Compliments of ecrimewales

Preventing e-Crime FOR DUMMIES®

e-Crime Wales Second Edition

Protect your business from the threat of online crime

Making Everything Easier!™

FREE eTips at dummies.com®

ecrimewales
edroseddcymru

e-Crime Wales is a partnership of organisations and agencies tackling the threat of e-Crime to the Welsh economy, a threat that currently costs Wales nearly £1 billion per year. Bringing together the four Welsh Police Forces, public and private sectors, e-Crime Wales shares intelligence and increases knowledge of risk and prevention amongst Welsh businesses.

Partneriaeth rhwng sefydliadau ac asiantaethau sy'n mynd i'r afael ag effeithiau niweidiol e-droseddau ar economi Cymru yw e-Drosedd Cymru. Mae'r bygythiad hwn yn costio tua £1 biliwn y flwyddyn i'r wlad. Drwy ddod a phedwar Awdurdod Heddlu Cymru, y sector cyhoeddus a'r sector preifat ynghyd, mae e-Drosedd Cymru'n rhannu gwybodaeth ac yn gwella dealltwriaeth o risg a dulliau atal ymysg busnesau Cymru.

www.ecrimewales.com
www.edroseddcymru.com

Ewrop & Chymru:
Buddsoddi yn eich dyfodol
Cronfa Datblygu Rhanbarthol Ewrop

Europe & Wales:
Investing in your future
European Regional Development Fund

ERDF

Llywodraeth Cymru
Welsh Government

Rhaglen
Llywodraeth Cymru
Welsh Government
Programme

Cymru Ddigidol
Digital Wales

Preventing e-Crime FOR DUMMIES®

E-CRIME WALES SECOND EDITION

by e-Crime Wales

WILEY

A John Wiley and Sons, Ltd, Publication

Preventing e-Crime For Dummies®, e-Crime Wales Second Edition

Published by
John Wiley & Sons, Ltd
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
England

E-mail (for orders and customer service enquires): cs-books@wiley.co.uk

Visit our Home Page on www.wiley.com

ISBN: 978-1-119-94518-5

Printed and bound in Great Britain by Page Bros, Norwich

10 9 8 7 6 5 4 3 2 1

Table of Contents

Introduction 1

About This Book 1
Foolish Assumptions 2
How This Book is Organised 2
Icons Used in This Book 4
Where to Go from Here 4

Chapter 1: Recognising Common e-Crimes 5

Falling for the Advance Fee Fraud 6
Flooding to Deny Service 8
Phishing Scams: Skilled Imposters 9
Installing Spyware 10
Digesting Spam 11
Losing Company Secrets and Resources 13
Using Unsecured Wireless Networks 15
Falling Prey to Virus Attacks 16
Handling Hacktivism 17
Scoping out Scareware 18
Facing Up to Fake Ads 19
Staying Secure in Social Media 20
Beating Botnets 21

Chapter 2: Protecting Your Business 23

Managing Employee Behaviour 24
Implementing IT Security Policies 25
Managing Your Emails 26
Protecting Customer Data 28
Disposing of Old Hardware Safely and Securely 31
Planning to Recover from Disaster 32
Securing Your Equipment 35
Working Safely from Home 36
Data Breaches 37
Sector Specific e-Crime Prevention Advice 38

Chapter 3: Defending Your IT Network 49

Typing in Ever-Changing Passwords 49
Updating Software..... 51
Backing Up Data 52
Repelling Viruses 52
Building a Firewall..... 53
Keeping Wireless Transmissions Secure..... 56
Muting Vocal Security Issues 58
Protecting Public WiFi..... 59
Cloud 60
Maxing Mac Security 61
Staying Smart on Phone Security..... 62
Watching Over Websites..... 63

Chapter 4: Safeguarding Yourself and Your Home 65

Protecting Your Home PC 65
Guarding Against Identity Theft..... 66
Shopping Safely Online..... 67
Banking Online Securely 68
Staying Safe while Social Networking..... 70
Recognising and Dealing with Spam..... 71

Chapter 5: Knowing What to Do if You're a Victim 73

Reporting an Incident to the Police..... 73
Informing about Financial Crimes..... 74
Identifying Illegal Content 74
Dealing with Viruses, Spyware, and other Malware 75

Chapter 6: A Dozen Best Security Practices 77

Use Strong Passwords..... 78
Use Anti-Virus Software 79
Never Accept Default Installations 79
Don't Run Unnecessary Services 80
Install Security Patches Immediately 80
Back Up Your Data..... 81
Protect Against Surges and Losses..... 81
Know Who You Trust 82
Enable Logging and Review Logs..... 82
Expect Protection to Fail..... 83
Manage User Accounts Well..... 83
Educate Your Users 84

Chapter 7: Almost Ten Questions to Ask a Security Consultant 85

Is This Your Day Job? 85
How Long Have You Been Doing This? 86
What Certifications or Training Do You Have? 86
Have You or Any of Your Staff Been Arrested or Charged with Illegal Computer Activities? 88
Do You Have Any Ties or Associations with a Particular Vendor? 88
Do You Offer Any Guarantees? 89
Do You Offer Support for Emergency Situations? 89
What Would You Do If You Discovered One of My Employees Doing Something Questionable or Illegal with My Computers? 89
Do You Have References or a Client List? 90

Chapter 8: Almost Ten Myths about Computer Viruses 91

My Computer Stopped – I Must Have a Virus 91
I Have Antivirus Software, So My Computer Can't Get a Virus 92
All Viruses Are Destructive 93
Viruses Can Damage Computer Hardware 93
I Need More Than One Antivirus Software Program to Be Fully Protected 93
You Can't Get a Virus from an Official Software CD 94
Antivirus Software Companies Create Viruses 94
Some Countries Sponsor Virus Writers and Hackers 95
Viruses Do Not Affect Macs 95

Chapter 9: Ten Tips to Prevent Data Loss Today 97

Identify the Information that Needs to be Protected 97
Find Out where Sensitive Information Resides 97
Recognise who has Access to Sensitive and Confidential Information 98
Discover the Processes Involving Sensitive Information 98
Spot When and Where Data Goes Offsite 98
Guard against Hardware Loss 99
Protect Information in Motion 99
Consider how Reports and Printouts are Destroyed 99
Look at How You Dispose of Outdated Technology 100
Start an Education-and-Awareness Programme 100

Chapter 10: More Than Ten Websites to Go to for Help 101

www.ecrimewales.com 101
www.getsafeonline.org 102
www.business.wales.gov.uk 102
www.iwf.org.uk 102
www.sans.org/resources/policies 103
www.ukpayments.org.uk 103
www.banksafeonline.org.uk 103
www.antiphishing.org 103
www.ceop.police.uk 103
www.thinkuknow.co.uk 104
www.cybermentors.org.uk 104
www.actionfraud.org.uk 104
www.knowthenet.org.uk 104

Appendix: Glossary 105

Introduction

Welcome to *Preventing e-Crime for Dummies*.

e-Crime generally refers to a criminal activity in which a computer or computer network is the source, tool, target or place of the crime. And despite the cyber connection, most e-Crime is just a new take on a whole raft of 'traditional' crimes such as fraud, theft, blackmail, forgery and embezzlement.

e-Crime has the dubious distinction of being notoriously difficult to detect and punish because of its sheer technical complexity and because unseen attackers can strike victims from hundreds or even thousands of miles away.

Due to the nature of e-Crime, and its ability to evolve with technology, new threats are emerging with alarming regularity. However, simply maintaining a better appreciation of the risks you face can have a significant effect on your ability to respond to them if the need arises.

e-Crime is an ever-increasing threat to businesses; however you can minimise most of the risks by following simple steps and procedures. This book is all about understanding e-Crime, how it can affect your business and, ultimately, how you can protect yourself from e-Crime.

About This Book

The majority of businesses can be confident that their existing IT (Internet technology) security precautions – invariably based on conventional, off-the-shelf anti-virus and firewall solutions – will provide them with sufficient protection from all significant online security threats. But the fact remains that thousands of businesses every year still fall victim to e-Crime, despite having such precautions in place – hence this book.

e-Crime is on the rise, with more and more sophisticated or creative ways of breaching IT security being unearthed every day. Simply relying on your existing IT security measures – if any – is

unlikely to provide you with sufficient protection against today's breed of hackers, scammers and virus designers, who are able to overcome traditional security measures with relative ease.

So, any business using a computer is at risk. If that computer or other electronic device is connected to the Internet, the risk is even greater, and criminals know this. You know better than we do that the information on your IT system is extremely valuable, so taking every precaution to protect it is essential. Protecting you, your business and your staff from the most common electronic threats may cost no more than you spend on locks and alarms for your office, so why take the risk?

This book explains the various types of e-Crime that your business could fall victim to, and how to take some simple yet effective steps to protect yourself from them.

Foolish Assumptions

While writing this book we made some assumptions about your knowledge of e-Crime, why you might be interested in this book and what you want to get out of it.

We assume that your reason for picking up this book might be one or more of the following:

- Your business uses computers or has an IT network connected to the Internet and is therefore at risk from e-Crime.
- You don't know much about e-Crime and you want to gain a greater understanding of it.
- You want practical steps to follow to minimise the risks of e-Crime.
- You want to keep business information and personal details safe and prevent security leaks.
- You want to know how to report an e-Crime to the relevant authorities.

How This Book is Organised

This book is divided into ten succinct and easily-digestible chapters, plus an appendix:

Chapter 1: Recognising Common e-Crimes

This chapter runs through common examples of e-Crime and provides useful tips for avoiding them or minimising the risks.

Chapter 2: Protecting Your Business

In this chapter we show you the not-always-technical steps and security principles you need to take to protect your business from e-Crime. We also offer a range of industry-specific advice.

Chapter 3: Defending Your IT Network

This chapter covers the areas you can consider looking at in order to provide your business with the best possible security devices.

Chapter 4: Safeguarding Yourself and Your Home

e-Crime can affect you at home as well as in your business. Chapter 4 shows you the basic steps to protect your home PC and how you can look after your personal identity online.

Chapter 5: Knowing What to Do if You're a Victim

This chapter explains the different places where you can report an e-Crime if you unfortunately become a victim.

Chapter 6: A Dozen Best Security Practices

From keeping your technology up to date to planning for glitches, this chapter is a small but useful collection of tips.

Chapter 7: Almost Ten Questions to Ask a Security Consultant

Don't even think about employing a security consultant without reading this chapter – it could save you a lot of time and money.

Chapter 8: Almost Ten Myths about Computer Viruses

Did you know that your computer can get a virus even if you've installed anti-virus software? This short chapter explodes some of the myths about viruses.

Chapter 9: Ten Tips to Prevent Data Loss Today

Chapter 9 is a call to action; a useful list of tips covering everything from safely disposing of hardware to encrypting data when it goes offsite.

Chapter 10: More Than Ten Websites to Go to for Help

We've packed a lot of information into this short book, but if you'd like to know more, head to this chapter.

Appendix: Glossary

Head here for easy-to-understand definitions.

Icons Used in This Book

Those little pictures in the margins are a *For Dummies* staple that point out information of special use. The icons we use in this book are:

The knotted string highlights particularly important information to remember.

This icon relates to technical stuff that you don't necessarily need to know and can skip over if you want to.

The information next to this icon is on-target advice you can put to practical use.

The bomb signals something to be careful about and highlights behaviours to avoid.

Where to Go from Here

Check out the section headings in this book and start reading wherever you like. This book is written with a sequential logic, but if you want to jump to a specific topic you can start anywhere to extract good stuff. If you want more information and advice, or the latest e-Crime news, visit `www.ecrimewales.com`.

No matter where you start out, we hope you end up with some useful information, so dig in!

Chapter 1

Recognising Common e-Crimes

In This Chapter

- Resisting pleas for money and information
- Guarding your computers and networks
- Protecting yourself from spies and spam
- Preventing loss of hardware and business secrets

Figures released by the Cabinet Office in February 2011 suggest that e-Crime could be costing the Welsh economy a staggering £974 million every year, through direct financial or intellectual property theft, disruption of communications or damage to business-critical data, with businesses being the top targets for criminals. Add to that the potential cost to companies and other organisations of damaged reputations, and you begin to understand the scale of the problem.

©PriceWaterhouseCoopers' Information Security Breaches Survey 2010 showed that 83 per cent of respondents had a security incident in the last year with an average cost of £27.5k. The worst incident cost the company concerned £55k.

The first step towards protection is a better understanding of the types and variety of threats currently being faced by businesses like yours. In this chapter, we guide you through the most common e-Crimes out there and make sure you have all the knowledge required to make key decisions in electronic security.

Falling for the Advance Fee Fraud

Advance fee fraud (AFF), also known as a *419 scam,* usually starts with you or your company receiving an email purporting to be from a government official of a foreign country, often from Africa or Asia. You're asked in this email to give relatively small sums of money or bank details in exchange for huge returns.

Figure 1-1 is a sample of such an email.

If you respond, you may end up giving away huge sums of money along with personal/business information, including name, address, telephone number and bank details which can later be used against your company or be used as part of another crime – never a good thing.

It's what criminals call the *confidence trick*, and if you fall for it, it can get your business into all kinds of trouble.

Follow these tips to handle such requests:

- Delete the email immediately. Even a reply refusing to accept the offer may encourage further contact. Request staff to do the same.
- Enable a good email filter to block many of these types of messages.
- Remember, if it sounds too good to be true, it usually is.

Lagos, Nigeria.Attention: The President/CEO

Dear Sir,

Confidential Business Proposal

Having consulted with my colleagues and based on the information gathered from the Nigerian Chambers Of Commerce And Industry, I have the privilege to request your assistance to transfer the sum of $47,500,000.00 (forty seven million, five hundred thousand United States dollars) into your accounts. The above sum resulted from an over-invoiced contract, executed, commissioned and paid for about five years (5) ago by a foreign contractor. This action was however intentional and since then the fund has been in a suspense account at The Central Bank Of Nigeria Apex Bank.

We are now ready to transfer the fund overseas and that is where you come in. It is important to inform you that as civil servants, we are forbidden to operate a foreign account; that is why we require your assistance. The total sum will be shared as follows: 70% for us, 25% for you and 5% for local and international expenses incidental to the transfer.

The transfer is risk free on both sides. I am an accountant with the Nigerian National Petroleum Corporation (NNPC). If you find this proposal acceptable, we shall require the following documents:

(a) your banker's name, telephone, account and fax numbers.

(b) your private telephone and fax numbers for confidentiality and easy communication.

(c) your letter-headed paper stamped and signed.
Alternatively we will furnish you with the text of what to type into your letter-headed paper, along with a breakdown explaining, comprehensively what we require of you. The business will take us thirty (30) working days to accomplish.

Please reply urgently.

Best regards

Howgul Abul Arhu

Figure 1-1: A typical 419 or AFF scam email.

Flooding to Deny Service

A *Denial of Service (DoS)* attack is an attempt to prevent you or other users in your business from accessing information or services.

The most common and obvious type of DoS attack occurs when an attacker floods a network with information, causing a system shutdown.

A DDoS (distributed denial of service) attack on the other hand, is an orchestrated DoS attack launched from multiple computers against one or relatively few targets. In this circumstance, the attacking computers are usually coordinated into a network (known as a botnet) so that, en-masse, they have a far greater effect than if the attack was launched from a single computer. Find out more about botnets in the section 'Beating Botnets' later in this chapter.

To prevent DoS interruptions, use these tips:

- Design your systems for survivability. Plan worst-case scenarios, and have accurate and realistic provisions for costing and business continuity. Take steps to ensure that your business could continue while under attack.
- Have your system administrators install software fixes to limit the damage caused by the attacks.

Contact your ISP (Internet Service Provider) if you think you have been attacked. If you cannot get through, it may be that you are one of many, so try alternative routes.

Timing DDoS attacks

Whether they're targeting a floral delivery website a few days before Valentine's Day or a haulage firm the week before its busiest weeks of the year, DoS criminals are capable of knowing which organisation to target at which uniquely crucial time. High-profile UK victims include online betting websites at times of high demand such as in the run-up to the Grand National.

DoS attacks are all about timing, and they always arrive at the worst possible moment for the victim, threatening websites during their anticipated busy periods. So, if your website typically gets a lot of traffic at certain times, shore up your security beforehand.

Phishing Scams: Skilled Imposters

A phishing scam is an attempt to make you think that a bank or other legitimate business is asking you to verify sensitive information, and trick you into sharing data such as your credit card number, bank account number, password, PIN (personal identification number), and such.

The notification looks to be genuine – check out the example in Figure 1-2 – as does the website you're directed to.

From: Citibank Service
[mailto:security@citibank.com]
Sent: Thursday, January 29, 2009 10:22 PM
To: ***************
Subject: Security Update
Dear Citibank Customer,
At Citibank, we value the trust you have placed in us by using our service to conduct your transactions. Because our relationship with you is financial in nature, the protection of your privacy is particularly important to us.
We are sending this verification notice to provide you with information about how Citibank safeguards your privacy, as well as to comply with UK government privacy guidelines that apply to financial institutions such as Citibank. The full terms of Citibank's privacy policy are available on the Citibank website, which you are welcome to review at any time.
Please verify your account information by clicking on the link below.
Verify your accounts here.

Figure 1-2: Today's scam artists are deviously creative in their phishing endeavours.

Phishing bait like that in Figure 1-2 certainly gets your attention. And check out those details: This official-looking message shows `security@citibank.com` as its originating email address – plausible. The language on the message appears to be genuine. And there's just the right note of urgency and reassurance to make you want to click on the link and let them know that you're legitimate – even though they aren't.

