

The British Chambers of Commerce guide to IT Security.



**BCC**  
THE BRITISH  
CHAMBERS OF  
COMMERCE



THE BRITISH  
CHAMBERS OF  
COMMERCE



## British Chambers of Commerce

The British Chambers of Commerce appreciates the power of technology and what it can do for your business. As well as the benefits, we understand the risks that can arise from using technology and, more importantly, we know that these risks can be minimised. That is why we have worked with Microsoft® to produce this guide, which we hope will help businesses like yours thrive and prosper safely.

We believe that it is important to understand all the computer security risks that are relevant to your business. Not only will this allow you to address them with confidence but also it will reduce the fear of the unknown. On a more practical basis, making your business safer and more resilient has obvious benefits.

Technology advice is only one aspect of our work. As an independent, non party-political organisation, funded by membership subscriptions, no-one is working harder on your behalf to make business better for everyone.

At all levels, local, regional and national, we provide a powerful voice. Our regular surveys, consultations and reports provide grassroots business opinion and strongly influence Government Ministers and officials, MPS and other decision-makers and opinion-formers.

We are the national voice of local business and the range of our involvement in helping businesses to grow and move forward includes: business training, networking, information and advice and international trade services. Increasingly, many of our services are also available online and all are uniquely tailored to individual business needs.

Currently over 135,000 businesses benefit from membership, from all commercial and industrial sectors and in every part of the UK. If you would like to join them or find out more about how membership can help your business, please visit us at [www.chamberonline.co.uk](http://www.chamberonline.co.uk).

## Microsoft bCentral™

Microsoft is the worldwide leader in software services and Internet technologies for personal and business computing. We offer a wide range of products and services designed to empower people through great software and we take our responsibility to business customers very seriously. We understand the unique challenges you face, and how the right technology can help your business to succeed. At Microsoft, we believe that the right technology is critical to overcoming core business challenges. But we don't stop at delivering great software. Microsoft bCentral.co.uk is an online information resource that is designed specifically for small businesses. It offers business-critical information, services and advice to businesses across the UK. It gives users comprehensive advice and tips on marketing, finance, technology and administration and can be found at [www.bCentral.co.uk](http://www.bCentral.co.uk).



# Computers

and the Internet are now indispensable to business success but they open us up to new threats, some of which are business-killers.

This is why I am delighted to introduce this, the third business guide we have produced in conjunction with Microsoft. Whereas the first two dealt with ways in which new technology can help business, this one shows how we can use it safely and confidently.

Although the topic can seem remote and somewhat technical, this guide does a good job of making it accessible to the business reader.

More importantly, it is clear that the steps required to achieve a reasonable level of security are not hard work, expensive or beyond the ability of anyone savvy enough to be running their own business.

A handwritten signature in black ink that reads 'David J. Frost'.

*David Frost*  
*Director General British Chambers of Commerce*

# contents

- 4 Why information security matters**
- 5 When bad things happen to good companies**
  - 6 Virus fever
  - 6 Gone in 6.0 seconds
  - 6 War driving
  - 7 How much are you paid?
  - 7 Script kiddies
  - 8 Email today, gone tomorrow
- 9 22 Questions that could save your business**
  - 9 General knowledge
  - 9 Plans, policies and people
  - 9 Physical security
  - 10 Information security
- 11 10 easy steps to improve security**
  - 11 Install virus protection
  - 11 Set up a firewall
  - 13 Keep your software up-to-date
  - 14 Use strong passwords
  - 14 Ensure physical security
  - 15 Take special care of laptops
  - 16 Connect remote users securely
  - 16 Lock down wireless networks
  - 17 Browse the web defensively
  - 17 Backup, backup, backup
- 19 How to write a security plan**
  - 19 Audit
  - 19 Plan
  - 20 Execute
  - 20 Monitor and repeat
  - 20 Finding the right technology partner
- 21 Intelligent Widgets Security Plan**
  - 21 Introduction
  - 22 Audit results
  - 24 Security plan
  - 26 Resources and budget
- 27 It's all geek to me: hacking explained**
  - 27 Networks, internets and the Internet
  - 28 Viruses, worms, Trojan horses, spam and hoaxes
  - 28 Why software is vulnerable
  - 29 How hackers hack
- 30 Information online**
- 31 Glossary**

# Why information security matters

The first law of security says it all: “Nobody believes anything bad can happen to them, until it does”. In fact, bad things do happen and surprisingly often.

More than two-thirds of UK businesses have lost a laptop or suffered a virus attack in the last year, according to the National High Tech Crime Unit. The risks involved are expensive. According to a DTI survey the average cost of a security breach is £30,000 and one in five incidents caused disruption lasting more than a week.

Fail to secure your computers and you run the risk of people accessing your private files, hijacking your resources, vandalising your website or infecting your system with viruses. Against these risks, the cost of upfront investment in security, whether it is a cash or time cost, seems like a sensible insurance policy.

It's common sense. You wouldn't leave your building unlocked at night. It's the same with information security. A few simple steps can make you a lot less vulnerable. So-called technology experts can make it seem like a huge and inscrutable problem. Luckily, it's much simpler than it looks.

The best approach is strategic. Step back, see how good (or bad) your existing security measures are and then make a plan so that information security becomes part of your day-to-day business operations and not just a one-off, box-ticking exercise.

This booklet contains a self-diagnostic questionnaire, detailed guidance on the steps you need to take to increase security and advice on creating a comprehensive plan.

It is written for the business person not a technician but don't be afraid to ask for professional support if you need it, either from your IT supplier or from a professional security consultant.

Of course, one hundred per cent security guarantees don't exist, but properly weighing risks and consequences against the cost of prevention is a good place to start. Now that IT is central to most businesses, doing nothing is simply not an option.

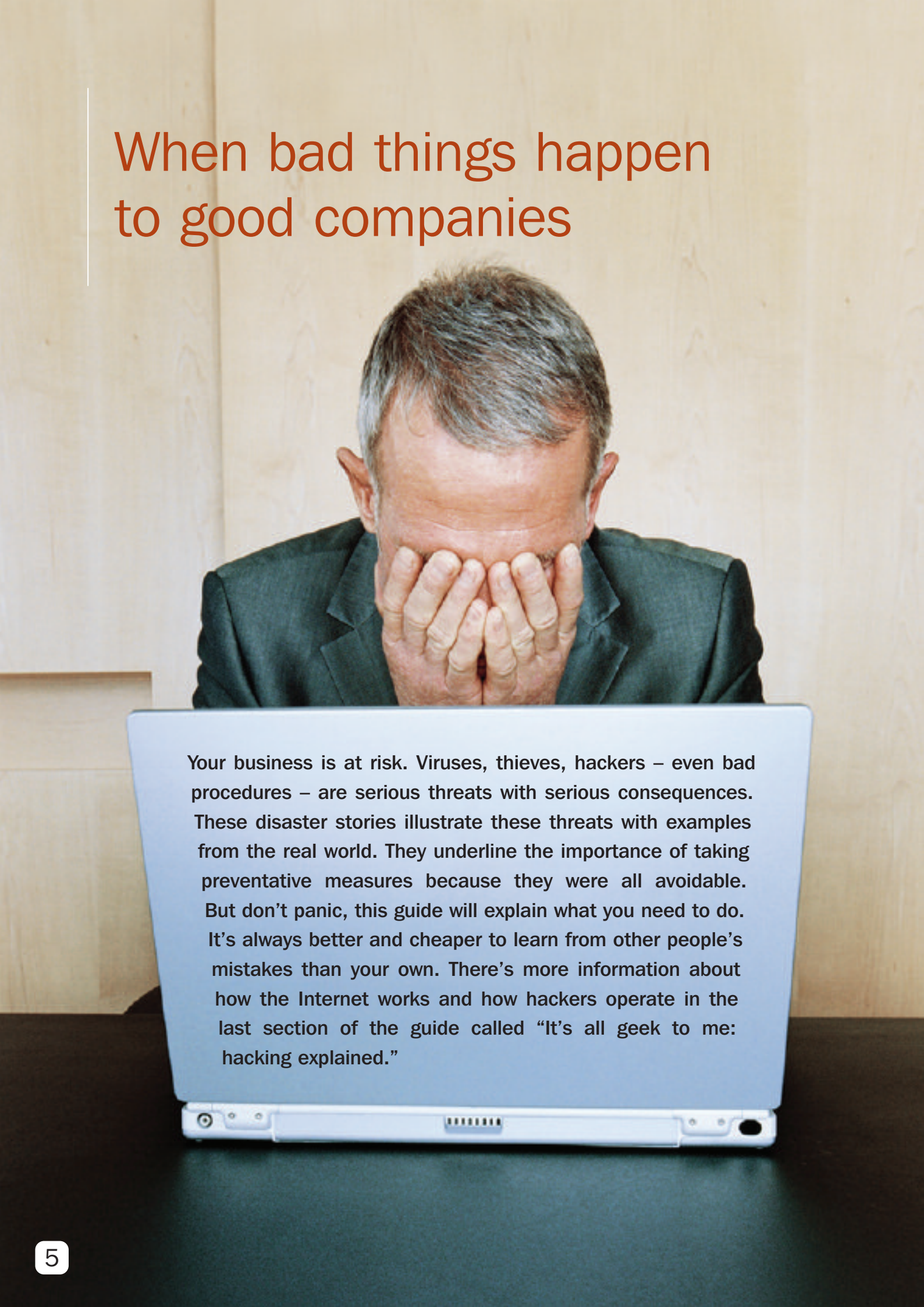
## 10 Easy steps to security

- 1. Install virus protection**
- 2. Set up a firewall**
- 3. Keep your software up-to-date**
- 4. Use strong passwords**
- 5. Ensure physical security**
- 6. Take special care of laptops**
- 7. Connect remote users securely**
- 8. Lock down wireless networks**
- 9. Browse the web defensively**
- 10. Backup, backup, backup**

“ Last year, 67% of companies suffered a virus attack

”

# When bad things happen to good companies

A man with grey hair, wearing a dark suit jacket, is sitting at a desk. He has his hands pressed against his face, covering his eyes, suggesting a state of distress or frustration. In front of him is a silver laptop. The background is a light-colored wood-paneled wall.

Your business is at risk. Viruses, thieves, hackers – even bad procedures – are serious threats with serious consequences. These disaster stories illustrate these threats with examples from the real world. They underline the importance of taking preventative measures because they were all avoidable. But don't panic, this guide will explain what you need to do. It's always better and cheaper to learn from other people's mistakes than your own. There's more information about how the Internet works and how hackers operate in the last section of the guide called "It's all geek to me: hacking explained."

## Virus fever

In April 2003, Internet users around the world started receiving emails containing pornography from friends and relatives. A few found their Internet access terminated because they were accused of sending spam emails. Others found themselves signed up to newsletters they didn't want. It was clear something peculiar was going on.

