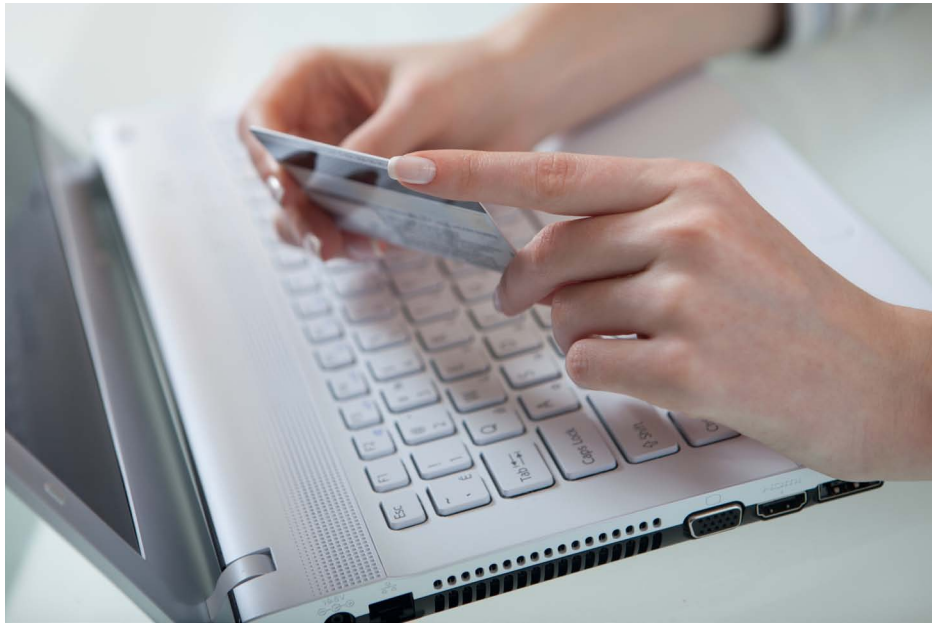
ROUGH GUIDES

THE ROUGH GUIDE to

ONLINE SAFETY

GET SAFE ONLINE .org

Get Safe Online
Free expert advice



THE ROUGH GUIDE to

Online Safety

www.roughguides.com

Published with the support of Get Safe Online

www.getsafeonline.org

Credits

Text: David Quainton
Text design: Peter Buckley
Editing: Richard Craig and Ian Blenkinsop
Proofreading: Susannah Wight and Stewart Wild
Production: Rebecca Short

Publishing information

This first edition published July 2011 by
Rough Guides Ltd, 80 Strand, London WC2R 0RL
Email: mail@roughguides.com

52 pages

A catalogue record for this book is available from the British Library.

ISBN 13: 978-1-40539-300-3

1 3 5 7 9 8 6 4 2

Association of Chief Police Officers

This booklet has been designed to provide reliable and independent information about online safety. It is not a comprehensive guide; it gives details of where further information can be obtained if required. Always remember to review your online safeguards regularly.

Stuart Hyde
Deputy Chief Constable, ACPO

Association of Chief Trading Standards Officers

The internet is an excellent place to find a bargain but you do need to be aware of what could be 'too good to be true'. This guide will raise your awareness of what to look out for and how to get help should things go wrong.

Karen Ford
Trading Standards

SOCA
SERIOUS ORGANISED CRIME AGENCY

Contents

Foreword

As Managing Director of **Get Safe Online**, I am keen to see any initiative designed to inform and educate people about how to improve and maintain the safety of their online activities. That is why we have worked with the computer and travel publishers Rough Guides and in partnership with the Association of Chief Police Officers (ACPO) and Trading Standards to create a wide-ranging guide to the main online security issues, written in a style that's easy to follow by everybody. It really does contain all of the information, hints and tips you will need to enjoy using the internet and sending and receiving emails whilst remaining protected from potential cybercrime. And if you're in business, how to keep it safe but still have the freedom to trade successfully.

Get Safe Online has worked closely with the Rough Guides team to provide the factual content for this book. Backed by the government and many public and private sector organisations, our website provides even more detail than this brief resource is able to and offers a user-friendly online guide containing the latest information and advice to help you keep safe online. You can find us at **www.getsafeonline.org**. I do hope you find the information you're looking for in *The Rough Guide to Online Safety* – either in response to a specific issue or to ensure safe ongoing use of the internet. From myself and the **Get Safe Online** team ... safe surfing!

Tony Neate (Managing Director, **Get Safe Online**)

www.getsafeonline.org

Introduction

Safety online is one of those things in life it is not a good idea to take for granted. Nor at the other extreme is it something to lie awake at night worrying about. The internet is now a fact of modern life for all of us: a source of fun, of income or simply an easy way of accessing information or buying stuff. In a way it would be surprising (given human nature) if all that online activity hadn't caught the attention of a few determined criminals. So while there are a few dangers online nowadays there is no need to fret unduly about the scale of the threat. Due to the vigilance of experts in the police force, business and government it is still (in the main) a relatively safe place to go about one's business if users observe a few sensible but necessary precautions. Even so, there's no smoke completely without fire, and those who do not pay attention to the idea of computer security face the real risk of being in that most unenviable of positions – that of being the lowest hanging fruit, those people most likely to fall foul of the dangers of the internet.

In a way, it's best to think of computer security in general as a gentle ramble across the countryside. You'll see some pretty nice things during your stroll, and in all likelihood will have a thoroughly enjoyable time, but there is a chance it will rain and you will get wet. Computer security measures, the type that will be detailed throughout this book, are like your hat, coat and umbrella. They may take a little extra packing, and in some cases cost a few pennies, but they will ensure that your wander proceeds without a hitch.

Numerous businesses and individuals fall foul of cybercrime every year; banks, for example, pay out hundreds of thousands of pounds covering credit card losses. This needn't be the case, and *The Rough Guide to Online Safety* will give you the tools to ensure that you become the fruit at the very top of the tree, at least risk of falling prey to internet villains or poachers.

Chapter 1

Securing your computer

Essential protection

It may well be the case that without even knowing it you're something of a security expert even though you haven't read this book. Because if you use passwords when you turn on your computer, or if you have antivirus software, or if you bank online, you will be using many of the techniques that protect your computer. Protecting your personal computer is a relatively simple process even if the nature of the threats can range from stealing hardware to highly sophisticated software that can embed itself on your computer.

What do hackers want?

Hollywood would have us believe that hackers fall into two categories: geeky types spending hours in dungeon-like rooms writing computer code, and sinister individuals or criminal gangs backed by dubious foreign governments intent on stealing national secrets or plotting something wicked.

For once, Hollywood can give itself half a pat on the back, because it's not that far wide of the mark, even if straightforward criminal activity is likely to be your prime concern. Gangs and skilled individuals operate all over the world and, thanks to the global nature of the internet, they have the opportunity to access all sorts of things they wouldn't otherwise be able to, such as **credit card details**, **bank account details** and **personal information**. Happily, most of their tricks can be avoided by being sensible online and making sure your computer is up-to-date with the latest protection.

From a hacker's point of view, the most common way to gain

Quick start: essential security measures

We'll go into these in more depth further on, but here are the four main points always to bear in mind when it comes to protecting yourself online:

INSTALL SECURITY SOFTWARE: Most threats to your security often appear in the form of malicious software or **viruses** so you need to ensure they are kept out. For this you absolutely need to ensure your computer is installed with **antivirus** and **anti-spyware** software and a **firewall** (see p.9). Check you have installed a spam filter or have an email account that comes with filtering (see p.11).

