Spotty Dog Computer Services

ABN 56 110 736 521

www.spottydog.com.au   info@spottydog.com.au

42 Blaylock Crt
Morayfield Qld 4506

Tel/Fax: (07) 5428-7905
Mobile: 0407 940 662

Virus/Spyware Notes

DONT'S:

1. **DO NOT** open e-mail attachments with the following file extensions, even if you know the sender:

.ade	.chm	.exe	.isp	.mdb	.msp	.reg	.shs	.wsc
.adp	.cmd	.hlp	.js	.mde	.mst	.scf	.url	.wsf
.asx	.com	.hta	.jse	.mdz	.pcd	.scr	.vb	.wsh
.bas	.cpl	.inf	.lnk	.msc	.pif	.sct	.vbe	
.bat	.crt	.isp	.mda	.msi	.prf	.shb	.vbs	

2. Even though the .doc & .xls file extensions have not been mentioned above, BE CAREFUL. Word & Excel documents can contain harmful Macros (A mini-program which will execute a series of commands in series). Also, it is now possible to infect a computer through some image file formats, primarily the WMF format, and recently JPG and BMP formats. This vulnerability can be addressed by making sure that your system is up to date with all Microsoft security patches.

3. **DO NOT** use Floppy Disks or USB Drives from unknown sources unless scanned first using your antivirus software, & even then be careful.

4. **DO NOT** believe any e-mail that tells you to delete Windows files stating that the virus cannot be detected by antivirus software. A lot of the time this is a hoax that tricks you into deleting critical Windows system files.

5. **AVOID** using Chat/Instant Messaging Software, they have **A VERY HIGH POTENTIAL** to compromise the security of your computer & **NEVER** accept attachments from Instant Messengers. **NEVER** install 3rd party upgrades to Messenger ie. Messenger Plus, and never download later versions of the Messenger program unless it is from the official website. **AVOID** using Internet Browser Add-Ins & toolbars like Yahoo & Google Companion, & never allow the installation of Hot Bar, My Search Bar etc, and be aware that social networking sites like MySpace and Facebook are targeted by the bad guys, and **NEVER** install 3rd Party upgrades for Facebook either.

6. **DO NOT** install Peer To Peer (P2P) programs like KaZaA, Grokster, Limewire, Frostwire, WinMX, IMesh, Bear Share etc, unless you are sure you want spyware installed onto your system, and the distinct possibility of virus infection & hacker attacks. All of these things are a security risk. They open up your computer to the internet & there are viruses written specifically targeting them. The same applies to Torrent software like BitTorrent and uTorrent.

7. **DO NOT** download & install free Screensavers. They are notorious for containing spyware.

8. **DO NOT** visit Porn, Casino, Pirate Software & Game Cheat sites. They are also notorious for putting viruses & spyware on your computer.

9. **DO NOT** click on any links in e-mails that say they are from your bank, or from Microsoft. These organisations never send unsolicited e-mails and it is a trick to make you give up your User Name & Password.

10. **DO NOT** believe any Pop-Up Window that tells you that Spyware has been detected on your computer.

11. **DON'T BOTHER** with Internet Download Accelerators or Memory Optimisers

DO'S:

1. **DO** use good antivirus software. If you want a free product, I recommend AVG Free antivirus, and the latest version also incorporates anti-spyware and a website analyser. Or for greater protection, I recommend Norton 360 which you can read about at http://www.spottydog.com.au/services/virus-and-spyware-removal/norton-360/.

2. **DO** regular checks for later versions of your antivirus software if it doesn't do it itself. Most products should update not only their virus definitions but the program itself.

3. **DO** regular Windows Updates http://windowsupdate.microsoft.com and download Critical/Security updates.

4. **DO** use software like Spybot Search & Destroy http://www.filehippo.com/download_spybot_search_destroy/ & Malwarebytes http://filehippo.com/download_malwarebytes_anti_malware/ & **KEEP THEM UP TO DATE**. Be sure to run scans regularly and check for **LATER VERSIONS** regularly. There is spyware around that cannot be removed by these programs, so the best solution is not to get the spyware in the first place. Prevention is better than cure.

5. **DO** use a program like Mailwasher (trial at http://www.mailwasher.net/mailwasher-free) to check e-mails before downloading them from the Mail Server.

