Computer Security – keeping your personal information safe

Many people store a lot of personal information on their computer. In addition to the contents of emails, there may be email passwords, tax file numbers, medicare number, internet banking details including PINS and passwords, full names and dates of birth of yourself and family members, and so on.

If this information falls into the hands of criminals, you may become the victim of identity theft.

Identity theft happens in a multitude of ways. It can range from somebody using your credit card details illegally to make purchases over the internet or telephone, through to having your entire identity assumed by another person to open bank accounts, take out loans, and conduct other business illegally in your name.

The Australian Government has resources on protecting your identity. Go to the website http://staysmartonline.gov.au and look at the information under the "Computers" tab.

1. Viruses and Trojans

If you do not have anti-virus software installed and being regularly updated (at least weekly), then you are at risk of being infected by viruses and trojans attached to emails. In turn these can generate infected emails and send them to others in your address book without you being aware of it. Trojans can also secretly transmit data such as passwords you type, to a remote computer.

If you don't have anti-virus software installed, we suggest you download a free product such as AVAST! Home Edition, and install it. Link: http://www.avast.com/

Remember that just because an email says it comes from someone you know, that does NOT mean that's true. It is trivially easy to forge the displayed sender address, and viruses do just that. If you receive an email with an attachment that you are not expecting, just delete it. And then empty the trash in your email system.

You can have your computer compromised by clicking on links in emails. Many unsolicited emails invite you to click on a link which may in fact connect to a website run by criminals or hackers. Most modern web browser software will warn you if the website is trying to install or run malicious software on your computer, but vigilance is needed. The best policy is to not click on links in unsolicited emails, ever.

Its not just your computer that can be compromised by a virus or trojan. Any device that has internet access can be affected – so a smart-phone (eg iphone, android, blackberry) or a tablet (eg iPad, Galaxy tab, etc) is just as vulnerable. You can and should install antivirus software on your phone or tablet if they are internet-connected.

2. Scams - requests for PINS, Passwords, personal information

Banks, government departments, internet service providers, etc will NEVER send emails (or make phone calls) asking you to provide your username, PIN or password. Any email which asks you to send that information or to click on a link to enter that information, will be fraudulent. Emails and fake websites can look and sound very believable, but please don't be deceived.

Never give anyone your PINS or passwords. Check out the Australian Govt website about scams at http://www.scamwatch.gov.au for helpful information about how to avoid being trapped by scammers (a polite word for criminals).

Likewise, don't give personal details to people calling you by phone. A lot of fraud is done by phone too.

3. Passwords, information sharing and Social Media

Always use a strong password for any accounts that are important, including your email account(s). Automated password cracking systems can guess many passwords, so you should use something which is not in a dictionary, does not contain your name or that of your spouse or children or pet, and does not contain your date of birth or address. Use a mixture of upper and lower case letters, numbers and perhaps an underscore or dash as well.

Think twice before disclosing personal information to anyone, especially via email (which is an insecure medium). For example, medicare number, tax file number, date of birth are things that very few others ought to know.

If you use social media sites such as Facebook, you should adjust the privacy settings so that people who don't know you well can't see much of your profile. And be cautious about what information you put on your profile or post on your page.

Web browsers often prompt you to "save" your password. If you do this for important accounts, anyone who can access your computer can also access these accounts! So having your computer secured is especially important; the next few paragraphs tell you how to do that.

4. Secure your computer hard disk against misuse

Your computer could easily be stolen, especially if it is a laptop. Its then a simple matter for anyone to read information on the hard disk drive of the computer, including emails, documents, and even passwords. Even if you have a login or screen-saver password on the computer, that can be bypassed easily once the machine is stolen. And if you have told your web browser to “remember” important passwords such as your online banking passwords, then the thief will have access to those as well!

The best precaution against unauthorised access to your computer is to install Disk Encryption software that encrypts your entire hard disk drive so that the computer cannot start up and the hard disk cannot be 'read' unless you enter a secret passphrase. This is discussed below, and you should consider the other options below as well.

a) Full Disk Encryption

Disk encryption software is the best way to secure your information. It prevents access to the data on your computer even if the machine is stolen or seized. Your computer works exactly the same as before, all that has changed is that no-one can use it until your secret passphrase is typed in.

For computers running the Windows operating system, which is the most common, you can use the free VeraCrypt software available at to encrypt the entire hard disk. You must invent a (reasonably lengthy) passphrase when you install VeraCrypt; this passphrase is the only way the information on the hard disk can ever be de-decrypted. Naturally the passphrase should be something that no-one else could possibly guess. The longer the passphrase, the less likely it can be cracked by hackers or criminals.

For Macintosh computers, FileVault is a system that protects files in your home directory and it can be found in the Mac OSX v10.3 ("Panther") operating system and later. If you have OSX v10.6 (Lion) or later, then it has FileVault 2 which can encrypt the entire hard disk.