GET UPDATES: Loopholes in software or computer applications are like open doors or easy windows to climb through for hackers and criminals. Software manufacturers have to constantly respond to new threats. They do so via **updates** that iron out any bugs or weaknesses. If you update regularly you are reducing the risks of the bad guys finding a way in. Switch on automatic update notification if you are given the option (see p.11).

PASSWORD PROTECT: Use strong smart passwords for log-in and network admissions. It is also a good idea not to use your computer in administrator mode if you don't need to. Have a user account for day-to-day use (see p.12).

USE ENCRYPTION: If you have a wireless network then use **encryption** to protect yourself from others looking over your communications ("eavesdropping") or just using it for free ("freeloading") (see p.14, 'Wireless security and encryption').

access to your personal information is also the best way – without your knowing. These days the vast majority of computers will give you a warning when you turn them on if they are not "secure" or "properly protected". What this means is that you have not installed adequate protection, usually called **antivirus** or **security software**. This protective software scans your computer for hidden programs that do one of two things: **record** what you've been doing, or **make changes** to the computer system. So if you use a computer even only occasionally you should ensure you use these fundamental protection measures.

The problems

Spyware

The first program to watch out for is also the most common. It's called spyware, which as it sounds, will "spy" on your system and gather the information you enter into the websites you visit. This will then be communicated (in secret) to a machine collecting the information when you are online. When infected with spyware you may notice changes when you **log-on** in the form of unwanted windows opening, or the computer being slower than it should be or through a number of other issues. More extreme versions will scan your hard drive for credit card details.

There are many ways to get infected with spyware with some of the easiest being:

- **Downloading software** (not checked or verified) from the internet.
- **Streaming files** – where you may be downloading but not necessarily copying – from illegal sharing websites.
- **Visiting dodgy websites:** some of these will install spyware on your computer.
- **Clicking email attachments** which are actually spam (see p.10). Beware of the temptation, especially when bored!

On the other hand, the easiest way to avoid infection is not to download anything that is not from a trusted source and also to keep antivirus software up-to-date.

Malware

Malware is short for "malicious software" and it is everything implied by that and more. Types of malware include computer **viruses** that can shut down your entire system and spread from computer to computer, programs that corrupt **applications**, and software that sends messages to everyone in your **address book**.

Although these programs can be very sophisticated, they can be beaten in fairly simple ways. Again, don't download or click on anything you are not sure about. Also be aware that you can download both spyware and malware without being online, through infected **USB**s (also known as thumb drives or key rings, see p.36) and **discs**. Use only trusted sources – it is vital that you only put into your computer devices you can be confident are safe.

The solutions

Security software

Firewalls

The best way to protect any computer system is to imagine it like a medieval castle. Every good castle needs strong walls and in the IT world that means a firewall. The firewall monitors all traffic in and out of your connection, making sure only information and messages you want to come into your front gate do so. Viruses, malware, connections with websites you don't want anyone else to have access to: these can all be controlled by the firewall, and it will become your first line of defence. Robust modern firewalls will allow you to modulate the level of security you require and provide reports to show the effectiveness of each setting.

Firewalls: a barrier to entry

If you're connecting to the internet through a wireless network,

it's vital that every computer on that network has a firewall installed.

Most modern computers come with a firewall as standard – Windows Firewall for example – but if you have an older machine or want more sophisticated protection, there's a whole range of free and paid-for firewalls available to download online.

Antivirus

Antivirus software is one of your computer's most important defences. It runs continually in the background while you're browsing the web, or just using your computer offline, scanning for potential threats.

It is likely that if you have a relatively new computer it will already come equipped with some sort of antivirus protection and it will tell you when that is set to expire. If you are not sure about what protection your computer has, if any, then do not worry, there are plenty of options. Simply typing "antivirus" or "computer security software" into a search engine will generate plenty of options. Many antivirus packages come as a "suite", which can also include a firewall and spam filtering. Visit **getsafeonline.org** for a list of reputable and safe antivirus or computer security vendors.

Email security

Email has become many people's window to the world and the primary method of communication when doing business. In this section of this book you'll find details of the sort of activities best avoided when using emails.

In most contexts taking measures to avoid viruses and spyware alone won't be enough; there is also the problem of **spam**. Spam – the name of which derives from the famous Monty Python sketch – is non-essential email sent in large volumes to a variety of email addresses. In a personal capacity it is worth setting up a secondary account that you use when you sign-up to online services or purchase items from websites. Such activity is a primary method of ending up on the lists used by spammers when they send their messages. Inevitably, this secondary account will end up full of unwanted messages, although general spam filters are much better than they used to be at separating the Viagra offers from the messages from your friends.

Which leads this page neatly on to spam filters. Creating what is, for all intents and purposes, a spam dump for personal emails is fine, but on a business level it is not practical. A business website needs to display contact information, so even with the most conscientious staff it will be spammed. Spam filters are software programs that prevent the emails from reaching your system and taking up valuable memory space, slowing down your system. For further advice concerning spam and spam filtering visit **getsafeonline.org**.

Updating

In a hospital, when a wound is dressed it is monitored until the dressing can no longer do its job and is replaced. With computer programs, whether at home or in the office, the same applies. Computer software is so complicated that, even after many hours of testing, it invariably has bugs (security errors or holes) that need attending to, and these fixes are distributed via a process that used to be called patching and now "updating".

Many software programs will communicate with the internet when you are online and let you know when they need updating. You may have experienced this already with iTunes updates or browser updates and, as a general rule of thumb, if they are available it is worth downloading them as soon as possible. When you do so look out for **authentication certificates**. These are a way of verifying that the update is real and not a method of getting you to download something you don't want to. If you see an option to update a software program and you doubt its authenticity, refuse the option to download. When you've done that, visit the program's website to see if there are any updates scheduled. In all cases if there is a patch it will be detailed somewhere on the software's official site.

Password protection

If you follow a few key practices at home you will find that the great majority of these security measures will also transfer to a working environment, especially if you work in a small or medium-sized business. To begin at the beginning is to consider what happens when you log in to your computer, which means passwords, as password security is likely to be the first thing you encounter – and a barrier to intrusion – when you turn your computer on. If you were a policeman, a password would be your riot shield. It keeps at bay all manner of nasty things, or people, and may well be all you need to keep safe. Just like a poor riot shield, though, a poor password or poor password policy could leave you thinking you are protected when, in fact, you are vulnerable.

Want to know what a good password policy looks like? Well here's your answer.

Keeping secrets

Having the world's most complicated password isn't a great deal of use if someone can easily find out what it is. Be sure you do the following:

- Don't write your password down on a piece of paper near your computer.
- Don't keep banking passwords and PINs in your wallet/purse.
- Don't keep your passwords stored on your computer.
- Avoid, if you can, having your computer "remember" passwords, especially if the computer is used by different people.

What makes a good password?

You can't create a good password without knowing what a bad one is, so here are a few dodgy ones with the reasons why:

P2ssword/access – commonly used because they are memorable, they are also rubbish. This not so fabulous disguise, such as the '2' in p2ssword, is both obvious and ineffective.

Your birthday/anniversary/pet's name – anything directly associated with you does not a good password make. It really doesn't take many guesses to realise your password is your first-born's middle name, especially if that's detailed on Facebook.

Dalglish1977 – Ah yes, you're a Liverpool fan. Don't write passwords associated with things you like: with the advent of social networking sites they are very easy to figure out.

123456 – There are 123456 reasons why this password is unacceptable.

