
Cyber Security Education & Awareness

Guide for User's

Release Q1 – 2010

Version 1.1



CONTENTS

- 1. Introduction**
- 2. Protection against Nasty Code**
- 3. System Security Maintenance**
- 4. Personal firewalls**
- 5. Wireless Security**
- 6. Protection of Information**
- 7. Phishing & Pharming & Scams**
- 8. Botnet's & Trojans**
- 9. Children-on-line & Safety**
- 10. Privacy and Internet Use**
- 11. Where to go for HELP**

I. Introduction

No matter if you are using computers & the Internet at work, or at home, security risks exist which could lead to compromise of **business**, or your own **personal data**? It could even be that if you fall victim to a **Scam** or **compromise**, it could cost you money!



It may be that you have either *young* or *elder* family members at home who also use computers, and the Internet for on-line banking, school work, and/or social activities, such as e-mailing friends, distant family members, or possibly using new on-line services such as Facebook, Bebo, or Friends Reunited. Again, such usage can create opportunities for those with **darker** intent, seeking to spoil use, in pursuit of their criminal on-line activities - or where children are concerned, with some other **sinister** mission. However, there is no reason why the use of computers, and the Internet cannot be enjoyed - it is just a matter of applying a little **security** and **personal safety**.

The Objective: The first objective of this **Security Education & Awareness Guide** for User's is to provide *practical, no-nonsense* information to assist any user, their family members, and friends, to increase their level of safety when using computers, and the Internet, both at *work* and at *home*. The

second objective is to strive to assist parents, and guardians to keep their young family members safe when using computers, and the Internet for school work, or pleasure, by providing some Best Practice information.

2. Protection against Nasty Code

It is a *fact* that if you *connect* to other systems, *share* media or data, or connect to the *Internet*, the chances of encountering **Malicious Code** are **extremely high**. So it is *essential* that adequate steps are taken to assure at *work*, or *home* based, your system(s) are *fully* protected & secure.



But What is Malicious Code? Malicious Code comes in many forms, ranging from self-replicating **Computer Viruses** and **Worms**, which can damage the way your computer runs. It could also be that such Malicious Code (known as **Malware**) could also be installing malicious components to your local PC which intend to steal personal information!

- Say your **Logon Credentials** for your on-line banking service, or possibly a **PayPal** account, *something to be avoided*.

But what do I do – at WORK? At work your system protection will be maintained, and kept up to date by the IT Team as a matter of their daily maintenance operations.

But what do I do – at HOME? Purchase, or obtain a *free* home user Anti-Virus application, install it, and keep it fully updated.

How will I know if I have been infected? Hopefully, with a good up to date Anti-Virus application installed, the risk of encountering such infections will be much *reduced*. However this does *not* guarantee that your system will be 100% protected. So, if your machine starts to behave badly, or is slow to start, or shows signs of a change to its normal operations, at work, call the Service Support Desk and log a call. They will then check it out, and confirm its status, and if infected clean the virus. If at home, check with the Anti-Virus vendor web site, or call their Service Support Desk.

3. System Security Maintenance

One of the most important aspects of system security is to ensure that your local *work*, and *home* based computer systems are fully up-to-date with security patches and updates, which have been issued by the vendor (say **Microsoft®**).

At WORK

At work your system will be subject to automatic patching by you ICT Team.

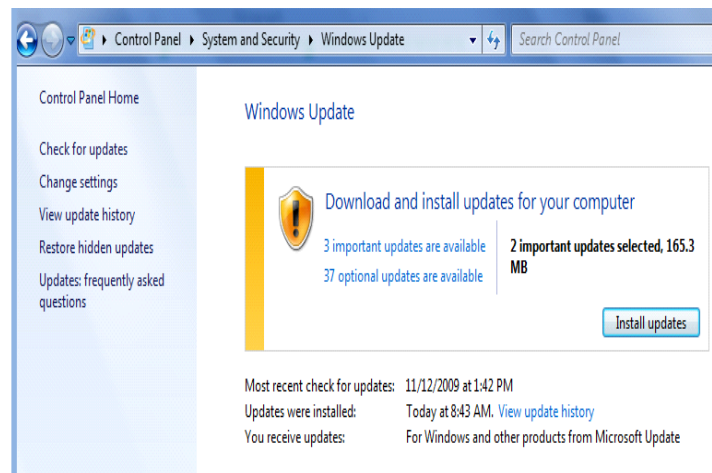
At HOME

Ensure that Automatic Updates are switched on – Consult your Vendor Manual.

