Safeguarding
and Wellbeing

BE CYBER SECURITY SAVVY

Start reading...

BE CYBER SECURITY SAVVY

Our top 10 tips to help you stay safe online

We are spending more time than ever online, whether that is working from home, communicating with our friends and family, or studying remotely. It is essential in our tech-focussed world, to be cyber security savvy.

We have put together our 10 tips to stay safe online:

1. Check the website

URL and web page security Before you visit a new website, and potentially expose sensitive personal information, ask yourself- is this website safe? Just because you may have received a link to a website, it doesn't necessarily mean it is safe. Before clicking the link, hover your mouse over the link to display the real URL at the bottom of your browser. This will show what it's linked to and if it's safe to proceed.

Once you have checked the URL is safe, ensure the webpage you are visiting is secure. The website must use HTTPS at the start of the URL or have a padlock displayed in the browsers navigation bar. This means the website you are using has a trusted SSL certificate and your connection is protected. If the website does not have a padlock, do not enter your password, bank details or any other sensitive information.

BE CYBER SECURITY SAVVY

2. Be aware of phishing

Phishing scams can come in the form of emails, text messages or instant messaging. They are often used to steal important data including login credentials and credit card details. These attacks are by hackers impersonating a person or an organisation, and can look genuine.

Never provide your personal or financial information to a website that has come from a link sent in one of these formats, especially if you are not expecting it.

Always contact the organisation directly to see if they sent the original message. You can also go to their website, without clicking on the link, if you suspect this is a phishing attempt.

3. Always check the senders email address

If you think an email may not be legitimate, an easy way to check is by looking at the sender's email address. Misspellings and typos will indicate that they are not who they say they are.

Scammers often change their email address to make it look like they are from the organisation they are pretending to contact you from. The email address can also be something entirely different to the sender's name.

If you receive an email that has an incorrect or misspelt email address, do not click on anything and delete the email immediately.

BE CYBER SECURITY SAVVY

4. If it looks suspicious, it probably is

If you have a feeling that something is not quite right, then it most probably is important to treat it this way. If you are not expecting to receive something from a sender, ensure the source is legitimate before going any further.

Be aware of fake calls, emails and messages. Many scams state that you are entitled to a refund or a claim if you fill out a form. Unfortunately, these are an easy way for hackers to get your personal and financial details. Therefore, if it looks too good to be true, it probably is!

Never give information to an organisation requesting payment. Criminals often target students pretending to be from legitimate organisations including the UK Home Office, UK Visas and Immigration and education agents, demanding money or a fine for a non-existent problem. You can report these types of calls to your Student Adviser.

5. Use secure passwords

Passwords are the first barrier against unauthorised access to your personal information. Using weak passwords, or the same for multiple accounts, can leave you vulnerable and make life easy for hackers.

When choosing a password, it is important to pick something that is not easy for potential hackers to decipher i.e. your middle name, pet names or your home town.