No legitimate company will ever ask you to send sensitive information via email. No bank or credit card company will ever ask you to enter your credit card's PIN on their website. It would be like asking you to write your credit-card number on a sticky note and posting it in the bank lobby.

Phishing scammers count on you not to think too closely about what you're doing, relying on the urgency and legitimate-seeming appearance of the message to get you to respond immediately.

You can find out more about phishing scams at `www.antiphishing.org`.

Installing Spyware

Spyware, as the name suggests, is software that covertly gathers information from your computer to use either for advertising or malicious purposes.

Installing new software can bring the risk of importing spyware and other viruses, especially if you download unchecked software from the Internet. Spyware applications are typically bundled as a hidden component of freeware or shareware programs. Once installed, the spyware monitors you or your company's activity on the Internet and transmits that information to someone else.

Spyware programs can collect various types of personal information, but can also interfere with your control of the computer in other ways. For example, the spyware may install additional software, redirect web browser activity, access websites blindly and expose your computer to even more harmful viruses or divert advertising revenue to a third party. Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other programs.

To safeguard yourself, use these tips:

- Institute strict controls over what software can be installed.
- Run an anti-spyware application.
- Scan your systems regularly to uncover spyware that has 'slipped through the net'.
- Update all your systems with the latest patches recommended by the software developers. New vulnerabilities are being discovered and exploited all the time.

Digesting Spam

Spam is the electronic equivalent of junk mail and although much of it is not necessarily criminal in intent, responding to it poses significant risks.

Thanks to the common availability of email address databases and the relatively small cost of sending emails, spam is a lucrative business and now accounts for the majority of all email messages.

Recent evidence suggests that some spammers have now teamed up with virus writers so that even more spam can be sent, using the infected computer to send spam to all the email addresses contained in a user's address book, for example.

Spam's direct effects include the consumption of computer and network resources, and the cost in human time and attention of dismissing unwanted messages. There are also the direct costs, as well as the indirect costs borne by the victims – both those related to the spamming itself, and to other crimes that usually accompany it, such as financial theft, identity theft, data and intellectual property theft, viruses and other malware (**mali**cious soft**ware**) infections, fraud, and deceptive marketing.

The very best anti-spam solutions today deliver 95 per cent effectiveness. Unfortunately, that's not good enough. An attack that gets through a 5 per cent gap in defences could cost your business thousands of pounds in lost business.

When most people think of security problems associated with spam, they think only about inbound spam received via email, but outbound spam can be a serious problem as well. Most outbound spam is not a result of staff deciding to make money or cause havoc; rather, it's the result of internal systems becoming infected by malware. Like all spam, it needlessly consumes network and storage resources and worse, it can damage a company's reputation if recipients discover the company is sending spam.

Defending your business against spam

If an anti-spam solution is going to provide the highest possible effectiveness, it should include all four of these components:

- **Verification Techniques:** These detect spam and spam volumes by using Internet standards and other business services to verify the identity of email senders. Verification addresses a large proportion of basic spam attacks, especially phishing attacks and Denial of Service (DoS) attacks.
- **Reputation Analysis:** This technology tracks the reputation of a large number of source IP addresses that a business encounters. The key advantage of reputation analysis is efficiency. To determine whether or not a message is spam, the system just needs to scan the message's IP address as opposed to scanning the entire message.
- **Content scanning:** This is the scanning of email contents for spam and malware. Content scanning is becoming increasingly important, because unlike techniques such as reputation analysis, which rely on analysing the source IP address, it can be used to detect outbound spam.
- **Behavioural Analysis:** This fills in the analytical gaps required to identify the most sophisticated attacks. Behavioural technology looks at attributes of all incoming mail and identifies insights and patterns indicating any abnormal behaviour. This works well for previously unseen, low-volume attacks.

Getting shot of spam

Perhaps the easiest e-Crime to avoid falling victim to, follow these steps to get rid of spam:

- Never, ever reply to a spam message. If you can tell from the subject line that a message is spam, don't open it - delete it.
- Don't forward an email from someone you don't know.
- Preview your messages before you open them or view a message's headers to see if a sender's email address is valid.
- Forward spam to your IT department so they can adjust your message filters.

Losing Company Secrets and Resources

Laptops now outsell desktops, wireless is rapidly replacing wired Internet access and your average mobile phone or iPhone can do almost any electronic thing you desire. The modern electronic and mobile business environment poses several problems for businesses trying to keep their data and their networks secure.

Being at risk electronically

When businesses were run solely out of an office, it was easy for management to keep track of what business secrets their employees knew and could be confident that all confidential information was secure.

Today, staff work wirelessly and remotely, and employees expect to carry out their work whenever they want, wherever they are, with a wide variety of electronic gadgets, many of which are capable of storing corporate data.

The increasing reliance on iPods, smartphones, PDAs (personal digital assistants) and USB (universal serial bus) sticks mean that most employees now have personal devices that can store huge amounts of data. Unfortunately, data can easily escape between devices, the devices can be connected to a laptop or PC with ease and are virtually impossible to trace.

It's not just your standard Blackberry or USB stick that poses a risk – thousands of different USB products currently exist and these devices are going to become more sophisticated and more readily available, so businesses need to be constantly on their toes to protect their data.

This electronic variety and mobility jeopardises business security – whether by intent or not – and makes IT networks vulnerable to outside influences, including viruses and spyware.

It's becoming increasingly difficult for IT managers – particularly in small businesses – to adequately protect company information. Companies looking to tackle the root of the problem through the standard anti-virus and network access control are also hitting a brick wall.

Make sure that you and all employees with access to confidential business information follow these rules:

- When working remotely, follow your security policies.
- Check every file copied onto company systems (from any source) for viruses.
- Encrypt sensitive data.
- Regularly back-up essential files and store copies in a secure place, away from the premises.
- Control access to business premises and computer systems.

Incidents of employee data theft is constantly growing: 4.5 million personal records were stolen from Monster.com, 800,000 were stolen from GAP and the UK Government saw 15 million individual records stolen in 2007. These statistics suggest that this type of threat does not focus on any specific industry: it can happen to any organisation at any point.

Losing hardware

Question: If a thief ran off with your laptop or PDA containing unprotected business-sensitive data, how would it damage your business? Answer: It could end up destroying it.

That answer holds for the loss of any device that has critical business data on it by any employee.

To lessen the chances of losing laptops and other electronic devices and to prevent some of the damage such a loss may pose to your business, use these tips:

- Maintain a list of your equipment (including serial numbers) and check your physical security.
- Password protect your hard drive and data.
- Mark your postcode on all hardware with an ultra violet pen.

Using Unsecured Wireless Networks

The affordability and ease-of-use of wireless networking technology has made it a popular feature in many business ICT (information and communication technologies) systems, allowing flexible access to files and communications resources without needing to 'plug in' to the network. Securing wireless networks is therefore of paramount importance.

Being so easy to connect to is a double edged sword for organisations deploying a wireless network. Without appropriate safeguards, your wireless networks can be maliciously abused with dire consequences for your business.

An unsecured wireless network can be easily compromised in a number of ways:

- Hackers can access sensitive files on your entire network, in the same way as if they were sat inside your premises at a workstation.
- Malicious individuals can launch viruses, spyware and other harmful code into your ICT system.
- Rogue users can use your expensive Internet connection without your knowledge, using up the bandwidth you've paid for and possibly visiting illegal websites and conducting illegal activities while looking like it's you.

Head to Chapter 3 to find tips on securing wireless networks.

Falling Prey to Virus Attacks

A computer *virus* is a program created to cause a nuisance or to damage computer systems and the data they hold. Viruses can replicate themselves, spreading from computer to computer.

These days the most common way a virus is activated is when the unsuspecting recipient opens an attachment sent via email. Viruses look harmless on the outside but can do real damage if you let them into your system. A virus may look like a game for instance, but install spyware (see 'Installing Spyware' earlier in the chapter) or *adware* (software that downloads or displays advertisements), which then opens a backdoor on the computer allowing an intruder to connect without your knowledge or consent. The virus could also contain *keylogging software* that records keyboard activity, which criminals could use to steal usernames, passwords, bank account and credit card details.

As more and more businesses use networks and high-speed Internet connections, viruses have become the most prolific and costly security issue facing small and medium-sized businesses. Viruses are used as delivery mechanisms for hacking tools, putting the security of your organisation at risk, even if you have a *firewall* (an electronic security system) installed.

The downtime for your company, as a result of data loss, can drastically influence your company's long-term success. And if you are a smaller company, this could mean the difference between having a business and going bust.

Fighting global infection

Opening unverified attachments is perhaps the most common cause of virus attacks; with 72 per cent of UK businesses receiving infected emails or files (83 per cent of UK large businesses) according to a respected survey undertaken by the Department for Business, Enterprise and Regulatory Reform (BERR).

In 2000, the 'ILOVEYOU' virus spread across the world in one day infecting 10 percent of all computers connected to the Internet and causing about £2.75 billion of damage. Upon opening the attachment, 'ILOVEYOU' sent a copy of itself to everyone in the user's address list, posing as the user, and thus spreading the virus very quickly.

The 'Love Bug' virus caused an estimated £7.5 billion of damage.

The top tips for protecting yourself from viruses are

- Introduce virus-checking software. Most anti-virus vendors offer solutions that can protect against most types of virus.
- Use a properly configured firewall between your office systems and the Internet.
- Do not open suspicious emails – especially don't open the attachments.
- Enable preview panes in your email system only after you remove all suspect emails. By previewing an HTML email you're still opening the code and therefore any malicious code.
- Have a clear IT policy for acceptable use of business systems, websites and email. Refer to this policy in employment contracts and provide training for procedures.

Handling Hacktivism

Hacktivism is the use of computers and computer networks as a means of protest to promote political ends.

As more and more companies put more of their operations online, the Internet becomes an increasingly attractive place to conduct a protest. For example, taking down important websites and denying access to legitimate business use of those sites gets a lot more attention.

A hacktivist uses the same tools and techniques as a hacker, but does so in order to disrupt services and bring attention to a political or social cause. For example, one might leave a highly visible message on the home page of a web site that gets a lot of traffic or which embodies a point-of-view that is being opposed. Or one might launch a denial-of-service attack to disrupt traffic to a particular site.

As always, companies need to make sure they're taking all the necessary steps to protect themselves against attacks. If you want to safeguard your IT system, you need to protect each component on your network, including PCs, routers, switches and all other connected users devices. Why? Because anyone who can access your network can also disrupt your network components and services.

Scoping out Scareware

Scareware consists of pop-up advertisements warning users of supposed security threats. As companies get smarter about recognising spam and phishing emails, scareware suppliers have started implanting triggers in the most unexpected places online, with research suggesting that 50 new 'scam tactics' are emerging each day.

Scareware can now be found in advertisements posted on popular mainstream media sites, among results from well-known search engines like Yahoo and Google and in messages on the most popular social networking sites such as Facebook and Twitter.

Using popular and misspelled search terms, criminals divert people to sites that are seeded with fake warnings about virus

infections. The pop-up warnings then claim that a visitor's PC is riddled with malicious programs and spyware.

Keep yourself ahead of the criminals by:

- Installing antivirus (AV) software on every machine and keeping the signature files current through automatic or manual updates at least weekly. Renew the automatic update capability annually as required to maintain a current virus signature file on every machine.
- Not downloading material from the Internet without first ensuring that your AV application is active.
- Educating all computer users to remove or destroy infected files identified by AV software.
- Educating all e-mail users not to open e-mail attachments from unexpected and unknown sources to avoid unleashing a new virus not yet blocked by the AV application
- Enabling the AV application to automatically check every file source on each machine when it is used (including CD, USB drives and so on).

Facing Up to Fake Ads

Internet advertisement networks provide attackers with an effective venue for targeting numerous computers though malicious banner ads. Such fake ads may take the form of Flash programs that look like regular ads, but contain code that attacks the visitor's system directly or redirects the browser to a malicious website.

The popularity of social media platforms such as Facebook has also led to a number of scams that spread virally across the social network, tricking users into taking surveys and earning the scammers money. Make sure as a user that you stay informed about the latest scams spreading fast across Facebook and other internet attacks.

Everyone in your organisation should be responsible for ad security. The host of the website should be actively involved in making sure that the content is malware free, the ad producers should also be active in preventing their ads from being hacked and the users should be alert as well.

Staying Secure in Social Media

Many businesses are now embracing the benefits in social networking to bring them closer to their customers and improve brand experience. While social networking services have advantages, they also pose risks to businesses, ranging from data disclosure to malware infection and copyright infringement. Look out for the following:

- **Malware and spam:** Social networking sites such as Twitter are sometimes targeted to direct users to malicious links; compromising the company and spreading viruses across shared folders and removable devices, such as USB sticks.
- **Malicious attacks and employee misconduct:** Employees can provide too much personal and sensitive information, expose lapses of judgement or even deliberately attack their own employers using online platforms.
- **Phishing:** Phishing allows criminals to gain access to a user's log-in details by directing them to a fake log-in interface. This then enables access to a wealth of personal details that allows e-criminals to build a profile of the user.

Top tips for employees

- Read carefully and in full the company's privacy policy
- Pay attention to what you post and upload
- Protect your work environment and avoid reputation risk
- Verify all your contacts
- Use your personal e-mail address for personal mail

Beating Botnets

Most organisations will not understand what Botnets are, or what effects they can have to the state of a business. Make no mistake, the consequences can be disastrous, and because Botnets do not discriminate, every business is vulnerable…

Understanding your enemy

Put simply, a botnet is a 'robot network' of PCs that has been infected by a virus to execute malicious actions that are unseen and unknown to legitimate users. This process is controlled by the botnet creator or 'herder'. Once infected, the botnet can be used to send huge volumes of spam email or can even use its strength to launch harmful, targeted attacks on other companies' websites.

There are two major types of botnet attacks businesses must be aware of; denial of service attack (DoS) and spam email. The potential knock-on-effects can include slowing your network service down and potential legal ramifications, where you may be liable for any damages an infection causes other organisations' or their customers' IT infrastructure.

Protecting your business from the bots

Businesses that are not adequately protected by IT security measures, such as antivirus and firewall software, are at the greatest risk of being corralled into a botnet, so it is vital your business has the necessary security policies in place. Make certain that these solutions are updated regularly, both to keep ahead of the evolving nature of threats and to ensure your security strategy doesn't go past its 'best before' date.

Chapter 2

Protecting Your Business

In This Chapter

- Making sure your employees follow security measures
- Instituting sound IT security for emails, customer data and threats from mobile devices
- Protecting your machines while you have them and getting rid of them safely
- Making plans for disaster
- Being secure when working from home
- Sector Specific e-Crime Prevention Advice

Although you may recognise the need to secure your business's computer systems and online access activities, you may be intimidated by the potential costs, the specialist expertise needed, or the time it may take to set up such security precautions.

In this chapter, we aim to help you better understand the need and benefits in securing your networks and computer systems – as well as helping you make sense of your cyber security priorities.

The information here represents the key security principles we suggest you consider as a starting point in developing an online security policy for your business.

If you unfortunately become a victim of one of the many different types of e-Crime, you can take a variety of courses of action to report or rectify it, depending on the nature of the incident. You will find links to report e-Crime through the e-Crime Wales website at `www.ecrimewales.com/report`.

Managing Employee Behaviour

The Internet has become a ubiquitous tool for business use, but it presents equally ubiquitous risks. Businesses utilising IT and the Internet need to ensure that their IT systems are not put at risk by employees who use those systems.

Whether your business operates an *'open-use' policy* (for example, not restricting access to any websites or web email, and allowing employees to access them at any point during the working day) or uses only emails and not the wider Internet, managing the risks involved with employee Internet use is a vital part of any effective IT security policy.

Employees may use the Internet without any regard for the risks to the business. And, unlimited use of the Internet for non-work related activity is dangerous for the following reasons:

- Employees may use the Internet to view inappropriate or sometimes illegal material on websites.
- Employees may knowingly or unknowingly download documents, email attachments or other media which can infect or disrupt the businesses IT infrastructure.
- Employees are using the Internet for their own personal use during work hours, thereby working less productively.
- Critical business information, such as company passwords, customer's information and sensitive corporate information can be needlessly exposed by employees surfing the Internet without due care and attention.
- Your business can be made legally liable for the behaviour of your employees using IT services, particularly if it endangers other organisations data or infrastructure.

IT security is a team game and the responsibility of every single employee in your business. Vital to this approach is making sure all employees understand their role within IT security, with their use of IT systems being productive and in no way endangering the business.

Starting an education and awareness programme at the workplace can be a good way to really bring home the dangers. Send out an email outlining each of the threats your organisation has faced or expects to face, and the implications of data

loss. Spoof an attack of some sort and as with fire drills, don't just do this once and assume that everyone knows what to do. The message and the process should be repeated regularly. The big difference between fire drills and data-loss education is that data threats are changing all the time.

Implementing IT Security Policies

To protect your business from e-Crime (we go through the most damaging crimes in Chapter 1), implement IT security policies that define what behaviour is and is not allowed. Outline the general rules to be followed by management and employees alike to ensure optimal working practice and to minimise IT security risks.

Make sure that the policies aren't lengthy or complicated; they should be an easily understood reference for all staff.

Follow these steps to design your IT protection rules:

1. **Start by asking yourself the following questions:**
   - What am I trying to protect?
   - Why am I trying to protect it?
   - What happens if I fail to protect it?

   The policies you develop should take account of the most common or most likely risks to your data, given the nature of your business and your computer usage.