As accusations flew around the Internet, security experts quickly realised that a new virus, known as 'Klez' was responsible. It used several tricks which helped it spread quickly. It conned users into thinking that infected emails were being sent by real people using addresses plucked from infected users' address books. This had the secondary effect of clogging up email systems with unnecessary warnings, replies and recriminations. It tempted users into opening infected messages with beguiling subject lines like "a very funny website," or "undeliverable mail."

As if this wasn't enough, later incarnations of the virus made users' files the vehicle for infection. It would trawl through an infected computer's hard disks and pick a likely-looking document, infect it and then forward it to other users by email. In many cases, this meant that people's private files were sent out into the public domain.

It exploited a problem in Microsoft Outlook® email software that had been discovered and fixed a year earlier with a free downloadable patch. Anti-virus software developers became aware of it and updated their detection software within days and yet the virus raged for several months. In other words, this destructive and aggressive virus was 100% preventable. Klez was one of the most virulent viruses of the year, but it is one of thousands that appear annually.

## Gone in 6.0 seconds

"I was playing pool in the pub with a friend. I had my laptop bag right by my feet. I thought I was taking good care of it but I didn't feel a thing when it was pinched."

A stolen computer can fetch up to 50% of its retail price. No wonder tens of thousands of laptops are stolen every year in the UK.

This hapless executive's story is repeated thousands of times a year and it doesn't end when the laptop is replaced. Lose a laptop, lose vital work. Nicholas Negroponte, founder of the MIT Media Lab, ran into



trouble when a security guard asked him the value of the laptop he was carrying. He replied, "roughly US\$1 to \$2 million". Although the replacement value of the computer was a couple of thousand dollars, the value of the information it contained was much greater. Imagine if it had been stolen. It doesn't help if you're a security expert – in March 2000 an MI5 agent had a laptop stolen at Paddington station and an MI6 agent left his computer in a cab after a pub crawl.

Given the number of computers stolen every year, it is surprising how few users bother to encrypt their data or use strong passwords that prevent unauthorised access and how few companies bother to train their staff on basic security measures.

## War driving

A war driver is not an extra from a Mad Max movie but a new breed of hacker. Anyone with a laptop, a cheap wireless network card, freely downloaded software and an antenna made from an old crisp packet can hack into wireless networks in homes and companies from hundreds of feet away.

Most wireless networks are completely insecure. An extensive 2002 survey found that 92% of wireless networks in London had not taken basic steps to restrict access. That's over 4,500 networks that are wide open to people freeloading Internet bandwidth or, worse, snooping on private data. More recently, KPMG, an accountancy firm, set up three 'honey pot' networks in London. Designed to look like normal wireless networks to intruders, they monitor illicit activity. They were hit, on average, 3.4 times a day. War driving is more than a geek prank – some of the intruders tried to access files and damage systems.

However, it is relatively easy to secure a wireless network and the majority of war drivers can be deterred or deflected by a few simple steps. It is an avoidable problem.

“ Last year, 77% of companies lost a laptop

”



## How much are you paid?

Would you like your entire staff to know how much you are paid? Or the entire company's payroll information? What would that information be worth to your competitors?

James is a senior manager in a successful manufacturing firm. His computer had a problem, so he called his IT department. A technician arrived quickly, logged into the network using his administrator's password and fixed the problem. Under pressure to get to the next job, he scuttled off as soon as he finished. He did not, however, log out of the system. James, being a canny career man, decided to have a bit of a rummage. He quickly found a spreadsheet that had information on the salaries of all his colleagues and the bosses above him. He made a mental note to ask for a substantial pay rise. Luckily, for his employer, that was all he did with the information; but imagine if he had been a disgruntled junior employee or about to jump ship.

Technology is only part of the answer. The best hardware and software isn't enough if you don't have good policies and procedures in place as well.

## Script kiddies

John, the web manager of a small commercial website selling niche software was very pleased with his new site. It was a big improvement on the old one. Now the company had its own web server and broadband connection, they didn't have to pay anyone to host the site. He went home on Friday night a happy man.

On Monday morning, when he got back to work, it was a different story. Over the weekend, hackers had gained access to the site and had deleted his carefully crafted site and replaced it with porn.

Not only that, but hundreds of thousands of people had been avidly downloading the porn from the site over the weekend. His bandwidth usage had shot through the roof and the company was facing a bill for thousands of pounds. His boss had already started to receive emails from customers complaining about the site.

An antivirus software developer reported earlier this year that corporate servers receive, on average, 30 attacks a week. Most of these are from dedicated amateur hackers, known as 'script kiddies', who use tools that are freely available on the Internet to probe corporate networks for weaknesses. These tools scan the Internet quickly and at random looking for vulnerable systems and then exploit any weaknesses they find. This means that a small, anonymous company is as much at risk as a well-known multi-national.

Many of these tools exploit known vulnerabilities that can be easily plugged. For example, back in 2001, a group of hackers calling themselves the SmOked Crew used a well-known and previously-patched vulnerability in web server software to deface websites belonging to Intel, Gateway, Disney and The New York Times. However, a patch to fix the vulnerability was available long before the attack but many administrators had not installed it. This vividly illustrates the need to take sensible precautions in general, and use up-to-date software in particular.

---

## Email today, gone tomorrow

Kevin was the managing director of a growing software firm. With 65 employees and a number of multi-national clients, the company relied on its email system to keep in touch. In particular, they used email to track change requests from their clients so it was a vital part of the company's business, like a lawyer's filing system or a doctor's records. Then one day, their email server had a catastrophic hardware failure and the data was corrupted.

"No problem," thought Kevin, "our IT guy has a backup so we can just restore it from that." In fact, the company had an elaborate tape library and dutifully kept offsite copies of its critical backups. It was only after a day's work trying to restore the email system from the backup tapes that the IT team realised that the data hadn't been properly backed up. They had never noticed the problem and had never tested whether restoring the data worked properly. Nor did they have any kind of disaster recovery plan. Information security isn't solely about getting the right hardware and software; it is about getting the processes right and concentrating resources on business-critical systems.

“ Less than  
a fifth of  
companies  
carry out  
security  
audits  
”



# 22 Questions

*that could save your business*

## General knowledge

### 1. What's a firewall?

- a. A method of protecting a computer network against unauthorised access from the Internet (1 point)
- b. A solid brick enclosure around a server room

### 2. Why do software developers issue patches to update their software?

- a. Because they didn't get the software right in the first place
- b. Because thousands of hackers are constantly trying to find previously-unknown vulnerabilities and the software companies want to protect users against these threats (1 point)

### 3. Which of the following are forms of hacking?

- a. Spoofing
- b. Tampering
- c. Repudiation
- d. Information disclosure
- e. Denial of service
- f. Elevation of privilege
- g. All the above (1 point)

### 4. Have you or your business suffered any of the following and taken active measures to prevent it happening again? (1 point each)

- a. Laptop theft
- b. Other computer theft
- c. Unauthorised disclosure of information by staff or outsiders
- d. Loss of critical data which wasn't backed up
- e. Virus infection
- f. Any kind of hacking or electronic intrusion

## Plans, policies and people

### 5. Do you have a senior manager or director overseeing security issues?

- a. Yes (1 point)
- b. No

### 6. Do you have an up-to-date security plan?

- a. Yes (1 point)
- b. No

### 7. Is there a manager responsible for ongoing compliance?

- a. Yes (1 point)
- b. No

### 8. Do you carry out regular equipment and software inventories?

- a. Yes (1 point)
- b. No

### 9. Does your company have up-to-date policies covering the following? (1 point each)

- a. Strong passwords
- b. Email and Internet use
- c. Software piracy
- d. Online purchasing
- e. Theft
- f. Data Protection Act compliance

### 10. Do your health and safety policies and practices take account of IT-specific risks, such as RSI and eye strain?

- a. No
- b. Yes (1 point)

## Physical security

### 11. What physical security measures do you take to protect your desktop PCs? (1 point each)

- a. General perimeter security including good locks, alarms and physical barriers
- b. Visitor access control
- c. Locked securely to desks
- d. Components security marked
- e. Not visible from the street on the ground floor
- f. Boxes from new computers disposed of discretely

### 12. And your servers? (1 point each)

- a. Kept in a secure room
- b. Access restricted to authorised, vetted personnel
- c. Adequate fire protection
- d. Each component security marked

**13. And your laptops? (1 point each)**

- a. Transported in padded but nondescript bags
- b. Secured by a cable lock when unattended
- c. Components security marked
- d. Data on the laptop encrypted
- e. Do you use a BIOS password and are booting from floppy or CD-ROM disabled?

**14. What physical security measures do you take to protect software and backups? (1 point each)**

- a. Application master disks and licence documents kept securely
- b. Backups stored in a fireproof safe or offsite

**15. Do you have a maintenance contract for your computer equipment?**

- a. Yes (1 Point)
- b. No

**16. Do you vet your IT staff or contractors?**

- a. Yes (1 Point)
- b. No

**Information security**

**17. Have you ever opened a file in an email from someone you didn't know because it looked 'interesting'?**

- a. Yes (-1 point)
- b. No (1 point)

**18. Which of the following defences do you have operating in your business? (1 point each)**

- a. Firewall

- b. A second firewall from a different supplier
- c. Anti-virus software
- d. Update virus 'signatures' on a regular basis
- e. Always install software patches when they become available
- f. Regular backups
- g. Centrally enforced strong password policy
- h. Spam filtering software

**19. Is your data regularly backed up?**

- a. No
- b. Yes (1 point)
- c. Bonus point: and we test restoring the data periodically

**20. Do you use the security features built into Internet Explorer and Outlook?**

- a. Yes (1 point)
- b. No

**21. Do remote users accessing your network use secure links, with encryption and strong passwords?**

- a. Yes (1 point)
- b. No

**22. If you use wireless networking, have you taken all necessary steps to prevent hackers eavesdropping or freeloading on your internet connection?**

- a. We hide the identity of our wireless network and prevent unauthorised snooping and access (1 point)
- b. Huh!? What? We just took it out of the box and plugged it in (-5 points)

**Questionnaire results**

**Less than 10** Don't just sit there. Panic!

**11 to 20** You know you need security but you either don't have the skills, time or confidence to do something about it. You are at serious risk and you need to take steps urgently to protect your business.

**21 to 30** You are like many people, some good intentions and some half-measures but in your heart you don't really think something bad can happen to you. There are things you can do now that will transform your security from 'barely adequate' to 'good enough'.

**31 to 40** You're doing pretty well. Look through this guide and see if there's anything you've missed. There may be a few tricks you've overlooked and some risks you haven't considered.

**41 to 50** You're close to security nirvana. It's probably worth scanning this guide to see if there's anything you've overlooked and don't forget about the need to keep reviewing your security and updating your plans.

**Over 50 points** Do you run a security consultancy?

# 10 easy steps to improve security

This section outlines the basic security measures that every company needs to take to help protect itself. Use the glossary and the section called “It’s all geek to me: hacking explained” at the end of the guide to explain anything that seems too technical. These steps are most effective if they are part of a comprehensive security plan that also factors in people, procedures and policies.

