Keeping yourself safe from Coronavirus IT scams

There are a number of IT scams that are currently circulating which are exploiting our desire to know more about Coronavirus. Others target our uncertainty about how we respond to the rapid changes to our working and studying practices, especially accessing resources remotely.

Email scams are one such scam which criminals use to hack into our computers or get our personal details. A scammer will send an email with an attachment (a PDF, MP4 or similar) and when you click on it, it will install some software (malware) which will infect your computer with a virus. Other emails may ask you to send your personal details or to validate your account in order to get more information.

It's really important to be able to recognise a scam so we've put together some tips to help you stay safe online both at work and at home.

1. Do not click on links or open attachments from people you don't know.

Phishing emails often have one or more of the following elements in them:

- Generic greeting e.g. Dear Sir, Dear Madam
- Poor grammar
- Sense of urgency
- Spelling mistakes
- Offer you a 'special offer'
- Mismatched URL or misspelt URL e.g. www.quml.ac.uk instead of www.qmul.ac.uk
- Request for personal information
- Request for login details to 'validate your account'

If you are in any doubt about whether this is genuine, be cautious and don't open it.

2. Make sure you have a strong password.

A good password is a combination of upper case, lower case, numbers and symbols between 8-15 characters. Don't choose something that is easy to guess like your own name, the name of your pets and children, or your home address.

Bad password: 12345abcde

Good password: D1!xeiR4%

3. Regularly update your anti-virus software

You should have anti-virus software installed on your computer and this should be regularly updated. New viruses are constantly coming online and you need to make sure that you're protecting your computer by ensuring it has the latest virus protection on it. You can set many of the anti-virus software products to auto-update, so don't ignore your computer when it is asking you to update your software.

If you have a computer with the Windows 8 or Windows 10 operating system, you should have Windows Defender anti-virus installed on it as default. Apple users will have a built in anti-virus X-Protect within their operating system.

For older operating systems such as Windows 7, it is encouraged that you upgrade your system where possible as Microsoft no longer provide support for those.

Anti-virus support for Windows 7 systems is still available and you can read more here.

4. Set up multi-factor authentication

Multi-factor (also known as two-factor) authentication is another layer of security which is in addition to your username and password. You'll be sent a separate code to another source (for example email address or phone number) and you'll need to input this in order to access your account.

Queen Mary already uses two-factor authentication on many of the essential systems you might be using.

Read more about about multi-factor authentication at Queen Mary and how you can set it up for Office 365 on your device.

If you want to learn more about keeping your computer safe, please visit the IT Services pages on Cybersecurity.

If you think you've clicked on a link and you need help to make sure your computer is safe or have an email you are unsure about, please contact the IT Service Desk servicedesk@qmul.ac.uk.