2. **Determine what you consider as acceptable business use of your Internet and email systems.**

   Casual or unrestricted use is typically the means by which viruses get into your network.

   You can download a personalised acceptable use policy with your business details in from `www.ecrimewales.com/policy`.

3. **Look at ways to protect your IT systems from all types of threats, both external such as viruses and internal such as theft of data.**

   Some areas your security policies should address may include:

- Login identification for using IT systems.
- Logical access controls – limiting access to information and restricting access to the level needed for each job.
- Confidentiality rules for customer and business information.
- Plans for business continuity management.

This list isn't exhaustive. For more examples visit `www.sans.org/resources/policies/` and download their template policies.

Not all attackers come from outside your organisation. This doesn't mean you should automatically be suspicious of every member of your staff, but don't rule out the possibility. Employees can compromise colleagues' machines using tools readily available from the Internet if your network security is poor. These hackers have tools to spy on others' actions, view information outside of their job function, and plant inappropriate content on others' machines.

No matter how comprehensive your security policies are, or how well you implement the controls, the security of your network ultimately depends on the people who use it. If everyone understands why security controls are needed and their own responsibilities for them, you're less likely to have a security breach.

Any information security initiative should be inclusive and accompanied by appropriate training. Communicate the policy to all employees, educate them on how to use it and get a written agreement to abide by the rules from everyone involved.

Make certain that you can enforce any policies you implement, and make clear that you will enforce them.

People are your best line of defence – especially if they're well trained and informed.

Managing Your Emails

Email has very quickly become one of the most common contemporary ways of sending and receiving information. The old

'familiarity breeds contempt' adage comes into play. Because email is so common and everyone uses it, it's very easy to become complacent when opening emails or attached files from sources you're not be entirely familiar with – which can cause very large, far-from-contemptible problems.

The most common way of transferring computer viruses, spyware or keylogging programs (check Chapter 1 for information on e-Crimes) onto a PC is via email – mostly in the form of attachments. As a rule of thumb, don't open any attachment from a source you're not familiar with. In many cases, it is good practice not to open the email itself – especially if you feel the origin is suspicious or if the subject matter is unusual.

Spam email is another significant problem – and while spam may not necessarily pose a critical threat to business security, the sheer volume of spam is becoming a major issue for some.

Spammers can acquire your email address in a variety of different ways – they may even have guessed it, as a lot of spam traffic is sent to randomly generated email addresses in the hope that some of them may prove genuine.

You can minimise your exposure to spam emails in a number of ways. Make sure that everyone in the company uses these tips:

- Avoid posting your full email address on public Internet forums or websites. Many spammers run software applications which automatically trawl the web looking for email addresses.

  If you must post your email details publicly, try to 'disguise' the appearance of your address. For instance, if your address is 'someone@xyz.org', represent it as 'someone-at-xyz-dot-org'. This makes it practically impossible for automatic scanning programs to recognise the address and record it, although people who need to email you can still recognise the addressing convention.

- Use a secondary or 'disposable' email account for public use, or for when signing up to online services. The account may still attract spam, but if this gets out of hand, you can simply delete this 'decoy' account and start another, without affecting your original or primary email address.

- Never reply to spam email even if the text contains a 'remove' option. This only serves to validate your email address and will most likely result in you receiving even more spam email than ever before. Simply ignore the email and delete it.

If spam email volumes are causing you significant concern, or if you find you're spending a considerable amount of time deleting them, then it may be worth considering one of the many commercially available 'spam filter' software packages.

As with spam, don't respond to any other email that you consider suspicious. Emails that purport to be from your bank, building society or other high-profile commercial organisations such as eBay and ask you to re-input your security information or passwords, are likely to be phishing scams, looking to steal your information. Other email propositions might offer lucrative rewards for helping a deposed African dictator launder some of his money!

As a general rule, if you're in any doubt about the validity of any email, or if you have never heard of the sender, simply delete it.

Most major business and financial institutions carry an email policy on their own websites; you may find it worth checking out a few of these sites.

Protecting Customer Data

The importance of protecting customer data has been brought right to the top of the political and public agenda recently with the high-profile loss of a significant amount of customer data from HM Revenue & Customs.

Whatever the precise circumstances, the loss at HMRC nevertheless demonstrates how data can go missing despite there being strict data protection procedures in place.

Understanding what the Data Protection Act means for you

It's been around since 1998, and all UK businesses should be fully compliant since October 2001. So just what is the Data

Protection Act and how does it affect your business? We give you the answer here.

The Data Protection Act 1998 is based on an EU directive requiring member states to protect the rights of people to 'privacy with respect to the processing of personal data'. Overseen by the Information Commissioner's Office (ICO), the Act governs the appropriate use of personal data by any organisation holding it.

The Act covers how organisations must handle personal information that can be used to identify the individuals concerned. This applies to all Welsh businesses dealing with individuals, be they members of the public, employees of business partners/suppliers or even their own internal staff.

Every organisation has a responsibility to adhere to the Data Protection Act, which typically involves having 100 per cent control and security over IT systems and databases. Should you fail protect individuals' privacy, you may be committing or facilitating an e-Crime.

Not abiding by the rules of the Act may mean:

- A £5,000 fine (unlimited if prosecuted in a Crown Court)
- Being charged with a criminal offence in many instances

Holding personal information carries a series of legal responsibilities under the terms of the Act:

- Data-controllers have to report to the ICO about how they hold and process personal data, what kinds of data they hold (particularly if these are deemed 'sensitive' such as information related to health records, ethnic origin, trade union membership or political opinions) and what purposes the data are held for.

  This report is placed on a public register.

- You must hold and use personal data in strict accordance with the eight principles of the Data Protection Act. These require that information is:
  - Fairly and lawfully processed
  - Processed for limited purposes
  - Adequate, relevant and not excessive

- Accurate
- Not kept longer than necessary
- Processed in accordance with individuals' rights
- Kept secure
- Not transferred outside the European Economic Area without adequate protection

- You must answer requests from individuals requesting access to information concerning themselves. (You may be able to charge a fee of up to £10 per request for this.)
- You must inform individuals when their information is collected. You can collect data only when an individual gives 'specific' and 'informed' consent.

Many organisations have broken the Data Protection Act and suffered the consequences, both in terms of fines and sanctions but also the more damaging issue of a tarnished reputation. The law exists to protect consumers, so companies that break it are justifiably held in poorer regard.

As well as having appropriate policies in place to remain in accordance with the Act, one of the most important actions Welsh businesses can take is to ensure any personal data held remains secure. Failing to respect the privacy of personal data strikes at the heart of what the Data Protection Act was designed to accomplish, and leaves an open door for e-criminals to walk through.

Encrypting data to keep it safe

One way to protect your customer data from hackers and thieves is to encrypt it. Encryption programs encode data or make it unreadable, requiring you to enter a password, or encryption key, to unlock it.

Encryption programs are built into some popular financial and database software, and some Internet service providers are now including encryption for wireless networks as a part of their service. Alternatively, you can buy a specialist encryption program to properly and effectively encrypt your business-sensitive information.

At the very least, computer files containing customer data, or business critical information should be password-protected,

although passwords can be relatively simple to hack. Most popular office software applications contain basic password-based security protection features.

Disposing of Old Hardware Safely and Securely

While businesses are starting to recognise that safe disposal of electronic waste such as computers and hard drives is a great step toward becoming environmentally friendly, many often overlook another issue it helps them address: protecting valuable data.

Recent security breaches in the public sector are simply higher profile repeats of similar breaches within the private sector that have surfaced with increased regularity over the past years. The thing is, they'll happen again next week and the week after unless businesses tackle the root cause of the problem and find ways to safely and securely dispose of their old hardware.

Companies need to establish and enforce policies so that you have a way to reclaim technology equipment when an employee upgrades to a new machine or leaves the company.

You can also draft guidelines for acceptable ways to retire a machine, such as reselling it online, sending it back to the manufacturer, or recycling it thorough hazardous waste programs.

Before disposing of any computer or data-storing machine, make sure that IT teams or senior members of staff erase all traces of applications and information from the machine so that company data isn't left on the old hardware.

Many people fail to realise that when you delete a file on your computer it isn't really deleted, it just gets hidden. The information is still there until it gets physically overwritten, which happens only if your hard drive is full and your computer needs to find more space or if you deliberately overwrite it while cleaning up your hard drive.

Searching the Internet turns up lots of software for erasing a hard drive. These programs work by overwriting your deleted files several times with meaningless data to ensure that they

are completely erased. Even then, it may still be possible to retrieve the original data, but only by dedicated experts with extremely powerful recovery software.

Another way to make sure the hard drive is wiped is to reformat it and re-install your operating system. Try this technical operation only if you're confident about what you're doing, or you know someone who is.

If you're still worried that the information on your computer may fall into the wrong hands, you can physically destroy your hard drive or possibly remove the hard drive from a computer before recycling it. You can take the hard drive out of your computer and either burn it, or drill holes in it so no-one else will be able to use it. However, this is an extreme solution, and it may be better to archive the old hard drive as you would old confidential paper files.

Planning to Recover from Disaster

An integral part of any business protection strategy must include plans for business to continue in the event of a destructive cyber attack or any other type of incident which damages or denies access to your operational business information – a *disaster recovery plan*.

The key objective of any disaster recovery plan is the ability to duplicate, isolate and then (importantly) restore critical business data and functions so that your business continues to operate effectively.

A disaster recovery strategy is worthless unless it actually works in practice. We know of far too many instances where businesses tried to restore their data from back-up files, only to find that their data is corrupted or only partly-recorded or that there are unforeseen incompatibilities between their back-up devices and their network storage systems. In any case, a critical part of a sound disaster recovery strategy is having 100 per cent certainty that your back-up data can actually be recovered and that your business systems can be fully restored.

The scope of any disaster recovery plan largely depends on the type – and scale – of your business. Having said that, it should at least cover the following basic considerations:

- Ability to maintain, or quickly resume, business operations.
- Safeguard your reputation, brand, image or market share.
- Minimise downtime caused by cyber attacks or other external factors.
- Prevent loss of custom through an inability to trade.
- Maintain confidence of employees, partners, clients and investors.

A well-structured and fully tested disaster recovery plan provides employees and managers with the confidence that if the worst happens, a process is already in place to ensure that business will continue, orders can be taken and staff will be paid. To that end, identify and take steps to protect areas of your business critical to its continued survival. These may include:

- Customer data
- Marketing/prospect data
- Order book and/or resource planning system
- Human Resources/payroll system
- Accounts/finance system
- Email/correspondence archive
- Operational/business process information

Obviously, how much of this list you use depends on the precise nature of your business.

You also need to consider (if you haven't already) the practical side of how to keep your data safe so that it can be accessed quickly and restored efficiently in the event of an emergency. Consider the following basic techniques for ensuring data is both adequately protected and readily available:

- Business data copied to tape/removable disk and stored away from business premises on a daily or weekly basis

- Copy backup data to an off-site location via a network link – this generally involves the use of storage area network technology
- Make use of high availability systems which keep both the data and system replicated and 'mirrored' off-site, enabling continuous access to systems and data

Staying Protected from Mobile Devices

IT managers and small businesses need to manage the security threats emerging from remote devices.

The first step is to assess where your business is vulnerable. Locating areas in the business with a much greater chance of having hardware lost or stolen, for example, means that you can focus your plan of action accordingly. A sales team that uses mobile devices on a regular basis is often a source of risk.

Data loss is either deliberate or accidental, so you need to communicate the importance of data protection and the legal implications of data theft to your employees.

Another way for companies to tackle this problem is to reduce and limit access to data, as restricting who can access what information can help to control the movement of important data. The easier data is to copy, the harder it is to control, so granting the right levels of access to the right people in your company is important.

Encrypting data on mobile devices is also a useful consideration.

A strict effective policy if data breaches have become common practice is to stop staff entering the workplace with personal devices that have storage capacity. They won't be tempted to copy data onto their USB or mobile phone and your data will be more secure.

Investing in technical controls in order to monitor and prevent data being copied is the key ingredient of the strategy in managing the threat of data loss. Additional password authentication also helps control who accesses certain systems, and security software can protect the company's hardware from theft or malicious attack through a USB port.

It is not necessarily a struggle for IT security to keep up with all the electronic gadgets and devices, but it is a struggle for them to keep up with how staff choose to use those items. Educating employees to try to alter their bad habits to good ones is vital.

Securing Your Equipment

Several high profile news stories over recent years recount instances where laptop computers were either been mislaid or stolen. Ironically, at least two of these high profile cases involved laptops belonging to members of the UK's security services.

The dangers of holding private/personal information, confidential customer data or financial information in un-protected or un-encrypted files is evident when computer equipment goes missing.

Implement appropriate security precautions and checklist procedures for employees who take company IT equipment off the premises – especially where this equipment relates to data held on mobile or portable devices like laptops.

Consider the consequences and potential impact of data loss. You need a contingency plans for when vital data goes missing. No matter how such information goes missing, back-up data should always be available to enable you to carry on your business with minimum disruption. (See 'Recovering from a Disaster' earlier in the chapter for tips.)

If you want good network security, you need to protect each component on your network, including PCs, routers, switches and all other connected user devices. Why? Because anyone who can access your network can also disrupt your network components and services. But don't focus your efforts just on internal devices – make remote and portable devices authenticate themselves to the network to limit who can see and access network services such as databases, shared files and printers.

Top tips for network security include:

- Typing in ever-changing passwords – these should contain a mix of upper and lower case letters, numbers and keyboard symbols.

- Updating software – without regular updates your systems may not be adequately protected against new cyber threats, as and when they emerge.
- Backing up data – regular back-ups ensure that your critical data is not destroyed in the event of a malicious cyber attack or physical incident, like theft of your computer hardware, fire or flood.
- Building a firewall – A firewall is designed to block the probing scans often associated with viruses, worms, and Trojan horses that can adversely impact your network.

As you can see there are so many aspects of network security that doing it all yourself is nearly impossible. Sometimes it helps to bring in an expert to help you through a rough patch or to get you moving in the right direction. When you have decided to bring in an outside operator, bear in mind that you're going to have to trust this person with a lot of sensitive data.

Working Safely from Home

Working at home, or using Internet or email while at home can present many risks. However, many of these risks can be mitigated with the application of a few 'good practice' security measures, and a degree of common sense!

Using your home computer

If you work at home predominantly on your personal computer, then at the very least you should consider updating, improving or upgrading your anti-virus and anti-spyware safeguards.

The risk of inadvertently passing viruses from your home computer into your work environment is also present, so good protection safeguards at home should be considered a 'must have'.

If you access your office network, or VPN (virtual private network) from home, then protecting your office passwords and access codes from spyware or keylogging programs that may be lurking on your home PC is critical.

Using your work laptop at home

Using an office PC or laptop at home may be considered a more secure option for home working than using your personal computer, providing of course your business has implemented 'best practice' IT security policies.

Transporting office equipment and critical business data between locations poses significant risks and you need to make sure you're doing all you can to protect data, passwords and physical security. (Earlier sections in this chapter offer pointers for each.)

Protecting against kids

You don't need us to tell you that your home is probably an entirely different environment to your office. If you have children or other guests in the house who may decide to take an interest in your laptop or PC, it's good practice to add (at the very least) some form of screen-saver password protection, to ensure that your machine can only be used by you and – critically – that none of your security settings can be changed or the integrity of your machine compromised while you're out of the room. Don't laugh – it happens every day and while any damage is usually repairable, you may not always be so lucky!

Data Breaches

There is quite a lot you can do to protect your company's data.

First of all, it is important to understand what data you have, where it sits and what risks it carries. Structured data from core applications normally lives in your datacentre. Traditional outside controls such as firewalls, intrusion prevention and access control at application, database and operating system level work well for protecting this structured data, but the simpler your IT infrastructure, the easier it will be to secure. If you have several different databases, combine them. Preparing for a move to the cloud is a good opportunity for a simplification exercise. See Chapter 3 for more on cloud security.

Make sure you have strong authentication in place. For example, don't let employees get in the habit of sharing passwords or leaving authentication tokens in their drawers. Any authentication solution you implement must be both difficult to hack and easy to use. A simple step that is often forgotten is to change the default passwords on all hardware devices in your network.

Data that leaves the database is not controlled by your perimeter protection and can grow without an audit trail. Encryption is essential, but has to be applied in the right place, where the data goes from being structured to its unstructured state. Data loss prevention (DLP) technology controls which data is allowed to leave the network and how, and can find and protect sensitive data. It will also let you set, manage and enforce security policies, playing an important part both in compliancy as well as in educating employees to act responsibly and keep information safe.

Sector Specific e-Crime Prevention Advice

The Welsh Government's business support is targeted at six key industry sectors. In the following sections we explain how e-Crime can affect these sectors and the steps businesses can take to protect themselves.

In addition, it is vital for the Welsh economy that entrepreneurship is supported to encourage more people to start businesses. New businesses rely on technology and the internet more than ever, so it is important they understand the threats and take steps from day one to protect themselves.

Unfortunately for all industry sectors, the infringement of IP is occurring increasingly in the workplace. For instance, there is report after report of illegal unlicensed software installed on company computer systems and the illegal or unlicensed copying of published material. If you don't keep a look out for this serious breach of company material, it could have serious repercussions for your company. Software piracy and other forms of copyright theft are illegal, with companies found to be using unlicensed software liable for prosecution. Directors can face fines of up to £5,000 in a Magistrates' Court and/or

six months in prison, and in the Crown Court, unlimited fines and/or up to 10 years in prison.

