Queen's University Belfast

Stay safe online over the holidays with our seasonal tips!

It may be the season of goodwill, but scammers still work over the holidays!

Check that payment pages are secure

Before you enter card details on a payment page, check that it's secure. Make sure the address starts with https (not http) and has a padlock or unbroken key symbol.

Beware of email scams and phishing attempts

Emails urging you to confirm delivery or verify your account may be scams. Don't click links unless you're sure they are genuine. If in doubt, don't respond – just delete.

Be careful if using WiFi when out and about

If you're using WiFi in a pub or café, there's no guarantee that it's secure. If you're shopping or banking online whilst out and about, better to use 3G/4G even if it's slower.

Check competitions on social media are genuine

There are lots of scams on social networks in the form of free prize draws for iPads, TVs, etc. Check that the profile and competition are genuine before entering.

Create secure passwords and keep them secret

Create a secure password using a combination of letters, numbers and symbols. Never allow someone else to use your Queen's University password!

Use 2-step authentication where possible

Use 2-step (2-factor) authentication with online accounts to avoid getting hacked. Usually the site will send a PIN to your phone if you login from a new device.

Look after your new smartphone or tablet

If you get a new smartphone or tablet, download a reputable internet security app and safeguard it with a PIN. Never leave devices unattended in public!

Don't forget to logout when you are finished

Always logout of any online accounts when you have finished. Just closing the window doesn't mean you've logged out and someone could still access your details.

Don't forget to follow ITQUB on Facebook and Twitter for advice and updates on using the IT facilities at Queen's University Belfast!

twitter.com/ITQUB

facebook.com/ITQUB