# Good Computer Security

***It's easier than you think and needn't cost you a cent***

*Presented to Southern Highlands Computer Users Group (SHCUG), June 7, 2011*

---

**Before we start: Two excellent free web services:**

**1. The easiest way yet to send large files and photos**

The free web service at http://min.us allows you to send files that are too big to email. Can send files up to 25MB without registering or 50MB if you register. Registration is free,

Just go the website and drag and drop the file you want to send to the web page. This will upload the file to the min.us server and generate a web link that you can email to the recipient of the file. When they click the link the file will be downloaded to their computer.

- No registration required
- Share link with a many people as you like
- Items stored permanently
- Easy to remember web address

2. **Take a full-length snapshot of any webpage**

This free service at http://urlcapt.com/ not only allows you take a snapshot of a webpage but also download the result as a JPEG, PNG image or PDF file.

- No registration required
- Images available as web links to share
- Can capture long pages that take up more than one screen

---

**Computer Security Revisited**

**1. Base case setup:**

- Microsoft Security Essentials for malware protection
- Windows Firewall
- Microsoft Updates Enabled
- Ensure other software is up-to-date by using Secunia PSI. In particular ensure Adobe Flash, Adobe PDF Reader, Apple QuickTime. (http://secunia.com/vulnerability_scanning/personal) (bit.ly/Jj7wT)
- Install a a website rating browser plug-in like WOT (http://www.mywot.com/) and make sure you only visit websites rated "Green" by the plug-in.
- Follow Safe Computing Practices (see attached sheet)

**2. Other issues:**

- Password security.

Use strong passwords and a different password for every site. Manage with a password manager like Roboform ($10 year) or the free online service LastPass (http://lastpass.com/) but ensure your master passwords is really strong.

Strong passwords consist of a minimum of 8 characters containing upper and lower case letters, numbers and at least one special character such as !@#$%^&*()_+.

Avoid using words that are found in the dictionary. If you must use them then munge them in some way so they are different.  For example replace letter o with zero and letter i with 1 and add some special character at the end

johnny101 is not strong

J0hnny101! Is strong

Pass phrases are better than passwords particularly when munged. A pass phrase like:

Chr1s L0ves “Mahler” is essentially unbreakable and not that hard to remember.

Another good pneumonic is to take the first letters of a line of poetry or a song and munge them.

“Down and out in Mobile with the Memphis blues again”

Dao1MwtMba:(  12 mixed character - unbreakable

- Password theft prevention

Use a limited user account (LUA). Easy to create from Windows Control Panel.  LUA not very practical for everyday use as difficult to install software and even make small changes to the system. Great though for improving the safety and security of browsing, particularly when banking or online purchases, as it is very difficult for malware programs to install themselves in a LUA. Just switch to LUA account when needed; it’s quick and convenient.

An alternative is use Trusteer Rapport (free) that creates a secure tunnel to designated websites. I strongly recommend this program to all users.

http://www.trusteer.com/webform/download-rapport (bit.ly/bTbU3o)

- Minimize public Wi-Fi risks

Puplic Wi-Fi networks without passwords are not secure. Networks with weak passwords are not secure. Anybody can read view what you are doing and depending on your PC setup, they may also be able to gain access to your computer.

When using public Wi-Fi networks use a public Virtual Private Network to encrypt your data such as HotSpot Shield (free but with ads) or OpenVPN (commercial but cheap).  At a pinch you can also use a TOR connection for browsing such as the TorButton add-on for Firefox or xBBrowser, a portable version of Firefox pre-configured with Tor)

TorButton https://www.torproject.org/torbutton/index.html.en  (bit.ly/eI9elB  Works with Firefox 4.0 but not later)

- Improve Router security

Make sure you have a strong password set on your router and make sure you are using WPA2 protocol.

WEP is not secure. WPA is OK when used with strong password

List of default router passwords: http://www.phenoelit-us.org/dpl/dpl.html (bit.ly/10UrU)

**Safe Computing Practices ("Safe Hex")**

1. Be very careful where you surf. Use the free WOT browser plug-in to help you stay away from bad sites

2. Never click on email attachments from unknown sources however tempting and attractive such attachments may seem. If you can't resist temptation save the attachment and open it in a sandbox such as the free sandboxie.com.

---

3. Only download files from trusted sources. These include:

- Files hosted on reputable download sites such as download.com, snapfilescom, softpedia.com, majorgeeks.com and other similar sites.
- Files mentioned in the editorial sections of major computer websites and publications such as PC World, CNet, Lifehacker and of course, Gizmo's Freeware.
- Open source software hosted on sourceforge.net, Mozilla.org and similar large open source sites.
- Files available for download from Microsoft, Google, HP, Dell and other reputable vendors.

4. Never install programs obtained from P2P networks including BitTorrent, eMule, LimeWire and others as many of these files are infected with malicious programs. Some of these malicious programs are so powerful they are capable of overwhelming all your security defenses.

5. Never install programs that friends give you on removable media unless you have verified that they are clean by submitting them to free web based file scanning services such as the free online virus scanner Jotti (http://virusscan.jotti.org/en) or Virus Total (http://www.virustotal.com/)

6. Never accept free toolbars, media players or other unsolicited software offered to you by a website. Simple as that, no exceptions.

7. If you are not using Internet Explorer 8 or 9 then we recommend you upgrade to one of these versions or better still, switch to an alternate browser such as Mozilla Firefox, Opera or Google Chrome. All these have a track record for better security than earlier versions of Internet Explorer and are arguably superior browsers as well. (IE9 is only available for Vista or Windows 7. It can not be installed on Windows XP or earlier).

8. Seriously consider using a Windows limited user account (LUA) rather than a normal account with full administrator privileges. LUA will block the majority of malware including, among others, all kernel mode rootkits.

Instructions for XP: http://www.ehow.com/how_5230032_create-user-account-windows-xp.html (http://bit.ly/k8ffZN)

Instructions for Win 7: http://www.youtube.com/watch?v=aOauG06S9wE (bit.ly/jwAXYW video)

9. You should seriously consider creating a fresh installation of Windows and then back up your PC using a drive imaging program. Then if in the future your PC ever becomes infected you can use the drive image to restore it to a pristine, infection free condition. If you are using the Business or Ultimate versions of Vista/Windows 7 you already have drive imaging capabilities built into Windows. See here for details:

http://www.howtogeek.com/howto/4241/how-to-create-a-system-image-in-windows-7/ (bit.ly/17Ajqp)

If you're using other versions of Vista/Windows 7 you can find a number of free drive imaging programs here:

http://www.techsupportalert.com/best-free-drive-imaging-program.htm (bit.ly/88C2M)

By following these simple rules the chances of your PC becoming infected will be dramatically reduced. Combine these practices with the security software suggested above and you are well on the way to safe, secure, infection-free computing.