Information Security and its implications for the Home User

In this current first world climate of burgeoning technology trends and the “internet age”, the security of your personal information is more important than it has ever been.

Not since the rise of the Third Reich has it been more important to the average consumer to ensure the information that constitutes “their person” be secure. We are seeing more frequent media reports of identity theft and fraud and the numbers of victims are increasing exponentially. In America alone, online identity theft complaints to the Federal Trade Commission (FTC) rose by 87.7% in 2002 against the previous year.

A test conducted recently by an American newspaper and IT security consultants[1] showed that a PC connected to the Internet without adequate protection was hijacked in around 4 minutes. Windows PCs make up roughly 80% of the computers connected to the Internet, and the vast majority of automated attacks are designed to locate and exploit known security weaknesses. However, for users of other operating systems, don’t be lulled into a false sense of security. Mac and linux/unix attacks are increasing exponentially with more specialised attacks. A hijacked PC will give the attacker full access to everything on your computer as well as the use of your computer to achieve other objectives such as attacking companies and websites. If like most people you store your passwords in a file on your computer – you may have already been compromised.

Here is an interesting scenario: In February 2003, Derek Bond, a 72-year-old retiree from Bristol, England, spent three weeks sleeping on the concrete floor of a South African gaol after his name and passport number showed up on an FBI wanted list as he arrived in the country for a vacation. In vain, he protested that not only was he ignorant of any supposed crimes he'd committed in America, but he'd never even been to the country. Release didn't come until the publicity surrounding his fate prompted an informant to point the FBI to the "Derek Bond" whom they did want to talk to—comfortably holed up in Las Vegas, after purloining the identity of the real Mr. Bond some 14 years before.

Bond's misfortune illustrates—to the extreme—the menace of identity theft. But it's not gaol time that worries people so much as impaired credit records and fraud. Armed with just a few pieces of information—information readily available from trash or stolen documents—identity thieves can take advantage of lax security at financial institutions to enrich themselves.

Lets start with the Internet

The web pages you visit to find information, do your banking, find recipes, and check your email, etc are often a complicated mix of technologies and programming. The truth is the web pages you visit on a regular basis may be hiding some very nasty little surprises and so may the emails you receive. The web pages you visit are made up of computer code, which tells your browser how to display the page and what to do if you click on a certain link. There are mixed technologies at work here and effects they can have on your PC and even personal life range from benign to catastrophic. Every time you visit a web page, information about where you have come from, where you are going and even your user id’s and passwords are stored on your pc (and in some circumstances tracked by other people, shared amongst webmasters, marketeers and others).

The technologies such as Java, ActiveX, Perl, even html itself can be used by people with questionable morals to gain access to the information you hold dear. Most of these higher level scripting and application languages can be used to deploy malicious payloads and commands.

They (malicious website owners) can track your surfing habits, abuse your Internet connection by sending this data to a third party, profile your shopping preferences, hijack your browser start page or pages, alter important system files, and can do this without your knowledge or permission. The security and privacy implications of these exploits should be quite obvious and undesirable on any system or network.

Know thy enemy
Im sure you have all heard about the “dark side” of the Internet, the part that seems to spawn the virii, worms, trojan’s and all the perceptible evil on the Internet. The term hacker has been used by uninformed media hacks for years to label these people, incorrectly. Hackers are people who explore computer systems and networks to learn, not to for financial gain. They are a vanishing breed and in the past tended to instigate positive change by reporting and sharing what they found and how they did things to the respective system owners. They are being replaced by a generation of underground criminals called correctly “crackers”. These are a different species altogether.

Some crackers destroy people's files or entire hard drives; they're called vandals.
Some novice crackers don't even bother learning the technology, but simply download tools or programs to break into computer systems; they're called ‘script kiddies’.
More experienced crackers with programming skills develop programs and post them to the Web and to bulletin board systems to share them with other people on their level. And then there are individuals who have no interest in the technology, but use the computer merely as a tool to aid them in stealing money, goods, or services – we can call them criminals. This last group generally leans more towards organized crime and tends to operate accordingly.

