RHACC

Richmond and Hillcroft
Adult Community College

How to stay safe online

Email and online shopping can make our lives a lot easier, but they also create new opportunities for fraud. Online scams are becoming increasingly common and sophisticated, so it's good to know how to keep yourself safe.

What are online scams?

Online scams take place when criminals use the internet to try to con people into giving them money or personal information. It’s estimated that £670 million is lost every year by victims of the most common online scams.

The most common online scams to look out for include:

Computer viruses

Computer viruses (sometimes called malware) are rogue programs which can spread from one computer to another. You may be sent an email with an attachment which when you click on it will release a virus.

Criminals can then use this to take control of your computer, or the virus may scan your computer for personal information. It can also slow your computer down, send out spam email or delete files.

You may even get a phone call from someone claiming to be from a well-known software company like Microsoft, saying there’s a problem with your computer and needing to get access to your it, including your personal details.

> Legitimate IT companies never contact customers in this way. This is a common phone scam – hang up straight away.

Online shopping

Be cautious when entering your credit card details and personal information on a shopping website, there's more information on this topic below.

Fake websites

Scammers can create fake websites which look official requesting you to provide personal or financial information. For example, a fake bank website may be set up asking you to update your account or security information. Often they will look very similar, and only a few tiny details may be different.

There are also websites which are set up to look like a copy of a service offered by government websites. For example, there are websites which offer to help you apply for a passport renewal or a new driving licence. Although they are not necessarily illegal, these websites charge extra money if you use them rather than going directly through the official government department.

> If you aren't sure about which website to use, go through GOV.UK, the Government's official website, to find what you need.

Email scams

Scammers will send bogus emails in the hope that people will enter their personal details. They may direct you to a fake website, trick you into thinking you've won a lottery or prize, or pretend to be someone you may know who has been stranded somewhere and needs money.

Some emails may also have a link or file attached for you to click on or open. These are sometimes called spam or junk emails. Opening these links or downloading the files may be harmful to your computer.

> If you see a suspicious email, don't reply with your details or open any links or documents. Delete the email straight away. If the email claims to be from an organisation, phone them directly using the phone number found on their official website and ask them.

Relationship scams

Scammers can use social networks such as dating websites or chat rooms. Once they've gained your trust, they'll start asking you for money, often by telling you an emotional or hard luck story.

Trust your instinct. If something feels wrong, it probably is. These tricks are hard to spot, so it's always worth talking to a friend or relative about it, especially if things seem to be moving fast. Never send the person money or give them your account details.

Be careful if the person starts moving away from the chat room or dating site to communicating by email or text message. If you arrange to meet, make sure it's in a public place, tell someone else where you're going and don't give away information too quickly.

Health scams

False and misleading claims may be made about medical-related products, such as miracle health cures, and fake online pharmacies may offer medicines cheaply. However, the actual medicine delivered to you can turn out to be poor quality, and even harmful to your health.

> Check if an online pharmacy website is legitimate by clicking on the 'Registered Pharmacy' logo on the website's home page – this should lead to the General Pharmaceutical Council website.

What should I do if I think I've been a victim of an online scam?

Scammers are constantly finding new ways to trick people and online scams are changing all the time. It's not unusual for people to get tricked, so don't suffer in silence and don't be embarrassed to report it.

If you're worried that your computer is not working properly or think that it may have a virus, then talk to a computer technician.

Contact Action Fraud

Contact the police then Action Fraud if you're worried something might be a scam, or you think you've been scammed. The information you give to Action Fraud can help track down the scammer

Report fraud

How can I protect my computer and stay safe online?

As well as being aware and cautious of common online scams, there are a few simple steps you can take to protect your computer.

1. Install security software (e.g. anti-virus, anti-spyware and firewall)

- Anti-virus software will look for and remove viruses before they can infect your computer.
- Anti-spyware software prevents unwanted adverts from popping up, tracking your activities or scanning your computer for personal information.