The next section of the guide covers writing such a plan.



resources. Some may allow outsiders access to your files. All of them take time to eradicate and, if passed on to friends, customers or colleagues, can be very embarrassing.

**How:** There are four simple measures that can dramatically reduce the risk of virus infections.

## 1. Install virus protection

**Summary:** Prevent virus infections by installing anti-virus software and updating it regularly. Don’t open suspect files. Use the security features built into your email software. Consider using anti-spam software.

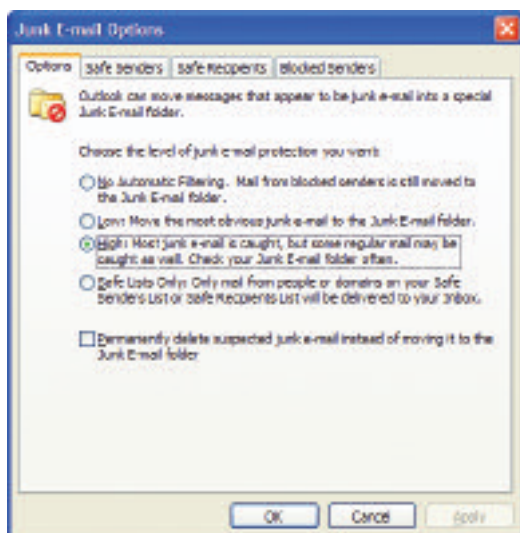
**What:** Viruses (and their cousins, worms and Trojan horses) are malicious programs that infect computers. The infection starts when a user runs an infected program, usually when it is attached to an email or downloaded from a website. Viruses can also be embedded in web pages and emails formatted to look like web pages (‘HTML format’ emails) and these can run simply when the page or email is viewed. Often these files are very enticing or deliberately misleading. Once infected, a PC can spread the virus to other users.

**Why:** Different viruses have different effects. Some delete or change files. Others hog computer

- **Buy and install anti-virus software.** This should be installed on every computer on a network. Virus scanners work by scanning the contents of incoming emails (and files already on your computer) looking for virus signatures. If it finds a virus, it will simply delete it. A signature is like a unique DNA sequence in the virus’s computer code. Since there are hundreds of new viruses a month, all anti-virus software has to be updated regularly with the latest signatures so that it can catch the latest viruses. Out of date software is no good. Look for software that will automatically download the signature information from the Internet. It is also possible, as an additional line of defence, to install software on an email server so that every piece of email coming into a company is scanned. Some Internet service providers do this automatically.



- **Don't open suspect files.** The golden rule is do not open any file attached to an email from an unknown, suspicious or untrustworthy source, no matter how beguiling it may seem. Be similarly careful when visiting suspect websites or downloading files from the Internet. Better safe than sorry.
- **Be aware that hoax emails about viruses (along with chain letters and other daft correspondence) are almost as common as viruses themselves.** Check with a trusted source, such as the manufacturer of the anti-virus software you use, before forwarding one of these emails on to other people. Educate other users to be similarly circumspect.
- **Use the security features built into Microsoft Outlook.** Microsoft Outlook 2003 has good security features built in and switched on by default. If you use Microsoft Outlook Express, there are a couple of things you may need to do. First, if you are running a version older than 6.0, upgrade to the latest version ([www.microsoft.com/windows/ie](http://www.microsoft.com/windows/ie)). Second, increase Microsoft Outlook Express security by turning on its ability to block certain types of file attachments. Here's what to do: **select Tools then Options, click on the Security tab, find the checkbox labelled "Do not allow attachments to be saved or opened that could potentially be a virus." Check it. Click the OK.** This ensures that the program will check with you before opening any potentially harmful program.
- **Block spam.** Spam is unsolicited commercial email and it's on the rise. Around half of all email being sent around the world is spam. Some of it carries viruses. Some of it is offensive. The average employee spends about an hour a day dealing with email, so it has a clear impact on productivity. Microsoft Outlook 2003 features automatic spam protection. To switch it on, **select Tools then Options and click on the Junk Email... button.**



Picture source: Junk Email Dialogue Box

Consider buying commercial spam-blocking software, from companies like Cloudmark or MailFrontier, especially if you use an older email program.

#### Where next:

For general information about viruses:

[www.microsoft.com/security/antivirus](http://www.microsoft.com/security/antivirus)

For a comprehensive list of suppliers see:

[www.microsoft.com/security/partners/antivirus.asp](http://www.microsoft.com/security/partners/antivirus.asp)

Anti-spam software:

[www.cloudmark.com](http://www.cloudmark.com), [www.mailfrontier.com](http://www.mailfrontier.com)

For an online database of known Internet hoaxes, see:

<http://hoaxbusters.ciac.org>

You can download an informative explanation of how spam works from MessageLabs:

[www.messagelabs.com/viruseye/research/default.asp](http://www.messagelabs.com/viruseye/research/default.asp)

## 2. Set up a firewall

**Summary:** Stop outsiders from hacking into your network over the Internet by installing a commercial firewall product and switching on Internet Connection Firewall.

**What:** Firewalls protect your local network from outside attacks by screening out unwanted communication. Think of it as a paranoid switchboard operator who only puts Internet 'calls' through when they are safe and tells everybody else 'he's in a meeting'. Firewalls block all traffic between your network and the Internet that you haven't explicitly allowed. They can also hide the addresses of the computers behind the firewall making the whole of your network invisible to outsiders.

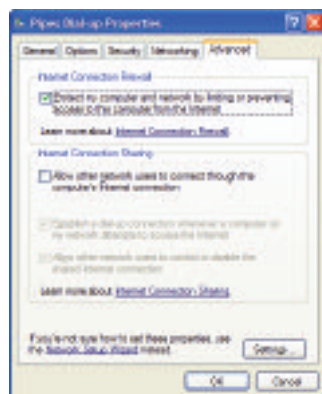
**Why:** Hackers with port scanners can scan through thousands of randomly chosen IP addresses and test each one of them to see if any ports are open. This means that they find your network and potentially target individual machines on it over the Internet, even if they don't know you exist. It's like dialling random numbers in the phone book. Armed with a valid computer address they can try to exploit vulnerabilities in software (especially if it hasn't been patched), try to crack passwords to gain access to the network or attempt to snoop on your data. A firewall isn't sufficient on its own to guarantee security, but it is the first line of defence.

**How:** Firewalls come in two basic flavours: hardware and software. Hardware firewalls are often integrated into the router supplied by your Internet service provider to connect your network to the Internet. Software firewalls typically run on a machine that sits between the Internet and the rest of your network. All firewalls provide similar functionality but what kind of firewall you need depends on how your network is set up and connected to the Internet. However, it is considered good practice to use two different makes of firewall.

If you have a single machine connected to the Internet by a modem or broadband connection, you can use Internet Connection Firewall, which is built into the Microsoft Windows® XP operating system. See below for instructions on how to set this up. You may want to consider adding a second commercial firewall for belt-and-braces protection. McAfee, Symantec and ZoneLabs, among others, make firewall software, and ZoneLabs is free for personal use.

If you have a small network sharing a single Internet connection via Internet Connection Sharing (a Microsoft Windows XP feature), then you can still use Internet Connection Firewall on the machine that is directly connected to the Internet and this will protect all the connected machines. If you use a commercial firewall, check that it supports Internet Connection Sharing. In addition, many Internet service providers supply a router to link their broadband connection with a network and these usually have firewall features. Check with your supplier to see if this is the case.

To switch on Internet Connection Firewall, **click Start and open the Control Panel, then click on Network Connections. Right click on the connection you use to get on the Internet (typically a modem or a local area network connection to a router) and select Properties from the pop-up menu. When the dial-up connection properties dialogue box appears, just check Protect my computer.** That's it.



Picture source: Internet Connection Firewall

A firewall can sometimes block activities that you want to allow, such as instant messaging or hosting multiplayer games. If this happens, don't switch off the firewall. In the case of Microsoft Internet Connection Firewall, refer to: [www.microsoft.com/security/protect/ports.asp](http://www.microsoft.com/security/protect/ports.asp) for further instructions.

For other firewalls, refer to the manufacturer's instructions.

#### What a firewall does NOT do

It is important to remember that a firewall is only the front line. No matter how effective it is, a firewall will not protect against:

- Malicious traffic that does not travel through it, for example traffic that gets into the network via a poorly configured wireless network.
- Attacks after a network has been compromised, for example if a hacker is able to exploit

*vulnerabilities in your operating system software or if it has been opened from within.*

- Traffic that appears to be legitimate.
- Viruses, including those that might seek to open a loophole in your security.
- Users and administrators who use weak passwords.

#### Where next:

Firewall software: [www.mcafeesecurity.com](http://www.mcafeesecurity.com), [www.symantec.com](http://www.symantec.com), [www.zonelabs.com](http://www.zonelabs.com)

For a technical description of how firewalls work see: [www.microsoft.com/technet/security/topics/network/firewall.asp](http://www.microsoft.com/technet/security/topics/network/firewall.asp)

To test your vulnerability: try ShieldsUP!, go to [www.grc.com](http://www.grc.com) and follow the links for 'Shields Up'

For an excellent introduction to the world of hackers, including interviews and useful background reading see: [www.pbs.org/wgbh/pages/frontline/shows/hackers/](http://www.pbs.org/wgbh/pages/frontline/shows/hackers/)

## 3. Keep your software up-to-date

**Summary:** Download and install the latest patches and updates for your software so you can stay one step ahead of the bad guys.

**What:** Hackers try to find and exploit bugs and loopholes in popular software, partly for kudos, sometimes for profit. When Microsoft discovers a vulnerability in its software it releases an updated version for people to download over the Internet. This is called 'patching'. Also, over time the fundamental architecture of computer systems becomes more robust and secure so that, for example, the Microsoft Windows XP operating system is inherently much safer than Microsoft Windows 95.

**Why:** Many virus infections and hacker attacks occur unnecessarily. Very often, patches exist that would have prevented the problem but users did not install them. If passwords are the door key and firewalls are your alarm system, installing patches is like making sure that you don't leave any windows open.

**How:** It's very easy to download and install the latest updates. For Microsoft Windows, go to [www.windowsupdate.com](http://www.windowsupdate.com), click Scan for updates and the website will automatically work out what you need to get, download and install the patches. For Microsoft Office, [www.officeupdate.com](http://www.officeupdate.com) does the same job.

If you are running an older operating system, particularly Windows 95 or Windows 98, you should consider buying an upgrade.

#### Where next:

[www.windowsupdate.com](http://www.windowsupdate.com), [www.officeupdate.com](http://www.officeupdate.com) (and click on Downloads and then click Check for updates), [www.microsoft.com/uk/howtobuy](http://www.microsoft.com/uk/howtobuy)

## 4. Use strong passwords

**Summary:** Don't make it easy for the bad guys to access secure systems by using easily-guessed or easily-cracked passwords. Educate users to select strong passwords.

