Plug IT In 6
Protecting your information assets

PLUG IT IN OUTLINE

PI6.1 How to protect your assets: the basics

PI6.2 Behavioural actions to protect your information assets

PI6.3 Computer-based actions to protect your information assets

LEARNING OBJECTIVES

1. Explain why it is critical that you protect your information assets.
2. Identify the various behavioural actions you can take to protect your information assets.
3. Identify the various computer-based actions you can take to protect your information assets.

PI6.1 How to protect your assets: the basics

We travel for our jobs, we work from home, and we access the internet from home and from our favourite hot spots for personal reasons — shopping, ordering products, planning trips, gathering information, and staying in touch with friends and family via email. Unfortunately, every time we use our computers or access the internet, we risk exposing both professional and personal information to people looking to steal or exploit that information. Therefore, we have prepared Plug IT In 6 to explain how you can protect your information assets when you are computing at home or while you are travelling.

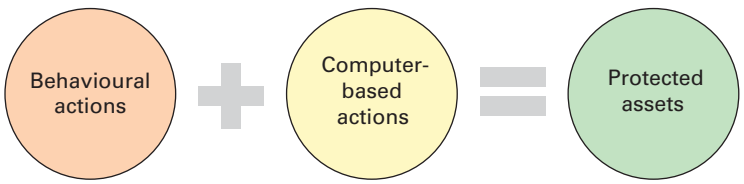

FIGURE PI6.1 Two types of actions can protect your information assets.

It is important to note that, when you are at work or when you access your university's network from home or on the road, it is hoped you have the advantage of 'industrial-strength' information security that your university's IS department has implemented. In all other cases, however, you are on your own and it is your responsibility to protect yourself. Protecting yourself is becoming even more critical because organised crime is increasingly turning its attention to home users. As businesses improve their information security, consumers become the next logical target. According to Symantec (**www.symantec.com**), which manufactures the Norton internet security products, if you connected an unprotected personal computer to the internet in 2003, it would have been attacked within 15 minutes. Today, that same computer will be attacked within seconds.

You can take two types of actions to protect your information assets: behavioural actions and computer-based actions (see Figure PI6.1). Behavioural actions are those actions that do not specifically involve a computer. Computer-based actions relate to safe computing. If you take both types of actions, you will protect your information and greatly reduce your exposure to fraud and identity theft.

Apply the Concept

Background

If you knew all the tricks thieves would use at the supermarket, you would know how to fend them off. The same is true online; although it is often much more difficult to know when you have left yourself vulnerable. Sometimes the best way to know what goes on is a simple tracking activity.

Activity

Spend one hour online. Keep up with every bit of information you put on the computer: user names, passwords, preferences you may complete, websites you may give your email address to and so on. If you visit a site and they know who you are, make note of that. Visit your junk mail at the end of the hour and see how many messages have been denied since you began the activity.

Deliverable

Compile your diary of events to submit to your tutorial group. Determine for yourself if you feel safe or unsafe because of behavioural or technical issues (or both!).

PI6.2 Behavioural actions to protect your information assets

You should take certain behavioural actions to protect your information assets. We discuss these actions in this section.

General behavioural actions

You should never provide personal information to strangers in any format — physical, verbal or electronic. As discussed in chapter 7, you are vulnerable to social engineering attacks at home as well as at work. Therefore, it is critical that you be on your guard at all times. For example, always verify that you are talking to authorised personnel before you provide personal information over the telephone. To accomplish this, you should hang up and call back the person or company, at a number that you obtain independently of the phone call. If the call is fraudulent, then the number the caller gives you will also be fraudulent. Credit card companies usually print their numbers on the back of their cards and/or on every statement. Further, you can find telephone numbers on your credit card company's website.

A very important security behaviour is to protect not only your personal information, such as your name, address and date of birth, but also your Tax File Number (TFN). A TFN is a unique nine-digit number issued only once during the lifetime of an individual by the Australian Taxation Office (ATO) to help the ATO and business organisations administer tax and other Australian government systems. There are a number of circumstances where an individual will be asked to provide their TFN, such as when starting work or changing jobs, applying for government social security income assistance benefits (i.e. Centrelink), opening a bank account and joining a superannuation fund. You should keep your TFN secure and only provide or disclose it to certain individuals or organisations for tax-related purposes. You should never provide your TFN when applying for work online — provide it only after you start work.

The TFN is the designated number that uniquely identifies each taxpaying individual in Australia and is therefore a 'prized' target for scammers and those wishing to perpetrate identity theft. Scams are designed to trick you into providing either money or information. Scammers can be very believable and will often quote your personal information such as your address, phone number and date of birth to sound more authentic. The scammers' intention is generally to commit fraud or undertake other illegal activities in your name such as access your bank account, take out loans or credit cards in your name, lodge false tax returns or fraudulently claim social security benefits from Centrelink. These activities can have serious consequences for you and your reputation, both financially and psychologically. This is why you should always be very guarded about providing any of your personal information (address, telephone numbers, date of birth, TFN). If you are uncertain, it is better not to provide any information and seek further validation of the requester's intentions and bona fides.

Another critical consideration involves your use of credit cards. Securing your credit cards is important because fraudulent credit card use is so widespread. One security measure that you can take is to use credit cards with your picture on them. Although some sales staff probably cannot read your signature on the back of your card, they can certainly compare your picture to your face. For example, the ANZ Bank will place your picture on several of its credit cards for a small fee. However, be sure to sign the reverse side of your credit card immediately upon receipt and ensure you destroy your old credit cards thoroughly before disposal.

You may also want to use virtual credit cards, which offer you the option of shopping online with a disposable credit card number. For no extra charge, you can sign up at your credit card provider's website and typically download software onto your computer. When you are ready to shop, you receive a randomly generated substitute 16-digit number that you can use at the online store. The number can be used only once or, in some cases, repeatedly, but only at the same store. The card number can also be used to buy goods and services over the phone and through the mail, although it cannot be used for in-store

purchases that require a traditional plastic card. Two card issuers that offer virtual cards are Citibank and Discover. (Recall our discussion of virtual credit cards in chapter 9.)

Also, pay very close attention to your credit card billing cycles. You should know, to within a day or two, when your credit card bills are due. If a bill does not arrive when expected, call your credit card company immediately. If your credit card is stolen and is being used fraudulently, the first thing the thief does is change the address on the account so that you do not receive the bill. Fortunately, you can view your credit card bills online. Further, most credit card issuers offer the option to receive your credit card bills via email. This process eliminates postal mail theft as a problem. In addition, when you write cheques to pay any of your accounts, particularly your credit card accounts, do not write your complete card number on the 'For' line of your cheque. Instead, write only the last four digits.

Another important action is to limit your use of debit cards. Debit cards are linked to your bank account, meaning that a person who steals your debit card and personal identification number (PIN) can clean out your bank account. In contrast, your liability with credit cards is usually zero (or a small amount). Instead, your credit card company bears the liability for fraudulent charges, provided that you notify the company within 60 days of the theft.