By applying the latest patches and updates as they are released from the vendor, you will be ensuring, as far as is practicable, any *new*, or *reported* security exposures, and/or vulnerabilities, which could allow *hackers*, or *criminals* to exploit your computer, have been fixed to ensure that the computer system is protected. A further personal system defence this can

result in is, in some cases it may also provide *increased* levels of protection against Malicious Code (AKA **Viruses**, **Worms**, and **Malicious Agents**).

Auto Update: The window to the right of this text is an example of Automatic Updates turned on under a **Windows 7®** computer.



Security Alerts: If you wish to remain fully updated with reports relating to current security exposure and updates, you may subscribe to the Vendor issued notifications, or to other third parties, who provide such a service – See **Section 11 - Where to go for Help** for more information.

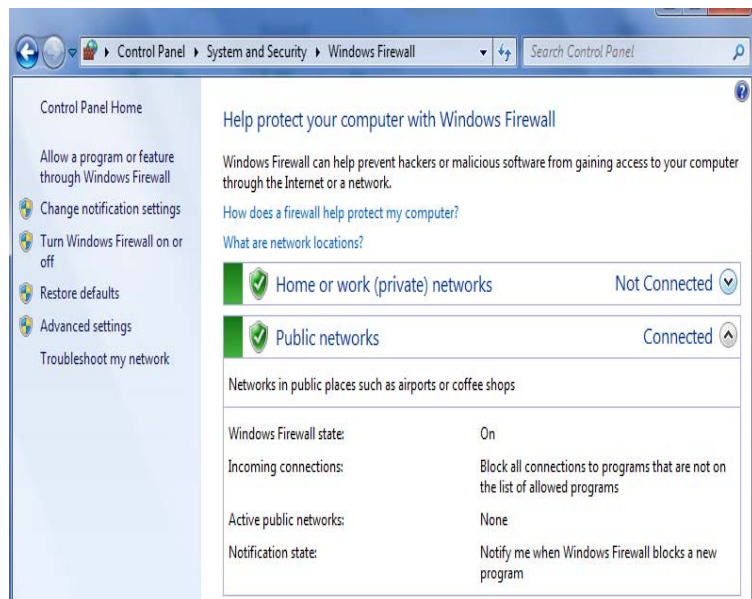
4. **Personal firewalls**

When you use the Internet at work, your ICT Team use a device, known as a **Firewall** to ensure that your on-line experience is secure and protected. In simple terms, this device controls what takes place between the PC, and the Internet. Thus, should some miscreant unauthorised party, attempt to infiltrate your system, his/her actions will be blocked – However, this level of protection does not always exist for most home users.

HOME Use:: For the Home User, they may either use the **Firewall** that is supplied with their system. Or they may purchase a third party supplied application. This will then accommodate them with a cut down version of the security

they enjoy when at their place of work.

The opposite image is an example of the Personal **Firewall** supplied with **Windows 7**[®]. This is auto setup and provides basic level protection.



For more information on the Windows **Firewall** (Supplied with **Windows XP**, **Vista**, and **Windows 7**[®]) consult the supplied guide for more information.

It is also well worth noting that *some* Anti-Virus applications supply the end user with Personal **Firewall** capabilities - one such example is the Panda Anti-Virus application.

5. Wireless Security

OK, so you may not use Wireless with your supplied Office Workstation or Laptop! But what about at home?



