Session 06

STAYING SAFE ONLINE

Introduction

- The World Wide Web is a fantastic resource, but as with everything, it has its risks
- PLEASE, invest some time going through, and acting on, the guidelines for staying safe at:

https://www.getsafeonline.org

- This session will give you some hints and tips on staying safe while enjoying this new online world
- Also, please check out the Digital Unite guides "How to stay safe online"

5A – Protect your PC

Anti-Virus

Some antivirus software can be downloaded for free from the internet – for instance AVG

Some have an annual subscription:

- Norton (by Symantec)
- McAfee (now part of Intel)

Some are included in an overall security package featuring a Firewall, Anti-spam etc.

The AV software I have personally used for many years is ZoneAlarm as part of their "Extreme Security" package

Windows Defender is built into the latest versions of Windows and helps guard your PC against viruses and other malware – it will turn itself off if you install another AV program

For a PC running an older version of Windows, download Microsoft Security Essentials

- Computer viruses are malicious programs that are designed to damage your computer or compromise your security
- Before using the internet, it's essential that your computer is protected by antivirus software
- Antivirus software will protect your computer by preventing an attack by or detecting and removing any viruses
- All antivirus programs have to be regularly updated, as new viruses appear on the scene
- Some antivirus also protects against spyware – software that collects information about the user, such as which websites they've visited

Firewall

If your computer's operating system is Windows XP, Vista , 7, or 10 it will already have the built-in Windows firewall

Some firewall software can be downloaded for free from the internet – for instance:

- ZoneAlarm Free Firewall
- Comodo Firewall

Other firewall software is bundled in (paid for) internet security suites; see PC Mag's:

- 15 best security software of 2016 UK

Acquiring any of these suites (any one in the top 10) is a really good investment; they usually come with additional features – anti-spam, anti key-logger etc.

Typical cost is £30-50 p.a. for a three user licence

- A firewall is a barrier between your computer and others on the internet
- Its purpose is to block attempts by malicious people to gain access to or destroy the information on your computer
- If you have broadband, it's especially important to have a firewall because your computer is permanently online, giving people (or their destructive or prying computer programs) plenty of time to try to attack it
- A firewall can consist of software – that is, a computer program – or hardware
- A software firewall is the most important one to have
- These days, most broadband routers incorporate a hardware firewall.

Test your Firewall

- Open your web browser and type www.shieldcheck.com into the address bar
- Click **Check My Firewall Now**

An example of an Internet Security Suite

- All security suites – like Norton, McAfee, etc. will have a panel something like this
- Just for interest, this package costs ~£60 for two years cover for up to 3 PCs - others will be similarly priced