The next group is a little more difficult to describe. ‘Spammers’, they are the people that send literally millions of junk (or unsolicited bulk) emails on a daily basis that ask us to buy a product/service or direct us to a website where potentially more vindictive activities may take place. Think of spam as the flyers in your mailbox or the people selling goods out of the back of a truck at traffic lights. Some of these promotions may be genuine, however the vast majority of them are not. The easy tell for this is the senders email address. If you are being offered Microsoft products at a vast discount to the retail pricing or the email itself does not contain a genuine reply to address or an opt out option with addressand contact details, there is a fair chance it’s not a Microsoft promotion or even the genuine product. Alternatively the makers of Viagra (Pfizer) distribute their products to be sold over the counter at pharmacists, not in conjunction with penis enlargement scams, sent from jills@qwerty.com or other such obviously non-legitimate email address.

This is a very basic round up of the Internet, now we move on to the lesser-known threats to your private information.

Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he/she is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology. Most social engineering attacks are perpetrated via telephone or more rarely, person-to-person contact with you.

Card Skimming uses a very small hand held device, similar to a mobile phone in size, to read the contents of the magnetic strip on your credit card. These readers can log hundreds of cards and are easily carried in trouser pockets. The ID thief simply swipes your card thru the skimmer to glean the information on your magnetic strip – that’s it – its over in less than 3 seconds.

A **Key-logger** is a parasitic software program designed to sit on a person’s computer clandestinely. The logger watches what you type (and where) and sends it to a location on the internet. Key loggers can assist crackers get hold of your bank accounts and other personal information. At work you are generally protected to a degree by corporate firewalls – at home you may not be. Install Antivirus and Anti-spyware software and update it weekly; install a firewall and update it regularly too.

Spyware/Malware (Malicious Software) is programming that is put in someone's computer (via visiting a website or a downloaded/emailed program) to secretly gather information about the user and relay it to advertisers or other interested parties. As such, spyware is a major cause for concern about privacy on the Internet. It can be blocked, stopped or removed with spyware removal tools, most antivirus products do not effectively handle spyware or malware.

Phishing is the act of sending e-mails to a user falsely claiming to be an established legitimate enterprise (banks, eBay, paypal, credit providers, holiday/competition draws, etc), in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, drivers licence, and bank account numbers, that the legitimate organisation already has. The Web site, however professional it may seem, is bogus and set up only to steal the user's information. Some are very professional and have fooled many IT experts. <refer to the tools section below for help on combating this type of scam>

A **Virus** is a parasitic program designed to enter a person's computer clandestinely. The virus attaches itself to files, pictures, documents, and other "attachments" such as zip files and screensavers and once on your system they are self-replicating. A virus will do everything it can to keep copying itself, and in certain circumstances will mutate just like real virii.

A **Trojan** is a malicious program that pretends to be a benign application or tool. It is designed to cause your computer to do something that is unexpected. Since it does not spread (not self-replicating) it is not really a virus, but has the same potential to do damage to your system and you. Trojans are normally like the myth, a cunning back door into your pc. They can open a communication channel with a cracker and the cracker can then use your pc against other targets, or just take all of your information (without you knowing).

A **Worm** is a parasitic program designed to replicate itself on your computer and then spread to other computers via email or a chat program. Worms were originally designed by crackers, to gain lists of legitimate email addresses for use in mass marketing (Spam).

A **Virus Hoax** is an intentionally deceptive warning circulating via email about an alleged computer virus threat. Some widely circulated email alerts, warning users of an alleged security threat from the "Budweiser Frogs Screen Saver", "Microsoft paying for email responses", "urgent Cancer donations for little boy", etc are some of the best-known examples of a *virus hoax*. The hoax achieves its goal of deception when users forward these on to their friends who may then act upon the false information contained within, or again send them on – increasing the load of mail servers around the world and simultaneously stroking the egos of their creators. Some chain letters / hoaxes have been circulation for over 10 years – which is more than can be said for most marketing campaigns.

Ok, So what do I do with all this information??

Here are some simple guides for all people to follow to help reduce the potential of you having your personal information compromised or stolen.