If you use a Linux operating system, there are various options for encrypting your hard disk. For example, the popular distros Ubuntu Linux and Linux Mint allow you to encrypt your home folder and swap file area when you install the operating system.

With some of these products, you can alternatively set up encryption for a specific folder/directory on your computer, to protect the contents of that folder/directory only.

Another advantage of using full-disk encryption is that when you decide to replace your computer, you “old” data is safe from criminals who might get hold of the discarded machine.

Possible negatives

There's one obvious down-side to disk encryption. If you forget your secret passphrase then you will never get access to the information stored on the computer again. You cannot call a "locksmith" and have a new "key" made. That's something you need to keep in mind.

b) Secure File Wiping software

If you want to permanently delete a file, you need to do more than just press the "Delete" button. When you delete a file (or an email) the system simply marks that space on the disk drive as being available for re-use. But the data is not actually removed.

A secure file wiper or eraser is a program that properly destroys the file you are deleting, rather than just marking it as unused. You use it to securely delete all trace of one or more files, instead of putting them in the normal trash/recycle bin.

For Mac users, version OSX 10.3 and later has a built in feature called "Secure Empty Trash".

Linux users can try WipeFreeSpaceGUI (http://sourceforge.net/projects/wipefreespace/files/)

Windows users can try the free version of Eraser (http://eraser.heidi.ie/). One downside is that Eraser downloads Windows .NET framework, which takes a while to install itself. On the plus side, Eraser can be scheduled to automatically erase unused space on the drive at regular intervals (eg weekly).

c) Shared computers – keeping your information separate

If you share a computer with another family member, and you want to encrypt the entire hard disk on the computer, make sure you explain to the other person about protection against identity theft, and perhaps show them this leaflet.

Obviously the other person with the passphrase will have access to anything you put on the computer. If you'd prefer to have some of your things kept private from other users of the machine, you can also use Truecrypt (on Windows, Mac or Linux machines) to create a separate private encrypted folder for which only you have the passphrase.

For email, you should get a separate email account for privacy purposes rather than sharing with another family member. Set a password on it so the other person(s) can't access your email. Google's gmail (http://mail.google.com) is a free webmail service with almost unlimited storage space, though there are many free email other services available.

d) Screensavers and password locking

In addition to protecting your disk drive by encryption, remember that if you leave it on and logged in whilst you are out of the house then an intruder could use the computer to access your information.

You should either turn the computer off when not in use, or better still, activate the screen-saver password lock facility. That will automatically lock the system after say 5 or 10 minutes of inactivity, and a password is then required to unlock it. This also stops inquisitive grandchildren or visitors from using your computer without permission! You can also lock the system manually; on a Windows system press the Windows key and the letter "L".

e) Keep your passphrase and password secure

All of the above precautions are useless if you write your passphrases and pins etc on a piece of paper and leave it where a thief or intruder can take it! You do need to think carefully about where to store your passwords and PINS in case you forget them; don't leave them lying around where a casual observer can find them. If you need to write down your account details, consider NOT writing down the password but instead using a cryptic clue to the password that you can easily remember but no-one else will be able to make sense of.

5. Safely disposing of a computer's hard disk drive

So your old computer is being given away or sold or sent for recycling? Unless your hard disk drive was fully encrypted as explained above, the person who receives your old computer could easily extract all your personal information from the disk drive even if you "deleted" your files.

It is not enough to delete something When you delete a file (or an email) the system simply marks that space on the disk drive as being available for re-use. But the data is not actually removed. At some stage in the future it might be over-written if programs need that space, but that might never happen, especially now that hard disk drives have such large capacities. A ten year old child with some readily-available 'undelete' software could retrieve your deleted files in moments.

Sometimes computers sent for "recycling" are actually sent illegally to Africa or Asia where the disks are stripped of any useful data by criminal gangs who then use it for identity theft, credit card fraud, bank account theft, and so on.

The Australian Federal Police's National Organised Crime Taskforce warns that before discarding computer devices we need to destroy hard drives or use secure disk-wiping programs to ensure the data can never be retrieved.

You can download free software that will let you securely erase the entire disk drive so that its almost impossible for anything to be recovered. Try DBAN (see http://www.dban.org/). Create a bootable CD or floppy disk with this software on it, reboot, and tell it to start erasing. A large hard disk drive may take several hours to be erased fully, but its worth doing.

An alternative is to open the computer, remove the hard disk drive (you may need a screwdriver), place it on a hard surface outside (eg the driveway) and give it a few whacks with a hammer till you can hear bits rattling inside when you shake the drive. That of course wrecks the drive so no-one can read it.

Of course, if you have already used full-disk encryption on the hard disk, there is no need to securely wipe or destroy the disk, though there's no harm in taking that extra precaution if you want to.

**