

# VicGUM<sup>®</sup> INTERNET SECURITY PRESENTATION

## February 2008 Meeting

The trend in 2008 would be expected to continue 2007's trend of "rapidly mutating virus and spam campaigns" with smaller targeted attacks, not like the large scale attacks of past years which made it into the daily media. The Web is the main source of ever increasing threats continuing to target businesses using websites to spread infections as opposed to simply using email messages. Also, a "raft of new scams have continued to place a heavy burden on businesses". Use of JPGs, GIFs and PDFs are emerging as a new type of spam vehicle with embedded malware code or malicious links. See <http://www.sophos.com/security/topic/malware.html> for more information on malware statistics and future trends. You are more likely to receive an email enticing you to go to a particular website which has malware on it rather than receiving an email with the malware attached or embedded – they know your computer is likely to have antivirus etc. protection on your incoming emails these days. However, it really doesn't matter what name is used or how you get attacked the objectives are always the same to cause you angst and more likely for their financial gain.

One of the main aims is to get your personal information so it can be re-sold, to the highest bidder and to get code onto your computer so it can be used to infect other computers connected to the Internet and so on.

Basically, the term malware is short for malicious software and it is used to describe the family of software nasties used by computer attackers, which include grayware, adware, spyware, viruses, trojans worms etc. It is suggested you see <http://en.wikipedia.org/wiki/Malware> for definitions, which is the safe website Wikipedia Free Encyclopaedia. A safe website is one that gives you information and nothing else. A lot of websites are set up to distribute viruses and malware to your computer while purporting to be assisting you to remove a possible threat. Be very careful and use common sense.

Ransomware is one of the newer threats. This can be where an email attachment you open encrypts your files including documents, photos and spreadsheets. You then receive a ransom request to pay money to stop your files from being deleted from your hard drive or to obtain the decryption key so you can use them again. These trojans are able to spread because users click on links they receive in spam emails or by surfing on infected or bogus websites.

According to Instructor Jon Schweitzer "You are at WAR with many enemies when you enter the Internet. You must have many good soldiers guarding your computer door. The items below are only the minimum required for your computer to remain alive."

This Statement is from the Computer Internet Security Website and Class for personal computers at home, which is given at the Los Angeles Regional Family History Centre and elsewhere. The Website was last updated on the 19<sup>th</sup> of April 2007 and can be found at <http://members2.1stnetusa.com/~a/comintsec/>

Your aim is to become an informed Internet surfer; knowledge is your best weapon.

One of the best ways to keep your data safe is to regularly back up all of your family history data, photos, *Word* documents etc. on to a CD or DVD or an external hard drive. Make sure you know how to restore the files before you have a problem (backing up is also a good insurance policy against malware, unrelated computer crashes, fire and theft!!). Always run your updated virus-checking program, *Spybot Search & Destroy* and *Ad-Aware 2007* before you back up your data or use your credit or debit card or your bank account information online.

*Ad-Aware 2007* from LAVASOFT is free for home (non-commercial) use and can be downloaded from <http://www.lavasoft.com> (click on the "Ad-Aware" tab at the top then select "Ad-Aware 2007 Free" then click the "Download" buttons on the pages which follow and you will get to the actual download site!). Earlier versions of *Ad-Aware* will be removed during installation of *Ad-Aware 2007*.

*Spybot Search & Destroy* is available from <http://www.safer-networking.org/en/index.html> *Spybot Search & Destroy* is also free for the home user but you are encouraged to make a donation to support further development. Note that *Ad-Aware 2007* is only for *Windows 2000, XP and Vista*, *Spybot Search & Destroy* is for *Windows 95* onwards but requires administrator rights for some/all functions in *Windows NT* onwards including *XP* and *Vista*.

When using *Ad-Aware 2007* it is suggested that you turn off the “Scan for MRUs (Most Recently Used files) by un-checking “Scan for MRUs” in the “Settings” screen’s “Scanning” tab.

Mary Landesman’s guides, see <http://antivirus.about.com/od/securitytips/a/removespyware.htm>, are very helpful especially the one about removing stubborn adware and spyware from your computer. Also, for further information on how to use the advanced options in *Spybot Search & Destroy* see <http://antivirus.about.com/od/securitytips/ss/hosts.htm>

Microsoft has its own *Windows Defender* which “... is a free program that helps you stay productive by protecting your computer against pop-ups, slow performance and security threats caused by spyware and other potentially unwanted software.” It detects and removes threats by spyware and other nasty or potentially unwanted software and has real time protection capabilities. This can be downloaded from <http://www.microsoft.com/downloads/> more than likely listed under the “Popular Downloads” at the top or the “Recommended Downloads” below this. *Window Defender* is for *Windows XP Service Pack 2 (SP2)* or later. (*Windows* validation is also required to prove you are running a genuine copy.)