**What:** A password is the most common way of authenticating your identity. Authentication relies on something you know (for example: a secret word or phrase or your mother's maiden name), something you are (such as a fingerprint or iris scan) or something you have (such as a crypto calculator or a physical key). Passwords are the most common because they are the easiest to use. However, they are also the most easily misused.

**Why:** Hackers use automated tools to crack passwords and can break a simple password in minutes. Social pressure or fraud can persuade users to divulge their passwords. The best security in the world is irrelevant if someone has your password.

**How:** First, let's look at weak passwords. These include:

- *Using no password at all.*
- *Using your real name, your user name or company name.*
- *A commonplace dictionary word.*
- *The most common password is 'Password' so that's an obvious one to avoid.*
- *Any password that you write on a post-it note on your monitor.*
- *A password you haven't changed in more than a couple of months.*
- *A password known by someone else.*

Conversely, a strong password (and it needn't be a word):

- *Is at least seven characters long.*
- *Does not contain your user name, real name, or company name.*
- *Does not contain a complete dictionary word.*
- *Is significantly different from previous passwords. Passwords that increment (Password1, Password2, Password3 ...) are not strong.*
- *Contains a mix of upper and lower case letters, numbers and keyboard symbols (i.e. ` ~ ! @ # \$ % ^ & \* ( ) \_ + - = { } | [ ] \ : " ; ' < > ? , . /)*
- *Is changed regularly.*

An example of a strong password is J\*p2le04>F.

Of course, a password you can't remember is no use at all, so there are some tricks that can make them more memorable. For example, Msi5!YOld (My Son is 5! years old), Ll5t5wds (Lucy !n The 5ky With Diamonds) or MyMOu5e (My Mouse).

You need to decide on a policy that balances security with practicality. Enforcing a tough policy on all users will mean that they just write down their passwords, creating its own perils. You can have different policies for different types of user and system – for example you might insist on stronger passwords for administrators or HR personnel.

Any policy also needs to take into account the risk of social engineering and human weakness. Encourage users to think of their passwords in the same way as they would think of a key to the office – don't leave it lying around and don't give it to strangers or colleagues.

Microsoft Windows XP and Microsoft Small Business Server 2003 have systems that can enforce a given password policy and lock users out who fail to comply. It is also sensible to set up computers so that they lock users out after so many minutes of inactivity. This prevents people from wandering away from their desks and leaving their computer wide open and still logged in.

### Where next:

To set up a lockout policy:

[www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/password\\_lockout\\_concept.asp](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/password_lockout_concept.asp)

Password policy:

[www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/password\\_group\\_policy.asp](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/password_group_policy.asp)

## 5. Ensure physical security

**Summary:** Keeping your office computers safe and preventing physical access to workstations and documents is a vital component of e-security and important in its own right.

**What:** Locks, alarms, lockable filing cabinets, visitor logging, computer locks, asset tagging.

**Why:** Not all catastrophes are caused by insidious hackers working over the Internet, sometimes a casual break-in can be more damaging and the best firewalls will not keep out someone sitting at your server or a local PC.

**How:** Here's a step-by-step guide and checklist for improving the physical security of your business information and computers:

1. Establish a security perimeter around the premises using, as appropriate, walls, self-shutting, lockable doors, alarms, security curtains etc.

2. Where outsiders do come inside the perimeter, make sure that these points are manned and that visitors are identified and logged as they come in and out.
3. Where possible, restrict access to sensitive areas, such as server rooms or HR records, with additional barriers. Review who has access to what on a regular basis. Only authorised users should be permitted to enter these areas and visitors should be escorted. Staff should be encouraged to query unescorted strangers in secure areas.
4. When picking a location for a server room or other vital area, consider risks like fire and flooding. If necessary, consider installing fire extinguishers.
5. Lock your doors and windows when they're not in use.
6. Test alarms regularly.
7. Have a 'clear-desk' policy so that people secure sensitive or valuable materials when they are not working on them.
8. Security mark PCs and their major components.
9. Log serial numbers of PCs so that they can be identified if stolen and recovered.
10. Unattended fax machines and mail hubs need to be protected.
11. Encourage users to pick up their documents from printers and photocopiers promptly.
12. Make sure that your policies for staff cover what equipment may be taken off-site. Sign valuable items out to individuals and make them responsible for their return.

You should also consider carrying out a complete risk assessment in conjunction with your insurance company and the local crime prevention officer and, possibly, independent advisors.

**Where next:**

[www.met.police.uk/computercrime](http://www.met.police.uk/computercrime) and [www.nhtcu.org](http://www.nhtcu.org)

## 6. Take special care of laptops

**Summary:** Take extra care with laptops.

**What:** Laptops by their very nature are easy to steal and easy for criminals to sell on.

**Why:** Out of roughly five million laptops in the UK, about 100,000 are damaged each year and another 67,000 stolen. Besides the hassle and cost of replacement, there is the risk that a stolen

laptop will contain hard-to-replace or confidential information. If the bad guys have physical control of your laptop they will almost certainly be able to access the data on it.

**How:** Here is our 10 point plan for laptop security:

1. Keep your laptop in a padded bag to protect it against knocks and falls, but don't use one that looks like a laptop bag or one with a prominent manufacturer's logo on it.
2. Always keep it in sight. This is particularly true in crowded public areas like train stations and airport security checkpoints, but also at meetings and conferences.
3. When travelling keep laptops in your hand luggage and don't leave them in hotel baggage-hold rooms.
4. Lock the laptop to something and consider removing the hard drive (if this is possible) when it is not in use. Consider purchasing a cable lock.
5. Security mark your laptop. Keep a record of your laptop's serial number and keep a note of all the software on it.
6. Never leave a laptop in plain sight in a locked car.
7. Don't let your laptop overheat, for example by leaving it in the boot of a baking parked car.
8. Always keep a backup of all the work stored on a laptop before a trip and, if possible, continue to make backups of work you do on the road. Emailing new documents home is one way to do this. Don't take sensitive files with you on a given trip unless you actually need them.

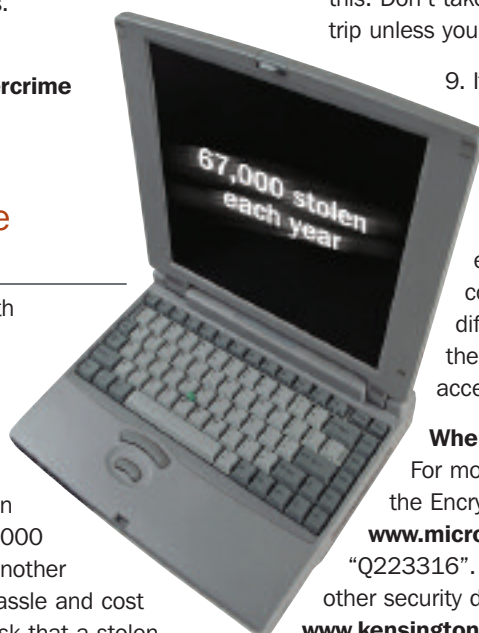


9. If possible, use a BIOS password and disable booting from a floppy disk or CD-ROM (refer to your computer manual to find out how).

10. Use Microsoft Windows XP's encrypted file system to secure confidential files. This will make it difficult for unauthorised users to open these files even if they have physical access to them.

**Where next:**

For more advice about the Encrypted File System go to [www.microsoft.com/support](http://www.microsoft.com/support) and search for "Q223316". Kensington make cable locks and other security devices for laptops: [www.kensingtonuk.co.uk](http://www.kensingtonuk.co.uk)



## 7. Connect remote users securely

**Summary:** Ensure that you make full use of encryption and authentication technologies when connecting to your company's network over the Internet.

**What:** It is very useful for remote users, people working at home, on the road or in branch offices, to have access to a company's network. Linking remote users and the network together over the Internet is very efficient because it means there is no need for dedicated (and expensive) leased lines and dial-in users can use a local phone number to connect to any Internet service provider rather than make a long-distance call back to the home office. Connecting over the Internet like this is called a virtual private network (VPN). Encrypting the data as it travels over the public Internet stops outsiders being able to read it and authenticating users makes sure that only legitimate users can connect.



**Why:** Remote access to networks, including email, is an important business capability. At the same time, making your network available to outsiders is a security risk. All data travelling over the Internet can be intercepted or interfered with.

**How:** First, make sure that your firewall is set up to allow VPN traffic.

Second, select a secure, encrypted communication protocol for the link. Windows XP supports the most common VPN format, Point-to-Point Tunneling Protocol (PPTP) as well as two newer, more secure formats: Layer-2 Tunneling Protocol (L2TP) and Internet Protocol Security (IPSec).

Finally, use strong passwords (or even better, biometric or token-based authentication such as fingerprint scanners or smart cards) to confirm the identity of users connecting to your network over the Internet.

### Where next:

To learn more about remote access (including virtual private networks):

[www.microsoft.com/technet/security/topics/mobile/default.asp](http://www.microsoft.com/technet/security/topics/mobile/default.asp)

## 8. Lock down wireless networks

**Summary:** Implement basic security measures to make wireless networks less vulnerable.

**What:** Wireless networking, which is sometimes known as Wi-Fi or 802.11 networks, use a radio link similar to a cordless phone to connect computers. Because they allow computers to be connected to a network without physical cables they make setting up a network very fast and flexible. They can be used to link PCs, laptops and PDAs to an access point which functions as a hub for all the computers connected to it. Alternatively, they can link computers together in an ad-hoc, peer-to-peer way without an access point.

**Why:** Precisely because they are wireless, they are more vulnerable than a cabled network. Anyone within radio range can, in theory, listen in or transmit data on your network. The point is that they don't need physical access to your hardware to do this. This can be a war driver in the car park snooping for secrets or a neighbour just trying to freeload off your Internet bandwidth. Freely available tools allow hackers to 'sniff' for insecure networks. Many manufacturers switch off the security features built into the Wi-Fi standard. Although this makes networks easier to set up, it means that by default most wireless networks are profoundly insecure.

**How:** The objective here is to make wireless networking as secure as possible on the assumption that someone will be snooping. Although the Wi-Fi standard defines things like encryption and access control, the way you set them up varies from manufacturer to manufacturer. This means that the advice will seem a little technical because it is only possible to say what you have to do, not how you do it. Consequently, you will need to refer to the documentation that came with your hardware to set these defences up.