Protecting your PC:

You have heard this all before but as a bare minimum you need to secure your PC using both an Antivirus product and a firewall. If you are unsure as to how to configure these products refer to the (reputable) vendor that sold them to you or ask the software makers via their website or phone support. Update both your software packages regularly – at a very minimum - weekly. Your antivirus and firewall should come with an up-dater application or instructions on how to do it. Master this skill, it's the first step.

Install an anti spyware program and update it regularly. Very similar to antivirus but more specialised and equally important.

Even if you have to call a consultant in for an hour or two to help you set it all up, this price is far less than the cost of trying to recover money stolen from bank accounts and claiming insurance, or worse. Look for somebody professional who has real experience in information security and not a friends/neighbours' son who is "computer savvy". If something really happens, are you genuinely prepared to gamble your entire bank balance(s), your house, credit rating and other personal information on the neighbours' son?

You will also want to update or patch your operating system regularly. Normally for windows users it's a very simple process of checking for updates and installing them automatically. These will help reduce the likelihood of vulnerabilities being exploited by unscrupulous crackers. You may want to refer to your consultant for this as well if you are unsure how to do this.

If you are concerned about security whilst surfing the web you may want to switch browsers. 2 very good browser alternatives are Firefox and Opera. Both are far more configurable than the default windows browser and neither uses ActiveX, which is a scripting language that the owners of malicious websites use (amongst many other technologies) to gather information about you, from your pc. The level of customisation you can achieve with these alternatives far outweigh the learning curve of the new browser.

Change your passwords regularly – if you are not changing your personal passwords for your online banking and other sensitive information sources regularly – then it is only a matter of time before someone else will get in.

Passwords:
Your passwords should be secure. That means that you should use a combination of letters, numbers and special characters (the number keys with shift). I suggest you use a pass-phrase rather than a password; such as "all alone" or "a11a10n#" - which is the same with the letter L swapped for 1's and the E a shift 3, and a Zero for a "O". As long as you remember your character substitution rules – you will never forget them. Your passwords should always be 6 or more characters in length.
Never use common name, family name or a word that could be found in a dictionary, even if you are going to spell it backwards – this is one of the most common ways of breaking into accounts and its called a dictionary attack. Another common attack is called brute force and it uses an incremental approach
Never use a date of birth – they are useless against most brute force attacks as pure numbers are very easy to crack.
Even if you just put two normal words together, it increases the complexity; and adding special characters makes it even harder. I suggest on a monthly basis you should change your passwords. If you think you have come up with a good one you may want to stick with it a little longer, but never more than 3 months.

Do NOT use your User Name(s) or home/work email address(s) in any online forums or discussion groups, use a completely different ID instead and use a 'disposable' web based email address (such as Hotmail or Yahoo)

Do NOT use the same password for more than one site. This is very dangerous, if for example, you had used the same password for eBay *and* Paypal, then it would take the fraudster a few seconds to completely hijack your auctions and accounts. Same story if you use the same password for your hotmail and internet banking.

NEVER, and I do mean *never click on any link, or complete any form in any email whatsoever*! That applies whether it is genuine or not, and this is because any link can be disguised with a little knowledge of HTML code. Emails (unless encrypted) are not secure and hence should be treated as public information. Almost all companies monitor emails on their infrastructure to some extent, unless you want the boss reading your party plans…

Phishing:

Do not respond to any emails from your bank, eBay, paypal or any other institution asking for your personal information. They do not request such information via email, its called Phishing. If you have any doubts call the institution using a number from the phone book or your statements and check with them the validity of the email first.

For those concerned about Phishing you can try the Netcraft toolbar for IE (& Firefox soon). http://toolbar.netcraft.com its a free Internet Explorer toolbar, which protects users against phishing sites. Whether a Phishing site is reported via the toolbar or through some other channel; Netcraft blocks access to known sites for everyone using the Netcraft toolbar.

Refer to the tool section at the end of this article for vendor references.

