

# eSecurity – Hype or Reality?

Presented by Rebecca Matthews, Protocol 1

eSecurity is a hot topic these days both on the Internet and in the media. But what exactly is eSecurity and what does it mean to the average person?

eSecurity is the securing of information that is stored electronically – such as on computer networks. eSecurity is an important part of maintaining any computer network and is constantly monitored by corporations, government departments and banking institutions to ensure that their data is protected at all times.

eSecurity can also refer to security measures taken while using electronic media such as email and the Internet.

While large organisation employee teams of IT security specialists to ensure they are protected from malicious harm and security threats, this is not a feasible option to most people – nor is it really all that necessary.

What kinds of threats are there? It's easy to get confused with all the hype around the latest virus attack or email hoax. Today, with the assistance of Federal government funding, local community group SeniorNet, in conjunction with the Australian Seniors Computer Clubs Association, is hosting this free seminar to help you, fellow seniors, in understanding what eSecurity means and how you can have a more positive computer experience.

## **Spyware, Viruses and Email Hoaxes – the Big Bad Wolf Knocking on Your Door!**

In the past 10 years, Australia has seen a huge growth in the number of computers now found in the average home. In Nov 2000, 2.7 million homes had access to the Internet. In comparison, at the end of December 2007, 6.14 million households had some form of Internet connection and 5.21million had broadband or similar access. This increase in the use of the Internet at home has in turn created an increase in the types and amount of eSecurity threats that await the unsuspecting person.

So lets have a look at what threats there are and what you can do to protect yourself from them.

- Viruses
- Adware & Spyware
- Email Hoaxes

## **What is the difference between viruses, adware and spyware?**

A virus is a piece of malicious software code written to cause some kind of damage to a computer system or network or even the Internet itself. Viruses spread, similar to their biological namesake, from one computer to another and can spread havoc wherever they go. They are most commonly spread by sharing files with others or through email attachments where they can be set up to send themselves to all the addresses in your email address book.

Adware is usually downloaded and installed along with some other program without your knowledge and unlike a virus doesn't spread by itself. Very often you click "OK" without reading the terms and conditions and by doing so you agree to have the files installed. An example is you see a "free" program on offer that you think might be useful and download it without thinking. Even some bogus anti-Spyware programs install adware and the website earns money from the ads that are clicked on.

The catch is that the extra files introduced are used to determine things like your surfing habits and the data

is used to serve up popup ads or redirect your browser to a page other than the one you wanted. Adware is not a security problem it is more an annoyance especially when you have ten different programs trying show ads. The amount of computer resources it uses up slows your system to a crawl.

Spyware is more malicious is designed to steal something from you – usually information! It can be downloaded by visiting the wrong types of websites or along with other files the same way as adware. Spyware can often be hard to remove as it can continually recreate itself and hide somewhere on your hard drive. Some of the programs can be used to install key loggers which can send back information about passwords and bank details etc

Programs such as Trojans can be used to allow access to hackers at a later date. From the story of the Trojan horse where the Greeks hid inside the wooden horse left as a peace offering and were wheeled in to the fort by the Trojans themselves. Then at night the Greeks crept out of the horse and opened the gates and let the enemy in. Trojans and adware unlike viruses don't spread themselves.

### **Email hoaxes**

If you receive an e-mail offer that sounds too good to be true, it probably is. Urban legends and hoaxes have been around for centuries, but their popularity is on the rise because the Internet makes it easy to spread fraud e-mails.

Many e-mail hoaxes will trick you into forwarding messages about fake viruses or other fabricated stories. These e-mails waste time, clog inboxes, and might cause embarrassment when they're proven untrue. But there are other, more insidious types of fraud that might end up costing you a lot of money.

Ever wondered if anyone makes the money promised in those work-at-home advertisements? Or if each forwarded e-mail will really mean a donation of 10 cents from Microsoft to an orphan's organ-transplant operation? The answer is no. These stories are urban legends, e-mail hoaxes and scams. They are but a few of what we like to call financial fiction.

One of the more common email scams is one that offers you a “work from home” offer – where you can earn \$1000/week for just a couple of hours of work on your home computer. Believe me, if you could make that much money on your home computer, I'd be at home right now doing just that!

You should immediately run from anyone who promises lots of money for little work that requires no experience. While there are companies that allow their employees to work from home, they require job skills and interviews, just like regular jobs. Work-at-home scams will ask you to purchase supplies and equipment from them to perform the "job." That's how they make their money. You will lose -- not make -- money.

Another real threat is the emails that supposedly come from your bank – you have probably received at least one. It looks legitimate, after all the email address says [customercare@westpac.com.au](mailto:customercare@westpac.com.au) and all they are asking if for you to confirm your account details by clicking on a link and entering your account information. You click on the link and are taken to what looks like the bank's website. So you merrily enter information – you may login to Internet Banking, or complete an online form with name, account number, PIN number perhaps.