As you are most likely aware, Wireless (or shall we say WiFi) protocols, including **Bluetooth**, allow the user to roam freely around the home, or in some cases, the workplace, removing the hassle of having to connect with those annoying cables. However in its basic **out-of-box** installation, WiFi can also be **extremely insecure**, making it easy for, say your *neighbour* to

use *your* paid for connection, to download pirate copies of music (that makes *you* the responsible person!). Or it could be that unauthorised person will be able to track *your* logging into *your* on-line banking session! *Now you wouldn't want that now, would you?* So what can you do to protect your WiFi use?

Secure your Connection: To assure you are as secure as possible when using WiFi, consider the Best Practice Security advice we have provide below.

Best Practice Security:

1. Use WPA encryption
2. Keep your Gateway Device up to date with the latest updates, patches, and fixes
3. Password protect your Broadband router
4. Consider using MAC Filtering – this will only allow computers, and devices you are aware of to connect to your Router
5. As previously mentioned – Use a Personal **Firewall**
6. Power down your Broadband Router when you don't require its use (say at **night**)

For more information consult your vendor guides or help pages

6. Protection of Information

Misplace your PC, or Laptop, and what do you do if you can't get it back? If you had the foresight to insure it, then I guess you make a claim, and buy a new one. If however, you did not, then you will need to stump up the cash, and purchase a replacement. But what about all your data (**Information**)

stored on the system – where can you buy that back from? Also consider if you had any information on the PC or Laptop which was **Personal** or **Sensitive** – *could* it be of use to say a *criminal*? So here two areas jump out, which are 1) **Data Backup**, and 2) **Data Security**.



HP Home Server

Data Backup: At your place of work, if you use a computer, this will be done automatically on your behalf. However at home this is not the case and you need provide some sort of a solution. The options here range from a Medium end solution, like s **HP Home (Media) Server**, through to an external USB Drive, of Service Provider Solution – **See Section 11 - Where to go for HELP** and for more information.

Data Security: There are a number of things one can do to protect information from prying eyes. The most obvious of which is to **encrypt** your information at either *folder*, or *drive* level. Thus even if some nasty person, with unknown intent does get access to you PC or Laptop, it will prove very difficult for them to also gain *easy* access to the resident information. Again some solutions are included at Section 11 - **Where to go for HELP**.

BACKUP + SECURITY = PEACE OF MIND

7. Phishing & Pharming & Scams



Phishing is where some person with criminal intent sends out an e-mail (the Hook) to get the recipient to divulge some valuable information. **Pharming** is similar item of interest.

As with many other areas of life – if something looks too good to be true, then it probably is! **Remember**, *there is no such thing as a free lunch*.

Scams can come in many forms, ranging from an offer of some extremely lucrative business opportunity, to assist a disposed king to liquidise his assets – after say a small scale military coup. Or it may be that you have won the lottery (*again*), and all the organisers need is a little information to pay you those millions of pounds sitting waiting for your collection.



REMEMBER: The objective of opportunistic Scams is to get the user to supply snippets of information. Say **Bank Account** number and **Sort-Code**.

So TAKE CARE and DON'T RESPOND

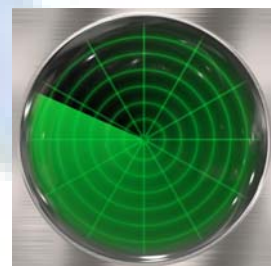
8. Botnet's & Trojans



How Do They Do IT? In simple terms *Hackers* and *Cyber Criminals* trawl the Internet looking for exposed machines that are not protected. When one is located, they do their best to **exploit**, and **recruit**! This is done by using some method of attack to

compromise the user – remember those unwanted mails, and those links you are sometimes sent – or maybe an attachment with a funny picture, or cartoon. However, in some cases these may be much more than that, with *embedded* malicious intent, and *subliminal* activity to infiltrate, and to take control of, and to own the logic of *your* PC from thereafter.

What Can I Do: Anti Virus's applications do detect any of these attacks, so ensure you have an up to date product protecting your machine. Consider using a Personal **Firewall** (See **Section 4**).