Sausages – maybe no one knows you like sausages, maybe it is a really clever password, but it would be even cleverer if you included a number as well. Passwords are harder to crack if they feature both letters and numbers.

Favourite things make bad passwords

On the positive side try to use a password (that you can remember) at least **eight characters** long; mix up **numbers and letters**, deploy **special characters** like *, & or % and throw in **upper and lower case** letters where the option is available. An example might be: M0usR4cer. Don't use that one, obviously, but if you use one like it then you'll be ticking all the right boxes. Be aware that although these passwords may be more difficult to remember, they are important. There are such things as "**password crackers**" or software that can very quickly guess a password by attempting many different combinations very quickly. The addition of numbers and case changes in a password and lengthening passwords makes for a greater number of possible combinations to crack.

Password changes

Often you will find your work or home system will ask you to change your password after a certain period of time, or perhaps you wish to change it because it has been compromised. In the latter situation try to come up with a password entirely different from the one you were worried about; in the former case it may be okay to change a single letter or number. In both cases make sure you memorise the new password, because on many systems three failed password attempts will see you locked out. Repeat the new password in your head a few times or think of a clever way to remember it.

Multiple passwords

In a world where you need a password for everything from social networking sites to your mobile phone, there is a strong temptation to use the same password over and over again. But, as pleasingly simple as this solution may seem, it's pleasing simplicity we're trying to avoid. Have a selection of passwords, perhaps one for home, one for work, and one for social networking sites. Doing this helps spread the risk if one of your passwords is compromised. For online banking you might want to have another completely unique password – the more important the information being protected by your password, the stronger your protection should be.

Wireless security and encryption

Buy virtually any new laptop and when you turn it on for the first time it will attempt to connect you to a wireless network. In any reasonably built-up area you will see a number of available networks and the majority of these will be security protected, but some will not. Be sure not to connect to any of them unless you have been invited to. Not only is it illegal, but your computer will become connected to a network that you do not know, with the unlikely but nevertheless possible consequence of your not only getting free internet access, but also giving away information you do not want to. Conversely, at home, if you are fortunate enough to have your own wireless connection, make sure it has robust **password protection** – in general it is a good idea to stick with the complicated password that comes as standard – because you don't want people you don't know accessing your wireless connection, not least because it will use bandwidth and slow it down when you want to use it.

In business, wireless connections are usually formed using a WLAN or "wireless local area network". It's the sort of acronym we've largely tried to avoid in this text; in this case, it does exactly what it says on the tin: it is a wireless network of computers accessible only over a local area (in this case your office). This network of computers can be protected from eavesdroppers or people trying to infiltrate it by following these rules:

- **Use the latest wireless encryption.** It will appear, at the time of writing, as WPA2. This will ensure your computers know what they are saying to each other, but outsiders' computers will not. Ensure too that your firewall provides protection for your WLAN.
- **Use a standard wireless network name.** BTBusinessHub-1866 is far less attractive to anyone scouring local wireless networks in the area than BobsSolicitors.
- **Limit access points to the system.** The fewer devices that can be accessed by the outside world, the less chance of anything going wrong.

Chapter 2

Digital security at home

Life online

Social networking

The internet has allowed people to interact in ways important, frivolous and everything inbetween, and perhaps the clearest manifestation of this are social networking sites such as **Facebook**, **YouTube** and **Twitter**.

Just as, in the real world, there are individuals on these sites who you would not want your children or colleagues to interact with, the overwhelming majority of people communicating online are completely harmless.

Facebook has become by some distance the world's most popular social networking site, and made multi-billionaires of its founders and investors. Because the site is designed to create links between people it has also become something of a target for online stalkers and bullies. Fortunately, there are reasonably robust **privacy settings**, found under the "**Account**" tab, that can be utilised to protect you and your family. If you have any fears about people finding out personal information, or seeing pictures of you that you do not want them to, just increase the privacy settings. Nearly all social networking sites, due to pressure from various groups, now offer protective features to allow you to control access to your pages.

Privacy violations

Many people have encountered problems where pictures, information or videos featuring them have been posted against their wishes. Some might even be offensive. However, social networking sites generally have a method of reporting such privacy violations, and these can usually be found by navigating the help pages or following links that you find at the bottom of the page. These admin links appear at the bottom of most social networking websites and are a useful way of getting in touch to make a complaint or raise an issue. Although most reputable websites will get back to you, some, despite repeated attempts to make contact, will maintain a suspicious level of silence. Look to contact the relevant industry sector ombudsman, such as Ofcom for the UK communications industry, as a second port of call. If none of this helps and you think it is worth highlighting, then contact the police.

Identity theft

One of the most upsetting forms of online security failure is identity theft. For many, having their details raked through or their image assumed online is a very personal violation. For others, identity theft results in financial loss. In either case, it is something best avoided and protecting yourself against.

Financial gain is perhaps the most common reason for identity theft. People often naively post their mobile phone numbers, addresses and even the name of their banks on Facebook. All this information is extremely useful to criminals.

When someone is trying to use your identity, the more information about you they have the easier it becomes, and often the more they have the more they can uncover. Could the information you give on Twitter and Facebook be used

to answer your security question if you forget your email password? The same email address that you list on Facebook? The same email address that your bank sends information to? Such information can be used to open new bank accounts in your name, obtain driver's licences and even create fake passports. Ask yourself the question: "If someone randomly came up to me in the street and asked me for a piece of information, would I give it to them?" If the answer is no, don't put that information online.

Best safety practice at home

Here is a handy checklist for home computing that you can use to make sure you are safe online. Remember, don't worry, there's no need to be paranoid, just remain security conscious.

- **Check your computer has a password when you turn it on.** Your password is the first level of computer security and helps protect you if you have physical intruders too.
- **Does your browser or computer display security messages when you turn it on or go online?** Read what they say as they may be your first clue that your security has been breached. It's not always the case but it may be a sign that you have a security problem.
- **Check the security and privacy settings on your browser.** Never set your browser to be less secure than the standard or default settings, and tighten them if you feel it's necessary. Your browser will generally prevent or advise you against pop-ups or sites that it determines are not secure, which is useful not least because pop-ups are terrifically annoying. Up-to-date browsers will give you the option of blocking reported attack sites and web forgeries. Using the latest version of your browser will ensure it has the most sophisticated security mechanisms, but on any version make sure you have warning messages turned on.
- **Do you have personal information stored in documents or written on notes around your computer?** Not a good idea. Be sure to store physical information as far away from your computer as possible. Do you have online banking passwords or details in your purse/wallet? Destroy in both cases.
- **Do you have information such as your phone number or birthday on social networking sites?** Remove if you do.
- **Could someone guess your passwords?** If you think they could, change them.
- **Back up your data.** If you have important documents, put them on a USB drive (but see p.36) and keep it safe and secure. Things could go missing from your computer.
- **Restrict access.** Make sure you know who is using your computer.
- **Educate others who use your computer.** You are only as strong as the weakest link.

Surfing kids

The internet is a wonderful place to learn about the world and an essential tool for anyone's general tuition. For children it's no different, but given how intuitive web browsing is these days, a ten-year-old with an inquisitive mind and a vague ability to spell (even this doesn't have to be anywhere near perfect) could find himself or herself on the sort of websites that no parent would ever want them to encounter.

Warn children about the problems that come with browsing

Happily, there are a number of ways to keep your children from the less desirable aspects of the internet, and they fall broadly into three categories: education, monitoring and protection. For further detail you may want to visit **ceop.police.uk** and **iwf.org.uk**, which offer advice on how to deal with the very worst aspects of online safety for children (see p.50).