Advanced Materials and Manufacturing

Much of our manufacturing has transformed beyond its historical origins in labour-intensive production lines and heavy engineering, and is now focused on specialised and diverse activities, particularly in high technology areas. With more investment going into research and development (R&D) at universities, the Advanced Materials and Manufacturing sector has become increasingly dependent on Intellectual Property (IP) protection in order to remain competitive in the marketplace. Common types of IP protection include copyrights, trademarks, patents, industrial design rights and trade secrets in some jurisdictions. For many Advanced Material and Manufacturing companies IP protects investment in innovation, with income streams generated by IP rights crucial in enabling creators and investors to dedicate time and resources to new projects.

Top tips for IP protection in the Advanced Materials and Manufacturing sector are:

- Check the physical security of computers and back-up files.
- Determine who has access to your systems. You should know and log usage.
- Develop a clear IP compliance policy to help to raise awareness within the business of the value of IP.
- Ensure only legitimate, licensed traders are allowed on work premises.

The key steps businesses in the advanced materials and manufacturing sectors need to take are:

1. Read more about intellectual property and copyright theft
2. Make sure your employees read, sign and understand an IT security policy
3. Implement and test a disaster recovery plan
4. Backup your data regularly
5. Please visit `www.ecrimewales.com` to access useful Factsheets, Videos and Policies.

Creative industries

The Department of Culture, Media and Sport describes the creative industries as 'those industries that are based on individual creativity, skill and talent.' As a result, the creative industries are populated by a vast number of very small businesses, including freelancers, micro-businesses and SMEs.

One emerging trend within the creative industries is that of the 'digital nomad'. Digital nomads are a product of the WiFi and laptop culture, existing in an 'always on, always available' space, where they can work from their office, home, local cafe, or car park – sharing large media files, such as music and videos on a regular basis. Unfortunately, this way of working for many businesses within the industry, brings its risks. Unlike wired networks, wireless signals can be intercepted and/or hijacked without the need to physically connect to your network. It is not uncommon for someone sitting in a car in the parking lot to be able to access an unsecured wireless network and jeopardise everything on the entire network.

New technology also presents significant threats as well as very exciting opportunities for the UK creative industry. The development of digital technologies and the internet is providing new routes to market and facilitates immediate feedback from consumer to producer. Quite simply, a creative business whether they are large or small, cannot ignore the potential e-commerce market. However, wherever the trade goes, criminals are likely to follow and find ways to expose any weaknesses in your online offering. One area in particular that criminals are increasingly targeting is the credit card transaction process, as this open doors to all your customers confidential financial data, which will end up being used for fraudulent purposes. Therefore, it is imperative for any online retailer to improve security levels and reassure customers and their investors of their authenticity, trustworthiness and legitimacy. If they don't, the customers will simply go to another site, or back to the high street.

Another major crime which sets to threaten the future stability of the creative industry is that of 'illegal file sharers.' An alliance of creative bodies and trade unions argue that over 50 per cent of web traffic in the UK can be attributed to people illegally downloading content. The groups believe this could place around 800,000 jobs in the film, television, music and software industries in peril. All of us who deliver digital

content risk having that content copied and reused without notice. You can help protect a piece by branding it strongly. Put the client name in the photo, or specific names inside the text, or call back to a specific server. Storing links within a file rather than in an external text file also makes it harder for anyone to change them. Any solution is hackable, but if you can increase the hacking costs you'll lower overall theft.

The key steps companies in the creative sector need to take are:

1. Be aware of intellectual property and copyright theft
2. Protect your IT network
3. Make sure your staff sign and understand an acceptable use policy
4. You're probably going to be using social media tools – understand the risks and ways of protecting yourself
5. Please visit `www.ecrimewales.com` to access useful Factsheets, Videos and Policies.

Information and Communication Technologies (ICT)

Being in ICT, you'd think it would be safe to assume that you have all the bases covered when it comes to deterring cyber criminals – well think again. Knowledge brings with it complacency and if you're not keeping on top of your own security responsibilities then the trust you have gained from your customer can go out of the window in an instant.

Every organisation, whether they reside in the ICT sector or not, has a responsibility to adhere to the Data Protection Act, which typically involves having 100 per cent control and security over its own IT systems and databases. If you have been brought in as an outsourcer and you fail to protect your customer's confidential information, you may be committing or facilitating an e-Crime. Please visit the Information Commissioner's Office website for more details: `www.ico.gov.uk`.

Businesses utilising IT and the Internet need to ensure that their IT systems are not put at risk by employees who use those systems. Whether your business operates an 'open-use' policy (for example, not restricting access to any websites

or web email, and allowing employees to access them at any point during the day) or uses only emails and not the wider Internet, managing the risks involved with employee Internet use is a vital part of any effective IT security policy. See the section 'Managing Employee Behaviour' later in this chapter.

Another common theme amongst companies in the ICT sector is having the latest technology. On the surface this doesn't seem to scream 'danger' but when it comes to disposing of old hardware, problems can arise. While businesses are starting to recognise that the safe disposal of electronic waste such as computers and hard drives is a great step toward becoming environmentally friendly, many often overlook another issue it helps them address: Protecting valuable data. Companies need to establish and enforce policies so that they have a way to reclaim technology equipment when an employee upgrades to a new machine or leaves the company. Before disposing of any computer or data-storing machine, make sure that IT teams or senior members of staff erase all traces of applications and information from the machine so that company data isn't left on the old hardware.

Every sector within the UK relies on the effective uptake and implementation of ICT, so passing down your expertise to customers can be a very effective way to build confidence and trust. Producing a basic toolkit for customers on how to recognise common e-Crimes, such as Advance Fee Fraud, Denial of Service and Phishing Scams for example, will not only help your customers better protect themselves but it will make your job in the long-term that much easier.

The key steps for businesses in the ICT sector are:

1. Make sure you comply with the Data Protection Act
2. Ensure you have a disaster recovery plan and regularly test it
3. Ensure your staff sign and understand an acceptable use policy
4. Dispose of old hardware safely and securely
5. Please visit `www.ecrimewales.com` to access useful Factsheets, Videos and Policies.

Energy and Environment

Creating a low-carbon economy in the UK has become an important priority for government, business and investors alike. As a result, the energy and environmental marketplace has become huge. Vital to the future of this growing industry is the protection of its enormous range of innovative solutions to environmental problems.

For many Energy and Environment companies Intellectual Property (IP) protects investment in innovation, with income generated by IP rights crucial in enabling those in the industry to dedicate time and resources to new projects. Unfortunately for the industry, the infringement of IP is increasingly common.

The top tips for IP protection are:

- Check physical security of computers and back-up files
- Who has access to your systems? You should know and log usage
- A clear IP compliance policy will help to raise awareness within the business of the value of IP
- Ensure only legitimate, licensed traders are allowed on work premises

The emergence of new industries naturally brings a wave of new businesses. Check out the section 'Business Start-Ups' for more on getting started with online security.

The Key Steps Energy and Environmental Sector companies need to take are:

- Understand how to protect your copyright and intellectual property
- Please visit `www.ecrimewales.com` to access useful Factsheets, Videos and Policies

Life Sciences

As the UK economy shifts its focus from traditional assembly line operations to products that require significant innovation

and highly skilled employees, industry sectors such as Life Sciences have become increasingly important to the country's future growth. With more investment going into research and development (R&D) companies within the Life Sciences sector have become increasingly dependant on Intellectual Property (IP) protection in order to remain competitive in the marketplace. Common types of IP protection include copyrights, trademarks, patents, industrial design rights and trade secrets in some jurisdictions. For many Life Science companies IP protects investment in innovation, with income streams generated by IP rights crucial in enabling creators and investors to dedicate time and resources to new projects.

Top tips for IP protection are as follows:

- Check physical security of computers and back-up files
- Who has access to your systems? You should know and log usage
- A clear IP compliance policy will help to raise awareness within the business of the value of IP
- Ensure only legitimate, licensed traders are allowed on work premises

Key steps you need to take are:

- Protect your IT network
- Please visit `www.ecrimewales.com` to access useful Factsheets, Videos and Policies

Financial and Professional Services

Criminals that use the internet to compromise and target the financial industry have one purpose – to steal money.

A cyber criminal can attack thousands of victims and transfer money out of the UK within hours. Whilst it is true that financial institutions generally reimburse victims, anyone who has fallen victim to online fraud knows the damage it can cause. It causes deep distress to victims and threatens the integrity of the financial services industry.

Whatever the precise circumstances, the high profile loss of confidential data at HM Revenue & Customs in 2007 nevertheless

demonstrates how data can go missing despite there being strict protection procedures in place. Every organisation, whether they reside in the financial services sector or not, has a responsibility to adhere to the Data Protection Act, which typically involves having 100 per cent control and security over its own IT systems and databases. Should you fail to protect individuals' privacy, you may be committing or facilitating an e-Crime. Please visit the Information Commissioner's Office website for more details; `http://www.ico.gov.uk/`

As a starting point it is crucial you identify the most critical/sensitive information that needs to be protected. This needn't be all the company's data – only the information that will make you negative front-page news if it ends up in the wrong hands. You then need to find out where that sensitive information resides - computers hold information in servers, desktops, laptops, external hard drives, mobile devices, mobile phones, PDAs – the list goes on. You also need to figure out who has access to sensitive and confidential information – and who needs access. Chances are that 90 per cent of the people who have access don't need it. Check it out, remove unnecessary access, and reduce the risk.

Remember, IT security is the responsibility of every employee in your business, and every employee must understand that they have a role to play. For example, critical business information, such as company passwords, customers' information and sensitive corporate information can be needlessly exposed by employees surfing the Internet without due care and attention.

Key steps for companies in the Financial and Professional Services sector to take are:

- Make sure your staff sign and understand an acceptable use policy
- Protect your customer data
- Be aware of the Data Protection Act
- Be aware of the Payment Card Industry Data Security Standard
- Be aware of phishing scams that may use your organisation's identity
- Please visit `www.ecrimewales.com` to access useful Factsheets, Videos and Policies.

Business start ups

Many start up businesses are under the mistaken impression that their size, or the minimal security steps they have already taken, will protect them from cyber attacks. This assumption is both inaccurate and dangerous.

Around 40 per cent of all the businesses launched this year were home-based – possibly reflecting the lack of credit available, or an increased concern amongst entrepreneurs regarding overheads. However, the shift from traditional office-based working has introduced risks that are not always obvious, and dealing with these risks requires a planned approach.

Remote working requires you to carry out the same information security duties as an IT department in an office situation. You are responsible for backing up your information, keeping these backups safe, keeping your equipment and software up to date and making sure people cannot read, overhear or steal your information.

Reliance on inexperienced or under-qualified IT consultants/suppliers, to help manage these threats, could potentially do more harm than good to your start up business. Any risk to a businesses IT system can have a severe negative effect, leaving a company office door effectively 'wide open' for criminals to walk into.

As more and more start up businesses have increased their productivity by using networks and high-speed Internet connections, viruses have become the most prolific and costly security issue facing small to medium-sized businesses. Three main types of virus exist – basic viruses, worms and Trojans.

As a start up, knowing how and to whom to report an e-Crime can be confusing so if you don't know who to turn to for help please visit `www.ecrimewales.com/report`. The e-Crime Wales team can assess your situation and give you advice via email. They will not report this to the Police unless you ask them to, but you are urged to report all incidents, so that the Police can consider all courses of action.

As a start up, you may not be aware of all the risks out there, so if you're unsure, please ask. Be proactive rather than reactive. As a responsible business owner, you should be doing all you can to protect your business, staff and most importantly – your customers. Without their trust your new business will struggle to remain competitive.

The key steps business start-ups need to follow are:

- Make sure your staff sign and understand an acceptable use policy
- Visit `www.ecrimewales.com` to access useful Factsheets, Videos and Policies.

Chapter 3

Defending Your IT Network

In This Chapter

- Using passwords
- Keeping your system current and backed up
- Protecting your network from viruses and unauthorised entry
- Securing wireless and VOIP transmissions

If you want good IT system and network security, you need to protect each component on your network, including PCs, routers, switches and all other connected user devices. Why? Because anyone who can access your network can also disrupt your network components and services.

But don't focus your efforts just on internal devices – make remote and portable devices authenticate themselves to the network to limit who can see and access network services such as databases, shared files and printers.

In this chapter, we go through the areas you need to look at in order to provide your business with the best possible security devices.

Typing in Ever-Changing Passwords

Ensure that all employees use passwords – and require them to change passwords every quarter or even more frequently.

Passwords may not provide you with adequate protection and security in themselves because they're relatively easy to

hack, especially if they're nothing more than derivatives of your date of birth, initials, children's names and so on.

What makes a good password? These elements:

- Contains a mix of upper and lower case letters, numbers and keyboard symbols: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : ' ; ' < > ? , . /. It needn't be a word at all and is harder to break if it isn't a word.
- Use super-strong passwords containing sixteen characters or more. Longer passwords are harder to guess or break than short ones.
- Doesn't contain your user name, real name or company name.
- Welsh words are always good as they are harder to guess
- Is changed regularly.

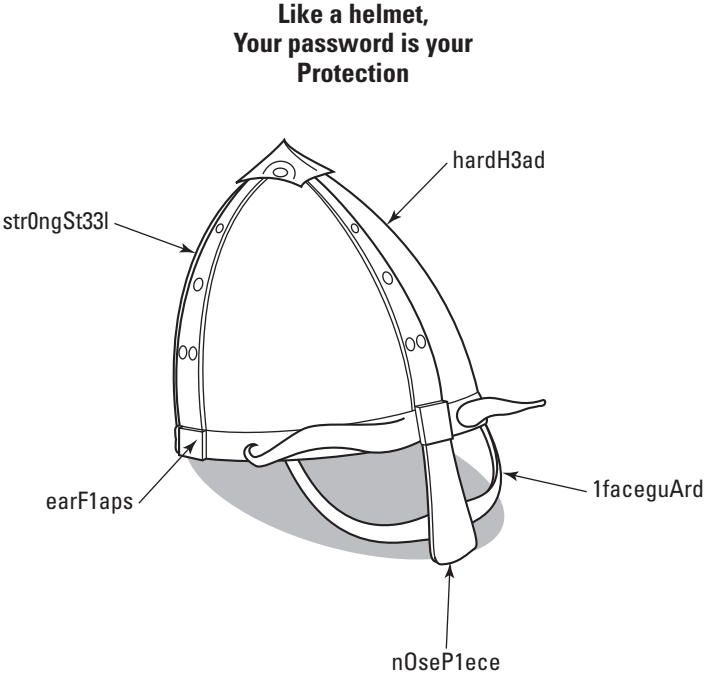


Figure 3-1: A security poster for education.

For a more secure and reliable way to authenticate users and prevent hackers from stealing passwords, you can use one of the many commercially available multi-factor authentication systems, which combine conventional passwords with a random code generator. Hackers must have a code generator in their physical possession in order to successfully crack the sequence.

Updating Software

All of your business software should be up-to-date and incorporate the most recent manufacturer *patches* – fixes from the manufacturer – and upgrades.

Without regular updates, your systems may not be adequately protected against new cyber threats, as and when they emerge.

Deciding on automatic updates

You can configure Windows Automatic Updates to operate in one of three modes:

- **Notify Only:** In this mode, Automatic Updates periodically queries Microsoft to see whether any critical patches are available. If they are, you click on 'Install' to make Automatic Updates download and install them on your computer. Choose this if you don't mind waiting for your computer to download the patches.
- **Download and Notify:** This is similar to Notify Only, except that Automatic Updates download (but not install) all available critical patches. If any critical patches are available, you click on Install and Automatic Updates installs the critical patches right away – you don't have to wait for a download to occur. One thing very nice about this feature is that the download occurs while you're busy with other things, and you can install the patches even if you're offline because they are already on your computer. (This is the favourite option for many users.)
- **Full Automatic:** In this option, Automatic Updates not only downloads critical patches from Microsoft, but also automatically installs all of them, at a time of day that you specify. This is a nice feature if you don't mind letting someone else decide which critical patches should be installed on your computer, without your permission.

Most operating systems and application software packages contain a provision for automatically receiving the latest upgrades over an online connection – most of which are free from the software vendor – so make sure that this function is enabled on all of your networked PCs.

Backing Up Data

If you aren't already, get into the habit of making regular (perhaps weekly) back-up copies of all of your important business data/information.

Aside from being good business practice, regular back-ups ensure that your critical data is not destroyed in the event of a malicious cyber attack or physical incident, like theft of your computer hardware, fire or flood.

Store a backup copy away from your office location and use encryption – or at least password protection – for any sensitive information about your company and customers.

Repelling Viruses

It may seem obvious, but make sure all of your PCs use anti-virus (AV) software, and if you're using Windows, add anti-spyware protection too.

Anti-virus applications are a low-cost means of protecting your systems and information from external threats. They look at the contents of each file, searching for specific characters or software code that matches a profile or pattern – called a *virus signature* – known to be harmful. For each file that matches a signature, an AV program typically provides several options, such as removing the offending pattern or destroying the file or email attachment that contains the virus.

An out-of-date anti-virus package may not be able to deal with emerging threats, so keep all your subscriptions current.

Intruders attacking a computer are most successful when they use a virus to gain access. When a machine is infected, software can be disabled and data destroyed, and the affected machine will attempt to infect other machines, consuming

available communications bandwidth, choking networks, and overloading servers.

To keep your networks in tip-top shape, use these tips:

- Follow the instructions to install antivirus software on every machine and keep the signature files current through automatic or manual updates at least weekly.