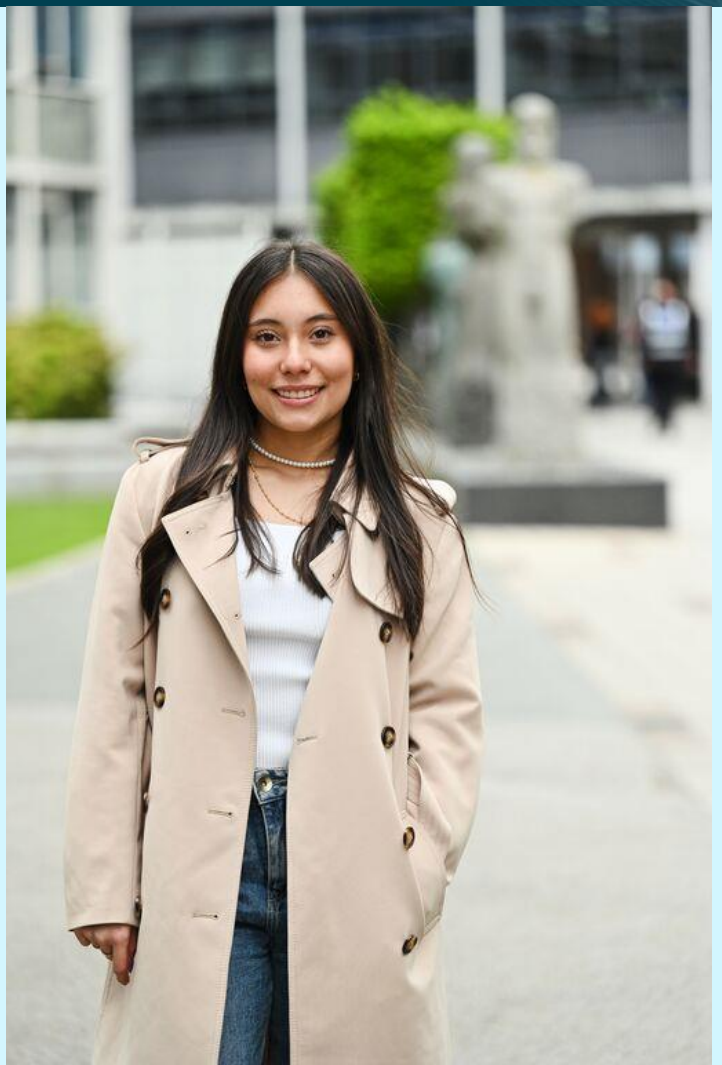
Use something that is hard to guess and is a combination of numbers, letters and symbols, and not related to your personal information in any way. Ensure you use completely different passwords for different accounts and never write passwords down.

BE CYBER SECURITY SAVVY

6. Protect your information

Always ensure your devices are protected by locking them when you aren't using them, particularly if you are in a shared or public space. Leaving devices unlocked is an easy way for your accounts to be hacked, as well as a potential GDPR breach which can have costly implications.

No matter how long you are away from your device, even if it's for a couple of seconds, always ensure all data is a away.



7. Protect your devices

As well as protecting your information, it is important to ensure all of your devices are protected by an antivirus software. There are various antivirus options available online to suit all budgets.

Often, devices do not come with this preinstalled and it is a package that needs to be purchased separately, therefore it is essential that you check you are protected before using your device.

Once you have antivirus software, keep this up to date and run regular scans to help protect you from malware and viruses, which could potentially compromise your personal information. This will also maintain maximum health of your device.

BE CYBER SECURITY SAVVY

8. Always log out of accounts

If you are working on a shared network, or using a public/unsecure Wi-Fi connection, ensure you always log out of your accounts when you have finished using them.

Often just closing the browser down does not fully shut down your session and this could leave your information/account vulnerable to potential hackers, or someone using the device after you.

Finally, be aware of checkboxes when you log into certain websites that let you stay logged in or remember passwords. Always ensure you have logged out of any accounts once you have finished using them.

9. Sharing isn't always caring

Sharing things online has become the norm to many of us, particularly when it's good news or something we are excited about.

However, it is worth being aware that posting pictures and personal information can actually make you a prime target for identity theft.

It is important to know who has access to your information on social media accounts. Make sure you review your sharing settings regularly and stay up-to-date with any platforms updates. All it takes is gaining a few minor details and a hacker can use their detective skills to compromise your personal and financial data.

