Session 11

STAY 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"

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.

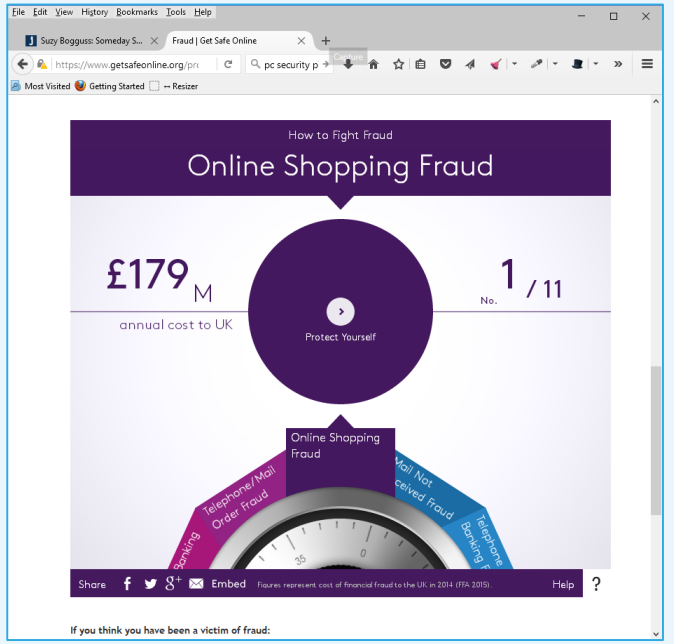
Never open email attachments unless you're confident that they're from a reliable source.

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/or 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

When doing anything of a sensitive nature on a shared PC, use the private browsing option

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.

Manage personal and financial documents securely.

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

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/

Four things to do …

1. Protect yourself by using strong passwords when transacting online
2. Only enter sensitive information on secure websites (look for https://)
3. Be very careful handling hyperlinks and attachments in e-mails
4. 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.

Project 01

CHOOSING A PASSWORD

Choosing a password

We're coming to a point in our learning journey where we will need to set up an e-mail account – and an associated secure password!

There is heaps of advice online about how to choose such a password – just Google it!

There are also websites that check the strength of a password – some better than others!

Obviously, use these as a guide and NEVER enter the real password you plan to use!

Here's one to try:

http://www.passwordmeter.com/

Key considerations:

- Make sure you choose a password you (and only you) can remember
- Do not write the password down – but by all means write down a prompt that makes sense to you (and only you)
- Use a password with at least 8 characters – mix numbers, upper and lower case letters and special symbols – more characters improves the security
- One technique I sometimes use is to choose the first letters of a song, poem, proverb or whatever, obfuscate them (mix them up), and then add a unique serial number at the end
- That way, I can safely write down the serial number for each different web site

An example of “obfuscation” and length

I chose the phrase:

“I love gardening but not when it rains” and turned that into !l9bNw!r

That would take just 9 hours for an average computer to crack

But, when I add 4 digits at the end, it would take 34 thousand years to crack!

So, I can keep a list something like this:

- M&S – 3465
- HSBC – 7893
- Microsoft – 9274

But only I know the preceding part !l9bNw!r

Check a password strength at https://howsecureismypassword.net/ but obviously **NEVER** enter your real or planned password

Which technique is more important?

Take the sentence:

"the wheels on the bus go round and round, round and round, round and round"

- Simple short:
  - twotbgrar – 22 minutes to crack
- Obfuscate it:
  - Tw0!69r@r – 275 days to crack
- Keep it simple, but make it longer:
  - twotbgrarrarrar – 13,000 years to crack
- Obfuscate it and make it longer:
  - Tw0!69r@rr@rr@r – 157 billion years to crack