

# Protecting Your Computer from Viruses, Spyware and other Nasties

Irene Fullarton  
Graeme Simpson  
John Donaldson

# Protecting Your Computer from Viruses, Spyware and other Nasties

**Covering the following topics**

- **What is Malware?**
- **Virus/Spyware Protection/Removal**
- **Virus Hoaxes**
- **Phishing and Vishing**
- **Spam**
- **Firewalls**
- **Wireless Network Security**
- **Summary of recommendations**
- **Questions**

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Viruses, Worms
  - Infects your computer
- Trojans, Rootkits, Backdoors
  - Conceals themselves on your computer
- Spyware, Botnets, Loggers, Dialers
  - Designed to make a profit for the perpetrator
- Collectively know as “Malware”  
(Malicious Software)

# Protecting Your Computer from Viruses, Spyware and other Nasties

- A “safe” website for more information on the definition of various Malware is:

<http://en.wikipedia.org/wiki/Malware>

- A “safe” website is one that only gives you information and nothing else
- For trends in Malware threats see:

<http://www.sophos.com/security/topic/malware.html>

# Protecting Your Computer from Viruses, Spyware and other Nasties

- One of the best weapons against malware is knowledge, if you are an informed Internet surfer you will be a safer one
- Using common sense also helps
  - If something sounds too good to be true ...
- An good way of protecting your data is to back it up **regularly** (also good for protecting against computer crashes or theft and fire etc.

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Spyware Removal and/or Protection
  - *Ad-aware 2007*  
<http://www.lavasoft.com>
  - *Spybot Search and Destroy*  
<http://www.safer-networking.org/en/index.html>
  - *Google Pack*  
<http://pack.google.com/>
  - *Microsoft Windows Defender*  
<http://www.microsoft.com/downloads/>

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Mary Landesman's guides have useful information on spyware and adware removal

<http://antivirus.about.com/od/securitytips/a/removespyware.htm>

- Mary also has a guide in using *Spybot Search and Destroy's* advanced options to help protect your computer

<http://antivirus.about.com/od/securitytips/ss/hosts.htm>

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Antivirus Protection
  - Is a **MUST** have item in your armory in the fight against malware
  - **MUST** keep it updated
    - set it up to **AUTOMATICALLY** update itself
  - Commercial and free versions available
    - Updates for commercial ones e.g. CA (Vet), Norton, McAfee etc. requires an annual subscription

# Protecting Your Computer from Viruses, Spyware and other Nasties

– Free versions encourage Internet users to have virus protection – no excuses ☺

- *AVG* free anti-virus software from Grisoft

<http://free.grisoft.com/doc/1>

- *Avast!* free anti-virus software and virus-cleaning tool from Alwil Software

[http://www.avast.com/eng/free\\_virus\\_protectio.html](http://www.avast.com/eng/free_virus_protectio.html)

- The paid versions of these programs offer more features and potentially better protection

# Protecting Your Computer from Viruses, Spyware and other Nasties

- A useful source of information on how to remove viruses is your anti-virus software vendor e.g.
    - Computer Associates (Vet)  
<http://www.ca.com/au/securityadvisor/>
    - McAfee threat centre  
[http://www.mcafee.com/us/threat\\_center/default.asp](http://www.mcafee.com/us/threat_center/default.asp)
    - Norton removal tools  
[http://www.symantec.com/norton/security\\_response/removaltools.jsp](http://www.symantec.com/norton/security_response/removaltools.jsp)
-

# Protecting Your Computer from Viruses, Spyware and other Nasties

- There are some programs that protect your computer from spyware
  - Might be worth considering if you have problems
    - *SpywareGuard*  
<http://www.javacoolsoftware.com/sgdownload.html>
    - *SpywareBlaster*  
<http://www.javacoolsoftware.com/spywareblaster.html>
    - *Spyware Doctor*  
<http://www.pctools.com>
  - Be careful though, some protection programs actually install their own “spyware”!! So check this site for information on which programs to avoid  
[http://www.spywarewarrior.com/rogue\\_anti-spyware.htm](http://www.spywarewarrior.com/rogue_anti-spyware.htm)