Education

First tell your children the dangers of browsing and let them know the risks of social networking, including chatrooms, or of clicking on things they shouldn't. For an excellent list of general safety tips, visit the page on good internet ground rules to establish with children at **getsafeonline.org**.

Monitoring

Many online retailers and most computer stores sell secret monitoring software that will log not only every website that anyone using your computer has visited, but also all of the programs installed or used. See **www.getsafeonline.org** for more information on this topic and content filtering programs. If you do not have monitoring software, it is still useful checking the **browser history** for websites visited but only if you have any reason to be concerned. If you do not, then consider this: you may provoke your children into concealing their surfing as a habit. If however you have real grounds for suspicion look especially for any time-gaps; the latest versions of the most popular browsers allow users to delete the browsing history over a period as short as an hour, leaving the rest in place and making it look otherwise normal.

Protection

The latest browsers and operating systems allow password protection and the banning of certain sites by users. Although the details vary from system to system, typing in "**parental controls**" to the **help** section of a browser will always bring up instructions on how to lock down certain sites such as internet chatrooms, or restrict access in general. There are thousands of chatrooms; usually they form part of a wider website, such as forums dedicated to a favourite football team, band or even brand of car. Along with social networking sites, such as Bebo or Facebook, chatrooms highlight a general danger of the internet – you never really know who you are talking to, or who your child could be talking to. The only real way to be sure of heading off such problems is to control or monitor usage very carefully.

Padlock protocol

The padlock should normally appear in the internet browser border rather than on the web page itself. Remember the web browser is the program (Mozilla Firefox or Internet Explorer for example) that lets users read or navigate web pages and is at the top of your screen, usually a grey bar. Any website can, and many do, have a padlock icon in the corner of the page in order to dupe users into believing it is a secure site. The padlock you are looking for does not actually appear on the web page, but on the right-hand side of the border at the bottom of your browser (which will usually be grey), near the bit where you can drag the window to expand or shrink it. It will only appear once you have started the payment process and the act of loading the page as you are waiting will generally take very slightly longer as a further indication.

TIP: Look out as well for **"http"** in the url changing to **"https"**, which is another sign that you have moved to a secure connection. Be aware, though, that this also can be faked.

Shopping online

There is a truly bewildering array of online shops, to the extent that in the UK online sales have long been outstripping the high street in terms of sales growth. Type any given object into a search engine and chances are you'll find a website selling it. Unfortunately, due to the non-face-to-face nature of the internet you never really know what you are going to get, so before purchasing anything online ask yourself the following questions:

Question 1: Is the website reputable? If the website is a huge and reputable retailer and is trusted by thousands of customers every day then you should feel more confident. Take care with smaller sites: see if you know anyone who has used one before to recommend it – there is no endorsement like experience.

Question 2: When making payments does a secure symbol (usually a padlock) appear in the bottom right of the screen? On computers with older operating systems, it may appear elsewhere. The padlock represents confirmation from the vendor that when a buyer is inputting card details they are doing so over a secure internet connection, one that cannot be monitored by someone else trying to steal your information (see box on p.21).

Question 3: Is a deal too good to be true? Does the website seem unusual? Did the payment process seem weird? If the answer is yes to either of these questions, cancel your shopping. Look out for poor spelling and grammar, odd word order, or pictures and images that do not look particularly professional. Most legitimate websites will also have many links to different pages; fake websites frequently have fewer, because they intend to keep you on the fake page. If you have any concerns about a website not being what it claims to be, it's worth checking out or reporting it to **actionfraud.org.uk**, which is the UK's national fraud reporting centre.

Question 4: Who are you doing business with? European law requires that traders who sell online must provide their postal address so you know who they are. Before you commit to buy, make sure you are going to be able to exercise your consumer rights should the goods not turn up or if they are faulty when delivered.

Banking best practice

No one likes a lunchtime queue in a high-street bank, yet there's an inevitability about the experience that almost makes it a kind of rite of passage. Online banking has become the saviour of lunch breaks everywhere, offering customers a way of managing their money without getting irate at a hapless bank clerk. Online banking is a good place to start when examining the perils of online security because it encapsulates the benefits and pitfalls of conducting business in general online. On the one hand it is easy, cheap and swift, on the other hand it opens a variety of avenues in which your personal or business information can be compromised.

What to look out for

The first thing to check when banking online is the URL (uniform resource locator – the words in the box at the very top of the page usually, but not always, including "www") and page layout of the site you are visiting. The URL is a unique address for a file that is accessible on the internet or, if you like, the web address of a specific web page. Major banks are excellent at trawling the web and locating and taking down websites pretending to be their own, but some do slip through the net. These spoof websites will generally look less polished than you might expect, and they will always have a slightly different **URL** – the unique code, usually beginning with "**www**" that sits at the very top of your browser. HSBC websites in the UK, for example, usually have "hsbc.co.uk" in the URL. Have a look at the page and at the URL; if it doesn't look right then think twice before you enter your account information.

TIP: If you purchase an item costing over £100 using a credit card, you get added protection if goods don't arrive as they should. Also, with other payment types, banks are sometimes able to reverse the transaction or prevent money from reaching the criminals, so if there's a problem act quickly.

Thankfully, the vast majority of banks exercise extremely cautious online policies. To access an account a user usually needs to have card details and a passcode. Some banks now also use a chip authentication device; this is a small machine given to customers which requires the account card and PIN to produce a unique identification number for the website. Others may ask you to log on using a separate "secure key". Both methods are more secure than using a conventional password (however smart it might have been) because these new devices generate a fresh password every time you log on. With all banks, read information on how to access official sites carefully and memorise any passwords or codes. Don't write passwords down; as you will discover later in this book, physical security (see Chapter 4) is as important as digital security when staying safe online.

Chapter 3

Scams and schemes

What not to look for

Tricks to get money or information from you are not confined to the covert programs that infect your computer. There are many upfront ways, all of which are just updated versions of the sort of confidence tricks that have been around for centuries and all of which can be easily spotted if you know what you are looking for.

eBay and auction sites

There are many popular shopping and auction sites these days, on which you can complete almost all of your shopping, should you feel the need.

Common **scams** on these sites include people not sending you items once you have paid for them, or buying something from you but cancelling the payment after you've dispatched it. Most of these sites have user rankings where people on the site rate who they are dealing with. To protect yourself, make sure that anyone you deal with has a selection of good **reviews** (though these too can be faked); if this is a possibility consider whether you want to pick things up directly.

Advertising

Many websites you interact with make money through selling advertising. Clever targeting means these adverts will often reflect your browsing, so if you announce on Facebook you are getting married, you will suddenly see more adverts for honeymoon destinations and florists.

During general internet usage you will also come across plenty of flashy adverts that promise you free items, or tell you that you have won a prize. Avoid clicking on them, or at the very least be wary. Although some are reputable, you may find yourself encouraged to sign up for something you don't want.

The terms **phishing** and **419** (see pp. 27-28) may be alien to you, but what they stand for are two ways of scamming by persuading people to interact with emails or messages they had not expected to receive and would otherwise generally delete.

Get-rich-quick schemes and scams

Either through spam emails or through stumbling across websites promoting them, it would be very difficult for you to spend a month of general internet use without stumbling across some sort of so-called get-rich-quick scheme. As in the offline world, where such schemes are as old as the invention of money itself, these schemes hardly ever lead to fortune and can often walk you down a path to financial ruin. In particular, if you are looking to earn money through online enterprise, you may be tempted by promises of a quick payout and large return. Unfortunately, for get-rich-quick you should instead read, "too-good-to-be-true".

