IT Security

A Quick Guide

Introductory Level

Designed for iPad. Applicable to other devices.

Revised November 2016

GUARDRAIL Tutorials

Importance of Security

Securing your computer is important, not only for your own safety, but also for anyone such as family and friends whose contact information or personal details are stored on your computer.

- Malware can ruin the software running on your computer, corrupt files and obtain confidential information such as internet banking details and personal information
- Anti virus and anti-malware programs will not protect you completely from security threats, it may just limit some of those threats
- Most security threats come from the internet, therefore it is important to secure your internet connection and be wary of attached files and hyperlinks associated with emails
- Backups of important data are an effective way to recover from a virus that destroys your files, or your computer is lost, stolen or somehow rendered unusable

Safe Security Environment

Anti Virus is Dead?

Antivirus software may now only catch about 45% of cyber attacks. Clearly we can no longer rely on antivirus or anti-malware software to protect us. We have to protect ourselves and ensure that any computers or digital devices we are using are not vulnerable to security exploits. We have to ensure that we are not the weak link in the security chain.

Almost everyone in the world of PCs has to worry about **installing** and **updating antivirus** and related programs, often at considerable trouble and expense. Apple and Linux users also have to be aware of certain threats, especially with regards online activities.

Ultimately security is in our own hands. We need to ensure that we do not allow opportunities for breaches of security through unsafe practises and lack of knowledge. It is all about having the **right mindset** and being aware of safety issues and keeping up to date with the ever changing threats. This is particularly true for **mobile devices** which are more easily lost, stolen or exposed to malicious WiFi networks within public spaces.

Regarding anti virus no longer being adequate, experts have come up with a different approach. Rather than constantly trying to block the bad software and websites which keep changing at a rapid pace, it is better just to focus on allowing access to good software and websites. **'White listing'** has become a much better option whereby only **known good software** is allowed to run on the protected computer, and only **known good websites** can be accessed. The whitelist software automatically checks with an online database before allowing the installation of any software, or the downloading of webpages from any website. The white list service will not slow down your PC like antivirus programs do, because it does not need to do regular scans. It scans your PC only once when initially installed and does not require endless updates.

Ransomware

The New Scourge

Ransomware propagates like a **trojan** or **virus** and executes on a computer from a downloaded file or a vulnerability in a network service. Often it will encrypt the files on the targeted computer and then throw up a message demanding a ransom payable through an online payment service such as **Bitcoin**. There are already thousands of variations of this exploit and some use other payment systems such as Ukash. Another type of ransomware known as **Leakware**, threatens to expose private information about the victim.

Since **Cryptolocker** ransomware was released around September 2013, thousands of people have been affected by having files encrypted on their computer and then confronted with a notice demanding they pay a ransom to restore their files.

Malware for Money

This is a good example of how criminals have exploited viruses and malware for financial gain. Previously viruses were usually created for the purpose of wreaking some dumb destruction on the victim's computer (especially one running the Windows operating system).

Valuable Backups

It is a good example of why it is important to have backups of crucial files in case of a disaster, because if the victim has access to an uncorrupted backup, then the files can be restored without paying the ransom required to obtain the encryption key necessary to decrypt the files encrypted by CryptoLocker. Of course, paying the ransom is no guarantee the victim's files will be restored because after all this is a criminal activity. A variant, CryptoWall, had probably accrued over $18 million in ransom by June 2015.

Worldwide businesses and organisations hit by cryptographic ransomware exploits have had to pay out the ransom in order to retrieve their encrypted files (they probably did not have reliable backups)

Internet Safety

Internet Safety

Be aware of viruses and other types of malware, violations of privacy, identity theft and harassment. The usual rules of safety you would apply in the physical world, normally apply in the 'virtual' online world also. You may also call it a 'cyber jungle'. The internet is only as safe as you allow it to be.

Usernames and Passwords

It is best to use **pseudonyms** (where possible) and strong non-personal passwords (such as that produced by a password generator). If you have a lot of different passwords for different services, use a password manager such as **LastPass** or Apple's **KeyChain**

Protection from threats such as **viruses**, '**trojans**', **worms** and **spyware**

- **Antivirus** for protection against viruses (self replicating malicious software)
- **Anti-spyware** for protection against software used to gather personal information
- **Firewall** to protect against unauthorised threats to your computer from the internet

Internet Safety

... continued

Scareware

Beware of ‘scareware’ designed to scare people into thinking they have a security threat and entice then into clicking a link to ‘fix’ the problem (thereby unknowingly installing the malware). By clicking the OK button on a malicious popup window, the user may actually activate malware installation.

Software Updates

Install them as they become available because often they contain patches for security vulnerabilities. Make sure automatic updates are ‘**on**’ especially for operating systems, internet browsers and software that has known security issues such as **Adobe Flash Player** and the Oracle **Java** platform.

Backup Data

Backup your important data to an external hard drive and/or a cloud service such as **Google Drive**, **iCloud**, **Microsoft OneDrive** or **DropBox**

Email Spam/Scams

Spam emails often contain links to **phishing** websites, or links that activate **malware**. Spam blockers on the internet are not able to filter out all of the spam. It is a problem that is not likely to go away anytime soon because the spammers are always looking for ways around the security.

Internet Safety

... continued

Email Spam/Scams

Scams are always for the purpose of obtaining money. They usually offer something that is too good to be true, or have you believe something bad will happen if you do not act upon the advice provided. A good example is the 'work at home' offer which will have you believe you can 'get rich quick' by following the proposed scheme which usually involves you paying for some dodgy software or system developed by expert con artists.