Do not use a personal mailbox at your home or apartment for anything other than catalogues and magazines. Use a private mailbox or a post office box. It is far too easy for thieves to steal mail from residential mailboxes when no one is at home for much of the day (see figure PI6.X). Think about the wealth of information that could be stolen from your mailbox: credit card statements, bank statements, investment statements and so on.

Destroy mail and old records with a cross-cut or confetti shredder before disposing of them. Recall our discussion of skip dipping in chapter 7. A single-cut shredder is not sufficient because, with enough time, a thief can reassemble the strips.

Another security option is to sign up with a company that provides proactive protection of your personal information. PayPal Australia is one example of a company that provides a protective layer between your financial (credit card) details and personal information, and the buyer or seller for online sales. This extra security layer utilises the latest security technology to safeguard users from online fraud. If you notice any unusual activity on your PayPal account that you did not authorise, then you can report it to PayPal and they will immediately lock down your account and begin an investigation to find out what is going on. The main advantage of this approach is that it further secures online sales against fraud, as no direct credit card details are exchanged with the buyer or seller because the online transaction and all online communications are encrypted.

Unlocked mailboxes leave owners vulnerable to identity theft. Consider all the personal documents you have delivered to your home address, and how easy it would be for a thief to access your mailbox when you're not home.

What to do in the event of identity theft

Your identity is one of the most valuable commodities you have and ties directly to your reputation. The ability to prove who you are is an important aspect of your life, particularly if you want to get a home loan, start a new job or buy something online. If you follow the behavioural and computer-based actions recommended in this Plug IT In, you will greatly reduce — but not eliminate — the chances that your identity will be stolen. If your identity is stolen despite these precautions, you should follow these ten simple steps to recover:

1. Secure your personal documents at home, when you are travelling and if you need to destroy them.
2. Secure your mailbox with a lock and when you move, redirect your mail.
3. Be cautious about using social media and limit the amount of personal information you provide.
4. Secure your computer and mobile phone with security software and strong passwords and avoid using public computers for sensitive activities.
5. Learn how to avoid common scams at **www.scamwatch.gov.au**.
6. Be cautious about requests for personal information over the internet, phone and in person in case it is a scam.
7. Investigate the arrival of new credit cards you did not ask for or bills for goods and services that aren't yours.
8. Be alert for any unusual bank transactions or missing mail.
9. If you are the victim of identity theft, report it to the police and any relevant organisations including your bank and/or financial institution and close all fraudulent or breached accounts immediately.
10. Order a free copy of your credit report from a credit reporting agency on a regular basis, particularly if your identity has been stolen.[1]

Once your identity has been stolen it is a long and difficult process to recover your personal and financial reputation and identity. In addition to these behavioural actions, the computer-based actions we discuss in the next section will further help you protect yourself.

PI6.3 Computer-based actions to protect your information assets

You can take many computer-based actions to increase the security of your information. First, we discuss how to determine where persons who use your computer have visited on the internet. Next, we briefly explain how to access social networking sites safely.

We then consider how to determine if your computer is infected with malicious software (malware) and what actions to take to prevent such infections. Next, we discuss how to protect your portable devices — for example, laptops and flash drives — and the information they contain. We follow with discussions of other valuable computer-based actions, how to protect your privacy when using the internet and email, how to recover from a disaster and how to protect yourself when computing wirelessly.

We also thoroughly discuss Microsoft Windows 7 and provide a section on Microsoft's Internet Explorer 8, because this browser has added security features. We do not discuss other operating systems and browsers because of space limitations.

Determining where people have visited on the internet using your computer

At home, you may have a single computer or several computers connected to a network. Although you may practise 'safe computing', other people who use your computer might not. For example, you might have housemates who use your computer. Their friends could be using your computer as well. You cannot be certain that these individuals take the same

safety precautions that you do. You can, however, identify the internet sites that anyone who uses your computer has visited. To accomplish this task, check the browser history. It is important to note that all modern browsers have a 'private browsing' mode in which the viewing history is not recorded. If someone uses private browsing on your computer, then you will not be able to check that person's browser history.

The dangers of social networking sites

You should never post personal information about yourself or your family in chat rooms or on social networking sites. In fact, you should access these websites and review any entries that you have made. The reason for these precautions is that potential employers are now searching these websites for information about you (see figure PI6.2). Well-known social networking sites include Facebook, Twitter and YouTube.

The good news is that social networking websites have added features to give us more control over our information. The bad news is that the privacy settings are not always easy to find and use. Your first decision is whether to make your profile publicly available or to keep it more private. More than 33 per cent of adult users allow everyone to see their profiles. In contrast, some 60 per cent restrict access in some way.

All of the major social networking sites give you control over public accessibility, but they have different mechanisms for doing so. With Facebook, for example, the default is a private profile, where users decide what information is publicly available. To make privacy adjustments on Facebook, follow these steps:

- Click on 'Settings'.
- Click on 'Privacy'.
- Work with the options you find there.

If you want to keep a low profile on Facebook, it is a good idea to look at the 'Applications' section in Privacy Settings. You may have shielded parts of your profile from public access, but that does not mean that you have done the same for Facebook applications that have access to much of your same data by default. For a full explanation of Facebook's privacy settings, see **www.facebook.com**.

On LinkedIn, most people want public profiles, and that is the default. The information that LinkedIn users share tends to be professional credentials, not details of their social lives, so there is less need for privacy. If you want additional privacy on LinkedIn, follow these steps:

- Click on 'Account & Settings' from your home page.
- Click on 'Privacy Settings' and scroll down to adjust your privacy settings.

One company, Reputation Defender (**www.reputationdefender.com**), will search out all information about you on the internet and present it to you in the form of a report. Then, at your command, it will 'destroy all inaccurate, inappropriate, hurtful, and slanderous information about you'.

FIGURE PI6.2 Increasingly, potential employers are checking applicants' social media presence, but users can control who has access to their content through their preferred website's privacy settings page.

Determining if your computer is infected

There are several signs to look for if you think your computer system is infected with malicious software or malware (discussed in chapter 7), including the following.

- Your computer shuts down unexpectedly by itself.
- Your computer refuses to start normally.
- Running the DOS CHKDSK (**CH**EC**K DISK**) command shows that less than 655 360 (640 kilobytes) bytes are available. To run the CHKDSK command, follow these steps:
  - Click on 'Start'.
  - Click on 'All Programs'.
  - Click on 'Accessories'.
  - Click on 'Command Prompt'.
  - Type in 'CHKDSK' and hit Enter.
- Your computer exhibits erratic behaviour, exhibiting some or all of these characteristics:
  - Your system unexpectedly runs out of memory on your computer's hard drive.
  - Your system continually runs out of main memory (RAM).
  - Programs take longer to load than normal.
  - Programs act erratically.
  - Your monitor displays strange graphics or messages.
  - Your system displays an unusually high number of error messages.

  Your email program sends messages to all the contacts in your address book without your knowledge or permission.

If you note any or all of these signs, then your computer might be infected with malware. You can then take the computer-based actions discussed later in this Plug In to rid your computer of this software. However, taking the actions discussed in the next section will reduce your chances of being infected in the first place.

