Safe Internet Use

The internet has revolutionised the way we live our lives – enabling us to read the news, enjoy entertainment, carry out research, book our holidays, buy and sell, shop, network, learn, bank and carry out many other everyday tasks. However, there are a number of risks associated with going online. These result from either visiting malicious websites or inadvertent disclosure of personal information.

The risks

The risks of visiting malicious, criminal or inappropriate websites include:

Viruses and spyware (collectively known as malware).

Phishing, designed to obtain your personal and/or financial information and possibly steal your identity.

Fraud, from fake shopping, banking, charity, dating, social networking, gaming, gambling and other websites.

Copyright infringement – copying or downloading copyright protected software, videos, music, photos or documents.

Exposure to unexpected inappropriate content.

When you use the internet, your browser (for example Internet Explorer, Opera, Chrome, Safari or Firefox) keeps a record of which sites you have visited in its 'history'.

When you use the internet, the websites you visit are visible to your Internet Service Provider, who will record details of your internet usage in accordance with legal requirements.

Use the internet safely

It is very easy to clone a real website and does not take a skilled developer long to produce a very professional-looking, but malicious site.

Being wary of malicious, criminal or inappropriate websites:

Use your instincts and common sense.

Check for presence of an address, phone number and/or email contact – often indications that the website is genuine. If in doubt, send an email or call to establish authenticity.

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

Roll 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 from either another website or an email.

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 user name, password or other security details IN FULL, are probably malicious.

Avoid 'pharming' by checking the address in your browser's address bar after you arrive at a website to make sure it matches the address you typed. This will avoid ending up at a fake site even though you entered the address for the authentic one – for example 'eebay' instead of 'ebay.

Always get professional advice before making investment decisions. Sites that hype investments for fast or high return – whether in shares or alleged rarities like old wine, whisky or property – are often fraudulent.

Be wary of websites which promote schemes that involve the recruitment of others, 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 from strangers.

Secure websites

Before entering private information such as passwords or credit card details on a website, you can ensure that the link is secure in two ways:

There should be a padlock symbol in the browser window frame, that appears when you attempt to log in or register. Be sure that the padlock is not on the page itself … this will probably indicate a fraudulent site.

The web address should begin with 'https://'. The 's' stands for 'secure'.

The above indicate 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. In other words, the communication between you and the site owner is secure, however a certificate is no guarantee that the site owner is the organisation or person you think you are communicating with … you need to carefully check the web page address to confirm authenticity.

When using websites that you do not know, look for an Extended Validation (or EV-SSL) certificate, which indicates that the issuing authority has conducted thorough checks into the website owner. The type of certificate held can be determined by clicking the padlock symbol in the browser frame which will launch a pop-up containing the details.

Do also note that the padlock symbol does not indicate the merchant's business ethics or IT security.

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 innocuous – 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.

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.

Safe use of browsers

The most common internet browsers enable you to manage your settings such as 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

Opera

Chrome

Safari

Firefox

Some browsers also have the ability to identify fraudulent websites by default.

Always ensure that you are running the latest version of your chosen browser that your operating system will support. Also, be sure to download and install the latest updates.

It is important to remember that turning on the private browsing setting or deleting your browsing history 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 possibly (if browsing at work) your employer, will still be able to see which sites you have visited or keywords you have searched for.

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

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

What to do if you encounter illegal material

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 IWF: 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.