  Renew the automatic update capability annually as required to maintain a current virus signature file on every machine.

- Do *not* download material from the Internet without first ensuring that your AV application is active.
- Educate all computer users to remove or destroy infected files identified by AV software. Make sure they know how to remove their machine from the network during this process and who to call for help if they suspect an infection.
- Educate all email users not to open email attachments from unexpected and unknown sources to avoid unleashing a new virus not yet blocked by the AV application.
- Enable the AV application to automatically check every file source on each machine when it is used (including CD, USB storage devices and so on).
- Require periodic AV examinations of all files on a regular basis, preferably weekly, to catch problems missed at other checkpoints.

Building a Firewall

A *firewall* is a dedicated appliance or a software program which inspects network traffic passing through it and denies or permits passage based on a set of rules. A firewall is designed to block the probing scans often associated with viruses, worms, and Trojan horses that can adversely impact your network.

A firewall is like a security guard at the entrance of an office building. He (or she) scrutinises each person (message, file or program) coming and going. He may want to look at each person's identification by examining their employee badge or other credential. If the person coming or going is carrying anything, he may ask questions about it. If the person is

a guest, the guard may request that the user sign their name into a visitor's log. The guard has a list of rules that he uses to determine whether each person coming and going will be permitted to pass through. Occasionally he needs to turn someone away, for one reason or another. He will detail each such denial so his boss can later view who was denied access and why. Occasionally, the guard will need to call his boss and ask if a visitor is permitted to pass through (in a firewall software program, this takes the form of a pop-up window that asks if a particular program should be permitted to communicate or not).

A firewall's basic task is to regulate the flow of traffic between computer networks of different trust levels. Typical examples are the Internet, which is a 'no trust' zone, and an internal network, which is a zone of higher trust.

Standard security practices dictate a 'default-deny' firewall rule which allows only explicitly approved network connections. Such a configuration requires detailed understanding of the network applications and endpoints required for the organisation's day-to-day operation. Unfortunately, many businesses lack such understanding, and therefore implement a 'default-allow' rule, in which all traffic is allowed unless it has been specifically blocked. This configuration makes inadvertent network connections – and therefore system compromise – much more likely.

Do you have a firewall?

A firewall is designed to block probing scans that are often associated with viruses, worms and Trojan horses. If you have installed either a software firewall or a hardware firewall, you have far better protection than people who have neither.

A software firewall is a program that runs on your computer, invisibly (in the background), much like an antivirus program. The software firewall program carefully watches all communication coming into and leaving your computer. Each network message – or packet – is examined to ascertain its type, origin and destination. These properties are then compared to a list of rules to determine whether each packet should be allowed to pass through or not. If the message is allowed to pass, the firewall lets it move along towards its destination. But if the message is blocked, the firewall won't permit it to pass – and it will fail to reach its destination, like a postal letter that's intercepted in transit and simply thrown away.

A hardware firewall is an electronic appliance installed on a network. Its internal function is essentially similar to the software firewall, except that its protection is more centralised. All the computers on the network are protected by the hardware firewall, so none of the bad traffic on the Internet is permitted to reach any of the computers on the network.

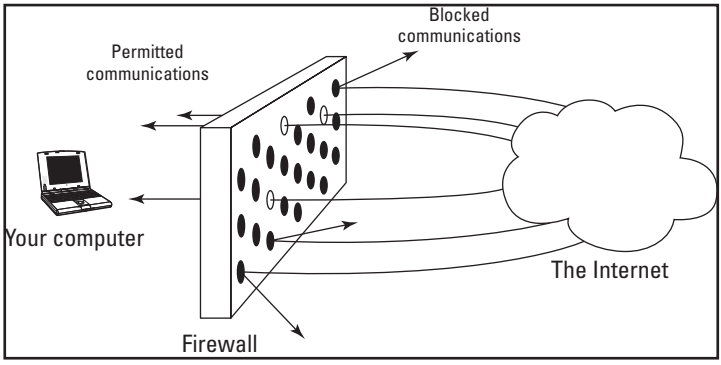


Figure 3-2: A firewall blocks unwanted communication from the Internet.

All firewalls screen traffic that comes into your network, but a good firewall also screens outgoing traffic.

The following list includes the most common features of firewalls:

- **Block incoming network traffic based on source or destination:** Blocking unwanted incoming traffic is the most common feature of a firewall.
- **Block outgoing network traffic based on source or destination:** Many firewalls can also screen network traffic from your internal network to the Internet. For example, you may want to prevent employees from accessing inappropriate Web sites.
- **Block network traffic based on content:** More advanced firewalls can screen network traffic for unacceptable content. For example, a firewall that is integrated with a virus scanner can prevent files that contain viruses from entering your network. Other firewalls integrate with email services to screen out unacceptable email.

- **Make internal resources available:** Although the primary purpose of a firewall is to prevent unwanted network traffic from passing through it, you can also configure many firewalls to allow selective access to internal resources, such as a public Web server, while still preventing other access from the Internet to your internal network.
- **Allow connections to an internal network:** A common method for employees to connect to a network is using virtual private networks (VPNs). VPNs allow secure connections from the Internet to a corporate network. For example, telecommuters and travelling salespeople can use a VPN to connect to the corporate network. VPNs are also used to connect branch offices to each other. Some firewalls include VPN functionality and make it easy to establish such connections.
- **Report on network traffic and firewall activities:** When screening network traffic to and from the Internet, it's also important to know what your firewall is doing, who tried to break into your network, and who tried to access inappropriate material on the Internet. Most firewalls include a reporting mechanism of some kind or another.

Without proper configuration, a firewall can become worthless.

Keeping Wireless Transmissions Secure

Many businesses now use wireless LAN (local area network), whose acronym is WLAN, connectivity because it's convenient, cheap and easy to install. WLANs allow for mobility around the office and deliver great flexibility. Unfortunately, they can also be insecure unless you take appropriate precautions.

Unlike wired networks, wireless signals can be intercepted and/or hijacked without the need to physically connect to your network.

To keep your wireless system secure, use these tips:

- Use encryption on your wireless access points (WAP). Make sure you have Wi-Fi Protected Access 2 (WPA2) – the latest security standard introduced by global, non-profit industry association, the Wi-Fi Alliance. You can select products that use this method by looking for 'Wi-Fi WPA2' in their specifications. WPA2 can operate in two modes:
  - **Personal mode:** Uses a pre-shared password or pass phrase for authentication. This simple approach ensures a computer can only get access to the WLAN if the password matches the access point's password.
  - **Enterprise mode:** This more sophisticated method is better suited to larger organisations needing stronger protection.
- Implement a Virtual Private Network (VPN) that encrypts all of the data that passes over the 'insecure' network so that it cannot be accessed by an eavesdropper.
- Install a firewall (see the preceding section) to separate an insecure part of the network from the secure area where your most critical data is managed.

  If your business uses the Internet, you probably have a firewall already in place, but don't assume that this provides protection for your WLAN.
- Keep the name of your wireless router generic. Your router identifies itself when it announces itself to the world. Rather than putting in information that makes it clear who owns the router or reveals your location or business name, use something common like 'wireless' or 'router 1' that doesn't give away anything critical.
- Position *access points,* which transfer data between your devices, away from the outside wall of your building to minimise leakage of radio signals. This limits the chances of interception from outside.
- Don't allow employees to add access points without management authorisation. One insecure access point can compromise your entire network.

Muting Vocal Security Issues

The general availability of high-speed, broadband Internet services has opened up the way for cheap telephone calls using the Internet. Voice over Internet Protocol (VOIP) means using the Internet for real-time voice conversations (as opposed to data exchange) and it is becoming an increasingly popular way to make telephone calls – principally because of the very low costs involved compared to regular telephone services, especially over long distance. Typically, calls are made via a PC's unique IP address using headsets or microphones, although handsets are now available which behave like ordinary telephones to all intents and purposes.

But, however ordinary making a call via VOIP may seem, the connection is still subject to the risks as any other form of unsecure Internet communication – especially if you're using VOIP over public or wi-fi services. However, by applying similar levels of security as you would during normal Internet usage, you can conduct VOIP conversations safely and securely – and certainly with no more risk than the 'traditional' switched telephone network.

Here are a few pointers to getting you safely onto VOIP services:

- It's absolutely crucial that your computer or network is properly protected. This means that your anti-virus, anti-spyware and firewall software must all be in place and up to date.
- Choose a VOIP supplier who offera secure encryption facilities. VOIP works over public Internet connections, which means there's a small risk of eavesdropping.
- Use passwords which are both strong and secure. Most VOIP services require password access – much like a regular Internet connection or a website log-in. Check 'Typing in Ever-Changing Passwords' earlier in the chapter for help guidance on how to select strong passwords.
- As with all other software-based services, check regularly with your ISP or VOIP service provider to ensure that your VOIP software is fully up to date with all available security patches and service enhancements.

At this stage, we don't necessarily advise replacing your conventional landline telephone with VOIP. By all means use

your VOIP service for as many of your calls as you like, but a power cut or other technical issues with your Internet connection can effectively leave you without a telephone service and – significantly – no means of contacting any emergency responders or utilities.

Protecting Public WiFi

As the world becomes dependent upon wireless and VoIP communication systems, so the risk and dangers of such an approach continue to rise. Wi-Fi technology now has the potential to bypass almost all existing IT security systems and open the door to hackers, unauthorised entry and just about every other security nightmare you can think of.

An unsecured wireless network can be easily compromised in the following ways:

- Hackers can access any sensitive files on your entire network, in the same way as if they were sat inside at a workstation
- Malicious individuals can launch viruses, spyware and other harmful code into your ICT system
- Rogue users can use your expensive Internet connection without your knowledge, using up the bandwidth you've paid for and possibly visiting illegal websites and conducting illegal activities while 'looking like it's you'

There are numerous straight forward and inexpensive measures you can take to secure your wireless network and enjoy its benefits without risk.

Five steps to protection:

1. Configure your wireless access points to 'turn-on' the in-built encryption feature. Most wireless access points will use 'WPA2' encryption which is strong enough to repel almost all attacks.
2. Configure your wireless access points to 'hide' or 'randomise' the ID name it uses to distinguish itself to users. Call it something that doesn't associate it to you, your business or location.

3. Configure your wireless access points to a unique password. All new access points come with a default password like '1234' or 'password' that most people never change. Make sure you change it to a secret password containing characters and numbers, and change it regularly.
4. Ban employees from adding new access points to the network without prior management authorisation.
5. Position wireless access points carefully to avoid areas outside your premises from being 'broadcasted' to. This will make it much harder for people to access your wireless network unless they are within the confines of your business.

Cloud

Cloud computing means that instead of all the computer hardware and software you're using sitting on your desktop, or somewhere inside your company's network, it's provided for you as a service by another company and accessed over the Internet, usually in a completely seamless way. Exactly where the hardware and software is located and how it all works doesn't matter to you, the user—it's just somewhere up in the in-definable "cloud" that the Internet represents.

Outsourcing the management of your business applications and data to a third party carries a myriad of benefits i.e. it lets you buy in only the services you want, when you want them, cutting the upfront capital costs of computers and peripherals. However, there are risks if you choose a poorly delivered or badly managed cloud computing service. This can include:

- Loss of control over your own data,
- Lack of access to your own data,
- Compliance breaches,
- Data protection
- Malicious insiders within your cloud computing provider.

Four-step plan to finding the most beneficial match with a chosen cloud computing provider:

1. Assess the risk of adopting cloud services
2. Compare different cloud provider offerings
3. Obtain written assurances from selected cloud providers as regards their security
4. Seek to reduce the security burden on your chosen cloud provider by ensuring your own house is in order

Maxing Mac Security

With the popularity of the Macintosh platform at the highest it's ever been, the manufacturer has become more vulnerable to cyber attacks. A number of anti-virus software products for Macs are out there, offering protection from e-Crime nasties, including viruses, worms, spyware and most other common forms of malware.

Good virus and malware protection is as much about common sense as it is good software. If you click a link in Google and it starts downloading a file – it's pretty safe to say that's a bad thing and you should delete it before it can do any damage.

The most critical step is to keep your Mac anti virus software up-to-date. Anti virus products for Macs are now widely available.

Other top tips include:

- Make it harder for criminals by hardening the common places malware targets. Run Apple's Disk Utility to ensure your file/folder permissions are correct. Harden newly created files by changing the default unmask.
- To secure your wireless network, enable your firewall.
- If you lose your machine, account logins and firmware passwords can't help anymore. Keeping your information encrypted is your only defence. You should use one of the various Mac password managers to keep all your confidential information.
- Authenticating an unknown app may get you in trouble, so having a second line of defence is now a must for most Mac users.

Staying Smart on Phone Security

There is a growing concern that mobility is beginning to jeopardise business security and IT networks are becoming vulnerable from the very thing that they are trying to incorporate. The increasing reliance of iPods, Smartphones and PDAs means that most employees now have personal devices that can store huge amounts of data and confidential information.

For instance, there are a number of possible methods to gain access to someone's voicemail unlawfully. To block this attack, you need to setup a new PIN to access your voicemail. By doing this you prevent automatic access to your voicemail. The customer service websites of operators should also be able to give you some good advice on PIN security and their voicemail service.

The growing operating systems on these powerful mobile devices is also tempting profit-motivated hackers to target these devices. Businesses need security tools that provide comprehensive protection: from the core of the network to the diverse range of endpoints that all IT managers are now forced to manage and secure, including all employee mobile devices.

This year, security firm Eset released details of a YouGov study it commissioned into mobile security. It stated that over a third of those employees surveyed were aware their Smartphone is under threat, but have not yet installed software to protect it.

To keep your mobile safe, you can

- Update your mobile phone's operating system regularly. Most manufacturers offer one every few months
- Think carefully about clicking on a link from someone you don't know or that is obscured by a URL shortener like Bit.ly
- Use caution when opening an attachment
- Consider installing a well known anti-virus system for your phone. Anti virus for the Android operating is widely available from the major security software organizations. Other operating systems, e.g. Apple's iOS may soon have anti virus software available as the amount of malware targeting their platforms increases.

- Create a security code to enter your phone
- Think of your phone as a computer, not just a device to make calls on.

Watching Over Websites

Most businesses see their websites as valuable pieces of property, but too few are doing enough to protect themselves. This new wave of website attacks carries a number of dangers for small to medium businesses across Wales.

Vandals often use hacking techniques to deface a website or destroy data and files, but there are also those who just want to steal resources or to cover their tracks by sneakily making use of hardware owned by legitimate businesses to carry out processing for illegal operations or to relay spam and viruses to others.

Protection doesn't have to break the bank, with the best defence against the majority of these types of attacks coming through installing and maintaining the latest versions of anti-virus and firewall software. As new threats are identified, updates are issued which can identify and neutralize most harmful operations before they have a chance to do any damage. Having a server fully managed by a reputable hosting company can also ensure that these defences are always in place.

It is also important to make the hacker's job as difficult as possible by obscuring any information that could be used to identify what software and versions the server is using. This will not only give you peace of mind but will also ensure your business can reap the rewards of operating online.

Chapter 4

Safeguarding Yourself and Your Home

In This Chapter

- Taking care with your home PC
- Foiling attempts at identity theft
- Spending online safely
- Doing your banking online
- Networking with confidence

Although e-Crime Wales and this book are here to protect your business from the dangers of e-Crime, you and your family may be at risk at home too.

As with protecting your business and company IT network, some simple steps and common sense can go a long way toward making safe online at home. In this chapter we show the basic steps to protect your home PC, safeguard your personal identity and shop and bank safely online. And, with more and more people posting on social networking sites such as Facebook, MySpace and Bebo, you need to know how to use these sites safely without putting your home and identity at risk – we tell you how.

Protecting Your Home PC

Online criminals are trying to attack your computer through self-replicating viruses and spyware (see Chapter 1 for information on e-Crimes).

Their intent is to steal from you or to attack other people. Either way, a successful attack stops your computer working properly. It costs criminals nothing to launch their assaults, so they don't care how many people are affected or what the damage is.

You need a multi-layered defence to keep criminals out:

- Security software including anti-virus, anti-spyware and a firewall programs – or a security suite that includes all three. Installing these safeguards is like keeping your doors and windows locked at home.
- Keep your computer up to date, block spam emails and use an up-to-date web browser to make it harder to get into your PC in the first place.
- Don't use your computer in administrator mode. It's safer to make a user account and log in with that for day-to-day use. In Microsoft Windows Vista, keep User Account Control switched on.
- Protect yourself against eavesdroppers and freeloaders by using encryption on your wireless network.

Make a regular backup of your music, pictures and other files as insurance to serve as a last resort safeguard in case you are affected by an e-attack.

Guarding Against Identity Theft

Your identity and your reputation are very precious. You need to look after them online.

Online crooks try to trick you into giving them your information, for example by sending fake emails with links to convincing but fraudulent websites (phishing). They want to spend your money, tap your bank account and use your credit cards.

To protect yourself against phishing and other e-Crimes:

- Block spam email – this also blocks most phishing emails.
- Use a modern web browser that warns you against known phishing websites.
- Don't give away your password or any other personal information to anyone.

- Choose strong passwords that use a mix of letters, numbers and punctuation. Use different passwords for different sites to make it harder for identity thieves.

Be careful about the information you give away about yourself online. For example, you can easily share information on blogs and social networking sites that helps identity thieves uncover your identity from public information piece by piece like putting together a jigsaw.

Shopping Safely Online

Millions of people buy online every day without any problems. With a bit of commonsense and knowledge, you can avoid problems with ecommerce.

