You, the Coronavirus, and keeping safe online

GET SAFE ONLINE .org

www.getsafeonline.org

COVID-19 Online safety

Right now, safeguarding ourselves, our loved ones, friends and colleagues from COVID-19 (Coronavirus) is uppermost in people's minds in the UK and around the world. After all, this is an unprecedented situation which warrants unprecedented precautions.

Also of great importance, however, is making sure we also remain safe in the virtual world during restrictions on travel, socialising, office life and other things we normally take for granted.

Why is online safety even more important than usual?

Invariably, a crisis affecting large numbers of people triggers a huge volume of fraudulent activity. With Coronavirus, expect fake ads for anything from vaccines to facemasks, links to sensational news and video, bogus charity appeals, and phishing emails claiming to be from travel, compensation and insurance companies or event/tournament organisers. Fraudsters know that at times like these, we may be too concerned or preoccupied to spot that something isn't right.

And if we're using the extra time on our hands to relax, there's also more chance that we could be letting our online guard down, whether we're social networking, gaming, dating, downloading or the many other things we take for granted.

We may not all be accustomed to working from home, so we all need to practice a number of important procedures and precautions, some additional to those we normally exercise in our workplaces and homes.

However Coronavirus is affecting your online life, please read these tips to help protect yourself, your family, finances, devices and organisation. And check out advice including passwords, payments, safe buying and updating your software and apps.

Coronavirus-related scams

Reported Coronavirus scams cost victims in the UK over £800,000 in a single month, according to Action Fraud. Here's how to help avoid them:

Be wary of approaches from supposed travel agents, tour operators, airlines, cruise companies, insurance companies or compensation firms promising to arrange travel, accommodation or event entry refunds: they may well be fraudulent. If in doubt, call the company you have been dealing with, on the phone number you know to be correct. These approaches can take the form of emails, texts, social media posts, direct messages, online advertisements and phone calls.

Be wary of ads for products such as facemasks, hand sanitiser, vaccines, cures and hard-to-get goods, as they could be for non-existent products. Never pay by bank transfer, and where possible pay by credit card as doing so provides additional protection.

As always, **don't click** on unknown links in emails, texts or posts, or email attachments. They could link to websites that capture your passwords and other confidential details or cause a malware infection, both of which can result in financial or identity fraud. They could also link to adult, hate, extremist or other content.

Think before you click

Our adversaries will not stop their cyberattack activities because of COVID-19. There is already evidence of phishing campaigns trying to extract sensitive information through installing malicious software. Techniques used include fake emails with links claiming to have important updates, which once clicked on lead to devices being infected with the malicious software. Please think before you click and remember the key ways to identify phishing emails:

- Many phishing emails have poor grammar, punctuation and spelling.
- Is the design and overall quality what would you'd expect from the organisation the email is supposed to come from?
- Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone you know?
- Look at the sender's email address and check whether it is valid. Check the email address by right-clicking on the sender's address and open Contact Card.
- If it sounds too good to be true, it probably is. It's most unlikely that someone will want to give you money, or give you access to a secret part of the internet.
- Your bank, or any other official source, should never ask you to supply personal information from an email.
- Report any email you believe to be suspicious, particularly if it is COVID-19 related. If you receive any unexpected work emails or those that are in any way suspicious, report them to Transputec:

General online security advice for working remotely

COVID-19
Online safety

- **DO** protect devices and information in a suitably secure and / or concealed location at home or while on the move.
- **DO** ensure that you are using a secure Wi-Fi connection (one that is password protected) and don't use public Wi-Fi if working remotely.
- **DO** ensure that information cannot be seen by others at home. Check that you are not overlooked and, if you have to leave your device then either lock the screen (Ctrl-Alt-Del) for short periods or turn it off for longer ones.
- **DO** disconnect smart home speakers (Amazon Echo, Google Home etc.) when making work calls or having work conversations, or at least be out of earshot of smart speakers.
- **DO** secure physical documents by locking away or concealing.

- **DO NOT** share your password with anyone else.
- **DO NOT** redirect your work email to a personal email account, and do not use your personal email account to routinely share work documents or conduct business.
- **DO NOT** have sensitive conversations on telephones in public. Minimise the ability to be overheard.

Get Safe Online

- Get Safe Online is the UK’s leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by a number of government departments, law enforcement agencies and leading organisations in internet security, banking and retail.

- For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

Coronavirus: what's true, and what's fake?
Get the answers
Ask Terry Tablet
Young people with an aptitude for coding or hacking have a life choice
Will yours choose the legal, or illegal path?