Computer actions to prevent malware infections

Many of the actions we discuss in this section are common sense, but surprisingly large numbers of people do not pay attention to them. Taking these steps will help you prevent a malware infection of your computer system. We begin by considering actions that you must never take with your computer.

Never open unrequested attachments to email files, even if they are from people you know and trust. Their computers may have been compromised without their knowledge, in which case the email could be a phishing attack. Recall from chapter 7 that a phishing attack involves tricking people into visiting a phony website and, once there, providing confidential information.

Never open attachments or web links in emails from people you do not know. These attachments can infect your system with a worm or virus. Similarly, these web links can be a phishing attack that can infect your system with a Trojan horse, turning your computer into a zombie or bot (short for robot). As we saw in chapter 7, when this occurs your computer is no longer under your control.

Never accept files transferred to you during internet chat or instant messaging sessions. These files are usually not from people you know and they can infect your system with malware.

Never download any files or software over the internet from websites that you do not know. Never download files or software that you have not requested.

Test your system

It is a good idea to test your system. Several websites provide free security tests. These tests send different types of messages to your computer to evaluate how well your system is protected from a variety of attacks. Free testing websites include Shields Up! (**www.grc.com**), Symantec Security Check (**http://security.norton.com**) and McAfee My SecurityStatus (search 'McAfee My SecurityStatus' on the web).

Microsoft provides a valuable scanning tool called the Microsoft Baseline Analyzer. This tool scans Windows-based computers for common security problems and generates

individual security reports for each computer that it scans. The Baseline Analyzer can be downloaded for free. You can also run free malware scans on your computer. Several companies, including the following, will scan your computer to identify viruses, worms and other malware, and offer suggestions about how to clean your system if it is infected.

- Trend Micro (search the web for 'Trend Micro HouseCall')
- Panda Software (**http://www.pandasecurity.com/usa**).

Install a security suite on your computer

Security suites are software packages that contain a variety of security products, such as anti-malware software, spam protection, email fraud protection, spyware detection, intrusion detection and monitoring software. These suites provide a great deal of functionality in one package. There is a question of whether the individual functions in a security suite can match the combined functions of a group of individual products. Therefore, we discuss individual products in the next sections.

Well-known security suites include the following, but there are many others.

- ZoneAlarm Security Suite (**www.zonelabs.com**)
- McAfee Internet Security Suite (**www.mcafee.com**)
- Norton Internet Security (**www.symantec.com**)
- PC-cillin Internet Security (**www.trendmicro.com**).

Install an anti-malware product on your computer

You should install an anti-malware product on your computer and use it, ideally at least once per week. Remember that every time you scan your computer for malware with your anti-malware product, you must update your malware definitions before you scan. Typically, anti-malware product vendors automatically update your malware definitions over the web.

There are free anti-malware products and commercial anti-malware products. In general, the free products are adequate, but the commercial products offer more functionality. An excellent resource offering a great deal of information on free anti-malware products, as well as many other security products, is **www.thefreecountry.com**. Go to Security > Free Antivirus Software to see their list of anti-malware products.

Well-known commercial anti-malware products include the following, but there are many others:

- Norton Anti-malware (**www.symantec.com**)
- PC-cillin (**www.trendmicro.com**)
- VirusScan (**www.mcafee.com**).

Install a firewall on your computer

A personal firewall is software installed on your home computer that controls communications to and from your computer by permitting or denying communications based on your security settings. A personal firewall usually will protect only the computer on which the software is installed. Nevertheless, firewalls perform essential functions.

Essentially, firewalls should make your computer invisible. This means that your firewall should not respond to internet requests to ports (i.e. communications links to your computer) that are not used for common internet use. In effect, your computer operates in stealth mode on the internet.

Firewalls also should alert you to suspicious behaviour. They should tell you when a program or connection is attempting to do something you have not instructed it to do, such as download software or run a program such as ActiveX. ActiveX (by Microsoft), which can execute programs downloaded from Internet Explorer, can be exploited by attackers trying to compromise your computer. To manage ActiveX in Internet Explorer, follow these steps:

- Click on 'Start'.
- Click on 'My Computer'.
- Click on 'Control Panel'.

- Click on 'Security Center'.
- Click on 'Internet Options'.
- Click on the 'Security' tab.
- Click on the button that says 'Custom level…'.
- Scroll down and choose the following:
  - The button for 'Download signed ActiveX controls'
  - The button for 'Download unsigned ActiveX controls'.

Firewalls should block outbound connections that you do not initiate. Your firewall should not let your computer access the internet on its own. If your computer tries to access the internet by itself, this is a sure sign that it is infected with malware.

As with anti-malware programs, firewall products can be either free or commercially produced. Again, the free products are adequate, but the commercial products offer more functionality. For a list of free firewall software search 'about.com free firewalls'.

Many companies offer commercial firewall software. These are some of the best-known commercial firewall products:

- ZoneAlarm Security Suite (**www.zonelabs.com**)
- Norton Internet Security (**www.symantec.com**)
- PC-cillin Internet Security (**www.trendmicro.com**)
- McAfee Internet Security (**www.mcafee.com**)
- F-Secure Internet Security (**www.f-secure.com**)
- Panda Platinum Internet Security (**www.pandasoftware.com**).

It is a good idea to test your firewall. However, it is best to use only those test websites that are run by actual firewall or security software companies. A good firewall test site is the McAfee HackerWatch site at **www.hackerwatch.org/probe**. The HackerWatch site allows you to do a basic probe test on your computer to see if your firewall is blocking ports that may be vulnerable.

Install an antispyware product on your computer

As with anti-malware products and firewalls, free antispyware products are adequate, but commercial antispyware products offer more functionality. Free antispyware products include these:

- Ad-Aware SE Personal (**www.lavasoft.com**)
- Spybot Search&Destroy (**www.safer-networking.org**)

Well-known commercial antispyware products include the following, but there are many others:

- CounterSpy (**www.sunbeltsoftware.com**)
- Spy Sweeper (**www.webroot.com**)
- Ad-Aware (**www.lavasoft.com**)
- SpyCatcher (**www.tenebril.com**).

Several companies offer free spyware scans:

- Spy Audit (**www.webroot.com**)
- Zonelabs (**www.zonelabs.com**)
- Norton (**www.symantec.com**).

Install monitoring software on your computer

Monitoring software logs keystrokes, emails, applications, windows, websites, internet connections, passwords, chat conversations, web cams and even screenshots. Companies that offer monitoring software include the following:

- SpyAgent (**www.spytech-web.com**)
- SpyBuddy (**www.exploreanywhere.com**)
- WinSpy (**www.win-spy.com**)
- SpectorSoft (**www.spectorsoft.com**).

Install content-filtering software on your computer

Content-filtering software performs many functions. It can block access to undesirable websites, and it can record and view all of the websites that you or other users have visited.

Content-filtering software provides many filter categories, thus enabling you to selectively filter content. Companies that offer this software include the following:

- Cybersitter (**www.cybersitter.com**)
- NetNanny (**www.netnanny.com**)
- CyberSpy (**www.cyberspyware.com**).