Pyramid schemes

Perhaps the most common form of online wealth-promising scam is the pyramid scheme. If you happen across a site or email asking you for money in return for information on how to get wealthy, then you have encountered a pyramid scheme. You'll then be encouraged to encourage others to enter into the same process, one that can be illegal, so be wary. Another form of pyramid scheme is the Ponzi scheme, which will invariably baffle you with financial jargon but pays returns to investors from their own money or from money paid in by subsequent investors rather than from any profit. The first investors are paid out from money paid in by new investors and may appear to be happy – thus building up some "trust"– but in the end you are unlikely to recover your investment. It is usual for the fraudster to vanish with the money invested or for the scheme to abruptly terminate when investors realise they are not receiving promised returns.

Ticketing websites to watch out for

Buying tickets to a large show, or to see a band or attend a festival, can become something of an online event. Every year hundreds of thousands of individuals frantically press the refresh button on their browser hoping to be first in line for Glastonbury Festival or Reading Festival, and every year a small number fall for the fake websites making money out of people desperate for tickets. Generally, for larger events, tickets will be sold via ticketmaster .co.uk, ticketline.co.uk, ticketweb.co.uk or seetickets.com – these are the largest players in the market. However, there are other companies specialising in ticket sales and just as many specialising in ripping you off. To make sure the tickets you are buying are legitimate, observe the following guidelines:

1: If you are looking to buy tickets for anything online, go to the official website related to the event and see the list of registered ticket sellers.

2: If the website you've found selling tickets is not on there, don't use it.

3: If it's a website with a dubious address – perhaps with a misspelling or a character out of place – promising tickets that are sold out everywhere else, then it is more than likely a website with a slightly odd address about to make sure you never see your money again.

Travel websites

As with the ticket sites mentioned above, there are plenty of travel websites created for the sole purpose of promising you a nice trip away and instead stealing your hard-earned cash. Stick to reputable and well-known sites for all online transactions (find more details on this in the "Shopping online" section of this book, p.21) and you'll be safe. Also, be wary of all but the most respected user-review travel websites. There are plenty of people working to seed travel websites with good reviews of their own venues. The experience you get when you eventually travel to the destination may be quite different.

Phishing

Phishing is a catch-all phrase for any email or social networking site message that encourages you to click on a link or give away personal details. These days the threat can also include "smishing"' which is essentially the same thing via text message. A suspicious email will probably look something like this:

From YourBank Card Customer Care

Dear Valued Customer
Our new security system will help you avoid fraudulent transactions and keep your credit/debit card details safe. Due to a technical update your card will need reactivating. Please click on the link to update your credit card.

We appreciate your time

YourBank Card Customer Care

If you click on the link in one of these messages you'll either inadvertently agree to downloading a computer virus or be led to a website where you'll be asked to enter your personal details. Getting into a spot of bother over these messages can be avoided by simply ignoring them.

Sometimes, especially in emails, these messages appear both professional and compelling. But **a bank, online auction house, social networking site or large business will never communicate with you in this way asking for such details**. Do not click on any links in unsolicited messages and you will be safer. If you are encouraged to click on any sort of link by someone you don't know, or if you suspect there's something not quite right about a link, then **do not click on it**. Obviously, if your best friend has a reputation for forwarding images or links to YouTube videos of piano-playing cats then give yourself a little more freedom to check out the feline fun. But if the message is from someone you don't know, just be aware.

419

These letter-based frauds are called "419 Scams" because around ninety percent of them originate from **Nigeria**, and article 419 of that country's criminal code deals specifically with this sort of scam. So popular and successful were they around ten years ago that 419 scams were said to be the fourth largest industry in the West African state. If you see one of these letters, **do not respond**. Even in jest. If you do, your email account will be added to a list of respondents and you will begin to receive more. They work by convincing the recipient that, for a small fee, they could be in line for a much larger windfall. However well written, however convincing they are, don't reply. If it looks too good to be true, then it usually is. Either that or there are millions of wealthy Nigerians who must be very puzzled why we won't take their money. Here's the sort of letter that has become familiar to email users over the last fifteen years:

From: Prince Joe Eboh

Date: Wednesday, April 21, 2011 12:53 PM

Subject: TRANSFER

Dear Sir/Madam,

I am fine today and how are you? I hope this letter will find you in the best of health. I am Prince Joe Eboh, the Chairman of the "Contract Award Committee", of the "Niger Delta Development Commission (NDDC)".

We overshot a foreign contract by US$25,000,000.00. But, because of the existence of some of the domestic laws forbidding civil servants in Nigeria from maintaining foreign accounts, we cannot transfer this fund to a foreign account. Hence we wish to transfer into your bank account as the beneficiary of the fund. We have also arrived at a conclusion that you will be given 20% of the total sum transferred as our foreign partner. To come to the arrangement we require details of your name, address, your private personal telephone/fax numbers, your full name and address, including your complete bank details where the transferred fund will be routed by Apex Bank.

Thanks for your cooperation.

Yours faithfully,
Prince Joe Eboh

Chapter

4

Keeping the office secure

Extra lines of defence

Employee and office best practice

Despite what others may tell you, it was golfing great Arnold Palmer who first said "It's a funny thing, the more I practise the luckier I get" in response to the assertion that his success was partially down to dumb luck. The same notion applies to computer security: the more you practise good security procedures and the more you train your staff the less likely you are to suffer compromised computer security or a mightily embarrassing data loss incident. So, here's another checklist for you, and one which is worth reviewing every couple of months no matter what size your business is:

- Do your staff members fully understand their responsibility for computer security?
- Do staff understand how viruses get onto computer systems and their effects?
- Do staff employ the same level of computer security when conducting business away from the office?
- Have all copies of software in your business been properly licensed and registered?
- Is someone in your business keeping up to date on security issues and alerts?
- Do you keep customer information on unencrypted or easy-to-access hard drives or even portable devices (see p.32)?
- Is access to private data restricted?
- Do staff regularly change and use robust passwords?
- Is website access restricted on your networks?
- Do you know who is using your computer systems at all times?
- Is your wireless or internal IT network secure?
- Are former employees' accounts – and access to intellectual property assets – terminated swiftly if they leave?
- Is all redundant hardware properly disposed of, and all the data erased?

For most companies and businesses you may want, and indeed it is advisable, to create a policy for computer security. There are plenty of websites dedicated to creating customised policies but you can do much worse than visiting **sans.org/security-resources/policies** as a very good starting point. An internet security training organisation with unrivalled industry connections, Sans claims to be the most trusted information security source in the world, and, by and large, it is true to its word. For more specific advice for small and medium-sized enterprises (SMEs), visit **getsafeonline.org**.

Training

Spam is a great example of the sort of security threat that can be managed with sensible security policies, and the best of all these policies is regular staff training. By informing staff of the dangers of viruses, of the dangers of replying to 419 emails, of the dangers of using work email addresses for website sign-up, your business will

Updating in the office

In business it is not realistic to apply patches and software updates every time they appear so you may want to turn off features that automatically update your system. Set aside a regular time, either weekly or monthly, and usually outside general working hours, to update your systems. Unfortunately, if you do it during working hours many of the programs will require rebooting, which could mean all of your staff clocking off early if the reboot fails or is slow for whatever reason. Occasionally, you will encounter updates marked "critical". Judge on a case-by-case basis whether you feel you can wait until the end of the day to activate the update, or simply shut off the program if it is not business-critical until the update is completed.

be in a much better position to cope with security threats.