Spam:

We'll see about 35 billion messages traverse the Internet daily in 2005. MX Logic a US based anti-spam vendor measured spam as accounting for 77 percent of all Internet email traffic. Do not respond to spam emails. Firstly it confirms your email address as valid and hence will put you on more lists (they share these lists of email addresses – especially the responders). Secondly, would you purchase a product or service from someone who approached you out of nowhere on the street, or knocked on your car window whilst you are stopped at traffic lights? It's ok to buy a newspaper at lights as you generally don't require any post sales support for a paper, but would you buy stocks, prescription medications, foodstuffs, wines, cameras, DVDs or software from the same guy? Most of us wouldn't – but you would be surprised by how many people actually give over their credit card details to these unknown advertisers via Spam or from pop-under advertising on web sites; only to regret that decision. If the product or service sounds very cheap, it may be because it is pirate or probably not the genuine article but 'Gray-Market' products. Gray-market products are products, either used or new, that are offered for sale by unauthorized third parties and not supported or warranted by the manufacturer/creator and generally of substandard production quality and more often than not stolen.

Protecting your Information

Whenever you divulge personal information be extra wary. If you are unsure whether the email or phone call is legitimate, ask for the persons full name then call the organisation back on a phone number from a statement or white pages to confirm.

Card Skimming When you hand over your credit/debit card in a restaurant or retail situation, how often do you ensure you can see what is happening to your card at all times? This is when skimming is most likely to occur. Police reports around the world report the most common targets for skimming is retail or restaurant customers. You are distracted by the purchasing experience and may not be taking as much notice as you think. By the time you get home, your credit card has been reproduced either in your home country or overseas and there are now 10-1000 copies of your card ready to be sold on the black market. It takes all of 3 seconds to skim and one email to shatter your life. A hint would be to go to the cashier and supervise the transaction from start to finish, if they swipe the card more than once, question the activity and ensure the cashier only swipes your card in the Eft-pos (electronic funds transfer at point of sale) device.

If someone asks you for personal information such as date of birth, drivers licence number, or address, instead of answering, ask yourself these questions first.
Why do they need that information?
What are they going to do with that information?
Is that information necessary to carry out the transaction you are involved in?
Will the person asking me, volunteer the same information to me?

If you are not comfortable providing this information, don’t – its your right not to provide it.

If you divulge personal information be as sure as you can that the recipient is who they say they are. If you are transacting online, be sure that you have spoken to your bank/credit provider about what levels of insurance you have for online transactions and understand their policies on protection of funds.

If you are purchasing from Ebay, use escrow / safeharbour if possible. Direct deposits into personal accounts are almost impossible to recover if you don’t receive your goods. Ebay is a haven for fraudsters, always check the referrals of a seller and make the effort to contact some of the previous purchasers to establish the credibility of the seller (if the purchase amount is more than you are prepared to gamble). I personally always try to communicate with sellers via email before I will bid on an item – that way I have a starting point of contact, especially if goods arrive damaged.

Social Engineering

Social engineering and other forms of interpersonal information theft are reliant on your empathy and unconformability with situations of conflict. In most cases, successful social engineers have strong people skills. They're charming, polite, and easy to like - social traits needed for establishing rapid rapport and trust. An experienced social engineer is able to gain access to virtually any targeted information by using the strategies and tactics of his/her craft.

We know that not all people are kind and honest, but too often we live as if they were. This idealistic innocence has become the fabric of the lives of most western societies and it's painful to give it up. We have built into our concept of freedom that the best places to live are those where locks and keys are the least necessary.

Most people go on the assumption that they will not be deceived by others, based upon a belief that the probability of being deceived is very low; the attacker, understanding this common belief, makes their request sound so reasonable or attractive or innocuous that it raises no suspicion, all the while exploiting the victim's trust and achieving their goals, at your expense.

The best locks in the world are useless if you open the door.

Protecting your kids

We have all seen on the media recently, stories of older men seducing younger children and adolescents into compromising situations. How does this happen?

I can speculate using some knowledge of my own from working with corporations as well as families. When children frequent ‘chat rooms’, it is very similar, in their perception to hanging out with friends. They like most of us, assume everyone in there is who they say they are. It obviously not the case, and the level of sophistication of the predators is growing every day.

There is no way to stop them except banning a child from ‘chatting’, which we know will only serve to heighten the child’s desire to chat. The one thing I have found that worked for my clients is the following.