This is one of the biggest security threats you will face when using the Internet. Because if you believe this email, and follow its instructions, you have not helped your bank with keeping your account details up to date. What you have done is help fraudster gain access to your banking details and quicker than you can say “Holy Cow Batman”, your life savings are transferred out of your account and into theirs.

I cannot stress this enough – your bank will NEVER email you asking for details or to update your details. Standard practice if there is a concern about your details is to send a letter asking you to go to your local branch and update your details with one of their friendly staff IN PERSON. If you are unsure about any email you receive from your bank, just go and ask at your local branch.

**Here are seven more telltale signs of a scam:**

1. You don't know the person who has sent you the message.
2. You are promised untold sums of money for little or no effort on your part.
3. You are asked to provide money up front for questionable activities, a processing fee, or to pay the cost of expediting the process.
4. You are asked to provide your bank account number or other personal financial information, even if the sender offers to deposit money into it.
5. The request contains a sense of urgency.
6. The sender repeatedly requests confidentiality.
7. The sender offers to send you photocopies of government certificates, banking information, or other "evidence" that their activity is legitimate (these are fake).

And finally we get to spam. Spam isn't a threat as such – more of an annoyance really. Spam is unsolicited emails that get sent to your email account – the electronic version of junk mail really. And like most junk mail you get in your letterbox at home, the content in most spam emails is junk – selling anything from a lifetime supply of Viagra to pirated copies of the latest software. Despite Australia's tough privacy laws, which do cover unsolicited emails being sent from Australian companies, everyone with an email account will encounter spam. This is because 99% of spam is generated overseas. Some spam can be dangerous in that there will be a link for you to click to go and view more details about the unbelievable products on offer – and instead you open yourself to having adware or Spyware installed on your computer instead. So just like email hoaxes – if it's too good to be true, it probably is! Delete the email!

And while we are on the topic of spam – another form is the chain mail types. Remember when you were a kid and you'd get a chain letter to copy out and send to 10 friends and you'd get a lifetime of good luck, but if you didn't you were destined to marry an ogre or a wife or husband? Well today, it's quite common to get chain letters as emails – urging you to forward them on to as many people as you know. Please don't! All it does it clog up everyone's mailbox – and let's be honest, how many of you really read those types of emails? Same for the emails that give warnings of the "latest virus threat" or stories of how someone went to the movies and woke up in a hotel bathroom missing a kidney. These are just urban legends and they urge you to pass them on in an attempt to create even more spam. So by sending them on to your friends and family, you are being a spammer as well!

So is it all doom and gloom? Is it best not to use the Internet at all? After all I have just told you, I wouldn't be surprised if you thought that!

But the Internet is a great source of entertainment and information (some of it even factual!) and many of the associated technologies are a low cost way to keep in touch with friends and family around the world. In order to have a safe and trouble free experience there are a few things you can do to implement your own e-Security.

In this article I will outline some techniques that you can do to make your Internet experience enjoyable and safe.

## Anti-virus Software

A good anti-virus software is key to protecting your computer from malicious viruses. There are many products available on the market, some with additional features that may also assist with Spyware and hacking. I won't get into the pros and cons of which brand is better but I will give you a checklist of what to consider when purchasing anti-virus software:

- **How much memory does it require to run?** Any more than 64Mb and you may find your computer becomes slower to operate, especially older systems.
- **How often does it receive updates?** A good anti-virus software will get updates at least once a day to ensure it provides the best protection.
- **How much is it to renew the subscription each year?** When you purchase anti-virus software, you are also purchasing a subscription to the daily updates. Generally this is one year – after that, you need to renew for another year to keep receiving those updates. Failing to renew and receive those updates will make the software useless.

## Adware & Spyware

There is software on the market that may assist with preventing Spyware or adware being installed. Because of the large amount of Spyware and adware that is created and released each day, it is difficult for any software to prevent all possible infections. Personally, I don't use commercial anti-Spyware software – instead I practice safe Internet usage measures.

99% of Spyware and adware infections occur by accident – generally when you visit a questionable website. By 'questionable' I don't mean of the adult nature (although they too can contain Spyware), but sites that provide "free" software. My Nanna used to always say "Nothing in life is free" and on the Internet, that is almost always the case.

So I don't download free or trial software unless it is a reputable company – such as Microsoft, Adobe and the like.

One of the more popular free downloads that contains Spyware is one that gives you smiley icons and images to include in your emails. Sure it makes your emails nice and pretty, but it also secretly installs Spyware that tracks where you go on the Internet and also can record and pass on your passwords etc.