Internet Explorer's Content Advisor utility allows you to block access to websites that meet specified criteria and to set your own tolerance levels for various types of internet content. To activate and configure Content Advisor, follow these steps:

- Click on 'My Computer'.
- Click on 'Control Panel'.
- Click on 'Security Center.
- Click on 'Internet Options'.
- When the Internet Options dialog box appears, select the Content Tab.
- Click on the 'Enable' button.
- You will see 13 categories. For each category, you can move the slide bar for increased restriction.
- After you have set the slide bar for each category, click 'OK'.

You can also block selected websites. To accomplish this, follow these steps:

- Click on 'My Computer'.
- Click on 'Control Panel'.
- Click on 'Security Center'.
- Click on 'Internet Options'.
- When the Internet Options dialog box appears, select the Content Tab.
- Click on the 'Enable' button.
- Click the Approved Sites tab.
- Enter the websites you wish to block, and click 'Never'.
- Click 'OK'.

Install antispam software on your computer

Antispam software helps you to control spam. Well-known commercial antispam products include the following, but there are many others:

- Cloudmark (**www.cloudmark.com**)
- MailFrontier Desktop (**www.sonicwall.com/**)
- SpamKiller (**www.mcafee.com**)
- Norton Antispam (**www.symantec.com**)
- SpamGourmet (**www.spamgourmet.com**)
- SpamAssassin (**http://spamassassin.org**).

You might also want to set up multiple free email accounts, such as accounts on Gmail. Then, as you surf the internet and are asked for your email address, you can use one of these accounts rather than your home or business email account. When your free email accounts are full of spam, you can close them and open new accounts.

Install proactive intrusion detection and prevention software on your computer

Recall from chapter 7 that anti-malware software is reactive in nature, thereby leaving you vulnerable to zero-day attacks. For this reason, it is important to add proactive intrusion detection and prevention software to your defences. One such product is Prevx (**www.prevx.com**). You can download and install Prevx for free, and it will scan your computer for malicious software. If it finds any, it will activate a free 30-day clean-up account and remove the malware from your computer. Once this period runs out, Prevx will continue to scan incoming programs and protect your computer from them. However, if you subsequently get infected and want to continue using Prevx, you must pay for one year of protection.

Manage patches

You should download and install all software patches immediately — for example, patches for Windows. Companies typically release patches to repair security problems. If you do not download and install patches quickly, your computer will be extremely vulnerable

to attack. Microsoft provides an automatic method that checks for and downloads any new patches. To enable Automatic Update in Windows XP, follow these steps:

- Right click on 'Start'.
- Click on 'Explore'.
- Scroll down and click on 'Control Panel'.
- Click on 'System'.
- Click on the 'Automatic Updates' tab at the top of the box.
- You can now configure when you want to download and install updates.

To open the Microsoft Update window in Windows XP, follow these steps:

- Click on 'Start'.
- Click on 'All Programs'.
- Click on 'Windows Update'.

If you click the 'Express' button, your system will be scanned and you will be notified if any new updates are available. You can then review suggested updates and install them.

Protecting your portable devices and information

Theft or loss of laptops, notebook computers, tablets, personal digital assistants, BlackBerrys and thumb drives, as well as the data contained on these devices, is a significant problem. You can take many proactive steps to protect portable devices and their data, including prevent the theft, use two-factor authentication and encrypt your data. You can also take reactive steps after a theft or loss has occurred. We consider all of these actions in this section.

Before we discuss these steps, there are two common sense precautions that many people forget. First, keep your laptop in an inconspicuous container. Laptop cases with your company logo simply draw the attention of thieves. Second, do not leave your laptop unattended in plain view — for example, in your car where it can be seen; instead, lock it in the boot of your vehicle.

One strategy to prevent the theft of a portable device is to use alarms. Laptop security systems operate by detecting motion, analysing the motion to determine whether a threat exists and, if it does, implementing responses. These alarms are battery powered, are independent of the computer operating system and operate whether the laptop is on or off. If a laptop armed with a security system is carried beyond a perimeter specified by the user, then the alarm assumes the laptop is being stolen. It can then prevent access to the operating system, secure passwords and encryption keys and can sound an audible alarm. One company that provides laptop security systems is Absolute Software's LoJack for Laptops (**www.absolute.com**).

Two-factor authentication means that you must have two forms of identification to access your laptop or notebook. The first authentication factor uses a token or biometrics. The second factor is your personal password. A token generates a one-time password that you must enter within a specified time limit. This password typically consists of six digits, which appear on the token's LCD screen. Companies offering tokens for two-factor authentication include Authenex (**www.authenex.com**), Kensington (**www.kensington.com**) and SecuriKey (**www.securikey.com**).

Fingerprints are the biometric used for two-factor authentication, by incorporating fingerprint readers into the laptop itself. See IBM (**www.ibm.com**) and Microsoft (**www.microsoft.com**). You can also use fingerprint authentication on your thumb drive with the SanDisk Cruzer (**www.sandisk.com**), the Lexar JumpDrive TouchGuard (**www.lexar.com**), the Sony MicroVault (**www.sony.net**) and the Kanguru Bio Slider (**www.kanguru.com**).

Data encryption provides additional protection by turning data into meaningless symbols that can be deciphered only by an authorised person. You can encrypt some or all of the data on your computer by using Windows XP's built-in encryption, folder-based encryption or full-disk encryption.

Windows XP's Encrypting File System allows you to encrypt files or folders. Follow these steps:

- Right-click on the file or folder.

- Click on 'Sharing and Security'.
- Click the 'General' tab at the top.
- Click the 'Advanced' tab.
- Check the box labelled 'Encrypt Contents to Secure Data'.
- Click 'OK'.

Beachhead Solutions (**www.beachheadsolutions.com**) and Credant (**www.credant.com**) also provide applications that allow you to encrypt files and folders.

Another step you can take to improve your security is to encrypt your entire hard drive, including your applications. See Mobile Armor (**www.mobilearmor.com**), the Kanguru Wizard (**www.kanguru.com**) and the PCKey (**www.kensington.com**).

If your laptop is lost or stolen, you can use laptop tracing tools or device reset/remote kill tools. For example, the XTool Computer Tracker (**www.computersecurity.com**), PC PhoneHome (**www.pcphonehome.com**) and LaptopLocate (**www.laptoplocate.net**) provide transmitters that secretly send a signal to their respective company control centres via telephone or the internet. This signal enables the company, with the help of the local authorities, internet service providers and telephone companies, to track your computer's location.

You can also use device reset/remote kill tools to automatically eliminate specified data on a lost or stolen laptop to prevent it from being compromised or misused. The solution works even when other security software or encryption methods fail. Examples of companies providing these solutions are McAfee (**www.trustdigital.com**) and Beachhead Solutions (**www.beachheadsolutions.com**).

Internet Explorer 9 offers a wide range of security features intended to protect your computer against malicious software; these features are discussed below.

Security features within Internet Explorer 9

Internet Explorer 9 (IE9) offers multiple, interrelated security features to help defend your computer against malicious software as well as safeguards to help ensure that your personal information does not fall into the hands of fraudulent or deceptive website operators. Together with Windows Defender, the security features in IE9 are an improvement over the security features of previous versions of Windows and Internet Explorer. IE9 has been improved so that it limits the amount of damage that malware can do if it is able to penetrate your system. Further, IE9 includes several features designed to thwart attackers' efforts to trick you into entering personal data on inappropriate websites. We discuss these features in this section.