Monitor the Internet activities of your kids. You can purchase software that will screen the websites they surf to; and you can even get commercial keystroke loggers that track the movements (site visits), userid’s and passwords of your kids. (The general reference is guardian software). Note the hours they are online and the levels of resistance when you try and drag them away at certain times. Predators generally rely on always being there for the victims when they “get online”. If you have the time, sit with your kids while they are online and simply listen and show you what they do. Another thing to check is the recent address list (the drop down bar next to where the internet address is typed. This should show you approximately, the last 20 sites that were visited manually (typed in).

Tools to help

For those concerned about Phishing you can try the Netcraft toolbar for IE & Firefox (soon). (http://toolbar.netcraft.com) is an Internet Explorer toolbar, which protects users against phishing sites. Whether a Phishing site is reported via the toolbar or through some other channel, Netcraft blocks access for everyone using the Netcraft toolbar.

Below is a list of a few of the more common packages in each category. Some do multiple tasks, including antivirus and firewall. Most of the integrated packages do not effectively remove spyware or manage the surfing habits for parental control.

Antivirus (and some firewall):

F-secure:	http://www.f-secure.com
Sophos:	http://www.sophos.com
Trend Micro:	http://www.trendmicro.com
Symantec:	http://www.symantec.com
Panda:	http://www.pandasoftware.com
McAfee:	http://www.mcafee.com
Computer Assoc:	http://www.cai.com
Central Command:	http://www.centralcommand.com

Firewall

Tiny Software:	http://www.tinysoftware.com
Zone Labs:	http://www.zonelabs.com
Black Ice:	http://www.blackice.com/

Spyware Removers:

Spyware Eliminator:	http://www.aluriasoftware.com
Spy Sweeper:	http://www.webroot.com
AntiSpy:	http://www.omniquad.com
SpySubtract:	http://www.intermute.com
SpyRemover:	http://www.itcompany.com
SpyHunter:	http://www.enigmasoftware.com
Ad-aware Pro:	http://www.lavasoft.com/

Parental Control Software

Cyber Patrol:	http://www.cyberpatrol.com
Net Nanny:	http://www.netnanny.com
CyberSitter:	http://www.cybersitter.com

I suggest a one of each approach for people who may not be the most computer savvy.

You may save a little money by purchasing an antivirus and firewall combined package, then I suggest you will also need a spyware remover.

If you have children under 15, parental control software is a “must have” if you cannot provide supervision long term. I cannot stress enough to take the time and read the literature that comes with these packages, so you can understand a little of how they work. As well as know if the kids have turned them off/disabled them to access sites that may be blocked.

Having all the right protective software installed and regularly updated is the best insurance policy to protect your privacy. Your own common sense is the best way to avoid the accident in the first place.

However, having said that, with the increasing speed at which crackers and vandals are exploiting vulnerabilities in our most common operating systems, there are no guarantees.

The Internet is an unregulated environment, and hence will always be an easy target for the unscrupulous to try and exploit the untrained, uninformed or apathetic.

The last place you'd look

Your garbage is a goldmine for those wishing to get a little dirty. Most of us are happy to throw out junk mail with our names, addresses and other personal details printed on them. I even know of a few people who throw out their bank statements unopened.

When disposing of documents and junk mail, here are a few tips:

1. Destroy the name/address section of the document
2. Destroy any personal details on the document (DOB, etc)
3. Do not throw away (in the same load of garbage) the destroyed sections of documents with the other parts.
4. Don't assume that just because you have put last weeks spaghetti leftovers on top of a document containing personal information, that a criminal wont get their hands dirty to get to your money.

When I say destroy I mean don't just rip off the top of the document – I mean destroy it and dispose of in a separate load of garbage or even a different bin altogether.

I personally take the confidential stuff and dispose of at work in the security paper recycling bins. If you don't have this facility look for an alternate disposal point.

It may sound like a lot of extra work and it may well take an extra 2-3 mins a day. However, this amount of time is nothing compared to the effort required to restore your financial records if you happen to fall victim of identity theft.

About the Author: Andrew Ockrim

Andrew worked in information technology for over 14 years for some of Australia's biggest corporations including IBM, CSC, Citibank, Catlex/Ampol, David Jones Ltd, NCR, Citibank and is currently working for the NSW Government in information security compliance.

[1] http://www.usatoday.com/money/industries/technology/2004-11-29-honeypot_x.htm