Risks you may encounter when buying goods online include

- Paying for goods that aren't delivered or getting goods which don't match the description of what you paid for.
- Delays and hassles with receiving your purchases and poor after-sales service.
- Misuse of your credit or debit card details.

Ways to avoid some of these risks include

- Deal with reputable sellers especially when buying from private individuals and overseas companies. Most sale websites give buyers and sellers a chance to rate each other. Read those reviews.
- Look for evidence of a physical address and telephone contact details.
- Don't judge a person or company solely by their web site. As with phishing scams, a good-looking website may be just a cover.
- Check the seller's privacy policy and returns policy.
- Use an appropriate, safe means of online payment to get some protection against non-delivery (see the next list).

To make online payments safely, make sure you use a secure website:

- Look for a padlock symbol in the bottom right of the browser window and for the website address to begin with 'https://'

  Don't be fooled by a padlock that appears on the web page itself. It's easy for criminals to copy the image of a padlock. You need to look for one that is in the window frame of the browser itself.

  However, the padlock is not an absolute guarantee of safety and it says nothing about the business's ethics. If you get a warning about a certificate be very cautious indeed.

- Click on the padlock to check that the seller is who they say they are and that their certificate is current and registered to the right address.

If you're using the latest browser technology and the seller has the latest website security, known as an Extended Validation SSL Certificate, your address bar may turn green when you are on a secure site.

Use common sense to avoid some scams:

- If a deal looks too good to be true, it probably is. Cross-check information on the internet and see if anyone else has had problems with the seller or with purchasing a similar item.
- Beware of work-from-home scams which promise easy profits but never pay.
- Be extremely wary of anything offered in an unsolicited or spam email.

Banking Online Securely

Banking online is very convenient, but you have to protect your password and personal details so criminals can't access your account in your name.

The most common risks associated with online banking are

- Phishing scams which try to trick you into disclosing your password and details by posing as a message from your bank. Phishing scams are like a fake cashpoint machine that looks like the real thing. (Check out Chapter 1 for more on fighting phishing.)
- Identity theft caused by viruses or spyware that give criminals access to your bank account and other personal information stored on your computer.

Don't be fooled by impostors. Keep these tips in mind as you bank online:

- A bank will never send you an email asking you to disclose PIN numbers, passwords or other personal information or which links to a page that asks you for this kind of information. If you click on a link in an email that takes you to a page that requires a password or personal information, it is very likely to be a scam.
- Always make sure you are using a secure internet connection to connect to your bank. Look for 'https' at the beginning of the address and the padlock symbol. ('Shopping Safely Online', earlier in this chapter, has more information about secure websites.).
- Although many trusted organisations send emails containing legitimate links (for example to websites that contain more information on a given subject), always be careful when clicking on them. It is better to enter your bank's address into your web browser directly or use a bookmark that you created using the correct address.

If you believe your details may have been compromised in some way, always contact the bank.

Use common sense when banking online:

- Learn your password and PIN. Destroy any written record as soon as you can.
- Use different passwords for bank and credit card sites. Don't use the same password for every website.
- Use strong passwords. (Chapter 3 offers tips on building good passwords.)

- Avoid using public computers to access your bank.
- Never give your personal security details, such as account number or PIN number, to anyone you don't trust completely.
- Don't fall for money-laundering scams. Be wary of any 'business opportunity' that involves receiving or holding money for strangers.

A good source for further information, including information about known frauds, is your own bank's website.

Keep tabs on your money: If you spot any unusual transactions in your statement, report them immediately.

Staying Safe while Social Networking

Keeping in touch via social networking sites is part of everyday life for most of us, but disclose too much information and you could become an easy target for criminals.

Some people update their social networks with every detail of their lives, revealing intimate details such as their date of birth and home address. In some cases criminals will use websites like Facebook and Twitter to find out when their potential victim is out of the house. Telling the Internet that you're off on holiday is as good as shouting 'I'm out – burgle me'.

As a nation, we are becoming increasingly comfortable with sharing more and more information on the Internet – websites such as Facebook, Twitter, LinkedIn and Flickr (among others) let you communicate online with friends – and strangers if you choose – and build networks linked by shared hobbies and interests. However, it's important to consider your personal security and to make sure your privacy settings are up to date. Otherwise, your casual online chatter could end up giving cyber criminals all the information they need to make you their next victim.

You can avoid these risks and enjoy social networking sites by following a few sensible guidelines:

- Don't let peer pressure or what other people are doing on these sites push you into doing something you're not comfortable with. Just because other people post their mobile phone number or birthday, doesn't mean you have to.
- Be wary of publishing any identifying information about yourself. In particular things like: phone numbers, pictures of your home, workplace or school, your address, birthday or full name.
- Pick a user name that doesn't include any personal information. For example, 'iestyn_glasgow' and 'mandi_liverpool' are bad choices.
- Set up a separate email account that doesn't use your real name and use that to register and receive mail from the site. That way if you want to shut down your connection, you can simply stop using that mail account. This is very simple and quick to do using free email accounts from providers such as Hotmail or Yahoo! Gmail. (Other services exist.
- Use a strong password that combines letters, numbers and keyboard symbols.
- Use the site's features to protect yourself. Use the privacy features on the site you use to restrict strangers' access to your profile. Be guarded about who you let join your network.
- Be on your guard against phishing scams that ask for bank account numbers or other personal information. (Chapter 1 tells you how not to take phishing bait.)

What goes online stays online. If you publish something, even if you delete it later, you have no control over how it is stored, copied or archived. So, don't say anything or publish pictures that may embarrass you later. As a general rule, if you wouldn't say it to your boss or your grandmother, don't say it online.

Recognising and Dealing with Spam

Clickjacking is a malicious spam technique of tricking Internet users into revealing confidential information or taking control of their computer while clicking on seemingly innocuous websites.

These methods have a habit of spreading like wildfire over the Internet because it only takes one person to fall for it to open doors to all their online connections. Before you know it, hundreds have been targeted with the same technique and you run the risk of reputation damage because it was you who initiated it.

Some of the best tips to keep you, your home and others safe are:

- Try to minimise the number of third party apps and services that you install or allow to access your account, learn how to remove or disallow them and get rid of any that you no longer use.
- Don't click links in messages, pop-up adverts, wall posts or even links sent to you by friends without checking first if the person intended to send it to you. The few moments it takes you to check could save you from falling for a phishing scam or worse, infecting your computer.
- Never, ever reply to a spam message. If you can tell from the subject line that a message is spam, don't open it – delete it. Blocking inbound spam can also reduce the risks, and good security management by your ISP can ensure that malicious connections are blocked.
- The only way to ensure spam becomes a thing of the past is by confronting it head-on. Learn how to report spam, so you can prevent unsolicited messages from entering your e-mail inbox. If we all take these simple measures, we can lead the way to stopping spam altogether.

Chapter 5

Knowing What to Do if You're a Victim

In This Chapter

- When should I report an incident to the Police?
- Financial crimes
- Reporting illegal content
- Dealing with viruses, spyware and other malware

If you unfortunately become a victim of one of the many different types of e-Crime, you can take a variety of courses of action to report or rectify it depending on the nature of the incident. In this chapter we explain the different places where you can report an e-Crime.

However, if you're unsure of where to turn to, let us know at `www.ecrimewales.com/report` and we can advise you on the best course of action.

Reporting an Incident to the Police

There are times when your computer system starts to act strangely. Your natural first reaction is to blame the computer and seek help from IT staff.

With the wide use of computers in industry today, businesses need to have the IT support on hand to remedy day-to-day problems. Invariably, IT support establishes whether a problem is a computer fault or unlawful activity.

Procedures with the Police

If you suspect a crime, telephone or visit your local Police station, keeping in mind that the first officer you contact is unlikely to be a computer expert, but someone who determines the type of incident and the most suitable person or department to deal with it.

In most instances a call relating to e-Crime isn't be treated as urgent, but assigned to a traditional beat officer. This first responder officer obtains all the relevant facts and either deals with the incident himself or ensures that the investigation is passed to a more suitably qualified officer.

If you suspect that you're a victim of an e-Crime, you can call the Police in Wales using the new non-emergency police number, 101.

Informing about Financial Crimes

If you believe you're a victim of identity fraud involving credit or debit cards, online banking or cheques, report it directly to the financial institution concerned. They are responsible for undertaking further verification and investigation, and reporting cases of criminal activity directly to the police as appropriate for suitable subsequent investigation. ***Note:*** This process is applicable to England, Wales and Northern Ireland only.

Changes to the reporting of plastic card, online banking and cheque fraud were introduced by the Home Office on 1 April 2007, following discussion with the Association of Chief Police Officers (ACPO) and the financial sector, to reduce the level of bureaucracy involved in fraud recording, and to streamline the reporting and initial investigation of such frauds.

Identifying Illegal Content

The Internet Watch Foundation (IWF) is the UK organisation for reporting illegal content, specifically child sexual abuse content hosted worldwide and criminally obscene and incitement to racial hatred content hosted in the UK. Report illegal content at `www.iwf.org.uk`.

By reporting illegal content through the IWF, notice is given to the Police or Child Exploitation and Online Protection Centre (CEOP) and notice sent to the Internet Service Provider (ISP) of any illegal content.

Dealing with Viruses, Spyware, and other Malware

Everyone who uses a computer whether at home or work is aware of the threats of viruses, spyware and *malware* (**mal**icious soft**ware**). These threats could well be classified as *nuisance crimes* and effectively covered by legislation but invariably impossible to investigate on a local basis. Most of the nuisance crimes originate from outside of the UK, and Internet Service Providers (ISPs), Anti-Virus and other software manufacturers work with each other to share information in the continued fight against malware.

The critical issue for you as either an individual or business is that you follow the advice we give in this guide and install and maintain with the latest updates anti-virus software.

Chapter 6

A Dozen Best Security Practices

In This Chapter

- Using technology to guard your technology
- Changing things up and keeping current
- Backing up what you use; not using what you don't need
- Protecting your equipment
- Establishing trust and verifying
- Planning for failures and managing change
- Sharing your plan

These security practices apply to networks of any size, shape, or form. If everyone followed these practices – even if they didn't install all the various security mechanisms – there would be fewer systems for hackers to hack because all systems would be that much stronger. You can (and sometimes should) use additional security mechanisms, but by following these simple rules, you make your systems much harder to crack for very little expenditure on your part.

If everyone applied the best security practices to their networks, we all would experience fewer attacks and problems.

Studies show that a majority of intrusions and attacks could have been prevented by some simple fixes or changes, so take this advice to heart. Who knows – it could save you a lot of money in the long run!

Use Strong Passwords

Let's start first with what *not to do* when creating a strong, secure password:

- Don't include parts of your name or email address
- Don't include personal information like your birth date, names of family members or street addresses.
- Consecutive numbers are a bad idea. You can basically mix '123456' or any other common combinations.

The good password rules are:

- **Use a mix of lower and uppercase letters:** Mixing up your cases adds complexity and safety to your chosen password.
- **Add numbers:** Using letters, words, and phrases for your passwords seems both natural and easy to remember, but it's much safer to diversify.
- **Add symbols:** Symbols are the real secret ingredient to security. Since there are hundreds of symbols a hacking program needs to run through to correctly lock down one character of your password, adding one extra asterisk or exclamation point can make it extremely difficult for intruders to pry open your personal accounts.
- **Use your full password length:** Most websites prompt you to create a code with a minimum and maximum amount of characters, often between eight and 14. Since each additional character increases your odds of staying safe, be sure to max out the length of your password. If you can enter 14 characters, don't stop at 10 – those extra four characters will work to your statistical advantage.
- **Set sensible security questions:** Most sites offer a means to reset your password should you forget it. This is also one of the most common ways to break into an account. If you are asked to provide answers to 'Security questions' consider whether the answers really are secure. Secure means that you are the only person who can answer the question.
- **Change it frequently:** Changing your passwords every six months is good, but changing them every three months is even better.

Do not use a single password on multiple sites; that way if one is compromised you don't have to worry about the others. Devise a way to differentiate your password for each site you use, for example putting the first and last letters of the web site name at the beginning of the complex password.

Password cracking software is becoming more powerful and is using the power of the cloud – examples can be found at `www.wpacracker.com`.

Use Anti-Virus Software

One of the easiest ways for a hacker to gain access to your system is via a *Trojan horse program* which looks like something common – a screen saver, for example – but works secretly in the background to plant a virus or spyware.

It's easy to get a fun looking attachment from a well-meaning friend, double-click it, and install a Trojan instead. You won't even know it has happened, either.

Some viruses can do serious damage to your computers as well as disrupt network traffic. Email viruses can quickly overload your email servers and bombard friends, family, and clients with copies of the virus. Some viruses are difficult to remove, too.

Anti-virus software can stop Trojan horses as well as those pesky, irritating email viruses that go around like crazy. They use a search engine combined with a database of known viruses to search your computer.

Anti-virus programs are relatively inexpensive, are tested by independent labs, and are easy to install. Just remember to update the software at least weekly in order to keep it operating correctly. It's just plain silly not to protect yourself this way.

Never Accept Default Installations

Many software programs have no security features, and those that do are installed by default and use only the weakest settings. On top of that, most default installations include the

running of services that you may not need. These additional services are not securely configured, either. Not only do hackers know about these weak configurations, they also know how to search for them – and they will find them!

Whenever you install an operating system or application, be aware of the security settings available for that software and make the appropriate changes. For example, the default installation of Microsoft SQL Server leaves a blank password, which you need to change. The default installation of Windows installs web server and FTP capabilities, which you may not need. Another thing you don't need are operating systems that include a Guest account with a blank password.

Finding suggestions on the security settings from the vendor's website or from any one of the numerous security websites on the Internet is easy enough. Just be sure to make the changes to all the affected machines on your network; otherwise, you defeat the purpose of the security changes.

You'd be surprised how much stronger your system becomes when it's securely installed and configured.

Don't Run Unnecessary Services

If you don't need a web server, don't let it run. If you don't need FTP or telnet, don't let them run. If you don't send mail on your system, then there is no reason to use a sendmail program or SMTP. These services all have exploitable security holes.

In any case, why have something running on your system that's not going to give you any benefit? All they do in the end is use up computing resources and expose you to security breaches.

Install Security Patches Immediately

All software, even security software, occasionally contains bugs or holes that can be exploited. Typically, the vendor has the appropriate fixes located on their product website along with any instructions you may need to apply the fix.

Why apply these patches immediately? Because agencies send out alert notices when major security problems arise. The hackers monitor these alerts regularly and when they see one of interest, they start looking for systems vulnerable to the problem. They count on the fact that most network administrators are too busy with their regular duties to stop everything to apply fixes and patches. This is one of the most common ways that hackers get into a system, and it falls into the category of 'it could have been prevented if . . .'

Make sure you're on the mailing list for your software vendors' updates as well as the security alerts sent out by various agencies and websites. When you download a patch, don't let it just sit there – install it immediately.

Back Up Your Data

The most complete security in the world won't protect you if all your data is lost in a fire or other disaster. Make sure that complete backups are done at least once a month and incremental backups are made daily. That way, if all your data is lost, you can usually recover everything up to the day before the disaster struck.

Test your backups once every three months to make sure they can be read. It's very easy to issue the wrong backup command and save files in a format that is not easily recoverable and data can become corrupted. Testing ensures that you are saved from the horror of finding you cannot recover from your backups.

Protect Against Surges and Losses

All electronic equipment should be connected to surge suppressors to prevent destruction in the event of power surges. Even if you don't live in an area prone to heavy weather with lightning, install surge protectors on every piece of equipment because all electricity sources can suffer from peaks and spikes. All it takes is one fried component to unsettle even the most stable computer.

In addition to surge protectors, install Uninterruptible Power Supplies (UPSs) on your most important computers. Most UPSs

have a battery pack that keep your computer running long enough for you to safely power it down. Most Unix systems suffer horribly when they are not powered off in the correct manner – resulting in corrupted data or operating system.

You can get UPSs with varying levels of battery storage. Some only keep equipment powered for 15 minutes while others have the capability to keep equipment running for several hours.

Know Who You Trust

Give each user or connection only the level of access they need to accomplish their tasks and no more than that. This goes for users, clients, and other networks you trust to connect with yours.

Knowing your users is important because you don't want to give too much trust to someone who has had problems with authority and has a chequered employment history. You can always start out with a low level of trust on the network and increase it as the employee shows that he or she deserves your trust.

Many Business to Business (B2B) networks have interconnectivity with a number of other corporate networks to increase efficiency. For example, one company may regularly need parts from another company and the interconnectivity means that they can quickly access inventory levels of the product.

You need to know that your business partners in these connections are trustworthy and that they have done their best to secure their networks against attacks. If you are connected to a network that has little or no security installed, an attacker can gain entry to that system and, because it has a trusted relationship with your network, the attacker can use that trust to access your network, too.

Enable Logging and Review Logs

It's important for your systems to keep logs of what happens on your network. This includes who is logging on and off, what applications are being run and by whom, and what connections are being made and by whom. Your operating system

has logs available, but only if you enable them. Firewalls and intrusion detection systems create very large logs with enormous amounts of data.

Your logs aren't going to do you any good if you don't actually read them regularly.

They can be tough to read, but there are log parsing utilities that can group and sort them for you to make it easier to review. You need to know what looks normal on your logs or you'll never know what an abnormal situation looks like.

You can find many log parsers or analyzers for Windows and Unix systems at `http://online.securityfocus.com/tools/category/71`.