Protected Mode

In Protected Mode, IE9 cannot modify any of your files and settings without your consent. Protected Mode requires you to confirm any activity that tries to place any software on your computer or to start another program. This feature also makes you aware of what a website is trying to do, giving you the opportunity to prevent it and to verify the trustworthiness of the site.

ActiveX Opt-In

ActiveX Opt-In automatically disables all but a small group of well-known, preapproved controls. Therefore, if a website tries to use an ActiveX control that you have not used before, IE9 displays a notice in the information bar. This notification enables you to permit or deny access when you are viewing unfamiliar websites.

Fix My Settings

Because most users simply accept the default setting on the applications they install and use, IE9 is shipped with security settings that provide the maximum level of usability while maintaining strict security control. Fix My Settings is a feature that alerts you when you might be browsing with unsafe settings on your computer. It does so by displaying a warning in the information bar as long as your settings remain unsafe. You can quickly reset your security settings to the medium-high default level by clicking the Fix My Settings option in the information bar. If you close your browser and it reopens with unsafe settings, you will see a notification page reminding you to correct your settings before you visit any websites.

Widows Defender

Widows Defender protects you against spyware and thus helps prevent malware from penetrating your system by piggybacking on spyware. This is a common mechanism by which malware is distributed and installed silently on the systems of unsuspecting users.

Personal data safeguards

IE9 provides the security status bar, located next to the address bar, which helps you quickly differentiate authentic websites from suspicious or malicious ones. This feature enhances your access to digital certificate information that helps you validate the trustworthiness of websites.

The security status bar provides prominent, colour-coded visual cues that indicate whether a website is safe and trustworthy. Earlier versions of Internet Explorer placed a gold padlock icon in the lower right corner of the browser window to designate the trust and security levels of the website. IE9 displays the padlock more prominently. You can also view a website's digital certificate information with a single click on the padlock icon. If IE9 detects any irregularities in the website's certificate information, then it displays the padlock icon on a red background.

The Security Status Bar also supports new Extended Validation (EV) certificates that offer stronger identification of secure websites such as banking sites. These sites have undergone a comprehensive verification process to ensure that their identity is that of the real business entity. IE9 highlights these validated websites with a green-shaded address bar and it prominently displays the associated business's name.

IE9 also provides an address bar in every window. This requirement helps ensure that you will be able to learn more about the true source of any information that you are seeing.

Phishing Filter

The Phishing Filter is an opt-in feature that maintains a list of potentially dangerous websites by scanning for suspicious website characteristics. The filter denotes known phishing sites by turning the address bar red. It then navigates users away from that page and displays a warning message about the potential for a phishing attack. For suspicious websites — meaning that a page has certain suspicious characteristics — the filter displays

a yellow address bar. Finally, it identifies acceptable websites by displaying the standard white address bar.

Delete Browsing History

IE9 provides a Delete Browsing History option for one-click cleanup so that you can easily and quickly erase all personal information stored in the browser. This feature is particularly important when you use a friend's computer or computers in public environments such as libraries, schools, conference centres and hotel business centres.

InPrivate

IE9 has a new security application called InPrivate, which features InPrivate Browsing and InPrivate Blocking. InPrivate Browsing helps prevent your browser from retaining your browsing history, temporary internet files, cookies, and user names and passwords, thus leaving no evidence of your browsing or search history. Today, websites increasingly access content from multiple sources, providing tremendous value to consumers. However, users may not be aware that some content, images and advertisements are being provided from third-party websites or that these sites can potentially track the users' behaviour. *InPrivate Blocking* enables users to block the information that third-party websites can potentially use to track your browsing history.

Domain Highlighting

This feature in IE9 helps you to see the real web address of the websites you visit. It accomplishes this task by highlighting the actual domain you are visiting in the address bar. This process helps you avoid deceptive or phishing websites that use misleading web addresses to trick you.

SmartScreen Filter

This feature helps protect you from online phishing attacks, fraud and spoofed or malicious websites.

Add-on Manager

This feature lets you disable or allow web browser add-ons and delete unwanted ActiveX controls.

Cross-site Scripting Filter

This feature can help prevent attacks from phishing and fraudulent websites that might attempt to steal your personal and financial information.

A 128-Bit secure connection for using secure websites

This feature helps IE9 create an encrypted connection with websites operated by banks, online stores, medical sites and other organisations that handle sensitive customer information.

Other actions that you can take on your computer

You can take some other actions on your computer for added protection. These consist of detecting worms and Trojan horses, turning off peer-to-peer file sharing, looking for new and unusual files, detecting spoofed (fake) websites and adjusting the privacy settings on your computer.

How to detect a worm

Worms are malicious programs that perform unwanted actions on your computer (see chapter 7). They exhibit the following characteristics that you can watch for.

- Your system exhibits unexplained hard disk activity.
- Your system connects to the internet by itself without any action on your part.
- Your system seems to be short on available memory.
- Your family, friends or colleagues notify you that they have received an odd email message from you, that they are sure you did not send.

Ordinarily, your anti-malware software should detect and remove worms. However, if your computer is currently infected with a worm, you may not be able to delete that file. In this case, you will have to reboot (start up) your system from a bootable disk and then delete the worm file from the Command Prompt. (Follow the steps for 'How to look for new and unusual files', which follows, to find the worm file.) Normally, when you reboot your system, the worm file should no longer be present.

How to detect a Trojan horse

Trojan horses are malicious programs disguised as, or embedded within, legitimate software (see chapter 7). You can determine if your computer is infected with a Trojan horse by following the steps listed here. These steps will enable you to see if your computer is 'listening' for instructions from another computer. They are based on the DOS-based utility program called Netstat (part of Windows).

The Trojan horse virus is named after a legend of the same name. In the story of the Trojan horse, Greece offered a wooden horse to Troy during the Trojan War. The horse masqueraded as a gift but concealed Greek soldiers within. Similarly, Trojan horse viruses appear harmless but can do a great deal of damage.

- Close all running applications and reboot your computer.
- When your computer restarts, do *not* establish a dial-up internet connection.
- It is okay to let your computer access the internet via a broadband connection (for example, cable or DSL modem).
- Open the DOS window:
  - Click on 'Start'.
  - Click on 'All Programs'.
  - Click on 'Accessories'.
  - Click on 'Command Prompt'.
- In the DOS window, type the following and press Enter:
  netstat –an>>c:\netstat.txt
- Close the DOS window and
  - Click on 'Start'.
  - Click on 'All Programs'.
  - Click on 'Accessories'.
  - Click on 'Notepad'.
- In Notepad, click on 'File' and then on 'Open'.

