

How to...

7

# Secure

your business



# You can

never be too safe



Are you worried about IT security? If not, you should be! It's easy to think it will never happen to you, but the reality is it probably will – and sooner rather than later.

According to a DTI survey, almost half the businesses in the UK suffered one or more malicious security breach in 2001-2. The average cost was £30,000 and 20% of the incidents caused disruption that lasted more than a week.

Alas, you can never be totally secure – unless you switch all your computers off and bury them in concrete. However, there is plenty you can do to limit the risk of an attack. The good news is that the Microsoft® Windows® XP Service Pack 2 contains some really significant security improvements, so make sure you have installed this update.

A good first step is to educate yourself and find out more. You'll find a wealth of readable information on the Internet and there are plenty of newsletters you can subscribe to. Failing that, ask around and find a reputable local IT professional with proven security expertise to advise you.



**Microsoft®**

# Check

## your system

To give you an idea of how secure you currently are, Microsoft has a free product called Microsoft Baseline Security Analyser (MBSA) which you can download from the Internet. To find it, type **MBSA download** into your Internet search engine.

MBSA will scan your computer for security vulnerabilities, supply you with a security assessment report, and offer you a list of corrective actions. If you have a network, you can even scan the entire network from a single computer, as well as scan both your servers and workstations.

Running MBSA on a regular basis will help ensure that your system stays up-to-date and secure. Amongst other things, it checks to see if you have weak passwords, missing security patches, security problems that Internet Explorer and Microsoft Outlook® might be open to and Office macro protection settings.

When you have downloaded MBSA, start it from your Programs menu and follow the instructions in the wizard.



# Avoid

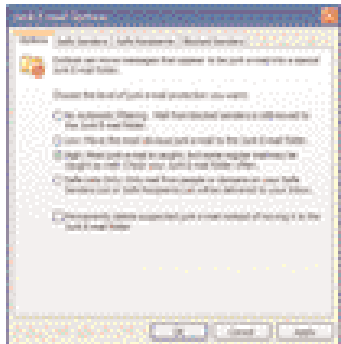
## viruses

Viruses are malicious programs that infect computers. The infection starts when you unwittingly run an infected program, which is often attached to an email. The email itself will probably look quite interesting since it is designed to make you want to open it and run the attached program.

There are some simple things you can do to minimise the risk of being affected by a virus.

1. Don't open suspect files, especially from someone you don't know!
2. Buy and install some anti-virus software and keep it up-to-date.  
This software scans your files and incoming emails looking for viruses. If you have installed Windows XP Service Pack 2, you will be prompted to install anti-virus software if you haven't already done so.
3. Microsoft Outlook 2003 has good built-in security features which are switched on by default to protect you. It is recommended that you don't lower the level of security.

Outlook will also help you filter out junk email. Check out these options by choosing **Junk E-mail** from the **Actions** menu.



# Set up a firewall

Firewalls are designed to protect your local network from outside attacks by screening out unwanted communication. There are basically two types of firewalls – hardware and software. A hardware firewall might be integrated into your router (if you have one), whereas software firewalls typically run on the machine that sits between the Internet and the rest of your network.

If you have a single machine connected to the Internet by a modem or broadband connection, you can use the Windows XP Internet Connection Firewall. To do this:

- Click **Start** and then **Connect To**
- Choose **Show all connections**
- Right click on the connection you use to connect to the Internet and choose **Properties**
- Click on the **Advanced** tab
- Click on the **Settings...** button in the Windows Firewall section (if you have a tick box here instead of the Settings button, just tick the box)
- Make sure that the **On** option is selected

If you have other machines which share this Internet connection using Windows Internet Connection Sharing, you can still use this firewall on the actual machine which connects to the Internet.



# Stay up-to-date

The bad guys who hack into systems or distribute viruses are looking for loopholes in software which they can exploit. When Microsoft discovers one of these loopholes, a patch is released to close it. To protect your system, you need to make sure you are up-to-date with these patches.

## Windows XP

Windows XP makes it really easy to stay up-to-date with the Automatic Updates feature.

With Automatic Updates, you don't need to worry about checking for updates since this tool will do it for you.

If you are not sure whether you have this turned on, click **Start**, choose **Help and Support** and then click the task labelled **Keep your computer up-to-date with Windows Update**. This will use your Internet connection to visit the Windows Update site and check for any updates you need. You will see notification on the right hand side of the Windows Update screen if you have Automatic Updates turned on or not. Click the options to turn it on, or change the settings.

## Microsoft Office

If you use Microsoft Office 2003, you can choose **Check for Updates** from the Help menu to do exactly that.

For older versions of Office, visit <http://office.microsoft.com/officeupdate> to find the latest updates.



# Safe surfing

By organising websites into different categories, Internet Explorer can control how much access they have to your computer. This is important because web pages can contain programs – most of which will be harmless, but others not.