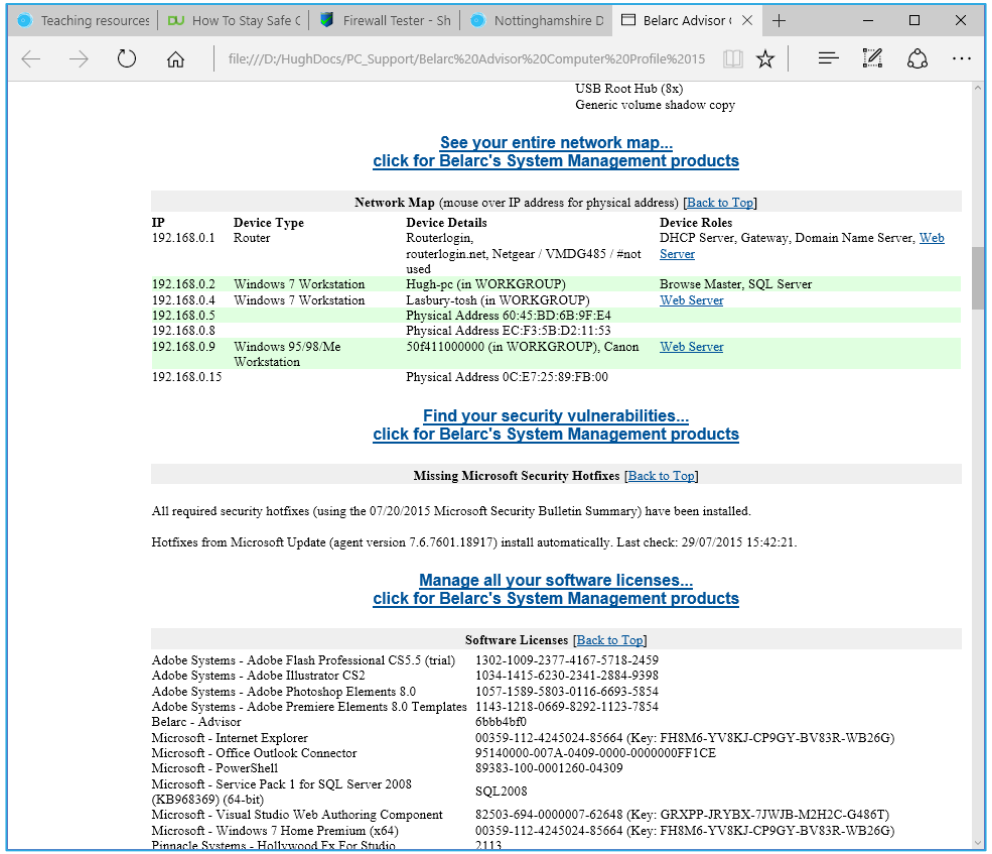
Other good practices

- Keep Microsoft Windows up-to-date through automatic updates
- Keep your browser(s) current by updating them when advised by the vendor
- Apply updates to your internet security packages – these are often called “definitions”
- Update other software you have installed from reputable suppliers e.g. Adobe, Apple, …
- If you use the internet on a shared computer, remember to use the InPrivate Browsing option in Internet Explorer or Microsoft Edge (other browsers have similar features)
- If you use wireless broadband, make sure it’s password-protected to prevent other people from using it
- Only install software from reputable, trusted suppliers and websites
- Email attachments can contain viruses so never open them unless you’re confident that they’re from a reliable source. If an email looks suspicious, it’s best to delete it.
- Use a tool like the excellent and free CCleaner to regularly ‘house-keep’ your PC – this gives you many options including deleting browsing history, downloaded files and much more

Prepare for the worst!

Even if it's not caused by malware, chances are your PC will "die" at some point!

- Regularly back up your personal files:
  - To a cloud-storage service and/or
  - To an external storage device – hard-disk or USB
- And, make sure your backed-up files are recoverable!!
- Keep an inventory of your installed software so you can recover it if the worst happens:
  - Keep any CDs in a secure location
  - Keep downloaded software in a folder that is covered by your backup regime
  - Use the excellent, free Belarc Advisor to record details of installed software including licence keys … don't forget to save the results and include them in your backup regime as well!



5B – Protect yourself

Be alert to Spam & Scam email

Do not open, forward or reply to emails which you suspect as being spam

Do not open attachments from unknown sources

Don’t click on links in emails from unknown sources

Check for obvious signs – poor grammar, mails not addressed to you personally, etc.

Apply e-mail filtering either through your mail client, webmail service and security software

Check junk mail folders regularly in case a legitimate email gets blocked by mistake

Never, ever include personal information such as username, password or bank details in an email

The vast majority of email sent every day is unsolicited junk mail.

Some of the risks:

- It can contain viruses and spyware
- It can be a vehicle for online fraud like “phishing”
- Unwanted email can contain offensive images
- Manual filtering and deleting is time-consuming
- It takes up space in your inbox

https://www.getsafeonline.org/protecting-yourself/spam-and-scam-email/

Avoid Fraud

Use strong passwords – mix letters, numbers and special characters. Keep them secret and don't use the same one for everything.

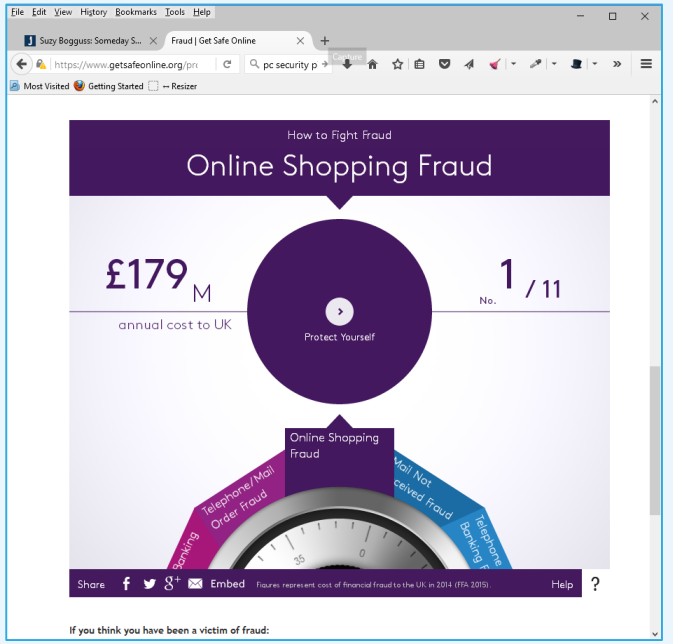
Never open email attachments unless you're confident that they're from a reliable source.

