



Your business assets are under attack

We'll help you protect them

You wouldn't dream of leaving your business premises unprotected, would you? You probably have a burglar alarm and maybe even CCTV to deter would-be thieves.

But what about your computer systems? What steps have you taken to ensure they're protected?

Computer crime is very real, and it could have a devastating effect on your business without you even realising it.

Help is at hand

In this leaflet, you'll find the guidance you need on exactly what the threats are, how to protect your business against them, who to trust, and what to do should your business come under attack.

Microsoft®

12 ways

Microsoft®

to protect your business

All it takes is a few simple steps to make your business a lot less vulnerable. To address the main risks, just follow our twelve-step plan.

1 Educate yourself

Reading this leaflet is a good start. For more information, there are plenty of good sources on the internet aimed at non-technical users. Spending an afternoon browsing these sites really could be time well-spent.

Technical jargon buster www.howstuffworks.com

Further security information www.bcentral.co.uk/security

2 Make a plan

Information security is more than just getting the right technology – you'll need to consider people, policies and processes.

The first thing to do is establish where you are now. Then, consider who you would turn to if your system went down and find a supplier who can service your computers and network regularly. Work with them to write a security plan that will protect your business.

To find a partner visit www.bcentral.co.uk/security

3 Install virus protection

As computer viruses can easily cripple your business in just a few seconds, comprehensive virus protection is essential. And as new viruses are emerging all the time, you'll need to download the latest virus 'signatures' regularly. Many anti-virus products offer automatic updates.

Directory of anti-virus suppliers

www.microsoft.com/security/partners/antivirus.asp

4 Set up a firewall

Firewalls are designed to stop unwanted Internet traffic getting into your systems. If you have Windows® XP, you should switch on the built-in Internet Connection Firewall. For the best protection, it's a good idea to have two firewalls from different manufacturers.

For Firewall software visit

www.mcafeesecurity.com

www.symantec.com

www.zonelabs.com

For information on Microsoft® Internet Connection Firewall

www.microsoft.com/technet/columns/security/5min/5min-101.asp

5 Stay current

Cyber criminals are constantly looking for weak spots to attack, so make sure your systems are up to date. Ideally, you should set your systems to download 'patches' automatically. If you are operating Windows 95 or 98, you should consider upgrading.

For updates visit

www.windowsupdate.com

www.officeupdate.com

6 Use strong passwords

Once a hacker has got your password, your security systems are worthless, so don't make it easy for them.

Avoid using obvious words and use a mix of upper and lower case letters, numerals and punctuation marks. Treat your passwords like your PIN and don't divulge them to anyone, change them regularly.

For information on strong password policies visit

www.microsoft.com/technet/columns/security/5min/5min-302.asp

7 Watch your emails

Most viruses arrive via email, so don't open anything that's unknown, unexpected or suspicious – even from someone you know.

To secure Microsoft Outlook® visit

www.microsoft.com/technet/columns/security/5min/5min-102.asp

For anti-spam software visit

www.cloudmark.com

www.mailfrontier.com

8 Watch where you're web browsing

Just browsing the internet can expose you to virus attacks because some websites can embed malicious programs in their pages. Internet explorer can help protect you from unknown or untrusted sites.

Learn more about IT security

www.microsoft.com/windows/ie/using/howto/security/settings.asp

9 Make remote access safer

Remote working is increasingly popular, but it has its risks.

Data travelling across the Internet can be intercepted and/or tampered with, so it's vital you control access to your network and encrypt any information in transit.

For more info on remote access visit

www.microsoft.com/technet/security/topics/mobile/default.asp

10 Protect your laptops

Having your laptop stolen could cost you more than just the hardware – without the right protection, the thief could access all your data too.

So, think twice about the data you keep on your laptop and, where possible, use BIOS passwords and encrypt your files

To encrypt your files visit

www.microsoft.com/technet/columns/security/5min/5min-205.asp

11 Ensure your wireless networks are secure

Wireless networks are flexible and useful, but they're not always secure. It can be easy for criminals to freeload off your Internet bandwidth and even gain access to your systems. Ensure you secure your system to prevent access.

To strengthen your wireless network visit

www.microsoft.com/technet/columns/security/5min/5min-106.asp

12 Backup frequently

Backups are the last line in defence against hardware failure, floods, fires and the damage caused by a security breach.


It's advisable to review your backup process, work out what data you need and how frequently it needs to be backed up. You should test restoring data from time to time to make sure your system works and ensure you keep critical backups offsite.

For more information visit

www.bcentral.co.uk/security

Nobody believes anything bad can happen to them until it does. In fact bad things do happen and surprisingly often.

Visit Microsoft® bCentral, the free online destination for UK small businesses, to find out how you can take simple steps to secure



your business and to request your free guide to securing your computer technology.

www.bCentral.co.uk/security

Useful contacts

To report Computer Crime call your local police station or Crime Stoppers on 0800 555 111

In a genuine emergency, always dial 999

For more information, visit www.police.uk or contact your regional computer crime unit via the National High Tech Crime Unit website www.nhtcu.org.

For suspected credit/debit card fraud The Association for Payment Clearing Systems (APACS) www.cardwatch.org.uk

For further guidance on securing systems The Department of Trade and Industry www.ukonlineforbusiness.gov.uk

For suspected mishandling of personal information The Information Commissioner www.dataprotection.gov.uk

For illegal sites, denial of Internet service attacks and the sabotage of networks Your ISP (Internet Service Provider)

For information and advice on technology for Small Businesses Microsoft bCentral www.bcentral.co.uk/security

For advice on checking credit applications Telecomms UK Fraud Forum (TUFF) www.tuff.co.uk

