Go Digital Newcastle
getting everyone online

Staying Safe Online

For Beginners

Digital Skills Sessions, by:

Newcastle Libraries

Newcastle City Council

Staying Safe Online

By the end of this session you will have learnt about:

- The risks associated with using the Internet
- Software that keeps your information safe on your computer:
  - Firewalls
  - Anti-Virus Software
  - Anti-Spyware Software
- How to recognise and prevent suspicious emails
- How to create strong passwords for use on websites
- How to shop safely on the internet
- How to recognize fraudulent websites
- Safe use of Internet browsers
- Cookies
- What to do if you encounter illegal information
- Where else to go for more information

The internet is a wonderful tool which has revolutionised the way we live our lives – enabling us to read the news, access entertainment, carry out research, book holidays, buy and sell, shop, learn, bank and perform many other everyday tasks.

Unfortunately, the features that make it easy for honest people to use can also be exploited by criminals and people intending to cause disruption. But you should not let fear stop you using the internet. There are a few simple precautions that can keep you and your personal information safe.

The Risks

The risks associated with going online result from either visiting malicious websites or inadvertently disclosing personal information.

The two main ways to avoid this are:

- Always be vigilant when supplying your personal or financial information online.
- Ensure that your Internet browser is up to date so that it can warn you of potentially harmful or criminal websites.

Making sure your computer is secure

It's important that your home computer is protected. You can do this with special programmes:

• Firewall software
• Anti-virus software
• Anti-spyware software

Firewalls

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. However, if your computer's operating system is Windows XP, Vista or 7, it will already have the built-in Windows firewall (*Fiona Syrett, Digital Unite tutor)*

.

Anti-Virus Software

Computer viruses are malicious programs that are designed to damage your computer or compromise your security. Before using the internet, it's important to make sure that your computer is protected by antivirus software. Without it, it's quite easy to download a virus unintentionally.

Antivirus software will protect your computer by preventing an attack by or detecting and removing any viruses. Some antivirus software can be downloaded for free from the internet – for instance, AVG and Windows Internet Security. Other types, such as Norton or McAfee antivirus software, have to be paid for with an annual subscription (approx £10-£40 per year).

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.

Anti-Spyware Software

Antispyware software helps protect your computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software such as Cookies.

- Many kinds of unwanted software, including spyware, are designed to be difficult to remove. If you try to uninstall this software like any other program, you might find that the program reappears as soon as you restart your computer.
- Microsoft Security Essentials is one example of a free download designed to help protect your computer against spyware and other types of malicious software

Emails

If you have an e-mail account, people may send you emails to try and access your private information such as bank account or credit card details. You may also get SPAM emails which are sent to thousands of people, usually advertising products or services. To protect yourself against these types of emails you can follow these tips:

- Don’t open an email from someone you have never heard of. Delete it immediately.
- If you do open it by accident, don’t click on any links. Never reply to a SPAM email
- You can put a block on unwanted SPAM email on your email account – this will also block most fraudulent emails too. Your e-mail account will alert you to some SPAM mail by placing SPAM in the ‘subject’ field].

- Use an up-to-date web browser as these can warn you against sites that may try to gain your information fraudulently.
- Don't give away your password or any personal information. No legitimate company will ever ask you for your password.
- If you suspect that an e-mail is fraudulent, hover your cursor over the link or logo (without clicking on it) so that it reveals the 'url' (the site to which you will go by clicking on the link). If this is a strange address, unrelated to the company name it is likely that the e-mail is SPAM.

Usernames and passwords

You often need to create usernames and passwords to register on certain websites.

Username: A username can be anything you want it to be. You may not want to use your real name as this will help keep your identity safe.

Password: You should choose a password that is memorable and not easy for someone else to guess.

The best types of passwords mix letters and numbers. This is known as a strong password as it is a lot more difficult to work out.

Examples of a bad password:

- password
- michaelsmith

Examples of a good password

- he770Mum
- Mik35th

- You use your username and password to log in to a website.
- It is safer to have different passwords for different websites.
- After you have used a website you should always log out/off.
- Remember: never give your password to anyone.

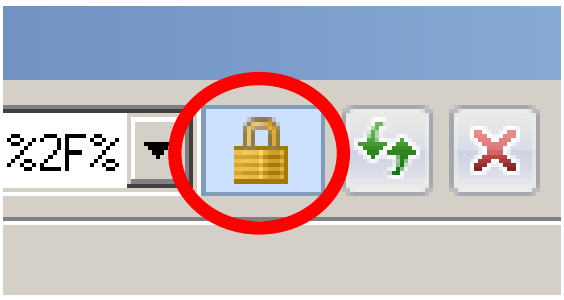
You can practice creating a strong password using the Microsoft Password Checker, at: https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx

Shopping Securely on the Internet

One of the benefits of the internet is the ability to shop from a wide range of stores and buy items on auction sites. To protect yourself when shopping online follow these tips:

