

You, Coronavirus and keeping safe online



Read our expert online safety advice about avoiding online Coronavirus-related scams and working safely from home during the outbreak.



Right now, safeguarding ourselves, our loved ones, friends and colleagues from COVID-19 (Coronavirus) is uppermost in people's minds here 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?

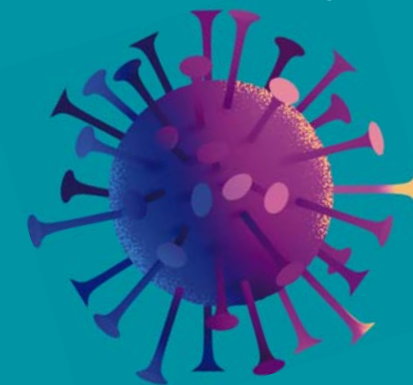
Invariably, a crisis affecting large numbers of people triggers a huge volume of fraudulent activity. With Coronavirus, expect fake ads for anything from vaccines to facemasks, links to sensational news and video, bogus charity appeals, and phishing emails claiming to be from travel, compensation and 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.

Business owners with employees not accustomed to working from home also need to take simple precautions additional to those we normally exercise in regular workplaces.

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.

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

#covidonlinesafety



Coronavirus-related scams

#covidonlinesafety

Reported Coronavirus scams can cost victims substantial amounts of money. 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.

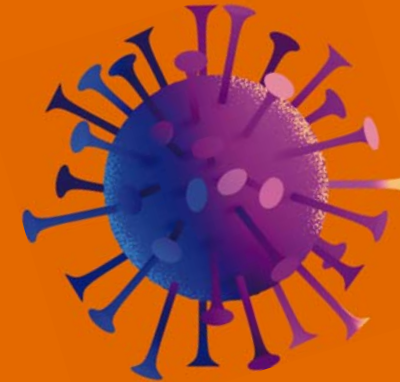


For comprehensive, practical, impartial advice about online scams, visit your [Get Safe Online website](#)

Working from home

- Ensure that cloud-based collaborative services such as file sharing and conferencing are secured with **strong passwords and two-factor authentication (2FA)**.
- **Set strong passwords** for new accounts or remote accesses and impose rules about password usage, such as not sharing, using a password manager and not using passwords for more than one account. For information about strong passwords, visit your Get Safe Online website.
- Consider whether it is safe and/or sensible to enable employees to use their **own computers and mobile devices** for work purposes ('bring your own device').
- If employees need access to your company's network, files and email, set them up a **virtual private network (VPN)**. Beforehand, read reviews for VPN security levels. Existing VPNs should be fully patched.
- Emphasise the importance of **protecting company-issued devices** in case of loss, theft or damage. Ensure they can be locked down in the event of loss or theft. Devices should be kept out of harm's way, for example from family members and visitors to the home.
- Employees should ensure that their **broadband routers are secured** to avoid unwanted intrusion, and if they are out and about, **avoid using Wi-Fi hotspots** whilst doing anything confidential.
- **If work conversations are confidential**, make sure they are out of earshot of any smart speakers that may be in the home.
- **Maintain your normal checks and controls**, including for data breaches, which could be more likely under the current conditions. It may also be worth notifying your insurance provider that staff are home working.
- **Report actual or attempted fraud** immediately to the appropriate authority.

#covidonlinesafety



For comprehensive, practical, impartial advice on safe online home working, visit your [Get Safe Online website](#)

Get Safe Online

#covidonlinesafety

Get Safe Online is the leading source of unbiased, factual and easy-to-understand information on online safety. This website is a unique resource providing practical advice on how to protect yourself, your family, your finances, devices and workplace against fraud, identity theft, viruses and many other problems encountered online.