- Use access points only rather than ad-hoc, peer-to-peer networks. Access points give more control.
- Switch off SSID broadcast. The SSID is the name of the wireless network. If you know this it makes it easier to hack in. In order to make setting up wireless networks easier, many access points are configured to broadcast this information to anyone who might be listening so that workstations can connect more easily.
- Choose an obscure SSID name. If SSID broadcast is switched off, a hacker has to enter the name of the network to connect, so like choosing a password, the more obscure the name the harder it will be to guess. By default most manufacturers use their own name as the SSID which means that even if broadcast is switched off, unless you change it most names will be easily guessed.
- If your access point allows it, restrict wireless access to normal office hours.
- Use MAC filtering. Each network card has a unique code called a MAC address. You can set access points to restrict access to certain, trusted MAC addresses. Although a MAC address can be

*hacked or deduced by an expert user this will filter out most casual intruders.*

- Switch on and use 128-bit WEP encryption to prevent eavesdropping. Use strong passwords for WEP.
- Restrict the ability of users (and network administrators) to set up 'quick and dirty' wireless networks, even temporarily. Manage wireless networks carefully and continually. One rogue access point can undo all the good work you do on the others.
- Make sure all your other security measures – passwords etc. – are in place so that you have a second line of defence against intruders.
- For maximum security, consider putting your access points outside your corporate firewall and have users connect into the network using virtual private networks with strong encryption and authentication.

**Where next:**

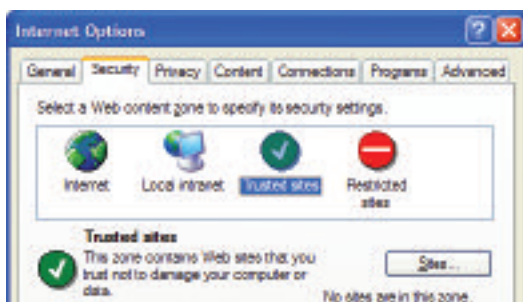
For more information on the risks of wireless networks see: [www.wardriving.com](http://www.wardriving.com). See your own manufacturer's website for detailed security guidance.

## 9. Browse the web defensively

**Summary:** Ensure that you browse the web safely.

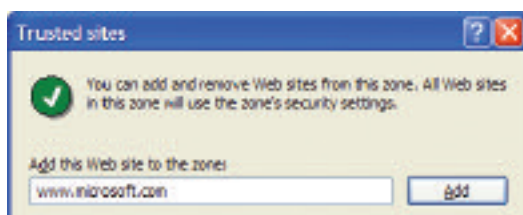
**What:** By categorising websites into different types, Microsoft Internet Explorer can control how much access they have to your computer.

**Why:** Web pages can contain programs. Normally these are innocent and do useful things like animation or pop-up menus. Sometimes, however,



Internet Explorer Security 1

Then click on the Sites button.



Internet Explorer Security 2

they can be harmful. In addition, files downloaded from the Internet can contain viruses.

**How:** Internet Explorer has a feature designed to restrict the damage that a rogue Internet site can do. It groups websites into one of three zones: Trusted, Restricted and Internet. When you start Internet Explorer for the first time, all sites are in the 'Internet' zone which has medium-level restrictions. You can allocate sites into the other categories. Restricted sites are the most constrained whereas trusted sites have maximum freedom.

To add a website to a different category, **go to the Tools menu and select Internet Options. Click the Security tab, and then click the security zone where you want to add the site: Local intranet, Trusted sites, or Restricted sites. Enter the name of the site you want to add to the list of Trusted sites and click Add. Then click OK twice.**

**Where next:**

For more detailed instructions and background information, visit:

[www.microsoft.com/windows/ie/using/howto/security/settings.asp](http://www.microsoft.com/windows/ie/using/howto/security/settings.asp)

## 10. Backup, backup, backup

**Summary:** Backup regularly as a vital insurance policy.

**What:** There are two parts to the backup problem: the hardware you use and your procedures. Having a fast, high capacity backup device is no good, if you don't back up all your data frequently enough. There are two basic kinds of backup: a complete backup and an incremental backup. The first is a complete copy of the data onto another medium – for example burning a CD with all your pictures on it. The second just backs up the data that has been added or changed since the last full backup – for example making a copy of only new pictures. This is generally going to be quicker and take less space but means you need each incremental copy of the backup for a full restore. Typically, you would use a full backup once a week and a fast incremental backup daily.

**Why:** Backups are the last line of defence against hardware failure, floods or fires, the damage caused by a security breach or just accidental deletion of data. Ask yourself what would happen if you lost all your critical business data – how long would it take you to recover? How much disruption and delay would occur?

**How:** First decide on the hardware. What are you going to use to backup? It depends mainly on how much data you have. There is also a question of price. Reusable media like tapes are more expensive to buy initially but can be overwritten. Write-once media like recordable CDs or DVDs are cheaper but can only be used once. Here is a rule-of-thumb guide:

Total data	Suggested medium
Under 700MB	Recordable CDs
Between 700MB and 5.2GB	Recordable DVDs
Between 2GB and 12GB	DAT Tapes
Greater than 12GB	DAT carousels or higher-capacity tape systems

Most CD-R and DVD+RW drives (the disc drives that can actually write CDs and DVDs respectively) come with easy-to-use backup software. Microsoft Windows XP comes with Microsoft Backup which will do full and incremental backups. Beyond that limit, you need to buy commercial software to run backups.

Also consider using highly resilient file servers (known as RAID Level 5) which stripe data across several disks at once which means that the server as a whole, and all the data on it, can survive the failure of a single disk drive. This is not an alternative to backup, but it does give extra business continuity. In the same vein, consider uninterruptible power supplies for servers.

Review what data is vital to your business and where it is. It may be distributed across individual PCs or stored on a central server. It may reside in your company's email system. It may be in the form of databases or word processor documents. Create a simple map of where the data is and try to quantify its importance. Your order book is more important than plans for the Christmas party, for example.

If data is stored on a variety of machines, it makes sense to schedule a regular backup on each machine to consolidate the data into a single place, typically on a server, so that it can be backed up in one go.

Identify who will be responsible for backups. Periodically test the integrity of backups by restoring some or all of the backed up data (but don't overwrite the existing data).

**Where next:**

For information about how to backup Outlook: [www.bcentral.co.uk/technology/office/tips/outlook/OutlookBackup.asp](http://www.bcentral.co.uk/technology/office/tips/outlook/OutlookBackup.asp)

For more information on how to use Backup, see: [www.microsoft.com/windowsxp/home/using/howto/maintain/backup.asp](http://www.microsoft.com/windowsxp/home/using/howto/maintain/backup.asp)



# How to write a security plan

You need a plan. Because e-security is not a one-off task, but an overlapping mesh of technology, people, policies and processes; a plan will help you co-ordinate the whole thing and make sure there are no gaps. It will also give a sense of proportion and priority.



There are four steps to creating a good security plan: audit, plan, execute and repeat.

First, find out where you are now. Use the questionnaire and 10 step plan earlier in this booklet as a checklist and apply it to all the computers in your business. Second, once you have completed the audit, prioritise action items according to the probability and likely impact of a problem. Third, taking each risk in turn, according to their priority, decide how to transfer, mitigate or avoid it (or, on consideration, live with it). Finally, put together a team, allocate resources and responsibilities and carry out your plan. Ensure on-going review and compliance.

A good plan today is better than a perfect plan tomorrow. By its nature, planning for e-security is a cyclical and repetitive process, never cut and dry, so it makes sense to execute a quick plan now and then refine and iterate it later.

## Audit

- Review your own skills and knowledge. Decide if outside help or training is required and find a partner if necessary.
- Analyse your current state of security using our questionnaire, 10-step plan and Microsoft Baseline Security Analyser.
- Identify assets that need to be protected, including hardware, software, data, documentation, people and their account information, administrative procedures and legal compliance (Data Protection Act etc.).
- Categorise your information according to its sensitivity on the following scale: public (website

data), internal (marketing data), confidential (payroll), secret (product designs or formulae).

- Identify services that are required, such as remote access, email etc.
- Predict threats: spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege. Consider using trusted third parties to test exposure.
- Calculate exposure for each asset and service against each threat:  $\text{probability} \times \text{impact} = \text{exposure}$  to generate an ordered list of security priorities.

## Plan

- Remember that the objective is not to eliminate all risk regardless of the cost, but to minimise the risks as far as possible. There are three main tradeoffs:
  - Functionality desired versus security required
  - Ease of use versus security
  - Cost of security versus risk of loss.
- For each risk plan, how to transfer, avoid, mitigate or (worst case) live with it.
- Create a plan that:
  - Includes a policy defining the organisation's security requirements and acceptable use
  - Has procedures for preventing, detecting and responding to security incidents
  - Gives a framework for enforcing compliance
  - Reflects the culture of the organisation and the resources available for implementation.

- Create a plan for dealing with a security breach (e.g. a virus attack):
  - What are the goals and objectives in handling an incident?
  - Who should be notified in case of an incident?
  - How will you identify an incident and determine how serious it is?
  - What should happen when an incident occurs?
- Create a project team. Include senior management, legal and HR, training and users. Give everyone clearly defined roles and responsibilities.
- Create a project timeline.
- Write it all up and get appropriate sign offs.

## Execute

- Communicate with staff, and provide training where necessary.
- Test measures for technical adequacy and obtain participant feedback.
- Modify the plan if necessary.
- Carry out the plan.

## Monitor and repeat

- Research new threats and include new risks as you become aware of them:
  - Subscribe to security bulletins
  - Train administrators and users.
- Modify the plan when changes occur in personnel, organisation, hardware or software.
- Ongoing maintenance such as virus updates, new user induction, backups etc.

## Finding the right technology partner

Finding the right technology partner to advise you can be trying, but it is important to get it right. Good support can make technology easier to manage and outsource a lot of time-consuming work. It can also ensure that you get the best possible advice and implementation.

### Where do you start?

Ask your colleagues, suppliers and peers who they use. Ask the local Chamber of Commerce for their input.

### What are you looking for?

Evidence of experience is essential. You're looking for someone to help you now but who can also be a long-term partner, so evidence of the ability to grow and develop as a company and support businesses bigger than yours helps. Use this checklist to select the right company:

- Do they understand your systems? Look for evidence that they can support the hardware and software you use now and that they have worked with similar companies.
- Are they sufficiently well-qualified? Check their credentials, references and qualifications.

- Do they talk your language? While it is important that they understand the technology, they need to be able to communicate it to you in everyday language and justify themselves in business terms. When you ask them a question do you understand the answer? Do their proposals ring true?
- Can they cope with your needs? Do they have the resources to meet your needs now? Can they commit to a specific schedule and budget for a given project? Will they be able to do the work with their own staff or will they have to sub-contract? Will they have the resources to grow with you in the future?
- What levels of support will they provide? Look for a service level agreement that sets out how quickly they will respond to problems and the level of after-sales support they offer.
- Ask about training. Can they provide it or recommend reputable partners?
- Are the responsibilities clear? Can they give a clear breakdown of what they will (and will not) do? Can they explain the step by step process by which they will complete a given project? Is everyone clear on what you have to provide?
- What is their fee structure? Depending on the project, it is possible to agree a flat fee, an hourly or daily rate, or an ongoing retainer. Are they willing to break down their cost structure and allocate costs to different stages or activities? You want accurate, exact and precise information before any work is commissioned.
- Is there appropriate documentation? They should supply you with a proposal for the work, including a budget, timetable and a reasonable specification. It should be in plain English. If this is satisfactory, you should have a written contract specifying what is going to be done and by whom, with dates, deadlines, equipment, costs and so on. Even if you do not have a formal contract drawn up by lawyers, make sure that the details of the work are written down and agreed in some form.

