STAYING SAFE ONLINE

> Technology is helping us cope with the coronavirus crisis and will play a role helping us out of it – but that means cyber security is more important than ever.
>
> **Ciaran Martin**, Chief Executive Officer, National Cyber Security Centre, 21st April 2020

Millions of hoax emails are being sent out to people each and every day with these numbers growing exponentially during the last few months. Covid-19 has caused a surge in phishing emails, with the National Cyber Security Centre (NCSC) removing more than 2000 online scams related to coronavirus in the month of April alone.

The surge in phishing emails comes hand in hand with the surge in internet traffic. Internet service providers have reported that daytime internet usage has more than doubled during the pandemic.

Ensuring that you are using your devices safely is therefore especially important at this time. Using advice issued by the Department for Digital, Culture, Media and Sport,[1] the following page presents some basic ways you can stay safe online.

What is a phishing attack?

Phishing is when criminals try to convince you to click on links within a scam email or text message, or give sensitive information away (such as bank details). Once clicked, you may be sent to a website which could download viruses onto your computer or steal your passwords.

How do I spot one?

Given the current coronavirus (COVID-19) situation, cyber criminals are sending emails that claim to have a 'cure' for the virus, offer a financial reward, or encourage you to donate. Like many phishing scams, these emails are preying on real-world concerns to try and trick you into clicking.

Where am I likely to come across a phishing attempt?

Most attempts are usually carried out over email, although the scam has now spread to social media, messaging services and apps.

[1] https://www.gov.uk/guidance/covid-19-staying-safe-online

Raytheon UK

1. Stay connected securely

You can stay in touch with friends and family by phone, video call or social media. This has been proved to help boost wellbeing.

For those of you using it for the first time, the National Cyber Security Centre has published guidance on how to securely use videoconferencing apps, including tips on how to securely install such apps, create a strong password and track who is joining your chat. They also recommend that you do not make meetings public, connect to people you know through your contacts or address book and never post the link or password publicly.

Find out more at: **https://www.ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely**

2. Stay Safe

In April, the Government launched its 'Cyber Aware' campaign, which offers actionable advice for people to protect their online accounts and devices. Its top tips for staying secure online include:

1. Turning on multi factor authentication for important accounts
2. Protecting accounts by using a password of three random words
3. Creating a separate password that you only use for your main email account
4. Updating the software and apps on your devices regularly
5. Saving your passwords in your browser
6. Backing up important data to protect yourself from being held to ransom

Find out more at:
https://www.ncsc.gov.uk/cyberaware/home

What is multi factor authentication?

This means that a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism.

For instance, when accessing an online account, you may be asked to provide a password, before then also receiving a text message with a code which is needed to complete the login.

3. Block unsuitable content

If you see harmful activity, report it to the site. You can also prevent unwanted content from appearing by setting filters on your home broadband and mobile networks. The UK Safer Internet Centre has advice on how.

Find out more at:
https://www.saferinternet.org.uk/

4. Protect against fraud

Criminals will use every opportunity they can to try and scam innocent people – beware of fraud and scams online including Covid-19 related phishing emails and text messages.

Report any suspicious emails to **report@phishing.gov.uk**, a new service run by the NCSC's Suspicious Email Reporting Service.

Find out more at: **https://www.ncsc.gov.uk/guidance/suspicious-email-actions**

5. Check the facts

Source – make sure information comes from a trusted source

Headline – always read beyond the headline

Analyse – check the facts

Retouched – does the image or video look as though it has been doctored?

Error – look out for bad grammar and spelling

6. Take a break

It's easy to feel overwhelmed with information at this time. Take a break!

Most devices should enable you to set up a screen time feature which will help limit the time you spend online.

7. For parents

a. Make use of parental controls

If you have downloaded new apps or bought new devices like web cams or tablets, remember to adjust the privacy and security settings to suit you.

b. Have a conversation with your child

Reduce the risk and talk to your child – the UK Council for Internet Safety has guidance on minimising children's exposure to risks online.

Find out more at: **https://www.gov.uk/government/organisations/uk-council-for-internet-safety**

With sites in Gloucester and Manchester, Raytheon UK is one of the UK's leading companies in cyber security.
For more information, visit: **https://www.raytheon.com/uk/capabilities/raytheon-in-the-uk/cyber**.
Follow us on social media to get more insight and articles from our team of digital experts: in **/company/raytheon-uk**

Raytheon UK