It is recommend that you use *Firefox* and not *Internet Explorer (IE)* as your preferred browser because it contains much better security features than *IE*. You can download it from <http://www.mozilla.com/firefox/> If you have been using *Internet Explorer* once you have installed *Firefox* click on the “Help” (last item on the top menu) and choose the second item “For Internet Explorer Users”. Here you have all the help you will need to easily convert to *Firefox*.

You can import your Favourites, cookies and stored-passwords so you can start using *Firefox* almost immediately. Updates to *Firefox* also update its security features so they are best download automatically. To do this click on “Tools” (top menu) choose “Options” then click on the “Advanced” button (last item on the top menu). Click on the “Update” tab and check the “Automatically download and install the update” option then click on the “OK” button at the bottom of the box. One really nice thing you will notice with *Firefox* is you won’t have all those pop-up ads clogging up your screen real estate. *Firefox* is also available for Linux and Mac.

## Free anti-virus software

GRISOFT <http://free.grisoft.com/doc/1> provides a free version of *AVG Anti-Virus*. The current version is 7.5 which will work on the *Microsoft Vista* operating system and Linux. Support for *Windows 98/ME/NT* will continue to August 2008 as a minimum. (The free Anti-Spyware set up contains the free as well as the paid version of *AVG Anti-Spyware*. After the installation, a free 30-day trial version containing all the extensions of the full version will be activated. At the end of the trial, these extensions will be deactivated and the program will turn into a feature-limited freeware version. The purchased license code can be entered at any time.)

ALWIL the producer of *Avast* anti-virus software has a free version for the home user which can be downloaded from [http://www.avast.com/eng/free\\_virus\\_protectio.html](http://www.avast.com/eng/free_virus_protectio.html) At the time of creating this presentation the latest version was 4.7. This anti-virus software can be used on *Windows 95* to *Vista* operating systems although some features require *Windows NT* or later.

The reason for the free versions is that the major problem is not that anti-virus programs do not detect viruses but, the fact that most users do not use any anti-virus software at all or, perhaps worse, the anti-virus software and/or virus definitions database is out-of-date.

Whatever anti-virus software you use make sure it is set to automatically download updates!

## **Virus Hoaxes**

BEFORE you send an email message to all your friends advising them about the new virus threat, and contribute to slowing down the Internet, check to make sure it is not a hoax. Hoaxes are usually spread via email. A virus hoax is a false warning of a non-existent computer virus. As such, they cause no harm to computer systems other than slowing down mail servers if spread in large numbers. However, some hoaxes go further, with a message giving directions to remove specific files from your system to get rid of the virus. This form is no longer a hoax but is, in itself, a virus because it tells you to remove some vital file that could cause your computer to malfunction or not work at all.

Before reacting to any virus warning even ones that appear genuine, check with *Sophos* <http://www.sophos.com.au/security/hoaxes/> or your anti-virus software supplier's website.

## **Phishing, Spear Phishing and Vishing**

Phishing usually targets the financial services. Examples are an email purporting to be from say the *Westpac* Bank asking you to contact them urgently and directing you to a link or purporting to be from *PayPal* saying something like “unusual activity has been noticed on your account”. The link in the email directs you to a website that looks like the real website but actually isn't. The aim is for you to enter your account details and password so they can be stolen. The Anti-Phishing Working Group (APWG) at <http://www.antiphishing.org/> is a good place to start learning about Phishing and how to avoid it.

Spear Phishing targets groups of people for example a group using a family Blog where the users post personal information that could be used in identity theft. The person who set up the Blog probably knew nothing about security and left it “open” to computer attackers.

Vishing pertains to VoIP (Voice over Internet Protocol); see <http://en.wikipedia.org/wiki/Vishing> for an explanation.

*Skype* is a peer-to-peer (P2P) VoIP application (peer-to-peer file sharing programs are applications that allow users to download and share electronic files). These applications are often associated with security risks such as the spread of viruses and worms and spyware. To reduce the risk only launch *Skype* when you need to use it, for example, when you are expecting an incoming call or making an outgoing call. Keep your calls to a reasonable length and when the call is finished, turn the application OFF. (Closing the *Skype* application window is not enough to turn it off.)