### Where next:

This is a big topic. There are two detailed guides to writing a security plan. First, Microsoft's at:

[www.microsoft.com/technet/archive/security/bestprac/bpent/bpentsec.asp](http://www.microsoft.com/technet/archive/security/bestprac/bpent/bpentsec.asp)

Second, the IETF has one at:  
[www.ietf.org/rfc/rfc2196.txt](http://www.ietf.org/rfc/rfc2196.txt)

For diagnostic tools visit:

[www.ukonlineforbusiness.gov.uk/healthcheck](http://www.ukonlineforbusiness.gov.uk/healthcheck)  
and download the Baseline Security Analyser from:  
[www.microsoft.com/technet/security/tools](http://www.microsoft.com/technet/security/tools)

There is an internationally recognised standard for information security certification called ISO 7799 or BS 7799. For more information see:  
[www.bsi-global.com/Corporate/17799.xalter](http://www.bsi-global.com/Corporate/17799.xalter)

To find a Microsoft Certified Partner, visit:  
[www.microsoft.com/uk/experts](http://www.microsoft.com/uk/experts)





# Security Plan

## Introduction

### About Intelligent Widgets

We are a twenty-person design and manufacturing firm developing widgets for the UK widget trade. Our manufacturing is done overseas. Our staff includes designers, manufacturing managers, sales and marketing personnel and the administrative team that supports them plus the senior management of the business, the co-founders Matthew and Tanya and the financial controller, Steve.

### Objectives

This is our first security plan. My intention is to take a broad view of the security risks facing the firm and take prompt action to reduce our exposure. Everyone remembers the virus attack we had earlier this year and we hope to avoid another disaster like that! However, I hope that by taking a wider view we may foresee and forestall threats that we do not know about yet. So this is also something of an insurance policy.

In writing this plan, I realise that we are limited in time, people and – of course – cash. Our main priority is to continue to grow a successful business. We cannot hope for CIA-like security and it wouldn't be good for our culture to turn Widgets into Fort Knox. The project team has weighed these constraints carefully in deciding what to do and has tried to strike a balance between practicality, cost, comfort and security measures. We are all convinced, however, that doing nothing is not an option.

I am taking responsibility for leading this review and ensuring that all the action items are carried out. I am concerned about the risks we face, although having reviewed the plan I am sure we can address them properly, so this project has my full support and is a high priority for the business.

*Managing Director*

## Circulation

Because this document contains important security information it is confidential. You are requested to keep it under lock and key when not actually using it and, please, don't leave it lying around or make photocopies. We will not be emailing this document or storing it on the server – paper copies only please. The following people are authorised to have a copy;

Matthew (Managing Director)

Tanya (Operations Director)

Steve (Financial Controller)

Tracy (HR Manager)

Jarndyce and Jarndyce (our lawyers)

Jeremy, MD of Friendly Geeks (our IT advisors)

## Project team

The project team includes:

- Tanya, project leader
- Steve
- Tracy
- Jeremy (from Friendly Geeks), advising and carrying out some of the implementation work.

In addition, we consulted with members of staff from sales, accounts and design to get their feedback on what they wanted and how the plan might affect them.

## Audit results

### Skills and knowledge

Friendly Geeks are familiar with the whole territory and will be our expert guides. However, we need to internalise as much of this knowledge as possible by doing as much of the work as we can. This will also help us save money.

Luckily, Steve is a bit of an amateur computer geek (all those hours playing Dungeon Siege). Since he wasn't au fait with security issues he has attended a training course.

Each member of the project team has read the BCC Security Business Guide as background.

The company as a whole is reasonably IT-literate but, with one or two exceptions, they see computers as a tool to get the job done and don't know much about how they work.

### Our network and systems

**PCs:** Twenty-two (one per member of staff plus two old machines acting as print servers).

**Laptops:** Six (one each for the directors, one for Steve and three for the sales team).

**Printers:** Two (one high-end A3 plotter and one printer/fax combi for general use).

**Servers:** One (running Microsoft Small Business Server 2003 which looks after files, the Internet connection and email).

**Internet connection:** 512kbp/s ADSL connection.

The server and several of the computers are linked by 100mb/s Cat5 Ethernet cable but the remainder are linked by an 802.11g wireless network with an access point. All computers run Microsoft Windows XP except for the two old print servers and two admin machines, which run Microsoft Windows 98.

## Security audit

We compared each machine against the checklist in the Security Business Guide. We also ran Microsoft Security Baseline Analyser with the following results:

**Virus protection:** Not present on six machines. Not up-to-date on four machines. Generally most users were aware of viruses but were a bit unsure about what they could do to prevent them.

**Anti-spam:** Many users have begun to complain about spam but no protection is in place.

**Firewall:** We thought the ISP's router included a firewall, but it doesn't; so we don't have one.

**Patches:** All the Microsoft Windows XP systems are up to date because they were automatically checking and downloading patches. However, several installations of Microsoft Office need patching and the older Microsoft Windows 98 machines are not patched at all.

**Passwords:** A random sampling found that most people aren't using passwords at all or had them written on post-it notes. In particular, none of the laptops are password-protected.

**Physical security:** We had the insurance people in last year, so the window locks, doors and alarms are pretty good. However, none of the computers are security marked and we didn't have a log of their serial numbers. We also noticed that everyone; accounts, Tracy and the two directors, are using the same printer which meant that there is a risk of confidential documents being left there by accident.

**Laptops:** All the laptops had shiny laptop bags WITH BIG MANUFACTURER LOGOS. No security locks.

**Wireless networking:** We're wide open here. It turns out that we just set the thing up and it worked so nobody touched any of the settings. However, it is wide open to snooping and freeloading.

**Web browsing:** Everyone thinks that having fast Internet access is a great perk but they are using it all the time and without much thought to the risks. We don't have a policy on acceptable use and no-one is taking any security measures.

**Backups:** We backup data on the server to a DAT drive on a weekly basis but we haven't tested restoring the data and unless people remember to copy local files across to the server they aren't backed up. This is unsatisfactory.

## Assets

Besides the physical property – computers and so on – our main assets are:

- *Our product designs and marketing collateral*
- *Records of our contracts with suppliers and the specifications and change orders*
- *Our email database and archive*
- *Sales orders and the customer database*
- *Financial/accounts information*
- *Paper HR and legal records stored in various filing cabinets*

All of these are considered secret and should only be accessible on a need-to-know basis. In addition, they need to be protected and backed up as safely as we can manage.

## Risks

We believe the risks break down into four main categories:

- 1. Hackers:** Viruses, worms, hijacking of our computer resources or Internet connection, random malicious use. These are the risks that anyone using computers connected to the Internet faces. High risk, high priority.
- 2. External threats:** Rivals, disgruntled ex-employees, bad guys after money, thieves. They are likely to use the same tools as hackers but, in deliberately targeting us, they may also try to suborn members of staff or use stolen material to blackmail or damage us. We need to protect our assets with physical and electronic security. High risk, high priority.
- 3. Internal threats:** Whether accidental or deliberate, a member of staff may misuse their privileges to disclose confidential information. Low risk, low priority.
- 4. Accidents and disasters:** Fires, floods, accidental deletions, hardware failures and computer crashes. Low risk, medium priority.

## Priorities

### 1. Hacker deterrence

- Firewall
- Virus protection
- Strengthening the wireless network
- Installing Microsoft Windows XP on the four Microsoft Windows 98 machines
- Ensure all machines are regularly patched
- User education and policies

### 2. Theft prevention

- Laptop security
- Security marking and asset inventory
- Move server into a secure, lockable room
- Security locks for PCs and laptops

### 3. Disaster prevention

- More frequent backups, with offsite storage
- Ensure backup of user's local data
- Offsite backup of critical paper documents

### 4. Internal security and confidentiality

- Strong password policy and user education
- Secure printers for accounts, HR and directors
- Review security for filing cabinets and confidential documents

## Security plan

---

### Action items

1. Select, purchase and install a hardware firewall (or get our ISP to provide one).
2. Switch on Internet Connection Firewall on the server.
3. Make sure our virus software is installed on all computers and that it is set to auto-update.
4. Select, purchase and install anti-spam filters on all computers or on the mail server (as appropriate).
5. On the wireless network: switch off SSID broadcasting, choose and configure a sensible SSID, switch on 128-bit WEP encryption, switch on MAC filtering and configure the access point to only allow traffic from the PCs and laptops in the office.
6. Buy Microsoft Windows XP upgrades and install them on the last four Microsoft Windows 98 machines.
7. Review all machines to make sure that they are fully patched and set them to auto-update.
8. Buy new nondescript laptop bags and laptop locks.
9. Security mark all PCs and laptops and their components.
10. Log all serial numbers.
11. Buy and install desk security locks for PCs.
12. Find a suitable, lockable room for the server and move it there.
13. Review backup procedures: Ensure that user data is either stored on the server or copied across regularly prior to backups. Implement daily incremental backups. Ensure that a full backup goes offsite once a week. Ensure that the backup is password protected and encrypted. Review paper documents and make photocopies for secure offsite storage of critical documents.
14. Configure Microsoft Small Business Server and individual machines to enforce reasonably strong passwords. Discuss with users what would be an acceptable balance of convenience and security (we don't want them writing down their new passwords all the time).
15. Configure workstations to log users out and require a password to log back in, if unused for more than five minutes.
16. Buy cheap printers for accounts, HR and the two directors so that they can have private documents printed securely.

## **Policy changes**

Tracy will update the staff handbook to include new policies on the following:

- *Acceptable use of email and the Internet*
- *Use of passwords*
- *Who can take company property away from the office and care of company property*
- *Compliance with the Data Protection Act*
- *Software piracy*
- *She will also review the health and safety policy to make sure it addresses any computer-related issues.*

Once she has completed a first draft it will be reviewed by the directors and the company's solicitors before being rolled out.

## **User education**

We expect to give up to two hours user training in small groups as a result of these changes to cover the following:

- *The importance of security*
- *Passwords*
- *Laptop security*
- *Virus prevention*
- *Safe Internet browsing*
- *Introducing the new staff policies.*

## **Project timeline and responsibilities**

The top three priorities: Firewall, virus protection and strengthening the wireless network, will receive urgent attention from Friendly Geeks. The remaining tasks will be done by our own staff in order of priority.

We expect the top three priorities to be completed within a week and the remaining tasks within thirty days. Steve will be responsible for purchasing and implementing the technical changes and Tracy for all the policy and training requirements. Tanya will oversee the project and be responsible for any other tasks that arise.