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Virus Hoaxes
  - Not all viruses are real
    - “Teddy bear” asks you to remove a valid system file
  - May not be computer malicious per se
    - “Plastics cancer link” email
  - Real issue is the amount of Internet traffic generated by all the emails you send warning others of a threat that doesn’t exist

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Many businesses have policies that preclude staff from sending virus warnings around
- They're not welcome on other community websites e.g. Roots Web Mail Lists either!!
- If you get a virus warning from someone then check it out on one of the following sites to see if it really is a problem or not

<http://www.sophos.com.au/security/hoaxes/>

<http://www.foax-slayer.com/plastic-cancer-link-foax.html>

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Phishing, Spear Phishing and Vishing
  - Phishing (no not that leisure pastime!!) usually targets financial institutions
    - Looks like it comes from your bank etc
    - Ask you to verify your account by clicking on a link to log into your account
    - You often don't even have an account with them or use their Internet banking
    - For more information on this see



<http://www.antiphishing.org/>

## – A Phishing Example

X-Original-To: gsimpson@mx4.netspace.net.au

Delivered-To: gsimpson@mx4.netspace.net.au

X-Greylist: from auto-whitelisted by SQLgrey-1.6.7

To: gsimpson@netspace.net.au

Subject: Important Notification: St.GeorgeOnline Verification Needed.

From: St.George Internet Banking <customer.services@stgeorge.com.au>

Reply-To:

Date: Wed, 30 Jan 2008 11:39:35 -0800

X-AntiAbuse: This header was added to track abuse, please include it with any abuse report

X-AntiAbuse: Primary Hostname - lisa.lts-marketing.com

X-AntiAbuse: Original Domain - netspace.net.au

X-AntiAbuse: Originator/Caller UID/GID - [99 503] / [47 12]

X-AntiAbuse: Sender Address Domain - lisa.lts-marketing.com

X-Source:

X-Source-Args: /usr/local/apache/bin/httpd -DSSL

X-Source-Dir: maxaffiliate.com:/public\_html/am/plugins/payment/secpay



**Dear Customer,**

St.George is proud to deliver a higher level of security for our online St.George clients through St.George Secure Access. As part of our ongoing effort to improve online security, there might be some security problem on your account. So we have decided to put an extra verification process to ensure your identity and your account security. Please click the weblink below

<http://www.stgeorge.com.au/> (<http://tom.swinnen.net/www/templates/madeyourweb/css/index.html>)

and logon to St.George Internet Banking to continue the verification process and ensure your account security, At St.George your privacy has always been important to us., Thank you.

**Sincerely,  
St.George Bank Limited  
Online Customer Service**

**For more detailed information on how to keep your online banking safe please visit [Privacy and Security](http://dacvass.com/web/help/css/stgeorge.com.au/?orc=personal).** (<http://dacvass.com/web/help/css/stgeorge.com.au/?orc=personal>)

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Your financial institution (and eBay, PayPal etc.) NEVER email you and ask you to “verify” your account – so ignore any of these requests
- Spear Phishing targets groups of people
  - e.g. a family Blog
  - tries to get personal information for identity theft
  - If you use MySpace or Orkut etc. to keep in touch with people, make sure you set your personal information to only be visible to group members otherwise anyone on the Internet can see it!

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Vishing relates to use of VoIP (Voice over IP) for more information see

<http://en.wikipedia.org/wiki/Vishing>

- Peer-to-peer (P2P) applications are another source of security risks
  - Skype for telephone calls and file sharing
  - BitTorrent etc for file sharing
  - Be careful when using these applications
  - Watch your kids/grandkids if they use your computer ☺

# Protecting Your Computer from Viruses, Spyware and other Nasties

– Use common sense when

- Clicking on links in emails, especially if you weren't expecting to receive it
  - I Love Thee <http://210.7.10.113/>  
IP Address : 210.7.10.113  
Location : Fiji (95% accuracy)  
Host Name : super5300-dialup113.is.com.fj
- Opening attachments to emails, again especially if you are not expecting them
  - So called “Kournikova virus” actual file was Kournikova.jpg.vbs not Kournikova.jpg!!