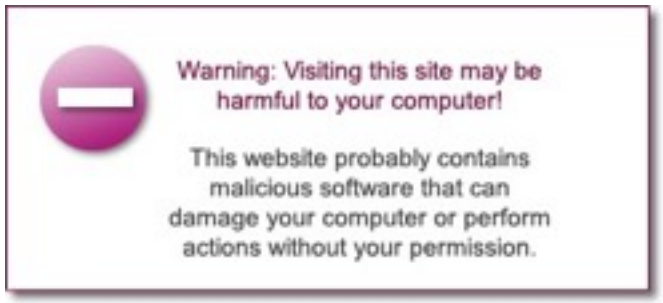
Unsolicited emails may contain attachments that are really viruses or malware disguised as something else (such as a 'malware removal tool'). The best defence is to adopt safe practices, and avoid dangerous ones (such as clicking without thinking).

A good resource for a quick rundown on scams is provided on the Australian Government's **ScamWatch** website:

SCAMS - PROTECT YOURSELF

Internet Safety

... continued



An example of the sort of warning displayed by a modern browser (Chrome) when trying to access a known malicious website

Unsolicited emails may contain attachments that are really viruses or malware disguised as something else. This is possibly the main threat.

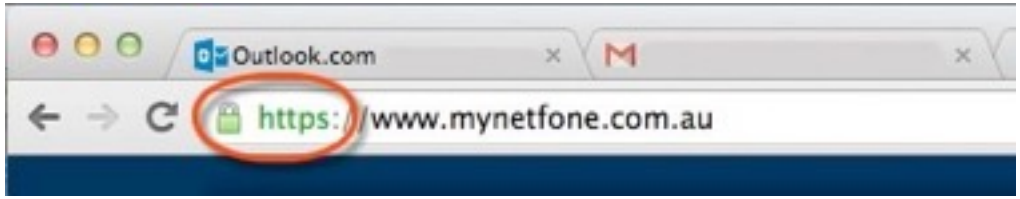
Safe Web Browsing is helped these days by the major browsers having the ability to block most malicious websites, for example:

- **Internet Explorer** - SmartScreen Filter
- **Firefox** - Phishing and Malware Protection
- **Chrome** - Google Safe Browsing

Safari also has inbuilt online protection features such as third party cookie blocking, malicious website detection and blocking, and sandboxing of plugins such as **Adobe Flash Player, Java**, **Silverlight** and **QuickTime** player should these be compromised.

Updating your web browser will provide a higher level of security against known exploits.

Online Transactions Security



All online transactions should be done over a secure internet connection. Look for **'https'** preceding the website address (URL). It will be accompanied by a **padlock** symbol (with slight variations between browsers). An HTTPS connection ensures any data sent over this connection is encrypted. If the data is intercepted by anyone, they will not be able to make sense out of it (it will appear scrambled and cannot be unscrambled without the encryption key).

HTTPS connections use **SSL** certificates which allow authentication and encryption in order to ensure transactions are private and secure. It is possible to check the details, and authenticity, of the certificate by clicking on the lock symbol of your browser.

Online Transactions Security

Phishing Scams

Phishing websites are one of the main methods cyber-criminals use to gain access to personal information and bank account details normally for the purpose of financial gain. Often they work by luring the victim to a lookalike website of a bank for example. The unsuspecting victim may provide a **login** and **password** into an input form and send these details to a criminal upon clicking the '**submit**' button.

Be wary of any sort of unsolicited email or other type of contact trying to obtain personal information or payment of any sort. Fraudsters often use this method of targeting unsuspecting victims.

Online Shopping

As with normal shopping, the usual precautions apply. Carefully check the product by doing a little online research. Check if the price is realistic and there are no hidden surprises. When paying use a secure payment gateway such as **PayPal**. Keep a copy of the transaction.

Online shopping is a very enjoyable, quick and convenient way of buying products or services. Try not to deviate from normal safe practice and there should not be any problems.

Social Networking Security

Social Networking

Facebook, **Twitter**, **Instagram**, **LinkedIn** to name just a few, pose a number of risks for users. One needs to be aware of the following issues:

- Legal issues regarding what you post online
- The potential consequences of providing personal information online
- Any images of yourself that you post online may be used against you
- Issues regarding the posting of images of children online
- Tracking of users' online activities, for example to facilitate targeted advertising
- Location services can provide information about your whereabouts (not always a good thing)

For more information: **GCF Learn Free - Internet Safety**

Summary - Security Tips

The usual:

- Use strong passwords for sensitive accounts such as online banking, Facebook and email
- Never trust unsolicited emails. Think before you click. Links in emails potentially activate malware or divert you to malicious or untrustworthy websites
- Don't disclose personal information online unless it is to a trusted service such as a government site or trusted institution that uses an encrypted connection (HTTPS)
- Clean your hard drive before disposing of old computers (special hard drive cleaning software such as **Disk Wipe** or **Eraser** can be obtained for free)
- Install and automatically update anti-virus, anti-spyware software
- Ensure your operating system (such as Microsoft Windows) is set to receive automatic updates
- Update all software, especially browser plugins and Oracle Java
- Use a firewall to block unauthorised connections to and from the internet
- Always use a passcode (or PIN) to lock your mobile device (such as iPad or smartphone)
- Keep up to date about the latest online safety and security advice by subscribing to email notices from a service such as **Stay Smart Online** (an Australian government website)