## **Response planning**

In the event of a security breach occurring, we will contact Friendly Geeks who have a one-hour callout policy during office hours and a four-hour call out policy at all other times to deal with serious incidents, such as a virus infection. In addition, Steve will monitor the security logs on the server and firewall regularly.

## **Ongoing maintenance and compliance**

Steve will be responsible for security on a day-to-day basis with Tanya taking overall responsibility.

Steve will continue his own self-education on the topic, subscribe to security bulletins from Microsoft and our anti-virus software supplier and he will liaise with Friendly Geeks on a regular basis to monitor compliance with the new policies.

On a monthly basis he will double-check that patches and virus scanners are up-to-date and the backup procedure is working properly. He will also be responsible for ensuring that new computer equipment is properly configured and up-to-date.

Tracy will be responsible for ensuring that new staff joining the company will be fully trained in the company's security policies and procedures.

There will be a full, formal review of this plan in six months time.

## Resources and budget

---

The following expenditure has been approved:

### **Software and hardware**

- *Anti-virus software*
- *Anti-spam software*
- *Hardware Firewall*
- *Upgrade the last four PCs to Microsoft Windows XP*
- *Security locks and new laptop bags*
- *Additional backup media*

### **Professional Advice**

- *Jarndyce and Jarndyce to review our rewritten staff policies*
- *Friendly Geeks for advice during the creation of this plan*
- *Friendly Geeks for help with implementation*

### **Internal Resources**

Although we are not paying for our own staff directly, to be clear about the allocation of resources and the time that is available for this work, we have authorised the use of internal staff as detailed above.



# It's all geek to me: hacking explained

“Time is precious. Life’s too short to get all nerdy about computers.” We agree. But to understand the threats that exist and the countermeasures, you need to know some technical stuff. Don’t worry – we’ll keep it to a minimum. We’re talking about external threats in this section, but don’t forget the risk of malicious users within your company.

## Networks, internets and the Internet

One computer on its own is a beautiful thing, a technical marvel. But it’s good to communicate.

Link two or more computers together using network cards and cables (or a wireless setup) and you have a local area network. This means that all the computers on the network can share data, email and access communal resources like printers, modems or broadband Internet connections.

Link two or more local area networks together and you have a wide area network. For example, you might link two offices together with a dedicated leased line.

An internet (note the small ‘i’) is a network of networks. Information from any computer in any given network can travel over the internet to any computer on any other network, with the internet acting as a sort of common carrier. Think of an internet as a motorway system linking local roads together.

The Internet (THE Internet with a capital ‘I’) is a global internet. All computers on the Internet communicate using standard protocols so that information from any computer on the Internet can reach any other computer on the Internet. This is where the trouble comes – until the point where you connect with a public network you are reasonably safe from external threats. Hook up to the public Internet and it’s like publishing your name, address and phone number and saying ‘hey look, we have computers here’.

### Packets

Information travels across networks in packets. A packet is a chunk of data, for example a page of text or a bit of a picture, plus an address which tells the network where the data has to go. Everything going over the Internet is broken down into packets: web pages, email, downloads, everything. Like cars on a road, packets share physical connections and travel in streams. Big data is broken down into a series of packets and reassembled at the destination, like a wedding party taking a fleet of taxis from the ceremony to the reception. As packets travel over the Internet they are effectively public.



## Ports and addresses

Each computer on a network has a unique numerical ID, similar to a telephone number, which is called an IP address. These usually correspond to a recognisable Internet domain (e.g. Microsoft.com). In addition, each computer that is connected to the Internet has a series of 'ports' that correspond to unique services that are accessible to outsiders over the Internet. For example port 80 is the one for web servers and port 25 is the port that is used to send email. Packets are addressed to a specific port at a specific IP address.

## Firewalls

A firewall closes ports that are not actually in use. This doesn't mean that you can't access services on other people's computers, just that outsiders can't get into yours. It also examines the packets that flow in and out of the network to make sure that they are legitimate and it can filter out suspicious packets. They can hide the identities of computers within your network to make it harder for hackers to target individual machines. Needless to say, a firewall works to rules you set.

## Servers

A server is just another computer attached to a network but it is usually there to do some special function such as share a printer, store files or deliver web pages. The thing to remember is that if your laptop or desktop is connected to the Internet it too is a kind of server and, without a firewall, it is capable of receiving unwanted Internet connections.

## Viruses, worms, Trojan horses, spam and hoaxes

Email is the conduit for billions of emails a year and an increasing proportion of them are not very pleasant. One email security firm scanned 413m emails in August 2003. 3% contained a virus, 52% were spam and 1 in 2118 contained some kind of pornographic image. There are five main email threats:

**Viruses.** This is a program which is designed to replicate itself, often hidden inside an innocuous program. Viruses in emails often masquerade as games or pictures and use beguiling subject lines (e.g. "My girlfriend nude") to encourage users to open and run them. Viruses try to replicate themselves by infecting other programs on your computer.

**Worms.** Like viruses, these try to replicate themselves but they are often able to do so by sending out emails themselves rather than simply infecting programs on a single computer.

**Trojan horses** are malicious programs that pretend to be benign applications. They don't replicate like viruses and worms but can still cause considerable harm.

**Spam,** or unsolicited commercial email, wastes bandwidth and time. The sheer volume of it can be overwhelming and it can be a vehicle for viruses. Much of it is of an explicit sexual nature and this can create an oppressive working environment and, potentially, legal liabilities if companies do not take steps to stop it.

**Hoax emails.** These emails, such as fake virus warnings, chain letters or implausible free offers, waste readers' time.

## Why software is vulnerable

Software developers do not set out to write unsafe programs. A typical operating system will be the product of thousands of person-years of work and will consist of millions of lines of code. A simple bug or oversight can provide an unexpected backdoor into an otherwise secure system. It is nearly impossible to write bug-free software. Of course, that doesn't mean developers should give up trying to achieve it.

Then there are the bad guys. Bank robber Willie Sutton said, "I rob banks because that's where the money is". It's the same with software. The more successful and widespread a piece of software is the more likely hackers are to target it. Of course, that doesn't mean users should accept it.



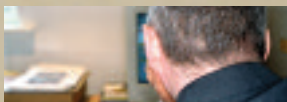
So there is a continual struggle between hackers exploiting weaknesses and developers seeking to close these loopholes down. It's the same thing with locksmiths and burglars or alarm manufacturers and car thieves. This is why software developers release upgrades and patches which fix known vulnerabilities and why you should install them.

## How hackers hack

Hackers have different motivations – profit, mischievousness, vainglory – but they all work in similar ways. There are a number of basic moves, all of which are capable of infinite variation:

- **Spoofing.** *For example, forging email messages or scanning Internet packets to acquire a valid password, with which to access a secure network.*
- **Tampering.** *Altering the contents of packets as they travel over the Internet or altering data on computer disks once a network has been penetrated.*
- **Repudiation.** *Buying something from an online auction and then failing to pay for it. Deleting or modifying a file in an untraceable or deniable way.*
- **Information disclosure.** *Stealing credit cards or personal information from a website. Accessing confidential files on a stolen hard disk. Distributing payroll information by email.*
- **Denial of service.** *Flooding a network with unwanted traffic to slow it down, or bombarding a server (for example an email server) with so much bogus traffic that it becomes unable to respond properly to legitimate traffic.*
- **Elevation of privilege.** *Improperly gaining administrative privileges on a network or getting a back door into an otherwise secure computer.*

Most hackers use the processing power of computers as their weapon. They might use a virus to spread a denial-of-service program to hundreds of thousands of computers (a so-called 'distributed denial of service' attack). They might use a password cracking program to try every word in the dictionary as a password. Of course the first passwords they will check are 'password', 'letmein,' 'opensesame' and a password that is the same as the user name. They have programs that random dial every IP address on the Internet looking for unprotected systems and, once they find one, they have port sniffers to see whether there are any ports open for attack. If they find one, they have a library of known vulnerabilities that they can use to try to gain access. For more deliberate attacks – for example, industrial espionage – a combination of technology and social engineering is most effective. For example, suborning members of staff, rifling through rubbish bins in search of revealing information or simply looking for passwords written on sticky notes by monitors.



# Information online

For information on technology options, change management and for guidance, comment, explanation and in-depth analysis of the latest developments in technology and how they may affect your business:

[www.bcentral.co.uk](http://www.bcentral.co.uk)

For information on starting and running a small business:

[www.chamberonline.co.uk](http://www.chamberonline.co.uk)

[www.ukonline.gov.uk](http://www.ukonline.gov.uk)

[www.smallbusiness.co.uk](http://www.smallbusiness.co.uk)

[www.ukonlineforbusiness.gov.uk](http://www.ukonlineforbusiness.gov.uk)

[www.bcentral.co.uk](http://www.bcentral.co.uk)

For business software and productivity solutions:

[www.microsoft.com/uk/office](http://www.microsoft.com/uk/office)

[www.microsoft.com/uk/windows](http://www.microsoft.com/uk/windows)

For information on software and the law:

[www.bsa.org.uk](http://www.bsa.org.uk)

For explanations of technical terms:

[www.howstuffworks.com](http://www.howstuffworks.com)

For general information on security:

[www.ukonlineforbusiness.gov.uk/informationsecurity](http://www.ukonlineforbusiness.gov.uk/informationsecurity)

[www.bcentral.co.uk/security](http://www.bcentral.co.uk/security)

For anti-virus software and email security:

[www.microsoft.com/security/antivirus](http://www.microsoft.com/security/antivirus)

[www.microsoft.com/security/partners/antivirus.asp](http://www.microsoft.com/security/partners/antivirus.asp)

[www.cloudmark.com](http://www.cloudmark.com)

[www.mailfrontier.com](http://www.mailfrontier.com)

[www.messagelabs.com](http://www.messagelabs.com)

<http://.hoaxbusters.ciac.org>

For firewalls:

[www.microsoft.com/technet/security/topics/network/firewall.asp](http://www.microsoft.com/technet/security/topics/network/firewall.asp)

[www.mcafeesecurity.com](http://www.mcafeesecurity.com)

[www.symantec.com](http://www.symantec.com)

[www.zonelabs.com](http://www.zonelabs.com)

To get the latest software patches and updates for Microsoft software:

[www.windowsupdate.com](http://www.windowsupdate.com)

[www.officeupdate.com](http://www.officeupdate.com)

For information about computer crime:

[www.met.police.uk/computercrime](http://www.met.police.uk/computercrime)

[www.nhtcu.org](http://www.nhtcu.org)

[www.kensingtonuk.co.uk](http://www.kensingtonuk.co.uk)

For mobile working and virtual private networks:

[www.microsoft.com/technet/security/topics/mobile/default.asp](http://www.microsoft.com/technet/security/topics/mobile/default.asp)

For information on backups:

[www.microsoft.com/windowsxp/home/using/howto/maintain/backup.asp](http://www.microsoft.com/windowsxp/home/using/howto/maintain/backup.asp)

[www.bcentral.co.uk/technology/buy/hardware/backup.asp](http://www.bcentral.co.uk/technology/buy/hardware/backup.asp)

For more detailed advice on writing a security plan:

[www.microsoft.com/technet/archive/security/bestprac/bpent/bpentsec.asp](http://www.microsoft.com/technet/archive/security/bestprac/bpent/bpentsec.asp)

[www.ietf.org/rfc/rfc2196.txt](http://www.ietf.org/rfc/rfc2196.txt)

[www.ukonlineforbusiness.gov.uk/healthcheck](http://www.ukonlineforbusiness.gov.uk/healthcheck)

For more technical information:

[www.microsoft.com/security](http://www.microsoft.com/security)

[www.microsoft.com/technet/security](http://www.microsoft.com/technet/security)

[www.howstuffworks.com](http://www.howstuffworks.com) for technical terms (e.g. internet, firewall, VPN).