Encryption

When you have a mobile phone conversation the message is encrypted, meaning that, although the person on the other end of the phone can hear you loud and clear (if you have been fortunate enough to get a signal), anyone trying to digitally listen in to your conversation would encounter the computer version of gobbledegook. The origins of this system actually involve Hollywood actress Hedy Lamarr and composer George Antheil, who created a device that hopped frequencies using the same system that made pianolas play automatically. Although encryption has come a long way since then, the reasons for it remain the same – it's a way of storing or communicating information without any unauthorised person finding out what that information is. Particularly in a business setting, this can be a very useful process indeed.

Here's the rub: although all virtual communication across wireless and mobile phone networks is encrypted as standard, encrypting files for storage has a reputation for being a bit of a pain in the neck. It can be a long process that takes up a lot of memory space and can also slow your computer down. But encryption is a necessary evil if you want to secure files safely. It's an added level of security should your network become compromised. Have a think where you want to store your important files, such as on a USB, CD or hard disk. See **getsafeonline.org** for further guidance on free or commercial encryption products for general tasks or smaller jobs such as a file or directory.

Compliance

This is a term entirely for businesses and nothing to do with Robocop, so if that disappoints you, then look away now. Compliance has become both a burden foisted on IT professionals and a business consideration that is important for any small and medium-sized business. Essentially it is the act of keeping your business in line with legislation.

Compliance courses and software have boomed, but, from an IT perspective, all they really do is make sure that you can provide accurate and quality reports on your business, and that you are storing information correctly. There are a few major Acts that require a level of compliance, and getting in line with these might be a little bit of an administrative headache, but in all cases they do have the effect of making the business that much more efficient when completed, and that can only be a good thing for a small or medium-sized enterprise (SME).

Here is a short list of Acts with which you may have to comply:

- **The Data Protection Act 1998** – asserts that all personal information about an individual must be held securely, with their permission, and that they must have access to it on request. They can also require you to delete it.
- **Freedom of Information Act 2000** – says that if you are a public sector body most of your information should be available within 28 days. If you do business with public sector bodies the same rules can apply.
- **Basel II** – European banking regulations, important for those in the financial sector.

- **Computer Misuse Act 1990** – an Act that prevents hacking in its broadest forms.

If you are a local business the last two of these Acts may not apply to you, but they are worth knowing about, if not knowing inside out as your business partners may have to. Online traders who are unsure about how laws apply to them should contact their local Trading Standards Office (**tradingstandards.gov.uk**) or the Information Commissioner (**ico.gov.uk**).

Customer data protection

As detailed on the previous page, data protection is important, not least because if you fail to comply with the **Data Protection Act** you could end up with a very hefty fine indeed. Although the legislation is fairly broad and has been around for long enough to have become a well-known issue for business, simply complying with the Act will not be enough to protect you from the ire of customers should your computer systems fail.

In simple terms, as a business you hold a lot of customer information and it is your job to protect it, especially if it is the sort that your customers would not want to fall into the wrong hands. Here's a handy checklist to make sure you are storing and managing your customer data securely:

- Make sure your customer data is encrypted (see p.32).
- Secure your computer systems and network. If you have a lot of sensitive customer information you become a more likely target of computer criminals.
- Educate staff – even the most loyal staff member can be forgetful; don't let them leave thousands of credit card details on an unprotected regular hard drive.
- Back up data. Losing customer data can be as damaging as letting it fall into the wrong hands. Have two or three copies of everything and keep them safe.

A Rough Guide to physical security for computers

Real world risks: at home or at the office

Chapter 5

Data loss

Sadly, for the powers that be, the majority of major physical data loss incidents seem to occur in the halls of government. Laptops left on trains, portable hard drives found in pub car parks, CDs going missing for no discernible reason – all of these have occurred in the last ten years. Because government files are public we find out about it, and because they handle so much sensitive data, newspapers write about them. In reality, the likelihood is that physical incidents of computer security failure are prevalent in all levels of business, while few people need reminding of the disaster of a stolen personal laptop. From 1998 to 2007, more than 1000 government laptops were stolen; imagine what the figure is for the private sector. Keeping in mind, then, that computer security is as much about keeping your CDs safe as it is installing an antivirus program, the next few pages will take you through the dos and don'ts of physical computer security.

USBs

USB: another acronym in the lexicon of computing terms. It stands for Universal Serial Bus, but you've no need to memorise that. All you really need to know is that USBs are the little devices that port into the side of your computer, and that they have become the standard method for transporting files between devices. USBs have become so prevalent that most people have access to one, either attached to their keyring or stuffed into their drawer at work. If you are involved in transporting any sort of important files – banking files or even a CV – then they will be packed with information that could be useful to the average, ordinary, everyday computer criminal. Given that they are small, USBs are easy to lose, so a policy concerning safe handling is worthwhile, but won't prevent the odd mishap. Instead make sure all data contained on a USB is encrypted (see p.14).

USB memory sticks can be fun *and* a security risk!

Portable hard drives

The big daddy of the USB world is the **portable hard drive**, which is one of various portable storage devices capable of storing mind-boggling amounts of data. As with USB drives it is sensible to encrypt all data held on these files. Although it may take longer to transfer and possibly be a more expensive process, it will give you a modicum of peace of mind should a file go missing.

When you are given portable hard drives or USBs by someone else, check for viruses and malware before you add anything from them to your system. Even the most unlikely companies have, in the past, inadvertently handed out devices packed with all sorts of nasty software. In 2010 IBM handed out a malware-infected USB stick to delegates at its AusCERT security conference. Delegates were surprised to get the infected devices, not only because they came from such a reputable company, but also because the conference was about computer security. There's a lesson here, to paraphrase a Mr F. Gump: the contents of USBs and portable devices are like a box of chocolates; you never know what you're gonna get.

Poison pill or a caramel cream? USB sticks may surprise you.

When managing staff that use USBs and portable devices, it is important to make sure they only use ones provided by your business and that they only use them for business purposes. The less interaction USBs in particular have with non-business critical devices the less likely they are to become infected or corrupted. Sometimes these devices can encounter problems when swapping data between a PC and a Mac, and they can also lose it, if removed before any data processing has been completed. Inform staff of these dangers: it will reduce chances of all sorts of problems.

Another fine mess

In 2007 Nationwide Building Society found itself subject to a fine by the Financial Services Authority (FSA) of almost £1m when a laptop was stolen from an employee with up to eleven million customers' personal details on it. Although it is fantastic that computer storage has become so efficient that all of that information could be stored on a laptop, it is nevertheless an example of how weak security points can be created. The question has to asked whether it was necessary to hold all that on one laptop?

Back-ups and fireproofing, paper and reports

If you've had a computer, laptop or any sort of digital computing device for any length of time you will probably be painfully aware that they are far from perfect machines. They get slow, become obsolete and can, seemingly without warning, crash. The stability of computers is something being addressed and most experts agree we are in a far stronger position now than we were ten years ago. However, accidents and unforeseen things happen: you have to expect the unexpected.

The unexpected, in a computer security sense, is loss of data. You can protect yourself against loss of data through backing up and/or storing your data in different ways. For every important file you have it is advisable to create two copies. Create a hard-drive which files can be sent to, or store files on a CD. It may be impossible to do this on a daily or even weekly basis, but leave it any longer than a month and even the smallest firm or individual with the least data could end up losing something irretrievable. Decide how often you need to backup files based on how much time it would take to replace data lost.

"Backing-up", as it were, can even involve the use of paper files and records. Although it is important to consider environmental issues, and the space taken up by paper files, they are still an important method of storing data especially for small businesses.