Expect Protection to Fail

Almost every security mechanism you can think of has an electronic element to it, and electronics can and do fail. Therefore, you shouldn't rely too heavily upon the protection being there – don't put all your eggs in one basket.

Firewalls, routers, intrusion detection systems and access control mechanisms often fail without warning, and you likely won't recognise that something bad has happened for some time. Your best defence is to prepare a plan of action ahead of time, and the best plan of action is to have a layered approach to security. Establish your perimeter with filtering routers, firewalls, and intrusion detection, but protect your interior with access controls and hardened software. If one layer of your protection fails, at least you have other forms of security to fall back on.

Manage User Accounts Well

As soon as a person terminates employment, disable his or her account. Don't wait a week or a month or a year.

While you're at it, look at all the other accounts on your network. Are there old accounts that should be deleted? Are there inactive accounts that should be disabled or removed? Are there any accounts that look strange to you? When was the last time anyone changed their passwords on their accounts?

Hackers often look for accounts that have been inactive for long periods and attempt to crack their passwords. A hacker needs only one account to get in. After the hacker has a legitimate account, he or she may be able to create administrative level accounts to gain full control of the system.

Managing accounts can be a real pain, especially if you have thousands of users on your network. However, these are the people you have given access to your system. Review user records on a regular basis to make sure that the accounts are accurate and have secure passwords.

Educate Your Users

Security doesn't happen in a vacuum. If people don't know the rules, how can they adhere to them? If people don't know what suspicious activity to look for, how can they know when to call security? Many companies make the mistake of spending lots of time and money to set up security rules and safeguards and then forget to tell the rest of their colleagues what they've done.

Don't make this same mistake, or you could lose an important security resource – the many eyes and ears of your users!

Your staff needs to know what dangers can appear, from viruses and Trojan horses to unidentified personnel snooping around the server rooms. They also need to know how to use the security tools you place at their disposal such as anti-virus software and encryption software. Your staff needs to know all this stuff, and they will be knowledgeable only if you make the effort to educate them. It doesn't have to be a fancy class with lots of bells and whistles, but it does have to inform and educate.

Whatever you do, don't educate via email – we all know that people don't read their email messages.

Chapter 7

Almost Ten Questions to Ask a Security Consultant

In This Chapter

- Looking into experience and training
- Checking references, associations and any criminal activity
- Finding out about support and ethics

A day may come when you decide to employ a security consultant, which is not a bad thing. There are so many aspects of network security that doing it all yourself is nearly impossible. Sometimes it helps to bring in an expert to help you through some rough patches or to get you moving in the right direction. If you can't find security consultants listed in your phone book, the Internet is always a good place to look.

But after you've made the calls and decided to bring a few people in for consideration, what do you ask? Here we give you the top ten questions and the acceptable responses to those questions. After you've gone through the interview, though, don't just rely upon the answers to your questions. Keep in mind that you're going to have to trust this person with a lot of sensitive data. Your gut reaction can be a guide as to whether or not you can actually work together.

Is This Your Day Job?

You may laugh at this one, but a lot of people who work as network administrators want to go out on their own and start a consulting company. However, they don't have the clientele built up enough to be able to give up their day jobs.

If your consultant is in this category, play it safe. This may be the perfect person for the job, but consider whether she will be able to give you the support you really need. The rest of the questions may help you decide.

How Long Have You Been Doing This?

Again, don't laugh because this is a completely reasonable question. If you were going to employ the person for a full-time position, you'd certainly ask this. Hopefully, you're not the first client for this consultant.

A good answer is at least three years. Security consultation isn't something that can be totally taught in university, and a person needs to have a number of years in real-life situations to be able to make good recommendations.

What Certifications or Training Do You Have?

Security training and certifications are a fairly recent development. Ten years ago it would have been difficult to find anyone who held certifications, but computer security wasn't a big deal then, either. Nowadays most good security personnel have at least one certification or another.

Some of the widely acceptable certifications are:

- **CISSP – Certified Information Systems Security Professional:** Testing is based on a general level of knowledge in all areas of security. Certification issued by ISC2 `www.isc2.org`.
- **SSCP – Systems Security Certified Practitioner:** Given by the same folks who issue the CISSP certifications. This is a slightly less stringent certification than the CISSP, but is more technically focused.

- **CISA – Certified Information Systems Auditor:** This general certification is issued by www.isaca.org.
- **CPP – Certified Protection Professional:** Issued by ASIS International at www.asisonline.org, this certification indicates a general level of proficiency in security management.
- **GIAC – Global Information Assurance Certification:** There are actual multiple levels to this certification, and each level indicates proficiency in a particular area of security. This is a relatively new program developed by SANS and governed by www.giac.org.
- **Security Certified Program:** Another good certification program with certification for both a Network Architect and a Network Professional. Get more information at www.securitycertified.net/ certifications.htm.
- **Cisco certifications:** Cisco Systems is a hardware vendor that offers network engineering certifications based on proficiency with their products. These are not security certifications, per se, but indicate a good level of understanding of networking technology. You can view the various certifications and training requirements at www.cisco.com/warp/public/10/wwtraining/certprog.
- **Microsoft certifications:** MS certifications come in all shapes and sizes and, because they are vendor-specific, indicate a level of knowledge with those products only. These are not security certifications, but some security knowledge is implied. You can obtain more information from Microsoft at www.microsoft.com/traincert/mcp/default.asp.

There are probably other certifications available, but these are the most common.

Just having a certification does not mean the person is an expert. You also have to take into consideration the number of years of experience the consultant has in the field and what her specialties are. None of the tests for certifications is easy, but don't rely upon certifications alone.

Have You or Any of Your Staff Been Arrested or Charged with Illegal Computer Activities?

This doesn't ask if the consultant or his staff has been convicted of any computer-related wrong-doing, just if they have ever been suspected of it. This is important because it may indicate whether or not the consultant is a reformed hacker or if the company employs former hackers. This is the consultant's opportunity to make an important disclosure, and it should be answered honestly. As a potential employer, you can check with your local law enforcement to see if the person has a record.

If the consultant answers yes, you need to take into consideration at what age this occurred. Many former or reformed hackers got into trouble in their teens and have truly changed their ways while others still dabble in the 'dark arts'.

Former hackers may have the skills for the job, but is their sense of honesty and dependability intact? You can get their permission to run a background check, but the doing the check may be a bit pricey for you.

Do You Have Any Ties or Associations with a Particular Vendor?

A tie to a particular vendor may indicate bias toward one set of security solutions as opposed to others. Ideally, you want someone able to look at all possible solutions without prejudice. On the other hand, if the consultant is a reseller for a particular vendor, she may be able to get better prices for the products.

Again, there are pros and cons to this, and the vendor should answer honestly.

Do You Offer Any Guarantees?

Believe it or not, the answer to this should be no. The reason is that no network can be made completely secure. New methods of breaching the security of networks are discovered every day. Additionally, the consultant may install a security mechanism that works, but he can't guarantee that you won't make changes to the system that alter the security level. Be wary of anyone who offers guarantees because it's nearly impossible to guarantee any security work.

Do You Offer Support for Emergency Situations?

What will the consultant do if the firewall she installed stops working? Will she help you track down an intruder if one penetrates the security mechanisms the consultant set up? Will the consultant be willing to be on call to you 24 hours a day?

The consultant should be able to at least offer this service at additional cost. If she can't offer it herself, then she ought to be able to offer some sort of support solution. If security consulting isn't her day job (see the first question), then she probably won't be able to commit to 24-hour support.

What Would You Do If You Discovered One of My Employees Doing Something Questionable or Illegal with My Computers?

This is an ethics question. No law or rule says the consultant must do anything, but he should feel duty bound to tell you what he discovered. This can be a very touchy area because things are not always as they seem. For example, finding

hacker tools on your network doesn't necessarily mean that your employees are hacking into your system. Those same tools are used to check for vulnerabilities in a system. Someone may have taken it upon himself to check the security of your system without your knowledge.

In any case, your consultant should be prepared to share with you any irregularities found in or on your network.

Do You Have References or a Client List?

Remarkably, the consultant may well answer, 'I have many clients, but I'm not at liberty to tell you who they are.' This is due to the confidentiality agreements between the consultant and her clients. Many companies don't want to advertise the fact that they've hired outside help. They also don't want others to know what the consultant did for them.

If your consultant can't give you a list of clients or references, she should be able to give you an idea of the types of work she has done and the sort of companies she's worked with. For example, she may be able to say 'I've installed firewalls and designed extranets for the car industry.' That sort of information is hard to confirm, but you should be able to get enough information out of the consultant to give you some feeling of comfort.

Chapter 8

Almost Ten Myths about Computer Viruses

In This Chapter

- Exposing ignorance
- Indulging in wishful thinking – and why that's a rubbish idea
- Being realistic about the damage viruses actually do
- Exercising prudence but stopping short of paranoia

Viruses are largely misunderstood by most people – including some computer professionals. Here we give you ten common misconceptions about viruses, and the straight unvarnished truth.

My Computer Stopped – I Must Have a Virus

If your computer stops, it could be because of a virus, but it probably isn't. Bottom line: It's in a virus's best interest to let the computer continue to operate so the virus can continue to use the computer to spread itself to other computers.

The 'best' biological viruses in nature are like this, too. If they kill their host too quickly, there goes their opportunity to spread. A 'better' biological virus – like a computer virus – may make its host sick, but well enough to keep spreading the virus.

That said, a virus writer could construct a virus that caused severe data damage only after it had been on the computer for an extended period of time. However, there is the risk (to the virus writer) that the virus may be detected and eliminated by antivirus software prior to the time it is programmed to inflict damage.

If you keep your antivirus program, firewalls (hardware and software) and antispyware software in good working order, you suspect hardware or Windows for a glitch and a virus last of all.

I Have Antivirus Software, So My Computer Can't Get a Virus

Wrong answer. Even with antivirus software, several different factors mean that a virus can still get in and/or hide in your computer:

- If you fail to keep your antivirus signatures up to date, then any new virus may be able to get inside your computer.
- If the 'real-time' antivirus mechanism in your antivirus software is turned off or deactivated (this can and does happen in the real world from time to time), then the virus can walk right into your computer while the antivirus program is sleeping.
- A brand-new virus can get into your computer even if you keep your antivirus signatures up to date. Remember, it can take a few days or longer for the antivirus software companies to detect, capture, and dissect new viruses before they can update their signature files. Even then, your computer will be protected only after it downloads the new signature file from the antivirus software company.
- If you've been running your computer prior to getting antivirus software and you've put any files on it from any outside source – even if you've never connected to the Internet – there could already be a virus on your computer.
- If you don't follow the installation procedures and skip the all-computer scan that most antivirus programs want to do when they're first installed, it's possible that a virus that you caught earlier is still lurking in there.

All Viruses Are Destructive

Some viruses exist only to replicate themselves, and other than that, they do nothing harmful.

But a purist would say that even these are harmful, because they upset their computer's balance. A system with even a benign virus is tainted, and there could someday be some unintended consequence of that.

Bottom line: This one's arguable either way.

Viruses Can Damage Computer Hardware

Some expert out there is going to have a good counter-argument, but for the most part, this fear is false.

Here's how it looks from the virus writer's perspective: Why aim for the hardware when there's so much brittle software that can be damaged? Go for the easy target first. Besides, if the virus hurts the hardware, how's it going to spread itself any further?

The purist would argue that a virus can damage computer hardware by giving it instructions that make the system misuse some part of itself (for example, by writing excessively to the hard drive), but few such hardware-eating viruses have been released. This is partly because there are so many different types, makers, and formats of computer hardware that one virus would be hard put to destroy all of them. Besides, nearly all computer hardware has built-in safeguards that prevent any real damage.

I Need More Than One Antivirus Software Program to Be Fully Protected

No, and no. As long as you stick with one of the ten or so well-known brands of antivirus programs, you'll find that they

all develop new virus signatures at about the same time. So if you're thinking of switching from <Brand A> to <Brand B> because you think that <Brand A> gets their virus definitions out sooner, don't waste your time.

If you're wondering whether this myth means you need to have two different antivirus programs on your computer, don't even try it. Because of the way they work, you can only have one antivirus program running on your computer. The antivirus install programs won't even install an antivirus program on a computer if it even suspects that there is one there already. The install program is trying to avoid a fight, and you should too.

You Can't Get a Virus from an Official Software CD

It's rare, but getting a virus from a software CD has happened, and it very well could happen again. The big software companies have very good and almost byte-tight procedures that eliminate the possibility that a virus can sneak into a software development lab and from there to a CD master.

It can happen, so we won't laugh if you scan CDs for viruses before installing software from them. Promise.

Antivirus Software Companies Create Viruses

Do the maths: The antivirus companies have enough business trying to keep up with viruses 'in the wild' that they'd be idiots to risk causing trouble for themselves.

This sounds as crazy as Microsoft and Intel being in cahoots to keep people buying newer computers! Makes an entertaining (if trite) premise for a film, maybe; doesn't hold up so well in reality.

Some Countries Sponsor Virus Writers and Hackers

This one's actually true. Three or four countries do have state-sponsored hackers, mostly aimed at disrupting things in the United States. Other countries recently targeted include Estonia and Kyrgyzstan.

Official attempts to disrupt and break into foreign information technology go back at least as far as the British code breakers who figured out the Nazi 'Enigma' encryption machine in World War II. The adversaries have changed over the years, but their struggle has kept pace with the development of cyberspace, and it continues today.

Viruses Do Not Affect Macs

Wrong answer. Macs are just as vulnerable to viruses. The most critical step to prevent viruses is to keep your Mac anti-virus software up-to-date.

Other top tips include:

- Make it harder for criminals by hardening the common places malware targets. Run Apple's Disk Utility to ensure your file/folder permissions are correct. Harden newly-created files by changing the default unmask.
- To secure your wireless network, enable your firewall.
- If you lose your machine, account logins and firmware passwords can't help anymore. Keeping your information encrypted is your only defence. You should use one of the various Mac password managers to keep all your confidential information.
- Authenticating an unknown app may get you in trouble, so having a second line of defence is now a must for most Mac users.

Chapter 9

Ten Tips to Prevent Data Loss Today

In This Chapter

- Identifying where sensitive information is and who has access to it
- Guarding electronic transmissions
- Disposing of hardware and hard copies safely
- Keeping employees aware of threats

If you're reading this chapter first, we're guessing it's because you're in trouble – or at least you think you might be. We've all been there, so here are some steps you can take *today*.

Identify the Information that Needs to be Protected

You aren't looking for *all* information, just the sensitive and confidential information – the stuff that will make you (horrible) front-page news if it wanders off! Start with the obvious – customer details and product designs – and work from there.

Now you know what you're looking for!

Find Out where Sensitive Information Resides

This sounds simple, but is it? Computer systems hold information in servers, desktops, laptops and external hard drives . . .

for starters. Then you have mobile devices, mobile phones, PDAs (personal digital assistants). After this come other gadgets such as digital cameras and perhaps USB storage devices. Finally, you have to list all the people with whom you share the information – partners, suppliers, and even customers.

Now you know where it is!

Recognise who has Access to Sensitive and Confidential Information

The quick answer is *only those who need it*. The actual answer is *more than you thought*. You need to figure out who has access – and who *needs* access. Chances are that 90 percent of the people who have access don't need it. Check it out, remove access where it makes no sense, and reduce the risk.

Discover the Processes Involving Sensitive Information

How is the information used and why? Information is the life-blood of an organisation, but a small leak is like a shaving cut – the blood goes everywhere! By finding the processes that involve the sensitive information, you can work to protect them first. Manual process steps are fine as a first step to a more comprehensive solution.

Spot When and Where Data Goes Offsite

If data is sent offsite – whether as a backup tape, portable drive (in or out of a laptop), or CD-ROM – it should be encrypted. Although guarding sensitive data should be your number-one

priority, it's good practice to protect *all* data that's going out for a stroll. Develop an encryption policy for sensitive and confidential information – and a process to go with it.

Track the items sent: Sign out, sign in, report. That way you know if something goes missing, but you won't have to worry – after all, *it's encrypted*.

Guard against Hardware Loss

What do people lose? Laptops, mobile phones, PDAs. These mobile endpoints must be protected. Laptop encryption and anti-malware needs to be at the top of your security list.

Protect Information in Motion

After protecting systems from physical theft, which is one of the easiest ways to leak data, you also have to look closely at protecting the data in motion.

Email is the number-one culprit here. Look out for distribution lists that contain email addresses that aren't within your company and consider putting a data-loss prevention application on the email gateway to prevent your data from getting into the wrong hands. Then look at other ways information might escape, such as instant messaging and web-based email.

Consider how Reports and Printouts are Destroyed

Nearly a quarter of all data-loss incidents are from printed matter. Sensitive information has to be *suitably* destroyed, and its destruction checked. Put document shredders near photocopiers and outside meeting rooms. If you're using a third-party shredder, ask: Do they shred onsite? If not, then *should* they – at least for some of the information?

Look at How You Dispose of Outdated Technology

How are old laptops, mobile devices and servers disposed of? Is the data on them adequately erased? Create a policy and a process to ensure that disposal is done correctly every time – even if that involves cremating the information – and that you have a report to prove it.

If you don't do a good job with the destruction and the server turns up on an auction site, the results can be a tad embarrassing. (Classic understatement there.)

Start an Education-and-Awareness Programme

Send out an email outlining one of the threats your organisation has faced or expects to face, and the implications of data loss. Send out another one next week, and another the week after. Spoof an attack of some sort; make it one that can identify the people who fall for it – that really brings home the dangers. As with fire drills, this isn't something that happens just once and then rests on the assumption that everyone knows what to do. The message and the process have to be repeated regularly. The big difference between fire drills and data-loss education is that data threats are changing all the time. (At least all that novelty makes for a more interesting drill than standing outside in the rain.)