IN ADDITION

There is an interesting study by a Danish security firm that found the main reason people get viruses is because they don't update their software. You can read it at http://net-security.org/malware_news.php?id=1863

The main reasons for getting infected are through old versions of Adobe Flash, Adobe PDF Reader, Java and Microsoft Internet Explorer. So if you use these, make sure you keep them up to date!

The conclusion of this study is that as much as 99.8 % of all virus/malware infections are caused by exploit kits and are a direct result of the lack of updating these five specific software packages.

Microsoft recently published a similar study where they found about 90% of virus infections were through unpatched software. Find this at http://www.theregister.co.uk/2011/10/11/zero_day_overrated_says_ms/

WHAT IS SPYWARE

• A general term for a program that surreptitiously monitors your actions. While they are sometimes sinister, like a remote control program used by a hacker, software companies have been known to use spyware to gather data about customers.
• A technology that assists in gathering information about a person or organisation without their knowledge. On the Internet, "spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties." As such, spyware is cause for public concern about privacy on the Internet.
• Also known as "adware". It is a hidden software program that transmits user information via the Internet to advertisers in exchange for free downloaded software.
• Some Web sites and commercial organisations track users' online activity through the use of what is called 'spyware'. Usually coming in the form of 'cookies' - these enable the cookie writer to build-up information about what you do and where you go on the Web.
• Software that tracks usage and reports it to others, such as advertisers. Usually the tracking is concealed from the user of the software.
• Spyware can also, at its worst, disconnect you from the internet & re-dial an international telephone number or an expensive 1900 number without your knowledge.
• Spyware can be broken down into two different categories, surveillance spyware and advertising spyware. Surveillance software includes key loggers, screen capture devices, and Trojans. These would be used by corporations, private detectives, law enforcement, intelligence agencies, etc. Advertising spyware is software that is installed alongside other software or via activeX controls on the internet, often without the user's knowledge, or without full disclosure that it will be used for gathering personal information and/or showing the user ads. Advertising spyware logs information about the user, possibly including passwords, email addresses, web browsing history, online buying habits, the computer's hardware and software configuration, the name, age, sex, etc of the user. As with spam, advertising spyware uses the CPU, RAM, and resources of the user's computer, making the user pay for the costs associated with operating it. It then makes use of the user's bandwidth to connect to the internet and upload whatever personal information it has gathered, and to download advertisements which it will present to the user, either by way of pop up windows, or with the ad banners of ad-supported software. All of this can be considered theft in the cases of advertising spyware that installs without disclosure. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.
• Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.
• Spyware is similar to a Trojan horse in that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.
• Because spyware exists as independent executable programs, they have the ability to monitor keystrokes, scan files on the hard drive, snoop on other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, consistently relaying this information back to the spyware author who will either use it for advertising/marketing purposes, sell the information to another party or perhaps steal from your bank account.

WHAT'S THE DIFFERENCE BETWEEN A SPYWARE, ADWARE AND MALWARE, ETC?

Spyware is software that gathers information about you as you surf the Internet. It is intended to track surfing habits in order to build marketing profiles. Spyware is often included in "free downloads" found on the Internet, from screen savers to pop-up blockers. It can be said that any software that sends data back to a third party without asking your permission is Spyware.

Adware is any software application which, while in memory, causes any advertisement to be displayed on the user's computer, from banners ads to pop-ups, or which hijacks and replaces advertisements found on other websites that you visit with advertisements provided by those directed by the adware instead.

Malware, short for malicious software, is any software application which is specifically designed to cause damage to your computer or intentionally disrupt its operating system.

Key Logger is software that, once installed on your computer, monitors every key stroke you make as well as websites visited, windows viewed, program executed, screen snapshots as well as files and documents that you have accessed.

Dialer is software that, once installed on your computer, will attempt to dial certain preprogrammed telephone numbers through your modem. If connected, you may see mysterious charges appear on your telephone bill, especially 900 numbers.

Hoax is something that usually spreads around the Internet via an e-mail notice from one of your friends who think they are doing you a favor by alerting you to some danger that the creator of hoax anticipates.

WHAT IS PHISHING?

