controls Emily can use the Internet safely. And with over 30,000 new Internet threats appearing daily, her parents know they are protected against online fraud, ID theft and phishing attacks.

What should I do if my computer has been compromised?

It's not always easy to tell if your computer has been compromised. More than ever before, the authors of viruses, worms, Trojans and spyware are going to great lengths to hide their code and conceal what their programs are doing on an infected computer. That's why it's essential to follow the advice given in this guide: in particular, install Internet security software, make sure you apply security patches to your operating system and applications and backup your data regularly.

It's very difficult to provide a list of characteristic symptoms of a compromised computer because the same symptoms can also be caused by hardware and/or software problems. Here are just a few examples:

- Your computer behaves strangely, i.e. in a way that you haven't seen before.
- You see unexpected messages or images.
- You hear unexpected sounds, played at random.
- Programs start unexpectedly.
- Your personal firewall tells you that an application has tried to connect to the Internet (and it's not a program that you ran).
- Your friends tell you that they have received e-mail messages from your address and you haven't sent them anything.
- Your computer 'freezes' frequently, or programs start running slowly.
- You get lots of system error messages.
- The operating system will not load when you start your computer.
- You notice that files or folders have been deleted or changed.
- You notice hard disk access when you're not aware of any programs running.
- Your web browser behaves erratically, e.g. you can't close a browser window.

Don't panic if you experience any of the above. You may have a hardware or software problem, rather than a virus, worm or Trojan. Here's what you should do:

- Disconnect your computer from the Internet.
- If your computer is connected to a local area network, disconnect it from the network.
- If your operating system will not load, start the computer in Safe Mode (switch on the computer, press and hold F8, then choose Safe Mode from the menu), or boot from a rescue CD.
- If you don't have a recent backup, back up your data.
- Make sure your anti-virus signatures are up-to-date. If possible, don't download updates using the computer you think is compromised, but use another computer (e.g. a friend's computer). This is important: if your computer is infected and you connect to the Internet, a malicious program may send important information to a remote hacker, or send itself to people whose e-mail addresses are stored on your computer.
- Scan the whole computer.

- If a malicious program is found, follow the guidelines provided by your Internet security vendor. Good security programs provide the option to disinfect infected objects, quarantine objects that may be infected, and delete worms and Trojans. They also create a report file that lists the names of infected files and the malicious programs found on the computer.
- If your Internet security software doesn't find anything, your machine is probably not infected. Check the hardware and software installed on your computer (remove any unlicensed software and any junk files) and make sure you have the latest operating system and application patches installed.
- If you have any problems removing malicious programs, check your Internet security vendor's web site for information on any dedicated utilities that may be needed to remove a particular malicious program.
- If necessary, contact your Internet security vendor's technical support department for further advice. You can also ask them how to submit a sample file for analysis by a virus researcher.

If you think you're infected:

- ✓ Don't panic.
- ✓ Disconnect your computer from the internet.
- ✓ Backup your data.
- ✓ Update your anti-virus signatures.
- ✓ Scan your computer.
- ✓ If nothing is detected, check for software and hardware problems.
- ✓ If you still have a problem, contact your Internet security software vendor.

A final note about identity theft

Remember that offline security is important too. Physical data can be used by identity thieves to access your online accounts. Invest in a shredder (ideally a cross-cut shredder) and destroy any document that includes personal data (name, address, date-of-birth, etc.) before you throw it away.

Buy a cross-cut shredder and destroy any documents that include personal data before you throw them away.

Useful web sites

www.kaspersky.co.uk	www.banksafeonline.org.uk
www.securelist.com	www.cardwatch.org.uk
www.getsafeonline.org	www.antiphishing.org
www.identitytheft.org.uk	

An extensive glossary of definitions for words and phrases used in this guide can be found online at <http://www.securelist.com/en/glossary>.