Beware of 'phishing' emails. These often look like they've come from a bank or similar institution and usually ask you to click a link to verify your identity. These emails should always be deleted.

When shopping online, only use reputable sites. The Shopsafe website has a directory of secure UK shops as well as advice on safe shopping.

Before entering any personal or payment information online, always check that you're on a secure website. This is indicated by a padlock icon at the top of the screen and a website address that starts with 'https://' (s='secure').

There's some great advice (and some rather disturbing statistics) at Get Safe Online



See also:

https://www.getsafeonline.org/protecting-yourself/safeguarding-identity/

Maintain your privacy

Ensure you always have effective and updated antivirus/antispyware software running.

Use secure websites when shopping or banking online.

Log out of secure websites when you have finished your transaction, as closing the window may not automatically log you out of the site.

Use strong passwords, change your passwords regularly and never reveal them to other people.

Make sure your home Wi-Fi network is secure.

Manage personal and financial documents securely.

Be cautious about who is trying to befriend you online including via email and social networks.

Use a disposable, anonymous webmail account for websites that demand an email address to register.

Some of the risks:

- Unencrypted email and most website interactions can be monitored, by your ISP.
- Via phishing - where an illicit email prompts you to click on a link to a bogus website which will collect your private or financial information.
- Using unsecured Wi-Fi networks.
- Not using secure websites when banking or making online payments, including those for purchases.
- Not using strong passwords, not regularly changing passwords, or revealing passwords to other people.
- Via spyware and viruses, including those that log your keystrokes to determine your online activity.
- Not managing personal or financial documents- both physical and electronic - securely.

https://www.getsafeonline.org/protecting-yourself/privacy/

https://www.getsafeonline.org/protecting-yourself/passwords/

Make provision for your ‘digital legacy’

Ensure your will includes your wishes regarding your online accounts and your login details, and lodge it safely.

The most important priority is to ensure that online accounts which involve payment information can be immediately closed down upon death to prevent fraud or identity theft or continued legitimate payments being taken. The respective companies or sites will be able to advise on what course of action to take.

Most social media, entertainment and other sites have procedures to cover the death of users – make sure that the sites you use most are listed.

When people die, they leave their physical assets and money to beneficiaries usually through a will.

Nowadays, most of us also leave behind various online assets, including our online profiles, email accounts, posts and other content in social media and content sharing accounts, and files stored in the cloud.

There is much confusion and an increasing amount of debate around what you should do to protect your digital assets for the benefit of those who survive and succeed you, or alternatively have accounts deleted.

See:

https://www.getsafeonline.org/protecting-yourself/digital-legacies/

Seven things to do …

1. Protect your PC by installing a firewall and anti-virus software – seriously consider investing in an integrated security suite that will cover both these aspects and usually much more
2. Keep your software up-to-date
3. Take regular back-ups of your personal files and use a (free) tool like Belarc to keep a catalogue of installed software
4. Protect yourself by using strong passwords when transacting online
5. Only enter sensitive information on secure websites (look for https://)
6. Be very careful handling hyperlinks and attachments in e-mails
7. Be circumspect about what you share, and whom you share it with, on social media

Nottinghamshire Alert is a messaging system that allows Nottinghamshire Police, Neighbourhood Watch and other public organisations to distribute messages concerning community safety to members of the public quickly and efficiently. Not just 'cyber crime' but worth signing up for their newsletter.

In your own time …

PLEASE TAKE SOME TIME TO REVIEW THIS MATERIAL AGAIN AND MAKE A COMMITMENT TO IMPLEMENT THREE OR FOUR OF THE KEY RECOMMENDATIONS BEFORE WE MEET NEXT.