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

Have you received email with a similar message? It's a scam called "phishing" (pronounced fishing), and it involves Internet fraudsters who send spam or pop-up messages to gain personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

Phishers send an email or pop-up message that claims to be from a business or organization that you may deal with, for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to "update", "validate", or "confirm" your account information. Some phishing emails threaten a dire consequence if you don't respond. The messages direct you to a website that looks just like a legitimate organization's site. But it isn't. It's a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

Here are some tips to help you avoid getting hooked by a phishing scam:

• **If you get an email or pop-up message that asks for personal or financial information, do not reply, and don't click on the link in the message, either.** Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organisation mentioned in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself. In any case, don't cut and paste the link from the message into your Internet browser, phishers can make links look like they go to one place, but that actually send you to a different site.

• **Use anti-virus software and a firewall, and keep them up to date.** Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge.

Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.

A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software "patches" to close holes in the system that hackers or phishers could exploit. Be aware however, that a firewall will ask you whether you want to block or allow programs, and if you are a novice user, you may well make the wrong choice and block a legitimate windows process or program.

• **Don't email personal or financial information.** Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organisation's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

- **Review credit card and bank account statements as soon as you receive them** to check for unauthorised charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances. If you use internet banking, review your accounts OFTEN!

- **Be cautious about opening any attachment or downloading any files from emails** you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security. See Do's & Dont's on page 1.

IDENTITY THEFT

It's important to protect your personal information, and to take certain steps quickly to minimize the potential damage from identity theft if your information is accidentally disclosed or deliberately stolen:

- Close compromised credit card accounts immediately.

- Monitor your credit card. Keep in mind that fraudulent activity may not show up right away.

- Consult with your financial institution about handling the effects on bank accounts.

- Contact relevant government agencies to cancel and replace any stolen drivers licenses or other identification documents, and to "flag" your file.

- Watch for signs of identity theft: late or missing bills, receiving credit cards that you didn't apply for, being denied credit or offered less favourable terms for no apparent reason, or getting contacted by debt collectors or others about purchases you didn't make.

Identity Theft: What To Do If Your Personal Information Has Been Compromised

The bottom line for online threats like phishing, spyware, and hackers is identity theft. ID theft occurs when someone uses your name, Social Security number, credit card number or other personal information without your permission to commit fraud or other crimes. That's why it's important to protect your personal information.

If your personal information is accidentally disclosed or deliberately stolen, taking certain steps quickly can minimise the potential for the theft of your identity.

If the Stolen Information Includes Your Financial Accounts

Close compromised credit card accounts immediately. Consult with your financial institution about whether to close bank accounts immediately or first change your passwords and have the institution monitor for possible fraud. Place passwords on any new accounts that you open. Avoid using your mother's maiden name, your birth date, a pets name, your phone number, or a series of consecutive numbers.

If the Stolen Information Includes Your Driver's License or Other Government-Issued Identification

Contact the agencies that issued the documents and follow their procedures to cancel a document and get a replacement. Ask the agency to "flag" your file to keep anyone else from getting a license or another identification document in your name.

Once you've taken these precautions, watch for signs that your information is being misused. For example, you may not get certain bills or other mail on time. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.

Continue to read your financial account statements promptly and carefully, and to monitor your credit reports every few months in the first year of the theft, and once a year thereafter.

ONLINE SHOPPING

Shopping on the Internet can be economical and convenient. Shopping on the Internet is no less safe than shopping in a store or by mail.

Shopping online offers lots of benefits that you won't find shopping in a store or by mail. The Internet is always open, seven days a week, 24 hours a day, and bargains can be numerous online. With a click of a mouse, you can buy an airline ticket, book a hotel, send flowers to a friend, or purchase your favorite things. But sizing up your finds on the Internet is a little different from checking out items at the shop.

If you're buying items from an online retailer or auction website, this advice may help you make the most of your shopping experience:

• **Know who you're dealing with.** Anyone can set up shop online under almost any name. Confirm the online seller's physical address and phone number in case you have questions or problems. If you get an email or pop-up message while you're browsing that asks for financial information, don't reply or click on the link in the message. Legitimate companies don't ask for this information via email.

• **Know exactly what you're buying.** Read the seller's description of the product closely, especially the fine print. Words like "refurbished", "vintage", or "close-out" may indicate that the product is in less-than-mint condition, while name-brand items with "too good to be true" prices could be counterfeits.