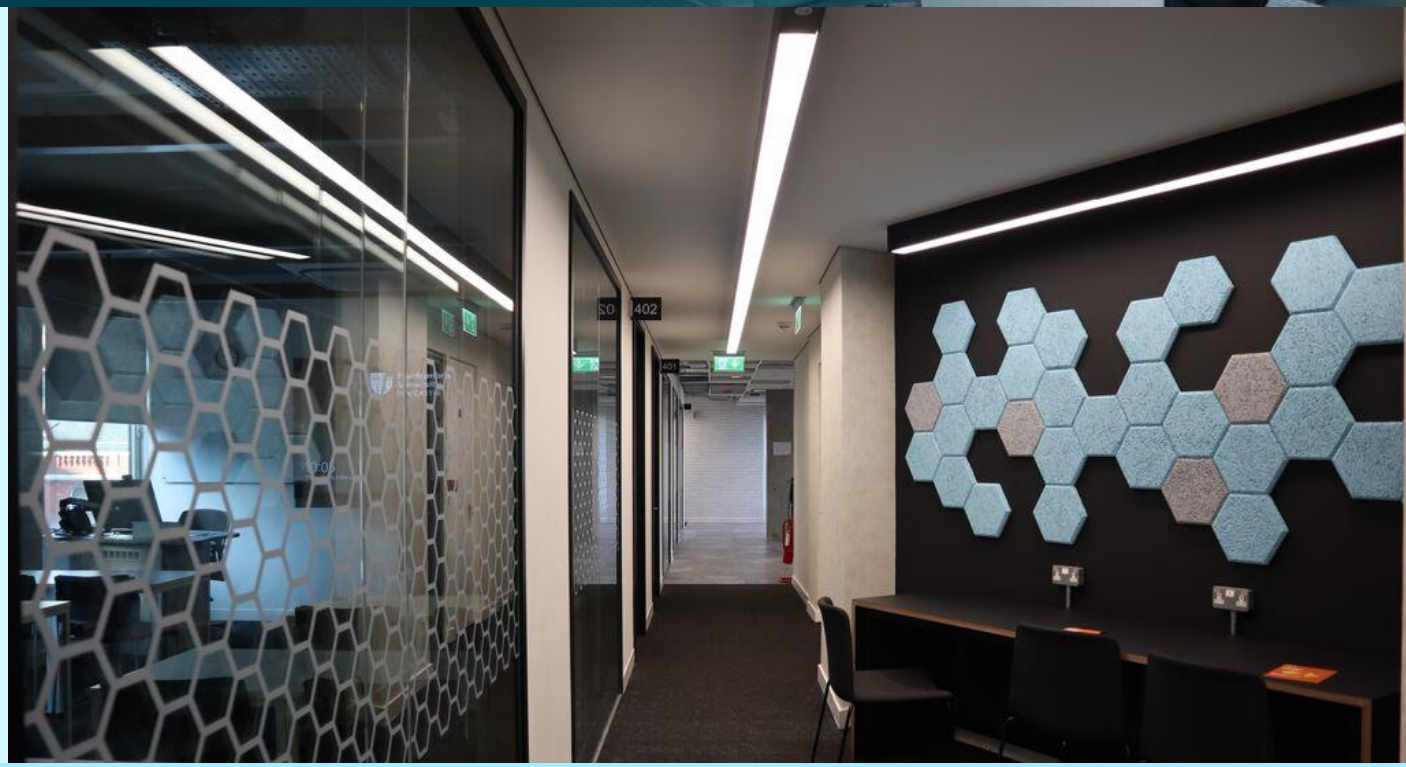
Remember to never share login details with others, even friends.

BE CYBER SECURITY SAVVY

10. Use a VPN

If you have a VPN (Virtual Private Network) it is important that you use it at all times, but in particular if you are using public Wi-Fi. A VPN encrypts all of your internet traffic including your IP address and geographical location, making this unreadable for anyone who intercepts it and invisible to unauthorised eyes.

Using a VPN will help to improve your security and protect your systems from targeted cyberattacks.



BE CYBER SECURITY SAVVY

Accessing Support After a Cyber Security Attack

If you have been affected by a cyber security incident, scam, or fraud, support is available from the following organisations:

- Citizens Advice – free, independent advice on dealing with the financial, legal, and practical consequences of fraud and cyber crime. Citizens Advice
- Victim Support – free and confidential emotional and practical support to anyone affected by fraud or cyber crime. Fraud - Victim Support
- Action Fraud – The UK's national reporting centre for fraud and cyber crime, where you can report incidents and receive advice on protecting yourself from further harm. UK's Home for Reporting Cyber Crime & Fraud - Report Fraud

If you believe your bank account or card details have been compromised, contact your bank immediately.

- Contact your bank straight away using the telephone number on the back of your bank card.
- Ask the bank to place security measures on your account or temporarily freeze it if necessary.
- Report any suspicious or unauthorised transactions.
- Work with the bank while they investigate any fraudulent activity and assess whether you are eligible for a refund.
- Update your security details, including passwords, PINs, and any compromised login information.
- Request replacement bank cards if your card details have been exposed.

Acting quickly can help reduce the risk of further fraud and increase the likelihood of recovering any lost funds."

If you're interested in finding out more information, please contact the Welfare Team on 0121 756 9578 or email: qahe.welfare@qa.com