- In the box provided, type:
  c:\netstat.txt
- Click 'Open'.
- You will see a number of active connections in a Listening state. Each active connection will have a local address. The local address will be in a form like this: 0.0.0.0.XXXXX (where the Xs refer to a sequence of numbers).
- If a Trojan horse is present, your system will be listening for one of the addresses listed here:
  - Back Orifice 0.0.0.0.31337 or 0.0.0.0.31338
  - Deep Throat 0.0.0.0.2140 or 0.0.0.0.3150
  - NetBus 0.0.0.0.12345 or 0.0.0.0.12346
  - Remote Grab 0.0.0.0.7000.

How to detect fake websites

A fake website is typically created to look like a well-known, legitimate site with a slightly different or confusing URL. The attacker tries to trick people into going to the spoofed site and providing valuable information by sending out email messages and hoping that some users will not notice the incorrect URL. (We discussed this attack, known as phishing, in chapter 7.) Products that help detect fake websites include the SpoofStick, the Verification Engine and McAfee's SiteAdvisor. These products are not definitive solutions, but they are helpful.

The SpoofStick (**www.spoofstick.com**) helps users detect fake websites by prominently displaying a new toolbar in your browser that shows you which site you are actually surfing. For example, if you go to Amazon's website, the SpoofStick toolbar says, 'You're on amazon.com'. However, if you go to a fake website that pretends to be Amazon, the SpoofStick toolbar shows the actual IP address of the website you are surfing, saying for example, 'You're on 137.65.23.117'.

Similarly, the Verification Engine (**www.vengine.com**) enables you to verify that the site you are visiting or are directed to via email can be trusted. If you move your mouse to the logo brand or image you want to verify, the Verification Engine will authenticate the trust credentials of the site you are surfing. In addition, during a secure communications session with Internet Explorer, you can move your mouse over the padlock to verify that the padlock is genuine and not a fraudulent graphic and the site uses a transport layer security (TLS) certificate (discussed in chapter 7) that contains the correct information about the company to which you are connected. McAfee's SiteAdvisor (**www.siteadvisor.com**) sticks a green, yellow or red safety logo next to search results on Google, Yahoo! and MSN. It also puts a colour-coded button in the Internet Explorer toolbar. Navigating the mouse over the button displays details as to why the website

Most browsers use a padlock icon to indicate when a website is secure. Google Chrome uses a green padlock icon in the top left corner, similar to the icon pictured.

is good or bad. SiteAdvisor also scores websites based on the excessive use of pop-up advertisements, how much spam the website will generate if you reveal your email address and whether the site spreads spyware and adware.

Protecting your privacy

In today's hostile internet environment, you must use strong passwords (discussed in chapter 7) and adjust the privacy settings on your computer. You may also wish to protect your privacy by surfing the web and emailing anonymously. In this section we discuss these actions.

Use strong passwords

You can use the Secure Password Generator at PCTools to create strong passwords. The Generator lets you select the number and type of characters in your password.

Remembering multiple passwords is difficult. You can use free software such as Roboform (**www.roboform.com**) to help you remember your passwords and maintain them securely.

How to adjust your privacy settings on your computer

Windows 7 allows you to select the level of privacy that you want when using your computer. Here are the steps to follow to adjust your privacy settings:

- Click on 'Computer'.
- Click on 'Control Panel'.
- Click on 'Network and Internet'.
- Click on 'Internet Options'.
- Click on the 'Privacy' tab at the top, and then the 'Default' button.
- Adjust the slide bar.
- Manipulate the slide bar to determine the level of privacy you desire.
- You will see an explanation of what each level means as you use the slide bar.
- The levels of privacy and their meanings are
  - Lowest (Accept all Cookies)
    - All cookies will be saved on this computer.
    - Existing cookies on this computer can be read by the websites that created them.
  - Low
    - Restricts third-party cookies that do not have a compact privacy policy.
    - Restricts third-party cookies that use personally identifiable information without your implicit consent.
  - Medium
    - Blocks third-party cookies that do not have a compact privacy policy.
    - Blocks third-party cookies that use personally identifiable information without your implicit consent.
    - Restricts first-party cookies that use personally identifiable information without your implicit consent.
  - Medium High
    - Blocks third-party cookies that do not have a compact privacy policy.
    - Blocks third-party cookies that use personally identifiable information without your explicit consent.
    - Blocks first-party cookies that use personally identifiable information without your explicit consent.
  - High
    - Blocks cookies that do not have a compact privacy policy.
    - Blocks cookies that use personally identifiable information without your explicit consent.
  - Very High (Block all Cookies)
    - Cookies from all websites will be blocked.
    - Existing cookies on your computer cannot be read by websites.

Note: A first-party cookie either originates on, or is sent to, the website you are currently viewing. These cookies are commonly used to store information, such as your preferences when visiting that site. In contrast, a third-party cookie either originates on, or is sent to, a different website from the one you are currently viewing. Third-party websites usually provide some content on the website you are viewing. For example, many sites rely on advertising from third-party websites, which frequently use cookies. A common use for third-party cookies is to track your browsing history for advertising or other marketing purposes.

How to surf the web anonymously

Many users worry that knowledge of their IP addresses is enough for outsiders to connect their online activities to their 'real-world' identities. Depending on his or her technical, physical and legal access, a determined party (such as a government prosecutor) may be able to do so, especially if he or she is assisted by the records of the ISP that has assigned the internet protocol (IP) address. To protect their privacy against this type of activity, many people surf the web and email anonymously.

Surfing the web anonymously means that you do not make your IP address or any other personally identifiable information available to the websites that you are visiting. There are two ways to surf the web anonymously: You can use an anonymiser website as a proxy server, or you can use an anonymiser as a permanent proxy server in your web browser.

A *proxy server* is a computer to which you connect, which in turn connects to the website you wish to visit. You remain anonymous because only the information on the proxy server is visible to outsiders.

For example, consider Anonymouse (**http://anonymouse.org**). When you access this site, you can click on a link called 'Your calling card without Anonymouse'. You will see the information that is available to any website you visit when you surf normally.

If you want to surf anonymously, enter the URL of the site you want to visit on the Anonymouse website where it says 'Enter URL'. For example, suppose you wish to visit **www.amazon.com**. You enter this URL where indicated on the Anonymouse website. When the Amazon website opens on your computer, the URL will look like this: **http://anonymouse.org/cgi-bin/anon-www.cgi/http://www.amazon.com/gp/homepage.html/102-8701104-7307331**. You are now anonymous at Amazon because Anonymouse is a proxy server for you, so Amazon sees only the information from Anonymouse. Keep in mind that although anonymous surfing is more secure than regular surfing, it is also typically slower. Other anonymizers include Anonymize (**www.anonymize.net**), Anonymizer (**www.anonymizer.com**), IDZap (**www.idzap.com**), Ultimate Privacy (**www.ultimate-anonymity.com**) and GhostSurf Platinum.

Another way to surf the web anonymously is to use an as a permanent proxy server on your computer. Here are the steps to take to do this:

- Click on 'Computer'.
- Click on 'Control Panel'.
- Click on 'Network and Internet'.
- Click on 'Internet Options'.
- Select the 'Connections' tab.
- Click on 'LAN Settings'.
- When the Local Area Network (LAN) Settings dialog box opens, check the 'Use a proxy server for your LAN' option.
- Enter the anonymizer's web address in the Address field (it is your choice of which anonymizer you wish to use).
- Enter 8080 in the Port box.
- Click 'OK'.