• **Know what it will cost.** Check out websites that offer price comparisons and then, compare "apples to apples." Factor shipping and handling, along with your needs and budget into the total cost of the order. Do not send cash under any circumstances.

• **Check out the terms of the deal, like refund policies and delivery dates.** Can you return the item for a full refund if you're not satisfied? If you return it, find out who pays the shipping costs or restocking fees, and when you will receive your order.

• **Keep a paper trail.** Print and save records of your online transactions, including the product description and price, the online receipt, and copies of every email you send or receive from the seller. Read your credit card statements as you receive them and be on the lookout for unauthorised charges.

• **Don't email your financial information.** Email is not a secure method of transmitting financial information like your credit card, or bank account details. If you initiate a transaction and want to provide your financial information through an organisation's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some fraudulent sites have forged security icons.

• **Check the privacy policy.** It should let you know what personal information the website operators are collecting, why, and how they're going to use the information. If you can't find a privacy policy, or if you can't understand it, consider taking your business to another site that's more consumer-friendly.

P2P (PEER TO PEER) FILE-SHARING

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. You simply download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free and easily accessible.

Sounds promising, right? Maybe, but make sure that you consider the trade-offs. File-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files you never intended to share. You may download material that is protected by the copyright laws and find yourself bogged down in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else.

To secure the personal information stored on your computer, we suggest that you:

- **Don't use it all, but if you must, setup the file-sharing software very carefully.** If you don't check for the proper settings when you install the software, you could open access not just to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents.

- **Be aware of spyware.** Most file-sharing programs install other software known as spyware. Spyware monitors a user's browsing habits and then sends that data to third parties. Sometimes the user gets ads based on the information that the spyware has collected and disseminated. Spyware can be difficult to detect and remove. Before you use any file-sharing program, you may want to install software that can prevent the downloading of spyware or help detect it on your hard drive.

- **Close your connection.** In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or "broadband" connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These "always on" connections may allow others to copy your shared files at any time. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.

- **Use an effective anti-virus program and update it regularly.** Files you download could be mislabeled, hiding a virus or other unwanted content. Use anti-virus software to protect your computer from viruses you might pick up from other users through the file-sharing program. Not all anti-virus programs block files downloaded through file-sharing, so check your program's capabilities and settings. In addition, avoid downloading files with extensions like *.exe*, *.scr*, *.lnk*, *.bat*, *.vbs*, *.dll*, *.bin*, and *.cmd*. (see Page 1)

- **Talk with your family about file-sharing.** Parents may not be aware that their children have downloaded file-sharing software on the family computer and that they may have exchanged games, videos, music, pornography, or other material that may be inappropriate for them. Also, because other peoples' files are sometimes mislabeled, kids may unintentionally download these files. In addition, kids may not understand the security and other risks involved with file-sharing and may install the software incorrectly, giving anyone on the Internet access to the family's private computer files.

SIGNS OF SPYWARE

If your computer starts to behave strangely or displays any of the symptoms listed below, you may have spyware or other unwanted software installed on your computer.

I see pop-up advertisements all the time. Some unwanted software will bombard you with pop-up ads that aren't related to a particular Web site you're visiting. These ads are often for adult or other Web sites you may find objectionable. If you see pop-up ads as soon as you turn on your computer or when you're not even browsing the Web, you may have spyware or other unwanted software on your computer.

My settings have changed and I can't change them back to the way they were. Some unwanted software has the ability to change your home page or search page settings. This means that the page that opens first when you start your Internet browser or the page that appears when you select "search" may be pages that you do not recognize. Even if you know how to adjust these settings, you may find that they revert back every time you restart your computer.

My Web browser contains additional components that I don't remember downloading. Spyware and other unwanted software can add additional toolbars to your Web browser that you don't want or need. Even if you know how to remove these toolbars, they may return each time you restart your computer. In addition, you may find that your Home Page has changed and even when you change it back, it reverts to something else by itself.

My computer seems sluggish. Spyware and other unwanted software are not necessarily designed to be efficient. The resources these programs use to track your activities and deliver advertisements can slow down your computer and errors in the software can make your computer crash. If you notice a sudden increase in the number of times a certain program crashes, or if your computer is slower than normal at performing routine tasks, you may have spyware or other unwanted software on your machine.