Storage

Once you have backed up, it is important to have a physical location for your data. In the advent of a fire or flood you want your data to be protected in a way that your general computer systems can't be. Allow some of your security budget to be spent on fireproof storage; it could save your business.

Perhaps the best way to highlight the danger of lax physical computer security is to scare the life out of you. Here are three true horror stories:

In 2008 a senior intelligence officer from the Cabinet Office was suspended after documents were left on the seat of a commuter train from London Waterloo. The seven-page file, classified as "UK Top Secret", contained a report entitled "Al-Qaeda Vulnerabilities" and an assessment of the state of Iraq's security forces.

Lesson: printed files are as sensitive as digital ones.

In 2005 in the US an employee of communications firm MCI lost a laptop containing personal information on about 16,500 current and former employees. The laptop had been left in an unlocked car. Thieves are looking for devices containing personal information; this information could be more valuable than the device itself. This counts in the office too: lock portable machines away or secure them to desks.

Lesson: keep mobile computers safe at all times.

Retailer Marks & Spencer was told it could face prosecution if it did not overhaul all of its data security after losing 26,000 employees' pension details. The Information Commissioner's Office threatened the retail giant with prosecution after the unencrypted data on a laptop was stolen from a contractor in April 2007.

Lesson: contractors are your responsibility too, so ensure security protocol extends to all parts of your business or risk prosecution.

Chapter

6

Mobiles and other devices

Security in miniature

Safety essentials

Many people these days are surgically connected to an iPhone, BlackBerry or personal digital assistant (PDA)(handheld computers as they used to be called). Mobile phones and the latest tablet computers have become so sophisticated that they can not only perform a lot of business functions, but they are also capable of containing reams of information useful to those with criminal intent. Also, they are relatively easy to sell on and they are so small they can be snatched and transported away with relative ease. Essentially, there's no bigger security risk than the little phone you carry around in your pocket or handbag. For details of resources and more information visit **getsafeonline.org**, which has a section dedicated to mobile phone security.

Here are eleven handy tips that will not only help keep your mobile or laptop secure, but are also applicable to devices such as iPads, tablet computers in general and most portable electronic devices.

Mobiles: a moving target

- **Keep it hidden** Unless you cling on to the 1980s yuppy dream, mobile phones are by necessity small devices. Although on one hand this means they can be easily whisked away by a thief, it also means they can be easily hidden. Don't leave them on top of open bags, on seats or visible in your car.
- **Security tagging** The best way to tag a small device is with an ultraviolet marker pen as the police recommend. Mark the phone and the battery (if it is accessible) with your name or your business name and contact details. It makes recovery more likely.
- **Use in-built security** Most devices have some form of keypad lock, which will buy you time if criminals are trying to access it and encourage many petty thieves to dispose of it. Use a password or PIN you can remember, but don't make it too obvious and hide your phone away from others when you enter it.
- **Register your device** There are many schemes for registering devices so they can be easily recorded as lost or stolen. The UK has a particularly useful and effective scheme in the form of the vast **immobilise.com** database. Sister sites **checkmend.com** and **nmpr.com** perform similar functions. Such schemes make it easier for police to return recovered items.
- **Record serial numbers** Printed somewhere on your mobile phone, usually on the battery or SIM card casing, is a fifteen digit IMEI number. Keep a note of it; it's a unique identifier. If you can't find it, then it can also be located by typing *#06# into most phones. Record it: you may be asked for it if your phone is stolen or lost.
- **Insure** You may have to insure mobile devices separately from your usual insurance. Check with your insurer and get yourself covered. It also helps in the event of damage.

- **Restrict alternative network usage**. Unsecured networks like non-password protected wi-fi connections are not only a security risk, but will also drain your battery. Avoid having Bluetooth turned on too – blue-jacking is the process of sending messages to open Bluetooth connections and can be annoying and an invasion of privacy.
- **Block premium calls and texts** Contact your mobile provider and get expensive calls blocked or you might face a hefty bill should your phone fall into the wrong hands.
- **Handle with care** Mobile phone viruses have not yet spread successfully despite the efforts of virus writers, though there has been some successful targeting of Android devices. But they could, especially with links and multimedia messages becoming ever more prevalent. Treat suspicious messages on your phone or PDA with the same care you would on your computer.
- **Synchronising your mobile** If you synchronise your mobile phone to your computer you may well end up inadvertently carrying personal information, otherwise stored on your computer, in your pocket. Make sure you know what data is saved to your phone.
- **Stay aware of new dangers** Keep up to date on future threats and recent developments such as anti-virus software for smart phones, via the website **getsafeonline.org**. Read on for details on some mobile-specific concerns.

Where next for hackers? The future of security threats

Your new favourite devices

In the last few years the number of devices competing with computers as business and information handling tools has rocketed. This is partially on account of the low cost and reduction in physical size of computer memory and partially due to some really rather superb innovations, such as the **iPhone** and the array of **tablet** PCs now on the market.

Happily, these devices have been far less likely to contain the sort of security holes associated with computers in the early years of this millennium. But that doesn't mean they don't exist. With any new device check various sources and reviews before you invest in it. More cautious users often hold back from buying until after initial release, just in case. Take the original iPhone. Initially it was plagued with battery and functionality issues, but once these issues were cleaned up in the second, third and fourth versions, the device became heavily adopted, even if the latter also had their share of glitches. However, increased use of mobile devices does bring with it new problems. If, for example, you walked into a coffee shop with an unsecured wireless network and used said network to do some banking on your mobile phone you might assume you would be relatively safe (and most of the time you will be). However, in relatively simple "man in the middle" or "Mitmo" hacking scams, a hacker places himself in the middle of your wireless communication without your even knowing, taking all of your bank details. The lesson here is that new technology can bring with it new danger. As usual, be aware and be careful, and keep up to date on sites such as **getsafeonline.org**.

Tablets: masses of information, accessible on Wi-Fi

Viruses

Back in 2005 there were various reports of viruses potentially infecting devices such as aeroplanes and cars. Theoretically, it is possible that a car that links to your mobile phone could inherit a virus from said phone. But, as previously revealed in this volume, there are no successful mobile phone viruses "in the wild" and what would anyone hope to achieve from creating one linked to a car? Viruses and malware are largely produced for financial gain, so the viruses of the future are likely to be similar to those of the past – designed to steal your information. At the moment

the computer industry is largely on top of the virus and malware threat, and by staying clued-up on the latest developments, you can be too. Mobile phones are becoming more sophisticated and using increasingly generic operating systems – Android, iOS (for iPhone), RIM BlackBerry and Symbian being the main players. The more people use these systems – and they are projected to have a roughly equal share by the end of 2012 – the more of a target they will become.

Social networking

Both for personal use and in business the increased use of social networking sites creates a security threat. That is compounded by the ease with which social networking sites can be accessed via mobile phones. Short of banning their use in the workplace, which would be very difficult to enforce, it's best to stay on top of security threats within these sites and keep staff as informed as possible.

As an example, in September 2010 a virus spread across the Twitter network preventing users from properly accessing it for a few hours – a nightmare for firms that use it for marketing purposes. There are also countless examples of companies and individuals seeing their security compromised by someone ill-advisedly clicking on a link on Facebook supposedly sent by a trusted "friend". Both Facebook and Twitter, which currently dominate the social networking market, are full of accounts and links created for less than honourable reasons. Consider at work whether social networking site access is advisable, and both at home and at work make sure that you treat anything you are unsure about with due suspicion.