Chapter 10

More Than Ten Websites to Go to for Help

In This Chapter

- Checking out the e-Crime Wales website
- Browsing helpful government sites
- Getting support for your business
- Banking, shopping and socialising safely

Thank goodness for the Internet! Not only did the Internet make it easy to research information for this book, but it is a real life saver for people who need the answer to their question NOW.

Without further ado, here are what we consider to the best websites for information (in no particular order of significance). Enjoy!

www.ecrimewales.com

The e-Crime Wales website is a comprehensive online resource for information about e-Crime. Log on to find out about different types of e-Crime and how they are perpetrated.

Find out how you may be vulnerable to e-Crime and the effects it can have on victims. Above all, discover how to protect your business, employees and IT networks from this very real threat.

Articles from e-Crime Wales and the industry are published regularly and keep you up to speed with the latest news and developments, and advice on how to report e-Crime in Wales.

You can also share your e-Crime experience; learning from the experiences of others is an excellent way of underlining the critical and devastating impact that e-Crime can have on a business. It is also an ideal way of helping everyone gain a better insight into the nature of e-Crime and the simple steps you can take to protect yourself and your business from enduring a similar experience.

www.getsafeonline.org

The UK's national Internet security awareness campaign is a joint initiative between the Government, including the Cabinet Office, Department for Business, Enterprise and Regulatory Reform (BERR), Home Office, the Serious Organised Crime Agency (SOCA) and private sector sponsors eBay, Microsoft, HSBC, Symantec and Cable & Wireless. It aims to raise awareness of Internet security issues amongst consumers and small and micro business.

www.business.wales.gov.uk

For business information, advice and support go to the Welsh Government's Business Support website where you can access information regarding support on everything from starting up and expanding your business to exporting your product and bringing your business to Wales.If you need to know about available financial support, property or the broadband and ICT networks in Wales, this website can help you find out more.

www.iwf.org.uk

The Internet Watch Foundation (IWF) is the UK organisation for reporting illegal content, specifically child sexual abuse content hosted worldwide and content hosted in the UK which is criminally obscene or contains incitement to racial hatred.

Reporting illegal content through the IWF prompts notice to the Police or Child Exploitation and Online Protection Centre (CEOP) and alerts the Internet service provider (ISP) of any illegal content.

www.sans.org/resources/policies

The SANS Institute is a large security training and conference company that offers excellent templates for IT security policies, which you can download from their site. These policies are a good starting point and cover the full spectrum of IT security, including acceptable use policies, password policies and remote access policies amongst many others.

www.ukpayments.org.uk

The UK trade association for payments and for organisations that deliver payment services to customers is also the main industry voice on issues such as electronic payments, electronic banking and e-banking fraud.

www.banksafeonline.org.uk

The UK banking industry's initiative to help online banking customers stay safe online, this website shows users the types of online banking scams around as well as how to spot them. You can also report a scam by forwarding suspect emails.

www.antiphishing.org

The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types. Visit this website for further advice on avoiding phishing scams and also to report suspicious emails.

www.ceop.police.uk

The Child Exploitation and Online Protection Centre is part of UK police and is dedicated to protecting children from sexual abuse wherever they may be. That means building intelligence around the risks, tracking offenders and bringing them to account, either directly or with local and international forces,

and working with children and parents to deliver their unique ThinkuKnow education programme.

www.thinkuknow.co.uk

On this site you can find the latest information on popular sites, mobiles and new technology. The site includes an area for people who work with or look after young people, with resources on online safety which can be used by teachers or at home. Most importantly there's also an area in which anyone can talk if they feel uneasy about someone they have contacted online.

www.cybermentors.org.uk

CyberMentors is all about kids helping kids online. Young people have the ability to guide and support each other, and this programme empowers them to do just that. The CyberMentors website has a social networking model to allow young people at different levels to mentor each other. As well as mentoring, the CyberMentors programme teaches young people how to safely explore the Internet and how to report and handle both cyber and real-world bullying.

www.actionfraud.org.uk

This site bills itself as the UK's national fraud reporting centre. It also has sections covering victim support, fraud prevention and self-protection across a wide range of criminal activity, including online fraud.

www.knowthenet.org.uk

This site contains a wide range of articles on getting the best out of the internet, whether you're using it for business or for pleasure. Amongst other things, it includes helpful advice on e-crime, data protection, dealing with viruses and preventing spam.

Appendix

Glossary

advance fee fraud: Any fraud that tricks victims into paying money up front on the false hope of receiving a large windfall later. See *Nigerian letter*

adware: A generic term referring to a class of software that causes a victim's web browser to display pop-up advertisements and advertising banners.

antivirus software: Software specifically designed for the detection and prevention of known *viruses.* You can also get more advanced packages with *spyware*/*spam* detection

attachment: Files, such as programs or documents, attached to an email. Attachments may contain dangerous *malware*.

authentication: The process for verifying that someone or something trying to enter a computer network is who or what it claims to be. In private and public computer networks authentication is generally done with passwords.

backup: Make copies of data to use to restore the original after a data loss event.

backdoor: A generic term referring to a method of gaining access to a computer without the owner's knowledge or consent.

bots: Computers that perform tasks without human input. Increasingly used for fraud and other malicious purposes.

botnet: A number of computers that have been set up to forward transmissions (including *spam* or *viruses*) to other computers on the Internet without their owners' knowledge or permission. Also known as a *zombie* army.

browser hijacker: A generic term referring to any piece of software which affects the functioning of a web browser against the user's wishes and perhaps without their knowledge.

bug: An error or problem in a computer program. A slang for *virus.*

certificate: A digital identity *authentification*. Also known as a public key certificate.

click-jacking: An attacker uses multiple transparent or opaque layers to trick web users into revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

cloud computing: The practice of using a network of remote servers hosted on the internet to store, manage and process data, rather than a local server of personal computer.

cold call scam: A scam where apparent Microsoft employees 'helpfully' call users claiming viruses are spreading through their computers. Concerned victims grant remote access to the alleged Microsoft caller to solve the problem, but in reality sensitive data is being captured, files compromised and the call recipient put at risk of identity fraud.

Conficker virus: The Conficker virus spreads through file-sharing, removable devices and shared computers with weak passwords, and it has infected more than ten million windows PC's worldwide to date.

cookie: A text file created on a computer by a website when a user first visits the site. It's used to store information that the website can use during the user's current and perhaps subsequent visits. May be used to provide targeted pop-up advertising (*adware*).

cyber-bullying: The use of the internet to bully, threaten and cause a person distress. Cyber-bullying can be carried out via instant messaging applications, email or social networking sites.

cyber-stalking: Using the internet, particularly social media to keep an eye on other people's activities including where they are and who they are with. Cyber-stalking is often a result of over-sharing personal information or having low privacy settings.

data breach: A data breach occurs when company-sensitive information is accessed illegally by a third party through hacking or any unauthorised access.

data flood: The act of sending so much data to a computer that its hard disk drive space is exhausted, causing it to become unresponsive or crash. An attacker may attempt this by sending the target very large email messages, for example.

Data Protection Act: A United Kingdom Act of Parliament which defines a legal basis for the handling of information relating to living people. It is the main piece of legislation that governs protection of personal data in the UK.

data miner: A type of *spyware* which gathers information from the computer on which it is installed and sends this information back to an attacker. This information might include users' logon details or credit card information typed into website forms, for example. Other data miners record users' Internet browsing habits which may be employed for legitimate marketing purposes.

DDoS attack (Distributed Denial of Service attack): A *DoS (Denial of Service)* attack launched from multiple computers against one (or relatively few) targets. The attacking computers are usually coordinated together, so they have a far greater effect than if the attack was launched from a single computer.

dictionary attack: The act of attempting to crack passwords by testing them against a list of dictionary words.

domain hijacking: The act of assuming or taking over a domain name, not necessarily illegally.

DoS attack (Denial of Service attack): An attack whereby the target is deliberately prevented from providing or receiving a particular service.

dumpster diving: The act of rummaging through the rubbish thrown out by commercial businesses or private residents searching for items of value. From an IT security point of view, an attacker may find all sorts of valuable information from the likes of discarded letterheads, utility bills, old credit card receipts, printouts and reports etc. which may be of great assistance to them in a potential attack.

419 fraud: See *Nigerian letter*.

e-Crime: The use of networked computers, telephony or Internet technology to commit or facilitate the commission of crime.

email bomb: A *DoS attack* in which a user's email account is targeted by bombarding it with more email messages than it can handle, thereby preventing the acceptance and delivery of legitimate email messages.

email filter: Software that filters out spam and other potential dangers from incoming emails.

email virus: Malicious computer code sent as an email attachment.

encryption: Converting data into a code so that it cannot be read without a key.

filter: A program that blocks potentially harmful or unwanted emails/programs.

firewall: Hardware or software installed on a computer or network to prevent unauthorised access over the Internet.

geotagging: The relatively recent phenomenon of posting up-to-date information on where people are and what they are doing. Often takes the form of 'checking in' to establish whether the person is in restaurants, hotels or shops.

hacker: A person who uses their computer knowledge to enter computers or networks without the owners' knowledge or permission often for malicious purposes.

hacktivism: Hacktivism is defined as hacking and activism merged together, where hackers use their hacking skill for political activisim usually to oppose a certain ideology or event or to achieve a political goal.

HTTPS: The method whereby page requests and page information between a browser and a web server is encrypted and.

identity theft: The fraudulent act of collecting sufficient personal information about an individual so as to assume their identity for the purposes of carrying out some other illegal or malicious activity.

insider threat: Danger employees pose to a business's computer system.

IP address: The unique combination of numbers that identify a computer on the Internet.

keylogger: A program which monitors and records keyboard activity. Although there are legitimate uses for keyloggers, an attacker can use a keylogger program to steal usernames, passwords, bank account and credit card details for example.

malware: A generic term referring to any piece of software written with malicious intent or which has a harmful purpose. *Adware*, *spyware*, *viruses* and *Trojan horse* programs are all types of malware.

Nigerian letter: A confidence trick in which the victim is persuaded to give comparatively small sums of money or bank details in exchange for huge returns. Too good to be true.

patch: A small piece of software designed to update or fix problems with a computer program or its supporting data. This includes fixing bugs, replacing graphics and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems.

pharming: An attempt to steal personal information using false web sites. A scam technique similar to *phishing*.

phishing: The fraudulent act of sending bogus, spam emails (which appear to originate from a legitimate organisation) which entice the recipients to visit a fake website (which is an almost exact replica of the organisation's genuine site) for the purposes of gathering personal or sensitive financial information from them.

pop-up: A supplementary and often unwanted window displaying an advertisment. Pop-ups may contain undesirable or otherwise unwelcome content and may have design elements that make them difficult or impossible to close.

rogue access point: A wireless access point that has been installed on a secure company network without explicit authorisation from a local network administrator.

root kit: Tools hackers use to infiltrate a computer or network.

scareware: Scareware consists of pop-up advertisements that appear to warn users of supposed security threats and offer the victim the chance to pay to download anti-virus software. Using popular and misspelled search terms, criminals divert people to sites that are seeded with fake warnings about virus infections. Never purchase the suggested software from these sites and if something is wrong with your computer, take it to an independent computer repair specialist.

spam: The electronic equivalent of junk mail or, as a verb, the sending of such. Thanks to the availability of huge email address databases and the relatively small cost of sending emails, spam is a lucrative business and now accounts for the majority of all email messages.

spoof: To falsify one's identity or the identity of a computer. For example, an intruder may spoof the *IP address* of the computer from which he is launching an attack in order to cover his tracks or to make it appear that another, innocent party is responsible. Often, spammers spoof the email address from which their junk mails are being sent so that they are more difficult to track down or take action against.

spyware: Software installed on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.

SSL: Secure Sockets Layers (**SSL**), are protocols that provide secure communications on the Internet for such things as web browsing, email, and other data transfers.

Stuxnet virus: The Stuxnet virus looks for industrial control systems and then changes codes to allow hackers to take control of the systems without users knowing.

Trojan horse: A program which has a hidden, malign purpose, other than the one it purports to have. For example, a program which claimed to be a game but which also secretly installed some spyware or adware components on a user's computer is a Trojan horse.

virus: Computer code written to replicate itself. A virus attempts to spread from computer to computer by infecting files. Besides spreading, viruses can be used for criminal activity or to do harm.

virus hoax: An email message warning the recipient of a non-existent virus going around. The message usually serves as a chain email that tells the recipient to forward it to everyone they know.

vulnerability: A flaw, bug or programming error in a piece of software which may be exploitable by an attacker to carry out some vicious act.

Wi-fi: Wireless technology brand owned by the Wi-fi Alliance that enables access to the Internet without cables.

worm: A type of *virus* that generally spreads without user action and distributes itself across networks. A worm can consume memory or network bandwidth, thus causing a computer to stop responding.

WPA / WPA2: WiFi Protected Access: a method of encrypting wireless networking (802.11) traffic as a protection against eavesdropping.

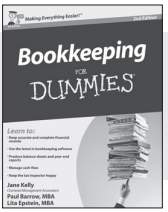
zombie: A computer taken over by an intruder and which can be used to attack other computers or websites, all without the knowledge or consent of the owner.

FOR DUMMIES®

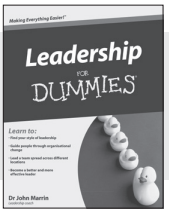
Making Everything Easier!™

UK editions

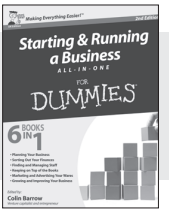
BUSINESS



978-0-470-97626-5

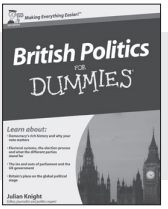


978-0-470-97211-3

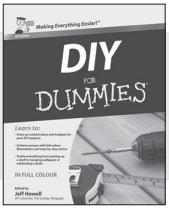


978-1-119-97527-4

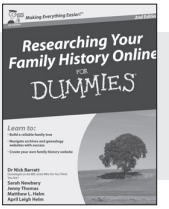
REFERENCE



978-0-470-68637-9

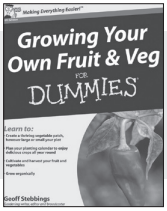


978-0-470-97450-6

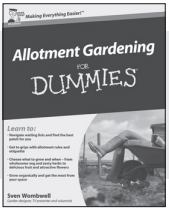


978-0-470-74535-9

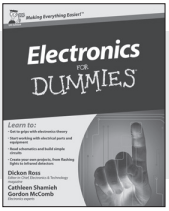
HOBBIES



978-0-470-69960-7



978-0-470-68641-6



978-0-470-68178-7

Asperger's Syndrome For Dummies
978-0-470-66087-4

Basic Maths For Dummies
978-1-119-97452-9

Boosting Self-Esteem For Dummies
978-0-470-74193-1

British Sign Language For Dummies
978-0-470-69477-0

Cricket For Dummies
978-0-470-03454-5

Diabetes For Dummies, 3rd Edition
978-0-470-97711-8

English Grammar For Dummies
978-0-470-05752-0

Flirting For Dummies
978-0-470-74259-4

IBS For Dummies
978-0-470-51737-6

Improving Your Relationship For Dummies
978-0-470-68472-6

Keeping Chickens For Dummies
978-1-119-99417-6

Lean Six Sigma For Dummies
978-0-470-75626-3

Management For Dummies, 2nd Edition
978-0-470-97769-9

Neuro-linguistic Programming For Dummies, 2nd Edition
978-0-470-66543-5

Nutrition For Dummies, 2nd Edition
978-0-470-97276-2

Available wherever books are sold. For more information or to order direct go to www.wiley.com or call +44 (0) 1243 843291

32812 (p1)

UnSecure Business

Your business is at risk from your staff's USB sticks

USB sticks are often used to help your employees transport files. These and other apparently harmless devices like MP3 music players and mobile phones are part of everyday modern life. If one of these devices is plugged into a computer on your network, your business could be at risk from viruses, malware and data theft.

You can get a lot of confidential documents on a memory stick.

Protect your business now

Our lawyers have written a FREE Acceptable Use Policy that you can personalise, print and give to your employees. It takes 20 seconds and could save you thousands of pounds.

Protect your business today, visit:
www.ecrimewales.com/policy

ecrimewales

For further e-Crime information and advice
download more factsheets at **www.ecrimewales.com/factsheets**

What is e-Crime and why does it affect you?

Understand the online threats to your business

e-Crime costs businesses time and money and the threats are increasing all the time. Do you know what the risks are to your business? Do you have the necessary protection in place?

Preventing e-Crime For Dummies explains how to identify the many threats and scams that can damage your business and provides practical steps and advice to minimise the risks. If you have been a victim, this guide shows you where and how to report the incident.

Discover how to:

- *Identify different threats and scams*
- *Protect your home and business*
- *Protect your IT network*
- *Report an e-Crime*

THE DUMMIES WAY®

- *Explanations in plain English*
- *'Get in, get out' information*
- *Icons and other navigational aids*
- *Top ten lists*
- *A dash of humour and fun*

Get smart! @ www.dummies.com

- *Find listings of all our books*
- *Choose from many different subject categories*
- *Sign up for eTips at etips.dummies.com*

ISBN: 978-1-119-94518-5
Not for resale

For Dummies®
A Branded Imprint of
WILEY