The best option for beginners is to buy a 'package' from a reputable provider (such as McAfee or Norton) which will include a range of security software. You can download these programs from the internet or visit a retail computer store for guidance.

Your internet service provider might also offer security software as part of your internet deal. There are also popular free security software programs available to download online, such as AVG, Avast and Microsoft Security Essentials.

2. Keep your computer updated

Every computer has an operating system (such as Windows or Mac) which is software that organises and controls all hardware and programs.

Your computer can be better protected from viruses if you keep the operating system updated. You should receive notifications when new updates are available, but you can also update your system manually.

3. Protect your wireless network

If you have a wireless router, check that your wireless network is secure so that people living nearby can't access it. It is best to set up your network so that only people with a wireless 'key' (i.e. password) can connect to your network.

If your network is secured by a password, users will be prompted for a password when they try to access the network for the first time and there should be a padlock symbol next to your wireless network. If this doesn't happen, your network isn't protected and anyone can connect to your network.

Read the instructions that came with your router to find out how to set up a wireless key and make your network more secure.

How can I protect my privacy on social networks?

Social networks (e.g. Facebook and Twitter) are a great way to keep in touch with family and friends, make new friends, look at photos, find out about local events and much more.

However, on any social networking site, you must guard against people who want to steal your personal information. Use the privacy features on the site to choose who can see your profile and your posts, and avoid publishing information that identifies you, such as your telephone number, address or date of birth

Keep yourself safe on social networks

- Get details on how to protect yourself on Twitter
- Read info on how to change your Privacy on Facebook

How can I stay safe when shopping and banking online?

Shopping online can be quick and convenient, but you need to protect your financial information.

Make sure that you're using a secure website before entering any personal details. There are ways to spot that a website is secure, including:

- the website address starts with 'https' - the 's' stands for secure
- the address bar is green, which is an additional sign that you're using a safe website
- a padlock symbol in the browser where the website address is(but don't be fooled if the padlock appears on the page itself)
- a current security certificate which is registered to the correct address. (this appears when you click on the padlock)

Be aware that a padlock symbol is not an absolute guarantee of safety. If you ever have doubts it's best to leave the page.

To help protect you while shopping or banking online, follow these simple tips:

- Beware of pop-up messages that warn you about a website's security certificate. They may direct you to a fake website that's designed to get you to hand over your security details.
- Use online retailers with a good reputation, as either high-street shops or established online stores.

- Look for the company’s full contact details. A reputable company will always display this information on its website.
- Cross-check information on the internet to see if anyone has experienced problems with the retailer.
- Find out where the seller is based because consumer rights vary from country to country. To find out more information about buying from sellers based in other EU countries, you can visit the UK European Consumer Centre website.
- Use the same credit card for internet transactions only. If anything goes wrong, you can always cancel this card.
- If a deal looks too good to be true, it probably is, and be cautious of anything offered in an unsolicited email.

Where can I find more information?

You may find these links useful

- Visit Get Safe Online for useful information
- Find out more about scams
- Download the Met Police's Little Book of Big Scams
- Download an information leaflet: Internet Security (PDF, 358 KB)
- Download an information guide: Avoiding scams (PDF, 4 MB)