A Rough Guide for when security fails

Worst-case scenarios

Chapter 7

If you have run through this book with a fine-toothed comb and implemented all of the suggested online and computer security measures, there is a much smaller risk of problems but sadly there is still a chance that your computer could become compromised or that your data could be stolen.

It may be that you do not initially realise that your security has been compromised. A successful piece of spyware, for example, will hide itself from detection as it goes about its business. Conversely, if your computer or your computer network begins to act strangely it is not necessarily a security incident; it could be a minor bug or one of the many gremlins that afflict any computer system. If you do find yourself in the unfortunate position where your hardware or data has become compromised, there is for each scenario a set of simple steps to follow to help get things back on track as soon as possible.

What are you going to do?

Physical loss or damage

- Stay calm and establish the problem. Determine what exactly has gone wrong.
- Catalogue the items that have been lost or damaged.
- Establish what data the device or devices contained that could now be lost. Find your back-up files.
- If it is a mobile phone, block it.
- If the device is lost, consider if it might have been stolen. If you believe the item to be stolen, report it to the police. If you believe it to be either lost or stolen, contact your insurer.

Network or computer compromise

- Stay calm. How do you know your network or computer has been compromised? Did someone physically sit at one of your computers or was the attack remote?
- What is missing? What damage has been done, if any, by someone having access to your computers or network?
- If data is missing, who does it affect? Is it just you or is it your customers or someone else? Establish who needs to be informed.
- Detail the exact problem and then contact the police.
- Try to establish how the compromise occurred and fix the security hole.

Infection

- Stay calm. Has the infection caused critical issues? Will it get worse? Will it help to shut down any of your systems?
- How do you know your computer or network is infected by a virus or malware? Have you run scanning software?
- Have you run software to remove the offending program from your system? Will running it affect the operational capacity of your system?
- Is it worth contacting the police? To your knowledge has anything gone missing? Can you determine if sensitive files have been accessed?
- Check software updates. Could security holes be due to failures there?

Who are you going to call?

There are many phone calls to make and many people to inform if you have a serious computer security breach. Here are the options; you should consider which is really relevant to your situation:

- **No one** In most cases a computer security issue will be very minor, such as a virus infection. It may be annoying, but don't trouble the police as they almost certainly won't be able to help you.
- **Staff** Inform all the staff who need to know exactly what has occurred. In doing this you can inform them of any immediate operational changes and also reinforce security procedures related to the mishap.
- **The police** Specifically if it is a case regarding someone stealing your financial details, taking a payment from you illegitimately or conning you in some way visit **actionfraud.co.uk** or call 0300 123 20 40.
- **Your insurer** Are you insured against data loss or theft? Let your insurer know as soon as possible what has happened.
- **A computer forensics firm** If you have a suspicion that your network has been breached, or that you are the victim of corporate spying, you may wish to think about calling a computer forensics firm. Many computer forensics firms now exist to help businesses that have fallen foul of cybercrime or perhaps industrial espionage.

- **The Information Commissioner** If your business has lost customer data, make contact via **ico.gov.uk** for advice on your responsibilities in this situation, or phone their helpline on 0303 123 1113.

What to do if someone else loses your data?

In a world brimful with contractors, suppliers and interconnectedness there is a good chance that a fair chunk of your data will, at any given time, be in the hands of individuals you do not know or who do not work for your company. If you are to entrust data to others, for whatever reason, then follow the rules that you would if it were you transporting it or using it:

- **Encrypt where possible.**
- **Back up any data before handing it out.**
- **Transport and use data only on approved devices.**

Make sure you are contractually covered beforehand. Write into any business contracts exactly how you think your data should be handled and boundaries for its usage, including a deadline for when it has to be either returned or destroyed. If the individual or firm that has lost your data cannot get it back, then try to establish the exact steps they took before and after its loss and the point at which the loss could have been prevented.

What to expect from police, banks, IT suppliers and providers

You'll encounter many organisations when dealing with data loss or computer security breaches of any kind. Here's what to expect of them.

The police

The first officer you contact is unlikely to be a computer security expert. So be clear in your own mind what the problem you are reporting is and be clear and concise in your explanation. Although a computer security incident is likely to be very upsetting and very important to you, in the overwhelming majority of cases it is not what the police would consider an emergency. An officer will treat your case as any other, before passing it on to someone, or a department, more qualified. In either case be patient; solving cybercrime offences can be a long process.

Banks

A few of us only hear from our banks with any urgency when our bank details have been stolen and could be used against our wishes. Fortunately for Joe Public, banks assume a certain amount of liability when this occurs and will, in most cases, replace all or most of our lost cash reasonably promptly. Because card details are so often stolen and traded, banks now have sophisticated systems to recognise if the details are being used in a manner that is considered out of the ordinary. Don't be surprised, then, if the first you know about your card details being compromised is the bank giving you a phone call.

IT suppliers and providers

If you have bought a computing device or software and you consider it to be faulty or insecure then the company that supplied it to you has exactly the same responsibility as one that sold you a faulty dishwasher: your consumer rights mean they need to sort it out. That said, any issues could quite easily be a result of inexperience at your end, and as suppliers supply the technology, they are a good place to start for information.

Explain any malfunctions or computer security incidents you encounter clearly and make sure they respond clearly – do not be afraid to ask for certain terms to be explained. Check all contracts with suppliers before they are signed, and make sure they have liability if the system failure is their fault.

Make sure that the company you are buying from has a contact number and a clear complaints or enquiry process on their website, and that it works. Less reputable firms will try to be as uncontactable as possible, and this is often a good sign to take your business elsewhere.

Resources

Top Starting Points

For more on the specific topics mentioned in this document and for updates visit **Get Safe Online** whose website is **getsafeonline.org.** This site is an essential starting point for matters of internet security with a focus on individual consumers and small business users. It provides expert advice from government backed by leading public sector organisations and online industry players.

Action Fraud **actionfraud.org.uk** National fraud reporting centre with 24-hour online reporting service. It is a sign of the times that scam emails and mobile phone fraud are so high up their list of concerns.

Child Exploitation and Online Protection Centre **ceop.police.uk** A service dedicated to preventing and dealing with the consequences of exploitation of children.

Internet Watch Foundation **iwf.org.uk** Provides an internet hotline for the public and IT professionals to report criminal online content in a secure and confidential way.

For Further Information

Apple **support.apple.com** Apple users can navigate from here to find security updates covering the full range of Apple products, from iMacs to iPads.

Bank Safe Online **banksafeonline.org.uk** The UK banking industry's response to online security with online advice primarily covering banking and financial scams and hints on best practice.

Childnet International **childnet-int.org** Awareness-raising pressure group, seeking to make the web a safer place for children. Also provides information and advice to parents, children and families.

Cyber Security Challenge UK **cybersecuritychallenge.org.uk** Runs a series of online games and challenges to test users' skills in cyber security and uncover fresh talent for the cyber security industry.

Insafe **saferinternet.org** Part of a European network that offers safer surfing advice specific to children and young people.

Microsoft **microsoft.com/security/** Computer giant behind ubiquitous Windows software provides general and specific advice on security.

Police Central e-crime Unit **met.police.uk/pceu/** A nascent national centre of excellence for combating e-crime in the UK.

Sans **sans.org** The largest information security training group in the world has lots of information and resources for business users.

Stop. Think. Connect. **stopthinkconnect.org** The first coordinated global campaign from government, business and non-profits, promoting online safety and vigilance.

Serious Organised Crime Agency. **soca.gov.uk** SOCA tackles serious organised crime that affects the UK and its citizens.