



Coronavirus (COVID-19) has had an unprecedented impact on the world and how we interact with each other.

Life as we know it, for the time being, has changed. We're spending more time online than ever before. Our devices are overloaded with news alerts, updates and unexpected (if always welcome) calls from relatives.

Everyone is preoccupied. And scammers prey on this

This means it's extra important to know how to avoid scams so you can keep yourself and your family safe online.

Read our top tips to avoid online scams during this pandemic.

1. Do your research

Scams today are more sophisticated than ever before. Scammers will appear like a trusted business or government official. They will have a professional website and they'll say all the right things. Take your time to work out if this is a real organisation. Ask them for ID or contact the organisation on a number you know and trust. If you're

still in doubt, Google the name of the company and 'scam', to see if any horror stories come up.

2. Don't click on unknown links

Whether it's an offer for a coronavirus testing kit or a refund on your holiday, never click on unknown attachments or links. Scammers prey on our health and money worries by sending us links to offers that appear too good to be true. Criminals use links to capture personal information or download viruses onto your devices. Both of which can result in financial or identity fraud.

3. Be suspicious

Don't take anything at face value during this time. Common scams at the moment prey on the fact that we're more vulnerable than ever. We're worried about our families, health, money and work. It will take us longer than usual to realise something isn't right.

4. Never give out personal information or money to anyone you don't trust

Never send money to people you don't know. Don't share logins, passwords or bank details with someone you don't trust. If someone pressures you for money or sensitive information up front it is most likely a scam.

5. Report it

And finally, report it. If you've been the victim of an online scam contact the [Citizens Advice Scams Action service online](#) or over the phone 0808 2505050. If you've been scammed out of money, report it to your bank first.

It's important we work together to keep our family and friends safe online. Share our top tips with your community to help protect them from frauds and scams.

Examples of online coronavirus scams

- Companies offering fake holiday refunds
- Virus testing kits or vaccines
- Overpriced or fake goods such as facemasks, hand sanitiser and hard-to-get goods
- Fake online resources such as sensationalist articles or false coronavirus maps
- Emails using voluntary action as a hook for people to share their personal details