How to email anonymously

The reasons for anonymous email are the same as those for surfing the web anonymously. Basically, you want to protect your privacy. When you email anonymously, your email messages cannot be tracked back to you personally, to your location or to your computer. Essentially, your email messages are sent through another server belonging

to a company — known as a *re-mailer* — that provides anonymous email services. The recipient of your -email sees only the re-mailer's header on your message. In addition, the re-mailer encrypts your messages so that if they are intercepted, they cannot be read. One possible drawback to utilising a re-mailer is that your intended recipients might not open your email because they will not know it is from you.

Leading commercial re-mailers include CryptoHeaven (**www.cryptoheaven.com**), Ultimate Privacy (**www.ultimate-anonymity.com**) and Hushmail (**www.hushmail.com**). The commercial version of Pretty Good Privacy (PGP) is available at **www.pgp.com**.

In addition, several free products for anonymous emailing and encryption are widely available. For example, the free, open-source version of Pretty Good Privacy, called Open PGP, is available at **www.pgpi.org**. For a list of these free products and a review of each one, visit **http://netsecurity.about.com/**. The Outlook email client that comes with Microsoft Office also allows you to encrypt outgoing email messages. This product is based on public key technology (discussed in chapter 7), so you must download and purchase a digital certificate. The first time you send an encrypted message, Microsoft takes you through the steps necessary to obtain your digital certificate.

The steps necessary to use email encryption in Outlook are as follows.

- Open Outlook and compose your message.
- Click the 'Options' button (you may need to select 'More Options', depending on your version of Outlook.
- When the Message Options window opens, click the 'Security Settings' button.
- The Security Properties window now opens.
- Check the 'Encrypt' message contents and attachments checkbox.
- For the time being, you should *not* check the 'Add digital signature to this message' checkbox because first you need to install a digital certificate.
- Click 'OK' in the Security Properties dialog box.
- You should now be returned to your message.
- Choose an address to send the message to.
- Click the 'Send' button.
- You see the 'Welcome to Secure Email' window.
- Click the 'Get Digital ID…' button.
- You now are taken to a Microsoft website with links to two digital certificate providers: GeoTrust and VeriSign.
- You have to register for the digital certificate at each provider; you need access to your email (and your telephone for GeoTrust).
- After the registration process, you click an installation button to install the digital certificate.
- When you start the installation, Microsoft may display a Potential Scripting Violation warning; click 'Yes' to continue.
- Once you get the digital certificate installed, you can click 'Send' in Microsoft Outlook.
- You may encounter problems if the people you are sending encrypted messages to do not have digital certificates; also, some email systems may not accept encrypted messages because antivirus scanners cannot scan encrypted email.

Thawte (**www.thawte.com**) offers a free personal digital email certificate.

It is a good idea to periodically check the trusted certificate authorities that are configured in your browser and verify that those companies can be trusted. If you use Windows 7, you can do so by following these steps:

- Click on 'Start'.
- Right-click on 'Explore'.
- Click on 'Control Panel'.
- Click on 'Network and Internet'.
- Click on 'Internet Options'.
- Click on the 'Content' tab.
- Click on the 'Certificates' button.
- Click on the 'Intermediate Certification Authorities' tab and check that the companies listed can be trusted.
- Click on the 'Trusted Publishers' tab and check that the companies listed can be trusted.

Erasing your Google search history

If you have signed up for Google's Personalised Search, then you can follow these steps to erase your search history. First you sign in to your Google account at **www.google.com/psearch**. You can examine the Search History page and choose days on the calendar to see every search you have made since you created your Google account. Click on the Remove Items button. Remember, however, that even after you remove items from your computer, logs and backups will still exist on Google's servers. To prevent Google from collecting this information in the future, select items such as 'Web', 'Images', and 'News' about which you do not want data collected, and then press the 'Pause' button.

Preparing for personal disasters

Disasters are not limited to businesses. You can experience disasters at home, such as fires and floods. Therefore, you should take certain steps to protect your information assets, whether they are stored on your computer (digital form) or in another form (hard copy). First and foremost, you should have a safety deposit box at your bank for your important papers. You should also have a fireproof safe at home where you can store other important papers. You should make a regular backup of your key files and keep these backups in the safe as well. You might also want to encrypt your backup files if they contain sensitive information.

Restoring backup files

You can use the Windows Backup utility to restore the backup copies to your hard disk. This is how you launch Backup in Windows 7:

- Click 'Start'.
- Click 'All Programs'.
- Click 'Accessories'.
- Click 'System Tools'.
- Click 'Backup'.

Windows 7 has a utility called Windows System Restore. This utility automatically restores key system files to the state they were in before you had problems. (Note: System Restore affects your system files, not your data files.) System Restore creates a 'mirror' of key system files and settings — called a restore point — every 10 hours, whenever you install a new piece of software or whenever you manually instruct it to do so. When your system encounters a problem, such as being infected with a virus or worm, you can revert to a restore point before the problem occurred, thereby putting your system back in working order.

To use System Restore:

- Click 'Start'.
- Click 'All Programs'.
- Click 'Accessories'.
- Click 'System Tools'.
- Click 'System Restore'.
- When the System Restore window opens, choose the 'Restore My Computer To An Earlier Time' option.
- Click 'Next'.
- When the 'Select A Restore Point' screen appears, you will see a calendar showing the current month. Any date highlighted in bold contains a restore point. Select a restore point from before the problem appeared, and click 'Next'.
- When the confirmation screen appears, click 'Next'.

Wireless security

Many home users have implemented a wireless local area network. The security considerations for wireless networks are greater than those for wired networks. The reason for this is simple. If you are wirelessly computing and communicating, then you are broadcasting, and therefore by definition, you are nonsecure. The most common reason for intruders to connect to a nonsecure wireless network is to gain access to the internet. Intruders

might also connect in order to use your network as a base for spamming or for other unethical or illegal activities. Finally, they may do so to gain access to your sensitive personal information.

Unfortunately, recent studies have indicated that three-quarters of all home wireless users have not activated any security features to protect their information. Unless you take the steps we discuss here, your information assets are extremely vulnerable.

Hide your service set identifier (SSID)

Your wireless router, which connects your home network with your ISP, comes with a default SSID that is the same for thousands or millions of routers made by the manufacturer. Therefore, an attacker can search for wireless networks by looking for a relatively small number of default SSIDs. For this reason, you should change your default SSID to a unique SSID and configure your wireless home network to stop broadcasting the SSID. A step-by-step guide to perform these security measures is available online (just search 'about.com change default SSID').

Use encryption

To avoid broadcasting in the clear, you must use encryption with your wireless home network. Wireless equivalent protocol (WEP) is an old protocol that is now very easy to crack and therefore should not be used. Instead, you should use wi-fi protected access (WPA2), which is the second generation of WPA. WPA2 is much stronger than WEP and will protect your encryption against attackers. (Note: Your wireless router must support WPA2. Otherwise, use WPA rather than WEP.) In addition, you should use a strong passphrase of at least 20 random characters on your router. (Chapter 7 provides specific instructions for creating strong passphrases.)

