

## A guide to keeping safe online for learners

### Introduction

The internet can be incredibly useful and fun to use. Being able to access and use the internet means you can keep in touch with family and friends, shop and bank online, pay bills, find any information you need from weather forecasts to bus timetables, and book tickets and appointments. You can also keep up to date with the news, read magazine articles, share photos, watch videos, listen to the radio online and much, much more.

However, anyone who uses the internet should be aware of the potential risks, and the best ways to stay safe online. Don't let the potential risks put you off using the internet, as some simple steps can help you to stay safe online. This guide will explain some of the main risks when using the internet, and give advice for ways to stay safe and secure.

### Use strong passwords and keep them safe

If someone else knows your passwords then they may be able to access personal information about you. Therefore it is important to keep your passwords private, and make them hard for others to guess. The harder it is for someone to guess your password, the safer your personal information will be. Here are some simple ways to make your passwords stronger:

- Make your passwords at least 8 characters long.
- Include a combination of upper case and lower case letters, numbers and symbols (for example *daFFodils1*)
- Do not include your real name, user name or scheme name in passwords.
- Change your passwords regularly.
- Don't use the same password for everything.

Remember to never write your password down or disclose it to anyone, and if you think someone else may know it then change it immediately.

### Using email safely

Email is a great way to keep in touch with family and friends and also to receive information from organisations you are interested in.

However, some online criminals send out emails called "phishing" emails (pronounced "fishing"). "Phishing" means being tricked into sharing personal information, such as banking details or passwords, with online criminals. These emails look like they come from banks or retailers, and are

trying to trick you into sharing your personal details. The emails can be very sophisticated and well designed, and it can be difficult to tell a phishing email from a genuine email.

Remember, your bank (and any other reputable company) will **never** send you an email which requires you to disclose any personal information, or link to a website asking you for this information.

Follow these simple steps to make sure you use email safely:

1. Never respond to an email asking you for personal details such as passwords or pin numbers.
2. Do not open attachments to emails unless you are absolutely certain they have been sent from someone you know and trust
3. Do not click on links in emails that you are not certain come from someone you know or trust.

### **Deleting internet browsing history**

Internet browsers sometimes store information that has been entered by the user on a website (such as usernames, passwords, address details and so on). If you are using a communal computer, especially for online banking or shopping, then you should delete the browsing history each time you have finished using the computer. Once you know how, this is quick and easy to do.

### **Using internet forums, chat rooms and social networking sites (eg Facebook)**

Internet chat rooms and discussion forums are areas on the internet where people can communicate with each other in writing. Social networking sites, such as Facebook, are websites that allow people to stay in touch with family and friends, share photos and videos and organise events.

When using internet forums and chat rooms, you should never disclose any personal information (whether in a public chat room or forum, or in private chat feeds or messages). This includes real name, address, telephone number, usernames and passwords, any banking details and date of birth. Usernames for chat rooms and forums should be pseudonyms instead of real names (for example a username like "Joe28" instead of "JoeBrown" or "Joe\_Leicester").

When using social networking sites you should also be cautious about what information you share and who can access your "profile" (your area of the website). The first thing you should do is take the time to learn about the privacy settings, and to make sure your profile is private, and can only be seen by the people you choose. Even then you should be careful about what information you post online.

### Shopping online safely

Shopping online can be very convenient, and you can often get cheaper deals than in the shops on the high street. However there are some risks when buying online – your goods may not turn up, or they may not match the description. There may be delays, poor after sales service, or misuse of your bank or credit card details. When shopping (and banking) online, you should be sure that when you type in personal details such as credit card details, that you are doing so on a secure web page. A secure webpage should have a padlock displayed in the browser window (rather than on the web page itself) – this will usually be in towards the bottom right of the browser window, or to the right of the URL bar.



The website address should also begin with **https://** (rather than **http://**). This shows you that any personal information you will enter on this page, such as credit card information, should be secure. If you are not sure that the page is secure, then do not enter any personal information, particularly banking details.

Other tips for shopping online safely are:

1. Look for evidence on the website of a physical address and telephone contact details.
2. Be particularly careful when buying from overseas companies.
3. Check the sellers privacy policy and returns policy.
4. If a deal looks too good to be true, it probably is.
5. Buy from reputable companies.
6. Be extremely wary of anything that is offered in an unsolicited (“spam”) email.
7. Use an appropriate, safe means of online payment to get some protection against non-delivery such as “PayPal”. PayPal includes buyer and seller protection, allows instant payments and gives buyers a degree of comfort that the identity of a seller has been confirmed.

### What next?

For more information and advice about getting online:

UK Online Centres offer free information, advice and courses to help you get started on computers and the internet. To find your nearest centre, call 0800 77 1234 or visit [www.ukonlinecentres.com](http://www.ukonlinecentres.com)



BBC First Click offers a free downloadable step – by – step guide to help you get to grips with internet basics.

[http://downloads.bbc.co.uk/connect/BBC\\_First\\_Click\\_Beginners\\_Guide.pdf](http://downloads.bbc.co.uk/connect/BBC_First_Click_Beginners_Guide.pdf)