## **Combining Vishing and Spear Phishing**

Internet users are finally getting wise to clicking on links in emails so a combination system is now being used. It is possible to obtain VoIP telephone numbers that are similar to telephone numbers in a particular area. Emails are then sent, using infected home computers, purporting to be from a certain bank or *PayPal* etc. containing the telephone number and asking the customer to call urgently. When the number is called a recorded message advises customers that there is a delay but to leave their name and account details and a contact telephone number and that they will be called back as soon as possible.

## **Spam Filtering**

One way to reduce or even eliminate the threats of malware arriving via your email is to use some form of spam filtering. Your ISP may have this available as a free or low charge option on your email account. However, some people prefer to manage their incoming mail themselves and determine which ones they want to receive. Software packages such as *Mailwasher* is one program used by some VicGUM<sup>®</sup> members. *Mailwasher Free* is a free version and is available from <http://www.mailwasher.net/>

*Mailwasher Pro* has more features and it is available from <http://firetrust.com/> It downloads only parts of your email and decides if it is “friendly” or “hostile” learning as it goes along with your input. Any junk or nasty emails are deleted on your ISPs server before *Mailwasher* opens your email program and you download only the friendly email remaining. See the August 2002 VicGUM® Newsletter for an article by John Donaldson on *Mailwasher*.

Another free spam filter is *SpamPal* <http://www.spampal.org/> which works in a similar way to *Mailwasher*.

Comparisons on the various spam fighting software available can be found at SpamCop <http://www.spamcop.com/>

So you never download to your computer all those emails saying you have “won the international lottery worth millions of dollars/pounds” or offering you “millions of dollars left in an account by some deceased person that needs to go overseas” or asking you to validate your bank etc. account (financial institutions NEVER email you asking for login information!!).

## Firewalls

Firewalls sit between data coming to and from the unsafe Internet and your safe PC or home network to keep you protected. They can be software based like the inbuilt *Windows XP* and *Vista* firewalls, *Zone Alarm* etc or hardware such as broadband Modem/Routers or Routers.

ZoneLabs has a free basic software firewall available for the home user called *ZoneAlarm*® <http://www.zonelabs.com/store/content/company/products/zna/m/freeDownload.jsp> (click the button under “Basic Firewall Only”). If you want more information they also have an informative page about firewalls <http://www.zonelabs.com/store/content/support/zasc/whyFirewall.jsp?dc=12bms&ctry=GB&lang=en#1> which has some good information about why you should run a firewall program and is well worth reading.

*Comodo*™ *Firewall Pro* Version 3 is another free firewall and it is available from <http://www.personalfirewall.comodo.com/>

If you are running an older operating system old versions of a number of security tools including *Sygate Personal Firewall*, are available for download from Old Version Security Tools [http://www.oldapps.com/old\\_version\\_security\\_tools.php](http://www.oldapps.com/old_version_security_tools.php) **However, remember these are not being kept up-to-date and will not protect you from newer threats.**

Software firewalls provide both incoming and outgoing Internet access protection. They detect and stop incoming attacks on special ports that are trying to get malicious access to your computer. They also provide application protection and let you know when programs try to access the Internet from your computer. You agree to the normal programs like your web browser or genealogy program (e.g. when checking for updates) to have access, but if it happens to be a malicious program or one you are not sure of you can deny access then do further checks to see if it is legitimate or not.

If you are using broadband (Cable or ADSL) it is very important to use a firewall as your computer is always connected to the Internet, not just for a period of time when you used dial up access. Your modem will most likely have a built in hardware firewall, or if you use a router to share your Internet access it will have one. This is very good at protecting you from attacks from the Internet, but does not offer any application protection. It uses Network Address Translation (NAT) to translate your public IP address (the one your ISP assigns to you) to a local private one the modem or router assigns to your computer or each computer if you have a network. So you can initiate Internet access and the modem/router will handle it for you, but if data comes in that was not initiated by your computer it drops/ignores it.

Gibson Research Corporation's site <https://www.grc.com/> has *ShieldsUp* to check your visibility on the Internet. This site will scan your PC and let you know which ports are open (very dangerous) or visible (potentially dangerous) or stealth (totally hidden – very good) on the Internet. A hardware NAT firewall results in a total stealth report, that is **all** ports are totally invisible to the Internet so anyone trolling the Internet for open ports will not see you.

## Google Pack

*Google Pack* <http://pack.google.com/> is a suite of free programs from *Google* which includes *Spyware Doctor Starter Edition* which will also protect your computer from attack. However, it is only available for *Windows 2000/XP/Vista*.