[www.cert.org/tech\\_tips/home\\_networks.html](http://www.cert.org/tech_tips/home_networks.html)

[www.ja.net/documents/factsheets.html](http://www.ja.net/documents/factsheets.html)

# Glossary

**802.11 (a.)** A standard for wireless networks that ensures interoperability between different manufacturers. 802.11 networks come in three different variants: a, b and g. 802.11b is the most common while a and g are much faster. Usually cards capable of faster speeds are backwardly-compatible to the b standard.

**Access point (n.)** A wireless hub that links together different 802.11 network cards to form an 'infrastructure' wireless network (as opposed to ad-hoc).

**Ad-hoc network (n.)** A wireless network that links computers on a peer-to-peer basis rather than routing traffic through a central access point.

**Administrator (n.)** A user with sufficient access rights to allow them to manage the access rights of other users and carry out other high-level computer management tasks.

**Anti-virus software (n.)** Software specifically designed for the detection and prevention of known viruses.

**Authentication (n.)** The process for verifying that someone or something is who, or what, it claims to be. In private and public computer networks (including the Internet), authentication is commonly performed through the use of passwords.

**BIOS Password (n.)** A BIOS is software code that links the operating system to the hardware – it is the most basic piece of software on a computer. It usually includes the ability to stop an unauthorised user starting the machine.

**Broadband connection (n.)** Broadband connections to the Internet differ from dial-up connections in two ways. First, they are much faster, typically ten times quicker than a modem. Second, they are normally left connected to the Internet permanently and not just when they are in use. Examples of broadband connections include: ADSL, cable modem and fibre-optic leased lines.

**Buffer (n.)** A region of memory reserved for use as an intermediate repository in which data is temporarily held before it is transferred between two locations or devices.

**Buffer overrun (n.)** A condition that results from adding more information to a buffer than it was designed to hold. An attacker may exploit this vulnerability to take over a system.

**Certificate (n.)** An encrypted file containing user or server identification information, which is used to

verify identity and to help establish a security-enhanced link.

**Compact Disc (CD) (n.)** A CD-ROM is a data version of a music CD capable of storing up to 700mb of data. Using a CD recorder it is possible to create new CD-ROMs. CD-ROMs cannot be changed after they have been written.

**Computer security (n.)** The discipline, techniques, and tools designed to help protect the confidentiality, integrity, and availability of data and systems.

**Cookie (n.)** A small data file that is stored on a user's local computer for record-keeping purposes and which contains information about the user that is pertinent to a website, such as user preferences.

**Cracking (v.)** Finding a password by trying many combinations and words.

**Critical update (n.)** A broadly released fix for a specific problem addressing a critical, non-security-related bug.

**DAT (n.)** Digital Audio Tape. Used to store data, a DAT tape can store up to 24 GB (although this assumes optimal compression).

**Decryption (n.)** The process of converting encrypted data back into its original form.

**Denial of Service Attack (n.)** By overloading a service, hackers seek to make it unavailable to legitimate users. For example, by sending millions of spam emails simultaneously to a mail server, ordinary traffic will get clogged up.

**Dial-up Connection (n.)** A dial-up connection uses a modem (or sometimes an ISDN terminal adaptor) to connect to an ISP. Usually these connections are quite slow and only open while the user is actually online.

**Digital signature (n.)** Data that is bundled with a message or transmitted separately and is used to identify and authenticate the sender and message data. A valid digital signature also confirms that the message has not been tampered with.

**Domain Name Server (DNS) (n.)** A server that converts recognisable domain names (e.g. Microsoft.com) into their unique IP address (e.g. 207.46.245.222).

**Download (v.)** To transfer a copy of a file from a remote computer to a requesting computer by means of a modem or network.

**Elevation of privilege (n.)** When a user (particularly a malicious user) gains more access rights than they normally have.

**Encryption (n.)** The process of converting data into cipher text to prevent it from being understood by an unauthorised party.

**Firewall (n.)** A combination of hardware and software that provides a security system, usually to help prevent unauthorised access from outside to an internal network.

**Hacker (n.)** Someone who tries to gain unauthorised access to a private system.

**Hoax email (n.)** An otherwise harmless email that is designed to cause alarm or get itself forwarded to other users (or both). For example a fake virus warning or a chain letter.

**Honey pot (n.)** A system designed to look like a regular network but which, in fact, monitors and traces unauthorised access.

**HTML Format Email (n.)** An email that uses HTML to make emails look like web pages.

**Hypertext Mark up Language (HTML) (n.)**  
The computer code that is used to describe the contents of web pages.

**Internet Service Provider (ISP) (n.)** A company that provides access to the Internet.

**IP Address (n.)** A unique address that is used to identify a computer on the Internet. In its basic form it is made up of four digits separated by dots, called a dotted IP address (for example 192.168.0.1).

**IPSec (Internet Protocol Security) (n.)** IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices.

**KB article (n.)** A technical document in the Microsoft Knowledge Base accessible through Microsoft.com.

**Key (n.)** In encryption and digital signatures, a value used in combination with an algorithm to encrypt or decrypt data.

**Klez (n.)** A particularly virulent species of virus.

**L2TP (Layer-2 Tunnelling Protocol)** L2TP provides security for transmission of sensitive information over unprotected networks such as the Internet.

**Local Area Network (LAN) (n.)** A local computer network for communication between computers.

**MAC Filtering (n.)** Each network card has a unique ID called a MAC. A wireless network access point can be configured to give access to specific network cards (and the computers in which they are installed), and excludes others on the basis of these MAC addresses.

**Mail bomb (n.)** An excessively large amount of email data sent to a user's email address in an attempt to make the user's email program crash or to prevent the user from receiving further legitimate messages.

**Mail relaying (n.)** A practice in which an attacker sends email messages from another system's email server in order to use its resources and/or make it appear that the messages originated from the other system.

**Malicious user (n.)** A person who has access to a system and poses a security threat to it. An example is someone who tries to elevate their privileges to gain access to unauthorised data.

**Microsoft Base Line Security Analyser (n.)** A free tool from Microsoft that searches computers for known security vulnerabilities and suggests remedies, available from [www.microsoft.com/mbsa](http://www.microsoft.com/mbsa)

**Patch (n.)** A software update.

**PDA (n.)** A portable digital assistant, typically a handheld computer like a Pocket PC.

**Port (n.)** Each network service on a given computer has its own port, like a telephone extension.

**Port sniffer (n.)** A hacker program designed to find open or unguarded ports.

**PPTP (Point-to-Point Tunnelling Protocol)**  
PPTP provides security for transmission of sensitive information over unprotected networks such as the Internet.

**Private key (n.)** One of two keys in public key encryption. The user keeps the private key secret and uses it to encrypt digital signatures and to decrypt received messages.

**Proxy server (n.)** A firewall component that manages Internet traffic to and from a local area network (LAN) and can provide other functions, such as document caching and access control.

**Public key (n.)** One of two keys in public key encryption. The user releases this key to the public and anyone can use it to encrypt messages to be sent to the user and decrypt the user's digital signature. Compare private key.

**Public key encryption (n.)** An asymmetric encryption scheme that uses a pair of keys for encryption: the public key encrypts data, and a corresponding secret key decrypts it. For digital signatures, the process is reversed: the sender uses the secret key to create a unique electronic number that can be read by anyone possessing the corresponding public key, which verifies that the message is truly from the sender. See also private key, public key.

**Public Key Infrastructure (PKI) (n.)** Generally, the laws, policies, standards, and software that regulate or manipulate certificates, and public and private keys.

**RAID (n.)** A Redundant Array of Inexpensive Disks. Instead of using one large, expensive disk, most servers use a RAID array. There are different levels of redundancy, so a RAID level 5 has the highest level of safety. A single disk in the array can fail or even be removed and the data remains safe.

**Router (n.)** A device that determines the next network point to which a data packet should be forwarded on its way toward its destination. Routers are used to move packets around the Internet and most broadband connections end with a router in your building that connects your LAN to the rest of the Internet.

**Script kiddies (n.)** Inexperienced hackers who use publicly available tools.

**Server (n.)** A computer that provides a service to other computers over a network.

**Spam (n.)** Unsolicited commercial email, also known as junk email.

**Spoof (v.)** To make a transmission appear to come from a user other than the user who performed the action.

**SSID (n.)** The SSID is the name given to a wireless network which enables users to find it.

**Strong password (n.)** A password that provides an effective defence against unauthorised access to a resource. A strong password is at least six characters long, does not contain all or part of the user's account name, and contains at least three of the four following categories of characters: uppercase letters, lowercase letters, base 10 digits, and symbols found on the keyboard, such as !, @, and #.

**TCP/IP (n.)** Transmission Control Protocol / Internet Protocol. The protocols, or conventions, that computers use to communicate over the Internet

**Technology journalist (n.)** A harmless drudge.

**Trojan horse (n.)** A computer program that appears to be useful but that actually does damage.

**Virtual private network (VPN) (n.)** A private data network that makes use of a public network, such as the Internet, by encrypting data at one node and using security procedures that provides a "tunnel" through which the data can pass to another node.

**Virus (n.)** Code written with the express intention of replicating itself. A virus attempts to spread from computer to computer by attaching itself to a host program. It may damage hardware, software, or data. Compare worm.

**VPN (n.)** See virtual private network.

**Vulnerability (n.)** Any product flaw, administrative process or act, or physical exposure that makes a computer susceptible to attack by a malicious user.

**War chalking (v.)** Using chalk symbols on walls to indicate the presence and configuration of an insecure wireless network.

**War driving (v.)** Locating insecure wireless networks by scanning for them with a portable computer and special software.

**WEP (n.)** WEP data encryption is defined by the 802.11 standard to prevent eavesdropping and access to the network by malicious users.

**Wi-Fi (a.)** See 802.11

**Worm (n.)** A subclass of virus. A worm generally spreads without user action and distributes complete copies (possibly modified) of itself across networks. A worm can consume memory or network bandwidth, thus causing a computer to stop responding.





THE BRITISH  
CHAMBERS OF  
COMMERCE