- Only use online retailers that have a good reputation as 'high street' shops (John Lewis, Argos, well known supermarkets etc), or established brands.
- Follow the security advice carefully on websites that you trust as its there to help you.
- Never download illegal software, music or videos.
- Make sure that you are on a secure site when you need to give credit or debit card details.
- Secure sites often display a padlock symbol either next to the address or at the bottom right corner of the page.
- A secure site will start with: **https://** The 's' is what indicates it is a secure site.
- You can find out more information about staying safe on the internet by clicking on 'Safety and privacy' section on www.bbc.co.uk/webwise

P



The above show that the website owners have a digital certificate that has been issued by a trusted third party, such as VeriSign or Thawte, which indicates that the information transmitted online from that website has been encrypted and protected from being intercepted and stolen by third parties.

Recognising Fraudulent Sites

Sometimes, a website might look like the real thing but may not be genuine. There are several ways to tell if a site is or is not what it seems:

- Check for presence of a company / organisation address, phone number and/or email contact as these often indicate that the website is genuine. If in doubt, send an email or call to establish authenticity.

- Check that the website's address looks genuine by looking for misspellings, extra words, characters or numbers or a completely different name from that you would expect the business to have.

- Hover your mouse pointer over a link to reveal its true destination, (displayed in the bottom left corner of your browser). Beware if this is different from what is displayed in the text of the link (see 'Emails').

- If there is NO padlock in the browser window or 'https://' at the beginning of the web address to signify that it is using a secure link, do not enter personal information on the site.

- Websites which request more personal information than you would normally expect to give, such as username, password or other security details IN FULL may be malicious.

- Avoid 'pharming' by checking the address in your browser's address bar matches the address you typed. This will avoid you ending up at a fake site for example 'eebay' instead of 'ebay.

- Be wary of websites which promote schemes involving recruitment, receiving money for other people or advance payments.

- If you are suspicious of a website, carry out a web search to see if you can find out whether or not it is fraudulent.

- Be wary of websites that are advertised in unsolicited emails.

Safe Use of Browsers

The most popular internet browsers enable you to manage your settings, including allowing and blocking selected websites, blocking pop ups and browsing in private. Respective browsers will tell you to do this in slightly different ways, so we recommend that you visit the security and privacy section of their websites, or the help area of the browsers themselves:

- Internet Explorer

http://www.microsoft.com/en-gb/security/pc-security/ie9.aspx

- Opera

http://www.opera.com/security/advisory

- Chrome

http://www.google.com/chrome/intl/en/more/security.html

- Safari

http://www.apple.com/safari/features.html#security

- Firefox

http://www.mozilla.org/security/

Some More Tips…

Always ensure that you have the latest version of your chosen browser that your operating system will support. Always download and install the latest browser updates.

Ensure you have effective and updated antivirus/antispyware software and firewall running before you go online.

Remember that even if you turn on 'private browsing' this will only prevent other people using your computer from seeing which sites you have visited. Your internet service provider, search engine, law enforcement agencies and (if browsing at work) your employer, can still see sites you have visited.

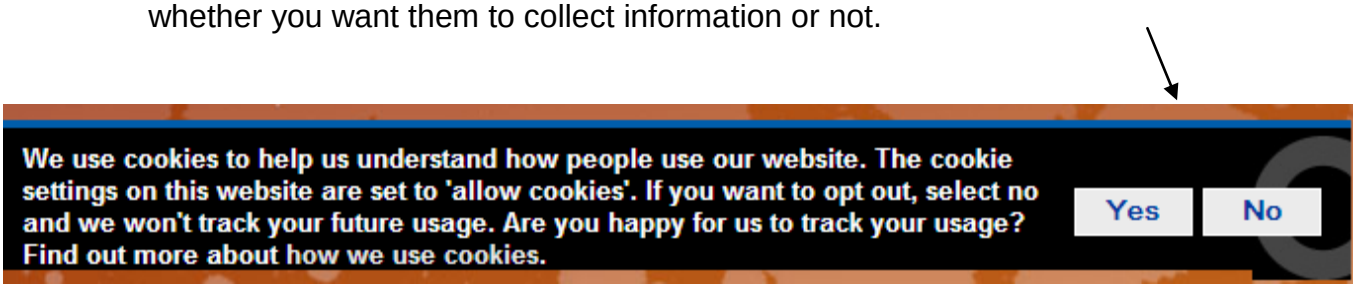
Always remember to log out of a secure website when you have completed your transaction, and before you close the browser. Just closing the browser does not necessarily log you out.

Cookies

Cookies are files on your computer, smartphone or tablet that websites use to store information about you between sessions. Most of the time they are harmless – carrying out tasks such as keeping track of your username so that you don't have to log into a website every time you visit it, and storing your usage preferences. However, some are used to track your browsing habits so that they can target advertising at you, or by criminals to build a profile of your interests and activities with a view to fraud.