One final thing I do is every couple of months, I run a free program called SpyBot Search & Destroy – while this is a free program, it is by a reputable company that provides the software to help remove Spyware from your computer. It can't remove the really bad Spyware (you'd need a good IT tech for that!) but it can remove the more common ones. Even an IT professional such as myself can still get caught out, so applying these few measures helps me stay Spyware free.

That said, I also make sure my kids don't use my work computer – kids, particularly teenagers, are the biggest culprits when it comes to having Spyware on a computer. They cannot resist downloading free and cute software and so open your computer to infection.

## Email Hoaxes

I can only say one thing about dodgy emails – if you don't know the sender DON'T OPEN IT. Certainly don't open any attachments (or run the risk of viruses and/or Spyware) and please don't forward it on to friends and family!

## Spam

The bane of all email users, there isn't much you can do to prevent all spam, but there are some things you can do to reduce it.

1. Check with your ISP – many ISPs, such as BigPond offer a spam filter for just a couple of dollars a month.
2. Don't give out your email address to all and sundry. Many times you have to fill out online forms on the Internet – if you do, try using a secondary email account, such as a Hotmail account. You can easily check these email accounts and they often have their own in-built spam filters that reduce the amount of spam anyway.
3. Don't spread it yourself! Please think twice before forwarding on funny emails, or possible email hoaxes

## Firewalls

Before I move on to the topic of securing your home wireless network, there is one other type of e-security that is commonly used and mis-understood. And that is having a firewall.

A firewall is a barrier to keep destructive forces away from your property. In fact, that's why its called a firewall. Its job is similar to a physical firewall that keeps a fire from spreading from one area to the next. In computing terms, a firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system.

A lot of people will tell you that at home you need to have special software to protect your computer from unwanted hacking – popular forms are marketed as “Internet Security Suites”.

There are two forms of hacking – people trying to get in via the Internet and information being sent from your computer without your knowledge – in other words Spyware. So provided you keep your computer free of Spyware, all you need to do is stop unwanted inbound traffic from coming into your computer. And for most people in this room, you will already have a firewall and probably are not aware of it.

How many people here have ADSL or cable internet? Ok, you will have received from your ISP or friendly IT person a router as part of that connection setup. As well as providing you access to the Internet it already has built-in a NAT firewall. So you are protected already! Congratulations!

For those people on dial-up, you will have a modem, but you can still protect yourself without having to purchase special software. If you have Microsoft Windows XP or the new Vista operating systems, it has it's own built-in firewall. Many “IT experts” will scoff at this firewall, but it must be noted that the Windows firewall has NEVER been broken. EVER. Sounds pretty secure to me!

The one thing these devices – the router and the Windows firewall will not protect you from is outbound traffic – or confidential information being sent from your computer. In other words Spyware – and we all know now how to prevent Spyware.

So remember, keep your computer free from Spyware and enjoy the protection of your built-in firewalls!

## Wireless networks – securing them from the teenager next door!

With the increase in broadband Internet connections in Australian households, comes also the increase in the number of computers in each home, as well as the increase in laptop ownership. Once you get that extra computer, you want to share that Internet connection between both computers. And you have paid that little extra for a laptop, you may want to enjoy the freedom of checking your emails from your back patio. So this

is when you purchase a wireless router – this allows you to share your Internet connection between multiple computers. It should be noted, that each computer also needs a wireless card that allows each computer to “talk” with the wireless router. If your computer doesn’t have one, you can purchase one. Most laptops purchased these days have a wireless card built-in by default.

If you purchase a wireless router “off the shelf” from any IT retailer, the router is often a “plug & play” – that is you plug it into your existing ADSL router and hey presto! Your wireless network is up and running and your computer and laptops can automatically connect to the Internet! “Fantastic!” you say to yourself!

And so does the teenager next door. This is because if you were able to connect to your wireless router without having to enter any passwords or forms of security and your wireless network is not secure. Sure your firewall may protect you from people access your information, but this will be the least of your problems.

If anyone else can connect to your wireless network, they can access the Internet via your broadband account. Which means when they download anything, it comes from your download limit given by your ISP. And because it is free, you can assured that your unwelcome “visitor” will not restrict themselves to checking their email – they will take advantage and download movies, music, games and if they are teenage boys, probably some pictures of naked ladies.

All of this extra downloading will mean either 2 things – depending on your ISP plan, you will have your connection slowed down when you reach your monthly limit or worse, if you have to pay for extra megabytes (Mbs) downloaded, you could get a very large bill at the end of the month.

So how do you secure your wireless network? Find a good reputable IT company and have one of their experienced techs to secure it for you. Takes no more than an hour and is well worth the investment.

***Rebecca is co-owner and Business Solutions Manager of Protocol 1, an Ipswich based IT company that provides IT business solutions. She has worked in the IT industry for over 14 years, developing user documentation and managing helpdesks for both government and private corporations.***