You may find these links useful

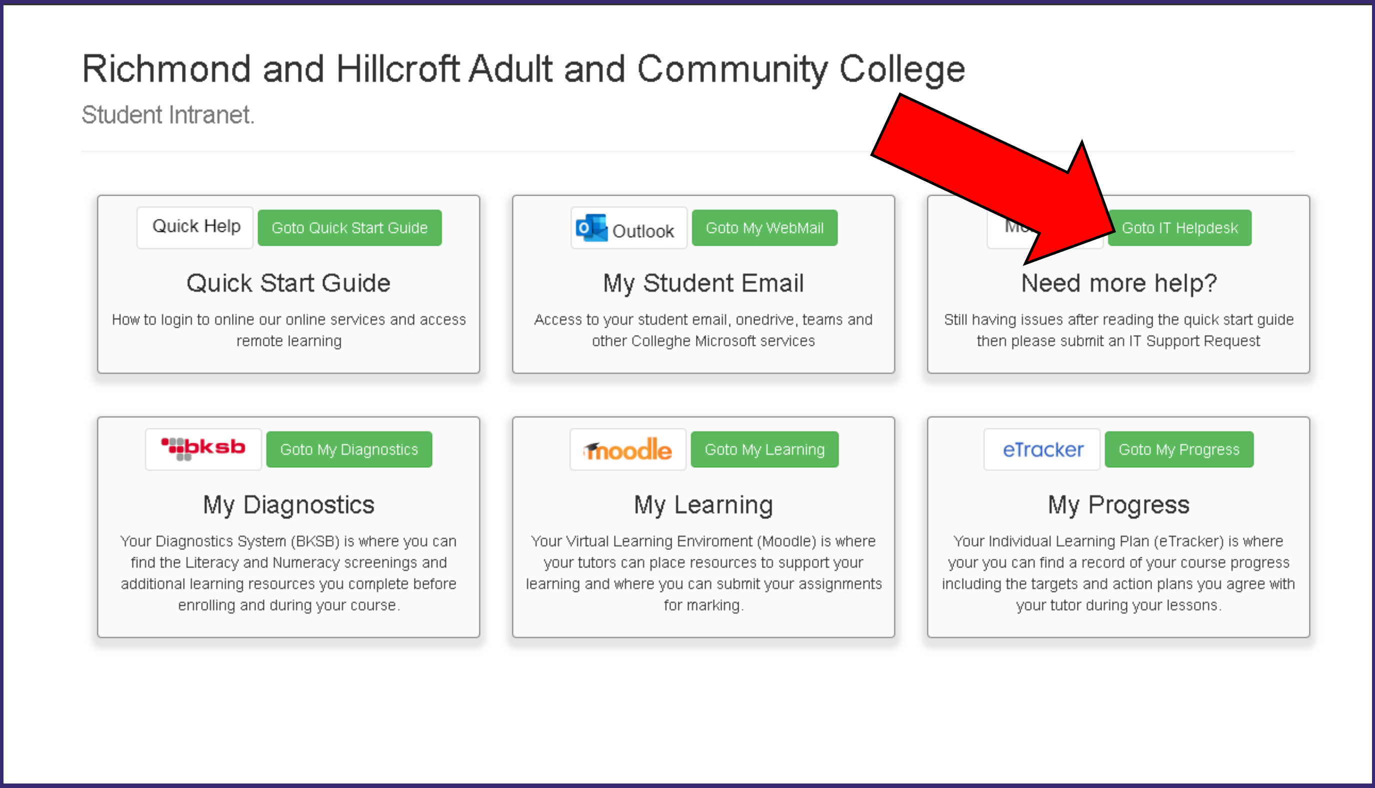
- Visit Get Safe Online for useful information
- Find out more about scams
- Download the Met Police's Little Book of Big Scams
- Download our information leaflet: Internet Security (PDF, 358 KB)
- Download our information guide: Avoiding scams (PDF, 4 MB)

If you are having an issue and would like our help,

Please contact the IT services using the link below

IT Services Helpdesk form

or go to my.rhacc.ac.uk and choose IT Helpdesk



Richmond and Hillcroft Adult and Community College

Student Intranet.

Quick Start Guide

How to login to online our online services and access remote learning

My Student Email

Access to your student email, onedrive, teams and other Colleghe Microsoft services

Need more help?

Still having issues after reading the quick start guide then please submit an IT Support Request

My Diagnostics

Your Diagnostics System (BKSB) is where you can find the Literacy and Numeracy screenings and additional learning resources you complete before enrolling and during your course.

My Learning

Your Virtual Learning Enviroment (Moodle) is where your tutors can place resources to support your learning and where you can submit your assignments for marking.

My Progress

Your Individual Learning Plan (eTracker) is where your you can find a record of your course progress including the targets and action plans you agree with your tutor during your lessons.