Staying Safe:

- Set your browser to warn you when a cookie is installed. Note that some sites will not work if you block cookies completely.
- Some browsers will let you enable and disable cookies on a site by site basis so you can allow them on sites you trust.
- Use an anti-spyware program that scans for so-called tracker cookies.
- There are also cookie management programs that can delete old cookies and help manage them. In addition you can use settings in some browsers to delete unwanted cookies.
- Use a plain text email display instead of HTML email so that tracking files and cookies cannot be included in email files.
- UK websites must gain your permission to enable cookies – you can choose whether you want them to collect information or not.



Example of pop-up message taken from:
http://safe.met.police.uk/internet_safety/get_the_facts.html

What to do if you Encounter Illegal Information

- If you come across content that you consider to be illegal such as child abuse images or criminally obscene adult material, you should report this to the Internet Watch Foundation: www.iwf.org.uk.
- If you come across content that you consider illegal such as racist or terrorist content, you should report this to the Police.

Further Information

The contents of this guide are based on trusted and freely available advice taken from the websites below where you can also find more information about staying safe online:

BBC First Click:
http://downloads.bbc.co.uk/connect/BBC_First_Click_Beginners_Guide.pdf

Digital Unite: http://digitalunite.com/guides/internet-security

Get Safe Online: https://www.getsafeonline.org/

Google: Online Safety Tips:
http://www.google.co.uk/intl/en/goodtoknow/online-safety/

Useful Links

Microsoft Security Essentials:
http://windows.microsoft.com/en-gb/windows/security-essentials-download

AVG: http://free.avg.com/gb-en/homepage

Norton: http://www.symantec.com/en/uk/

McAfee: http://home.mcafee.com/

Jargon Buster

The following is a list of commonly used terms relating to Internet safety and security that you may find useful:

Term	**Meaning**
Anti Virus	Programmes that you can install on your computer which will identify and protect you from viruses and spyware.
Cookies	Files on your computer, smartphone or tablet that websites use to collect and store information about you between sessions.
Copyright	One danger of using the internet is inadvertent copyright infringement – copying or downloading software, videos, music, photos or documents without realising that they are protected.
Inappropriate content	Illegal or disturbing website content.
Malware	Malware is short for 'malicious software', and similarly to 'spyware', is a term to describe unauthorised programs that are downloaded to your computer and cause disruption or damage to software or hardware. Sometimes, malware is designed to use your computer's 'resources' (such as memory) and other times it is simply designed to create an unpleasant experience. Malware can be accidentally downloaded through spam emails, or when downloading files from untrustworthy websites, such as file-sharing websites.
Online fraud	Usually perpetrated by fake shopping, banking, charity, dating, social networking, gaming, gambling and other websites.
Pharming	Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent.
Phishing	E-mails or requests designed to obtain your personal and/or financial information and possibly steal your identity.
SPAM	Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail.
Viruses and spyware (known as malware)	Programmes built into certain websites that can damage the files on your computer.

Online Safety Scorecard

Questions	Things to look for…	Where to look…	Scoring criteria		
Is the site written by a respected and reliable source?	• .gov.uk - Government • .ac.uk - University or academic institution • .nhs.uk - NHS • .org.uk – Charity or non-profit organisation • .com – Commercial • .co.uk - Commercial	In the adress bar where the URL stands	.gov.uk .ac.uk .nhs.uk .org.uk .com .co.uk	Score 1 Score 0	
Is the information up-to-date?	Are the pages dated? This should include the dates the site/page was created and or last reviewed	Usually on the bottom of the page.	Pages dated Pages not dated	Score 1 Score 0	
Are all the links working correctly?	Broken links reflect a poorly maintained site	When you click on a link you are redirected to a "404 Error Page – Page cannot be found"	Links working Links broken	Score 1 Score 0	
Does the site have sufficient privacy protection?	Does the site require you to register, enter your e-mail address, or answer personal questions before you can access information? Personal information may be sold or shared	Does not apply to online shopping sites or social media sites.	No information required Information required	Score 1 Score 0	
Is there a privacy policy?	If personal information is collected, does the site have a privacy policy that clearly states how the information will be used?	Usually in the link collection on the bottom of the page. Links may be called 'Policies', 'Privacy Policy', 'About' etc.	Privacy policy No privacy policy	Score 1 Score 0	
				Total Score (out of 5)	

Newcastle Libraries Disclaimer

The internet is a worldwide network of computers, and we have no control over the information available on it. Information available on the Internet may be inaccurate, biased or of poor quality. We can accept no responsibility for the validity or quality of information available.

We cannot vouch for the security of internet sites; therefore you should take care when giving out personal details, follow the advice in this guide and be aware that any financial transactions are undertaken at your own risk.