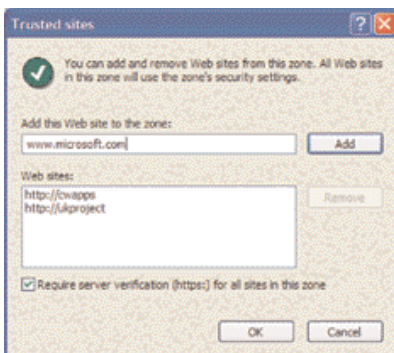
When you first start Internet Explorer, all sites will be placed into the 'Internet' zone with medium security settings.



You can then add one or more website addresses to the 'Trusted sites' zone. You would do this if it is a site you know and trust and you want to use its functionality. This would require you to lower your security settings.

Similarly, you can add suspect sites to the 'Restricted sites' zone to limit the damage they can do to your computer.

To work with these settings in Internet Explorer choose **Internet Options...** from the **Tools** menu and then click on the **Security** tab. You can then click the zone you want to add website addresses to, and use the **Sites...** button to add the address.



# And finally...

All of the previous steps are procedures everyone can, and should, follow. But there is still yet more you can do!

## Backing up

Regular backing up of your data is a vital insurance policy. Look out for other guides in this series for more information.

## Strong passwords

Don't make it easy for the hackers to access a secure system! A strong password is more difficult to crack and should contain at least seven characters which are a mixture of upper and lower case letters, numbers and symbols. A password should not relate to your name or company name, you should change it regularly and never write it down!

## Physical security

Use locks, alarms, computer locks, visitor logging and anything else that it takes to keep your computers where they should be. Take particular care of laptops. Carry them in a bag that doesn't look obviously like a laptop bag, and never let them out of your sight.

## Seek advice on network security

You need to ensure that your remote users are connecting securely to your network, and that your wireless networks are also secure. If you do not have skills in this area, then it is a good idea to find a local IT professional with proven security expertise. Ask colleagues, suppliers and friends who they use and don't be afraid to ask for customer testimonials.

## Write a security plan

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

### Audit

Review your skills and knowledge, and assess your current state of security.

### Plan

When planning, include your company security policies and procedures for detecting and responding to security incidents.

### Execute

Communicate the plan to your employees, test procedures and modify them if required.

### Repeat

Continual review and ongoing maintenance is key for security

## Spread the word

Make sure that your employees understand the importance of security, and appreciate that part of their role is to keep your business secure.

# Find the help and support you need

## on Microsoft's products and services

**Software support:** There are a number of ways you can get help, advice and support from Microsoft. Microsoft® bCentral is a great starting point to guide you to the help and support you need and includes links to the specific areas listed below.

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

**Technology:** This area provides information on how you can get more from your software investments, as well as help with specific tasks you're trying to carry out.

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

**Security:** This section covers information and support on protecting your system including anti-virus options, networking systems and secure online purchasing.

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

**Unresolved or specific technical support queries:** Microsoft has a dedicated website with centralised support resources. Here you can download software, review common issues related to your product, search the technical database (Knowledge Base), join a Newsgroup and check the status of an ongoing query.

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

**Newsgroups:** This page provides access to Newsgroups across a range of topics. Discuss issues with others who use Microsoft products, including advice from Microsoft Most Valuable Professionals (MVPs). Read interesting posts, search for specific topics, answer a question, or post your own question to any of the many groups.

[www.support.microsoft.com/newsgroups](http://www.support.microsoft.com/newsgroups)

**Free support calls:** Retail customers may be eligible for 2 telephone or online support incidents at no charge. To find out if you are entitled, either telephone us on **0870 60 10 100** (8am-6pm, Mon-Fri), or submit your technical support incident online via the Microsoft UK support site to see if it is validated.

**Links to other Microsoft resources from:**

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

Microsoft has a large number of websites designed to help you get more from your software, as well as keep it up-to-date and reliable. From this page you can follow the links to:

- **Microsoft UK home** – the place for everything Microsoft with information and resources on the entire Microsoft product range (including Microsoft Windows, Microsoft Office and servers) as well as the latest news and community offerings
- **Office update** – to ensure you have the latest add-ons, security features and other tools on your PC
- **Windows update** – similar to the Office update site, this section is dedicated to Windows
- **Office for Macintosh** – find out more about how Microsoft supports the Mac and what's available – from help to the latest products available
- **Licensing compliance** – be sure you're using the right software
- **TechNet** – an information and community programme for IT professionals, providing valuable free resources packed with technical answers and insights
- **Microsoft MSN®** – for the latest consumer news and views

# Microsoft Guides

in this series:

1. How to... Connect with your customers
2. How to... Make sense of your financial data
3. How to... Create a website
4. How to... Create brochures and flyers
5. How to... Create and mail a newsletter
6. How to... Secure your wireless network
7. How to... Secure your business
8. How to... Do more with Windows XP
9. How to... Do more with Outlook
10. How to... Protect your data

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