Filter out media access control (MAC) addresses

Every piece of networking hardware has a unique identification number called a media access control (MAC) address that looks like this: 00-00-00-00-00-00. (This MAC address is only an example.) You should compile the MAC address of all computers on your home wireless network. Then, instruct your router to connect only with those computers, and deny access to all other computers attempting to connect with your network.

To find the MAC address of your computer (if you run Windows), follow these steps:

- Click on 'Start'.
- Click on 'All Programs'.
- Click on 'Accessories'.
- Click on 'Command Prompt'.
- At the cursor, type 'ipconfig/all'.
- Hit 'Enter'.
- The MAC address will be the physical address.

Limit internet protocol (IP) addresses

You should instruct your router to allow only a certain number of IP addresses to connect to your network. Ideally, the number of IP addresses will be the same as the number of computers on your network.

Sniff out intruders

A variety of wireless intrusion detection systems will monitor your wireless network for intruders, alert you when are on your network, display their IP addresses and their activity and inform them that you know that they are there. Commercial products include the Internet Security Systems (**www.iss.net**) wireless scanner and AirDefense Personal (**www.airdefense.net**). AirSnare is a free wireless intrusion detection system.

Using a public hotspot

When you travel, keep in mind that most public wireless providers and hotspots employ no security measures at all. As a result, everything you send and receive is in the clear and has no encryption. Many intruders go to public hotspots and listen in on the wireless computing and communications taking place there. If you must compute wirelessly at a public hotspot, you should take several precautions before you connect.

- Use virtual private networking (VPN) technology to connect to your organisation's network (discussed in chapter 7).
- Use Remote Desktop to connect to a computer that is running at your home.
- Configure the Windows firewall to be 'on with no exceptions'.
- Only use websites that use transport layer security (TLS) for any financial or personal transactions.

Test your wireless network

After you have finished all the necessary steps to protect your wireless home network, it is a good idea to test the network for vulnerabilities. A free wi-fi vulnerability scanner has been created by eEye and is available for download (just search 'eEye download' for the link). This tool scans your vicinity looking for wireless devices to test. When you run it, it generates a detailed report that outlines all of the security problems it finds.

Wireless security software

For extra security, you can purchase wireless security programs. Trend Micro (**www.trendmicro.com**) has added Wi-Fi Intrusion Detection to PC-cillin, which also includes a personal firewall, antivirus software and antispyware software. The software warns you when an unknown user tries to access your wireless network. Zonelabs (**www.zonelabs.com**) has a product called ZoneAlarm Wireless Security that automatically detects wireless networks and helps secure them.

McAfee (**www.mcafee.com**) provides a free scan to check the security of the wireless network connection that you are using. The scan works only with Internet Explorer. Go to **www.mcafee.com**, click the section for home users and look under Free Services for McAfee Wi-Fi scan.

BEFORE *YOU GO ON . . .*

1. Why is it so important for you to protect yourself?
2. What are the two types of action that you can take to protect yourself?

Apply the Concept

Background

Although computer-based actions are extremely important to the security of a computer, they all begin with the decision to protect your information assets. There are many, many tools available to you to help protect your information. It would be a good idea to become familiar with the many tools available (many of which are presented in this Plug In).

Activity

Visit the McAfee product website called 'Site Advisor'. Look for the 'how it works' link at the top of the page. You will see that this simple tool makes it easy for you to be more aware of the security level of the sites you are visiting.

Download and install this tool and browse the web for 30 minutes or so. Visit the sites you routinely go to and write down the security rating each is given by McAfee. After going over your list of sites, does this make you want to change any of your habits?

Deliverable

Submit your list to your tutorial group along with any resulting behavioural changes you plan to make.

SUMMARY

1 Explain why it is critical that you protect your information assets.

We live in a digital world. Unfortunately, every time we use our computers or access the internet, we risk exposing both professional and personal information to people looking to steal or exploit that information. It is your responsibility to protect yourself in our hostile, digital environment. Protecting yourself is becoming even more critical because organised crime is increasingly turning its attention to home users. As businesses improve their information security, consumers become the next logical target.

2 Identify the various behavioural actions you can take to protect your information assets.

> Do not provide personal information to strangers in any format (physical, verbal or electronic).
> Protect your Tax File Number (TFN).
> Use credit cards with your picture on them.
> Do not sign the back of your credit cards. Instead, write 'Photo ID Required'.
> Pay very close attention to your credit card billing cycles.
> Limit your use of debit cards.
> Do not use a personal mailbox at your home for anything other than catalogues and magazines.
> Use a cross-cut or confetti shredder.
> Sign up with a company that provides proactive protection of your personal information.

3 Identify the various computer-based actions you can take to protect your information assets.

> Check to see where anyone who may have used your computer has visited on the internet.
> Never post personal information about yourself or your family in chat rooms or on social networking sites. Use the privacy features provided by social networking sites to limit public access to your profile.
> Never open unrequested attachments to email files, even those from people you know and trust.
> Never open attachments or web links in emails from people you do not know.
> Never accept files transferred to you during internet chat or instant messaging sessions.
> Never download any files or software over the internet from websites that you do not know.
> Never download files or software that you have not requested.
> Test your system.
> Run free malware scans on your computer.
> Have an anti-malware product on your computer, and use it (ideally at least once per week).
> Have a firewall on your computer.
> Have an antispyware product on your computer.
> Have monitoring software on your computer.
> Have content-filtering software on your computer.
> Have antispam software on your computer.
> Have proactive intrusion detection and prevention software on your computer.
> Manage patches.
> Use a laptop security system.
> Use two-factor authentication.
> Use encryption.
> Use laptop-tracing tools or device reset/remote kill tools.
> Look for new and unusual files.
> Detect fake websites.
> Use strong passwords.
> Surf the web anonymously.
> Email anonymously.
> Adjust the privacy settings on your computer.
> Erase your Google search history.
> Personal disaster preparation: backup, backup, backup!
> Wireless security
>> Hide your service set identifier (SSID).
>> Use encryption.
>> Filter out media access control (MAC) addresses.
>> Limit IP addresses.
>> Sniff out intruders.
>> Change the default administrator password on your wireless router to something not easily guessed.
>> Use VPN technology to connect to your organisation's network.
>> Use Remote Desktop to connect to a computer that is running at your home.
>> Configure Windows firewall to be 'on with no exceptions'.
>> Only use websites that use transport layer security (TLS) for any financial or personal transactions.
>> Use wireless security programs.

>>> DISCUSSION QUESTIONS

1 Why is it so important for you to protect your information assets? Can you assume that your organisation's MIS department will do it for you?

2 Discuss the differences between behavioural actions that you should take and computer-based actions that you should take.

>>> PROBLEM-SOLVING ACTIVITIES

1 Using one product suggested in this Plug IT In or a product you find, do the following.

- Test or scan your computer for malware.
- Test your firewall.
- Scan your computer for spyware.

2 Follow the steps in this Plug IT In to see if you have a Trojan horse on your computer.

>>> ENDNOTES

1 'Identity security', Australian government website, www.ag.gov.au.