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Spam Filtering

- Reduces or even eliminates Spam

- Names based on a Monty Python skit

- [http://en.wikipedia.org/wiki/Spam\\_\(Monty\\_Python\)](http://en.wikipedia.org/wiki/Spam_(Monty_Python))

- <http://www.youtube.com/watch?v=wZ7YedEopp4>

- Provided by ISP for free or low charge

- Manage spam with your own antispam program

- See a comparisons of antispam programs at

- <http://www.spamcop.com/>

# Protecting Your Computer from Viruses, Spyware and other Nasties

– *Mailwasher Free*

<http://www.mailwasher.net/>

– *Mailwasher Pro (provides more features)*

<http://firetrust.com/>

– *SpamPal*

<http://www.spampal.org/>

– They all filter mail

- Deleting the spam at your ISPs server
- Download the remaining “good” mail

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Use a different mail program
  - “less susceptible” to attack than say Outlook or Outlook Express
  - *FastMail*  
<http://www.fastmail.fm/>
  - *Eudora* (currently going open source)  
<http://www.eudora.com/>
  - *Thunderbird*  
<http://www.mozilla.com/thunderbird/>

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Use an alternate “more secure” web browser to Internet Explorer

- Firefox

- [www.firefox.com](http://www.firefox.com)

- Opera

- [www.opera.com](http://www.opera.com)

- Keep your computer updated with the latest security patches

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Firewall - sits between the “hostile” Internet and your computer
  - Software firewall
    - A program running on your computer
    - Provides network and application protection
    - Free basic software firewalls
      - *ZoneAlarm*®  
<http://www.zonelabs.com/store/content/company/products/zna1m/freeDownload.jsp>
      - *Comodo*™ *Firewall Pro*  
<http://www.personalfirewall.comodo.com/>

# Protecting Your Computer from Viruses, Spyware and other Nasties

– Hardware firewall

- Provided by your Internet modem or router

– John Donaldson will now discuss firewalls

– ZoneLabs has an informative page on firewalls

<http://www.zonelabs.com/store/content/support/zasc/whyFirewall.jsp?dc=12bms&ctry=GB&lang=en#1>

– Gibson Research Corporation

- Has some tests to check your firewall
- ShieldsUP! Checks computers visibility on Internet

<http://www.grc.com/>

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Wireless Networks
  - More popular now and easier to set up
  - Used to wirelessly connect laptops, PDAs etc to a wireless Modem/Router
  - Desktop usually connected with a cable
  - Others can see your wireless network
  - Security issues you must address
    - Change the admin login name and password
      - Everyone knows the defaults set by the manufacturers

# Protecting Your Computer from Viruses, Spyware and other Nasties

- Implement encryption either WEP or the more secure WPA if possible (minimum requirement is *Windows XP SP2* and *Windows Mobile 2003 SE*)
- Security issues you should address
  - Hide the Service Set Identifier (SSID)
    - It's the wireless network name
    - It makes your wireless network harder to find if hidden
    - Not perfect as wireless scanners can still find you
  - Use Machine Access Code (MAC) address filtering
    - Only allow your devices to connect to the network
    - Not perfect as it is possible to replicate the MAC addresses
  - The more you do the better your security

# Protecting Your Computer from Viruses, Spyware and other Nasties

- In summary
  - Use a Software firewall especially if not using a Hardware firewall
  - Use a Hardware firewall if possible
  - 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

# Protecting Your Computer from Viruses, Spyware and other Nasties

- 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 ... !!” ☺



Questions ?

Any