## Macintosh Operating system

If you are using a Mac <http://www.firewallguide.com/macintosh.htm> has many links relating to Mac security issues and Articles and Information to Help You Secure your Apple Macintosh Computer [http://netsecurity.about.com/od/secureyourmaccomputer/Articles\\_and\\_Information\\_to\\_Help\\_You\\_Secure\\_Your\\_Macintosh\\_Computer.htm](http://netsecurity.about.com/od/secureyourmaccomputer/Articles_and_Information_to_Help_You_Secure_Your_Macintosh_Computer.htm) contains links to a number of articles which currently includes “Mac OS X Maximum Security” and “Mac OS 101: Security Resources”.

## Wireless Networks

Laptops and PDAs sold in recent years have wireless network capability built in, and many people set up a wireless network at home to share their Internet connection and sometimes printers between their various devices. Also *Windows XP* and *Vista* has made it much easier to set up home networks including wireless ones.

If you set up a wireless network you need to set up some basic security options in your router otherwise anyone within reach of your wireless signal can use your Internet connection – at the very least they can use up your download allowance, at worst they can use your connection for malicious purposes.

Change Admin Name and Password - The first thing to do is change the router login name and password. The factory default for manufactures and their equipment models is public knowledge e.g. login name is “admin” password is “password”!! If you don't change these then any of the following security measures can be defeated because someone can log into your modem/router and remove/change them. Note do not use your ISP login name or password.

Use MAC address filtering – every network device in the world is assigned a unique Machine Address Code (MAC) address which can be used to filter access to a wireless network. You find the MAC address of each device (PC, PDA etc.) and enter it into the router, then turn on MAC Address Filtering – this will only allow devices with the registered MAC address to access your network. This not only applies to wireless connections but any PC or other device connected by a cable otherwise they wont get access either.

To find the MAC address under *Windows XP/Vista* select Start then Run and type in “cmd” in the text box and run it to open a command window. At the prompt type “ipconfig/all” and look for the Ethernet Adapter, the Physical Address is the MAC address, six pairs of hexadecimal numbers e.g. 20-3F-89-CE-66-E4. Type “exit” to close the window.

To find the MAC address of a HP PDA select Start, then Settings, then the System Tab, then Asset Viewer, then expand the Wireless LAN item and the MAC Address is shown. Other brands of PDAs will have a similar process, consult your user manual if necessary.

Hide SSID – a Service Set Identifier (SSID) or network name is assigned to a wireless network. It should be something unique and nondescript and can be up to 32 characters long (don't use VicGUM or VictorianGUM etc.). Don't leave the default SSID e.g. NB5580 for a NetComm NB5580 router as this would indicate that you may not set up security at all and invite attempts to connect. The router broadcasts the SSID so that devices can find and connect to the network. However, this also lets everyone in range know there is a wireless network about and is a potential target for malicious attack. So once you have set up all your wireless devices then they will have the network name details stored so you can turn broadcasting of your SSID off. If you need to add a new device or reset an existing device you can manually input the SSID or turn broadcasting on again temporarily.

WEP or WPA Encryption – the most important security option to set up is Wired Equivalent Privacy protocol (WEP) or the later and better Wi-Fi Protected Access protocol (WPA). To run WPA you need *Windows XP Service Pack 2* or later and *Windows Mobile 2003 SE* for later for PDAs. If your PDA is running *Windows Mobile 2003* you may be able to update the system – often requires reloading all your operating system and other software again, not a trivial task.

You need to follow the method for your router, but generally you enter a Passphrase that generates four 64 bit 10 digit keys or 128 bit 26 digit keys which you then load into the other devices or allow the system to automatically send the key. Use the 128 bit encryption if all of your wireless devices will accept them as the longer the key the better the security.

Following these relatively simple to implement options above will make your wireless network secure from the local neighbourhood geeks.

## Finally

If you notice something unusual on your computer like information coming from a URL other than you expect to see, put the details into *Google*. Chances are someone else has had the problem and has already found the solution. If not, run updated versions of your virus-checking software, *Spybot Search & Destroy* and *Ad-Aware 2007*.

Summarising:

- Use a Hardware firewall if possible
- Use a Software firewall especially if not using a Hardware firewall
- Run *Spybot Search & Destroy*, *Ad-Aware 2007* and probably *Microsoft Defender* regularly
- Use an **automatically up-dating** virus checker
- Consider using a spam filter on your email
- Keep your computers software updated with security patches etc.
- Use encryption (WEP/WPA) as a minimum on any wireless network you set up (don't forget to change the login names and password too!!)
- Use common sense when visiting websites and clicking on links you are not sure of
- Do not respond to any spam you get – it tells the spammer they have a “live” IP address
- Remember the old adage if you receive “an offer that seems too good to be true, well ... !!” ☺