BRIT COLLEGE

INVEST IN EDUCATION

Student Internet & Online Security

The internet has transformed 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 dangerous websites or accidentally revealing personal information.

The Risks

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

- **Viruses and spyware** (collectively known as malware)

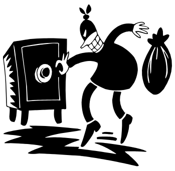
  Malware infects devices and can cause damage to the system, loss of information or leakage of confidential information.

- **Identity theft**

  Criminals can steal your identity through many ways so that they can pretend to be you and use your personal information for their own benefit; for example, using your financial information to buy goods.

- **Phishing** - designed to gain 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 software, videos, music, photos or documents that is protected by copyright law is a crime. The creator of these materials can have you persecuted by law. Copying work from the internet for assignments and claiming them as your own also violates copyright law.

- **Exposure to unexpected inappropriate content**

  You may accidentally see offensive or inappropriate content online through web searches, pop up adverts, by clicking unknown links or on social media.

Web History

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'.

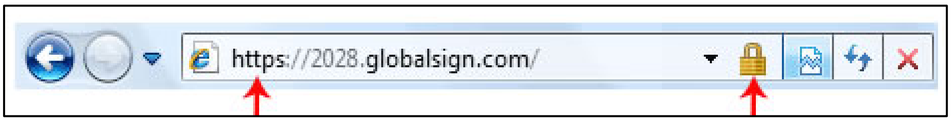
It is important to remember that turning on the private browsing setting or deleting your browsing history will only prevent other people using your computer from seeing which sites you have visited. Your internet service provider, search engine, law enforcement agencies and possibly your employer (if browsing at work), will still be able to see which sites you have visited or keywords you have searched for.

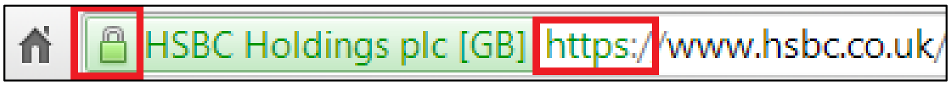
Secure Websites

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 address bar 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’.





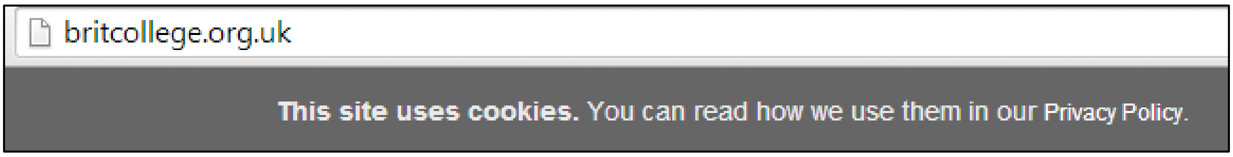
The above indicate that the website owners have a certificate to show that their website is secure. This means that the information you enter (such as your card details) are protected from being stolen by criminals.

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 user name 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.



britcollege.org.uk

This site uses cookies. You can read how we use them in our Privacy Policy.

- Use an anti-spyware program that scans for so-called tracker cookies. You can also 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.

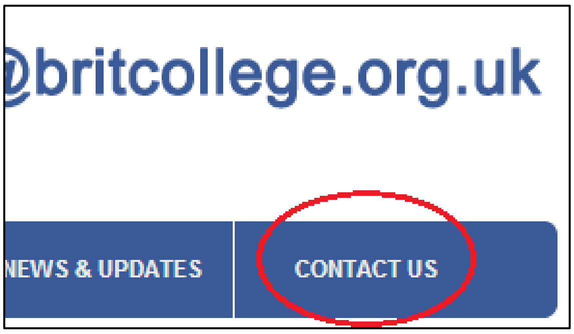
Identifying Risks Online

It is very easy for criminals to copy a website and create a fake that looks exactly like the original. For example, you may accidentally use a fake website to do your banking. This would mean that your bank details would be available to the criminals who have created the fake site.

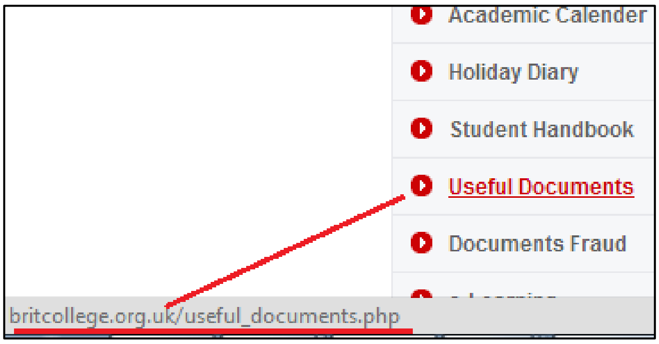
Look out for these signs to make sure the sites you visit are safe:

- Check that the website's address is genuine by looking for misspellings, extra words, characters or numbers or a completely different name from that you would expect the business to have. Look at the address bar after you arrive at a website to make sure it matches the address you typed - for example 'www.ebay.co.uk' instead of 'www.e.bay.co.uk'

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



- 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.



- Websites which request more personal information than you would normally expect to give, such as user names, password or other security details IN FULL, are probably malicious.

- 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.

- Always get professional advice before making investment decisions. Sites that hype investments for fast or high return – whether in shares or property – are often fraudulent. If something sounds too good to be true, it probably is!

- Be wary of websites which promote schemes that involve the recruitment of others, receiving money for other people or advance payments. Do not click on adverts or pop-up adverts.

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.

Mobile Security

If you use the internet on your mobile, you could be exposing yourself to many risks.

- **Open WiFi Networks**

  Connecting to a wireless network that does not require a password leaves you open to threats as it is unsecure. Any information you enter through an unsecured network can be accessed by others and used by them. Your mobile phone and other portable devices are especially vulnerable to this.

- **Mobile Virus**

  Like computers and laptops, mobile phones can also be infected by viruses. These can be unknowingly downloaded alongside apps, by opening attachments or by clicking unknown links in text messages and chats. These viruses can collect your personal information and pass them onto a third party to use, or damage your phone. They can also spread to your PC/laptop if you connect your mobile.

- **Protection**
  You can install virus scanners to protect your mobile against these threats. Your network carrier or operating system may provide updates which you should install to keep yourself protected.

Internet Do’s and Don’ts

✘ Do not illegally download free media such as films, music, software etc. Viruses can install themselves along with the free download.

✘ Do not overshare personal information on social media accounts. No matter how private your profile is, it is still on the internet and therefore available to others, so be mindful about what you post.

✘ Do not store payment information online. This can be used by hackers to make purchases through your bank account.

✘ Do not download attachments or click any links in an email from an unknown sender. Do not provide any personal information such as passwords, even if the email seems genuine. Use caution and delete any suspicious emails.

✘ Do not access the internet through unsecured WiFi networks as these leave you open to threats. If you do, make sure you do not enter any personal information.

✓ Make sure your passwords are secure and kept secret. Change your passwords regularly and avoid using the same password for all accounts.

✓ Always remember to log out of your accounts before you close your web browser. Closing the browser does not necessarily log you out.

✓ Make sure you are running the latest version of your browser and install any recommended updates.

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

✓ Use your instincts and common sense.

If you require any more information or support, feel free to contact the IT Department who will be more than happy to help!

Brit College, 602 Commercial Road, Limehouse Lock ,London E14 7HS
T: +44 (0) 207 265 8497 **E**: info@britcollege.org.uk