My Web Browser was Hijacked, that is, your browser takes you to sites other than those you type into the address box.

Keys that don't work. For example, the "Tab" key that might not work when you try to move to the next field in a Web form)

Random Error Messages. For no apparent reason you see error messages. These messages can be caused by poorly written Spyware programs and cause errors within the operating system.

ARE YOUR KIDS EXPOSING YOU TO SPYWARE?

If your computer starts to suddenly slow down or you begin to see pop-up windows, even when you're not browsing the Internet, you may be the victim of spyware and other unwanted software. Spyware is software that is automatically downloaded to your computer without your notice, and is often attached to another file you have chosen to download or install. Spyware can also be downloaded to your computer when you click on banner ads on Web sites.

The types of unwanted software programs that kids accidentally download are usually annoying and may slow down your computer, but are typically not dangerous.

If your children regularly use your computer, they may be visiting sites or downloading files that could be exposing your computer to spyware and other unwanted software.

Types of downloads that may contain spyware

• Free games downloaded from the Internet
• Music, movies, and other software file-sharing programs downloaded from the Internet or from other computers
• Animated characters for your desktop
• Free screen savers downloaded from the Internet
• Toolbars for your Internet browser
• Free pop-up blockers that appear on your computer when you are online

Not all of the programs listed above will contain unwanted software. The key to helping prevent the installation of spyware is to download programs only from sources you trust and to read all security warnings, license or user agreements, and privacy statements associated with any software you download or install on your computer.

Encourage your kids to ask your permission before they download anything from the Internet. If you're not sure if the program they want to download contains spyware or other unwanted software, ask a knowledgeable friend or enter the name of the program into your favorite search engine and see if anyone else has reported that it contains spyware.

"Mum, Dad - I promise I didn't download anything"

Sometimes your children may accidentally infect your computer with spyware or other unwanted software without even knowing they've downloaded anything. Some popular sites for kids may try to download programs without your kids even asking for them. Your children may see a warning notifying them that a Web site wants to download a program. They may click random buttons on the window just to get it to disappear. What they click on might just be "I agree."

If you don't think your kids understand what it means to download programs only from trusted sources or if you think they probably won't read all the warnings and agreements that appear while they're surfing the Web, you may have to take a few extra precautionary measures with your computer.

HOW TO HELP KEEP YOUR KIDS FROM DOWNLOADING SPYWARE

If your kids surf the Internet, chances are they're going to want to download games, music, and other programs that may expose your computer to spyware or other unwanted software.

Here are a few steps you can take to help your kids download and install software more safely.

Step 1: Talk with your kids

Depending on the ages of your children, you may be able to teach them not to download software from unknown sources on the Internet. If you can convince them to ask your permission before they download anything, you will go a long way toward keeping unwanted software off of your computer.

Consider adding Web sites that you feel are safe to your Favorites list and only allowing your children to download software from those sites.

Step 2: Monitor your children's activity on the Internet

Keep the computer in a place in your home where it can be easily monitored and limit the length of time your child can spend on the computer. If your children are under 10 years old, you may want to be online with them at all times.

Step 3: Give your child a limited user account

Windows XP allows you to create multiple user accounts for your computer. Each user can log on separately and has a unique profile with his or her own Desktop and My Documents folder. As a parent, you can give yourself an Administrator account with full control over the computer, and give your children Limited User accounts, with restricted controls that will help prevent them from downloading programs that may contain spyware or other unwanted software.

IF ALL ELSE FAILS

I have found a fairly simple solution to resistant spyware and pop ups. First disconnect from the Internet and from your power source. Be sure that all power is off for ten minutes.

While you wait for all traces of electrical activity to cease, load up a 12 gauge shotgun with pellets that are anything from BB to Triple OO Buck. Fire shots through the case so that the Motherboard, CPU, RAM, and especially the Hard Drive(s) are totally obliterated.

If you are unsure of the damage, try another shot from another angle. Be careful because sometimes a badly wounded pop-up will charge at you and try to inflict more frustration before it dies.

Remove what is left to the garage - not the curb! Tell the Police when they arrive that you didn't hear anything and maybe it was just an engine backfiring.

I hope this helps. It worked for me and I like to help people with their problems.