Script for workshop

Things to bring: Projector; 2 laptops; Laser pointer (green); Video cable; Handouts; Script; Plugstrip; Extension.

Setup: log into 909 wifi, mailwasher download on taskbar, WMatch on taskbar, wifi info in Word displayed, Powerpoint on taskbar.

(Slide 1)
Welcome - everyone should have a handout that gives more details about some of the things I will present. Feel free to ask questions but please make them questions that I have the answer to. (maybe a break in the middle?)

(Testing a new device – HP tablet)

I am using a Windows 7 computer for this presentation but have included a few items about both Windows XP and Windows 8. For that reason I might occasionally pause to change computers. Toward the end I may comment on Apple, Linux and Chrome systems.

All set?
==========
I'll minimize the PowerPoint for a moment. Ignore the clutter and notice the background color. The default is either blue or a photo. It was found that blue energizes the brain - but do you really want an energized brain just before you go to sleep? If not, change the background to green (*'how to' on handout*).
==========

(Slide 2)
Now for some security and safety tips – the easiest one to do is cover your camera. (demo?) Unless you are Skyping with someone, do you really want anyone else to be watching? How do you cover your camera – with a piece of tape and paper or a Postit note.

==========

(Slide 3)
One of the most important things you need is a good anti-virus program. There are many highly rated programs and most new computers come with a 'trial' copy of either McAfee or Nortons. Unfortunately, at the end of the 'trial' period, they charge you to maintain your protection. For various reasons, I am not a fan of either of these.

There are, however, several highly rated FREE programs available. I am currently using AVG Free on two of my computers and BitDefender on another one – in addition to the paid version of both of these. The free versions usually ask you to reload the software every year which can be a hassle while the paid versions give you the latest updates and most comprehensive protection. This applies even to older XP computers. (comment on XP)

==========

(Slide 4)
The second most important action you can take is to install the available updates. This can be a real pain in the time zone but most updates close security holes that have been discovered.

==========

(Slide 5)

One thing to beware of is the 'Additional Software' that some (non-Microsoft) programs attempt to also install. (show Adobe update)

Be VERY CAREFUL about installing any 'additional' or 'optional' unneeded software.
Make sure your browser is up to date as this is your first line of defense. The handout lists the way you can determine if Internet Explorer or Firefox are up to date.
==========

(Slide 6)
One thing that can create browser problems is too many toolbars. You only need, at most, one toolbar. See the handout for information on removing the toolbars from either Internet Explorer or FireFox.
==========
(Slides 7, 8 & 9)
BEWARE of on line phishing! Phishing and spoofing are the two biggest sources of malware. ALMOST ALL of the major break-ins are a result of someone clicking on a link that leads to the installation of malware.

Notice the 'FROM' – a good phisher will spoof this address so it looks like it came from Chase (from someone at the University of North Carolina at Greensborough) or Yahoo (Azusa Pacific University).

If you have the time, LOOK UP (do not click on the return link!) the actual e-mail of the company that you are supposed to provide an update to. Check to see if you can find an e-mail

address for their fraud department and forward the message to them. (In these cases I looked up the IT help line at each of the schools and forwarded the message to them. One responded that they took this quite seriously and would deal with the person.)

If it came from a 'friend' send an e-mail to him (DO NOT USE 'REPLY' and ask him. (Walter's story - reply came from 'Walt'.)

==========

(Slides 10 & 11)

Be very careful about opening any e-mail without a subject or just a one or two word subject – especially something like 'Enjoy' or 'You will like this' or 'A good opportunity'. If possible, open in text mode and check the link. If there is only a link and very little else, DO NOT click the link. Go to the sender and ask if he/she really sent it.

Opening in text only will also show if an address/link is spoofed for phishing purposes. (Show Mailwasher)

==========

(Slides 12 & 13)

Protecting your friends when you send e-mails. Use bcc: Unless absolute necessary, DO NOT put all of the names in TO: or CC:. BCC: means that all of the names except yours is hidden. It also avoids the possibility of a 'Reply All' embarrassing error.

==========

(Slide 14)

To avoid disaster, backup your data. The Microsoft backup utility works fine and there are other backup programs that do the same job. Most can backup any CHANGED data so you do not need to do a full backup every time.

Creating a restore point is vital since, should some type of malware infect your system, you can then return your system to how it was on some previous date. (NOTE: this does not always work.) See the handout for how to get to the backup utility and to create a restore point.

==========

(Slide 15)

What do you keep your backup on? DVD or flash drive? DVD's are probably the best BUT it can get expensive and cumbersome burning a new DVD every time you do a backup, even if it is for a small change in your data. Flash drives are much better but also more 'fragile' and certain protocol must be followed to insure their integrity. Before plugging in a flash drive, touch the METAL part of the case of the computer (or the back of a laptop, especially in cold weather, as this will discharge any built up static charge. Before removing a flash drive, be sure to 'dismount' it by clicking on the icon then 'Eject the drive' and wait until you are told it can be safely removed. (example.) My favorite program for backup is WMatch from PCmagazine. (Show from taskbar).

==========

(Slide 16)

The death of the cellphone!

Cell phone tracking in stores and by police.

Can your cell phone be hacked? Yes but, at this point why bother. Android & Windows Beware of Apps (flashlight tracker)

Guard your smart cards – example of Ventra charging both the Ventra card and the smart card

Can your car be hacked – depends on what you have in it – an OnStar or similar wifi connection – yes
Apple Mac's and Linux systems.
==========
(Slides 17 & 18)
Thanks for being here. Please do not be scared but DO be careful!