Above all other considerations 1) **Never** open e-mails from people you don't know or recognise, 2) If you do, **Never** open any attachment, or click on any embedded links, and 3) **DO NOT RESPOND** (as you are telling the sender, you exist!

JUST TAKE CARE, & SURF SAFELY

9. Children-on-line & Safety

Children love to use the Internet, for school work, as well as keeping up with friends. On line games, e-mail, good old **Facebook**, and other such exciting

on-line play things, all provide endless hours of enjoyment and pleasure. However as many parents realise, this same playground can also have similar dangers to the streets – *predators*, and *unsavoury* people may be lurking just around the corner (or in this case **Screen**) – but that should not stop the enjoyment if sensible steps are taken.

What to Do? The most obvious thing is to speak with your kids, and raise their awareness. Secondly, be proactive and use some of the features provided with your computer. For instance see below for the Parental Controls Options which is provided with **Windows 7®** – this will help keep you children safe whilst they are enjoying their on line time.

Who are CEOP?

CEOP are a Government agency set up for the protection of children, and offer advice and direction

See Section 11



Danger: When kids talk to other kids in chat rooms, unless they know for sure who they are, **take care.**

Conclusion: Parents would never let their kids go out on the streets, unless they know they are safe, and with people, and friends they know. So, approach the interconnected world of the Internet in the same way – raise the level of understanding, and where possible, apply some technical controls to keep those little ones safe and sound.

10. Privacy and Internet Use

The Internet and all of those new and shiny **WEB 2.0** applications are great little tools and toys for the family and friends to play with. Facebook, Bebo, and those great offering from Google. This is not a security issue in every sense of the word, however, users of the new interconnected world should consider their levels of exposure, and privacy so that they may make a judgment as to just how *much* information they *divulge* about their *on*, and *off* line life.

Choice: It is all down to risk, and personal choice. At the end of the day, arriving at a decision, as to your own personal appetite for your online profile, as to what information, and conversations will be shared, with whom, and on what basis.



Did you Know: That when you log out from a Google Account, your searches are logged for **180 days**. That the next generation Google's service will allow a user to track on the image of a face of a person they *don't* even know, to find out more information about that person!

Remember: The more information you give away on-line, the more exposed you may be – so consider the options.

Options: To limit and manage any personal on-line exposure, be sure to setup the view and security preferences (e.g. Facebook's new Privacy Settings) on your application of choice, so that you *only* to share with others what you wish to

Remember: Information is Published on the Internet, may be for **LIFE**.

11. Where to go for HELP

The following free applications and services are available to protect and enrich the end user experience when using the Computer, and the Internet:

Children & Safety:



Child Exploitation and Online Protection Centre (CEOP)

<http://ceop.gov.uk/>

Onlinefamily - Norton - free Tool

<http://www.symantec.com/norton/products/parental-controls/online-family.jsp>



Family Protection - Symantec

<http://www.symantec.com/norton/familyresources/index.jsp>



Windows 7 Parental Controls - Microsoft

www.microsoft.com

On line Help:



e-Victims - free help with scams and other crimes

www.e-victims.org



Secunia - free alerting service

www.secunia.com

Anti-Virus Protection

123 Pall Mall, London, SW1Y 5ED

+44(0) 207 096 2843 + 44(0) 788 162 5140



Free Anti-Virus for Home Users - Security Essentials from Microsoft

http://www.microsoft.com/security_essentials/



Free AVG Anti-Virus for Home Users

<http://free.avg.com/gb-en/download-avg-anti-virus-free-edition>

Personal Firewall



XP, Vista, and Windows 7 Firewall – Supplied with O/S

www.microsoft.com

Backup Solutions:



Back up & Restore – Supplied with Operating System – Microsoft

www.microsoft.com

Encryption Solutions:



EFS Encryption – supplied with XP Pro, Vista Ultimate, and Windows 7 Ultimate

www.microsoft.com



Windows BitLocker – With Vista, and Windows 7

www.microsoft.com

TAKE CARE, BE SAFE, AND SURF SECURE