

Beware of online scam's

1) More people may fall victim to [#onlineshopping](#) fraud as they self-isolate due to [#COVID19](#). You are a victim of online shopping fraud if you buy something online that never arrives.

Find out more at: <https://www.actionfraud.police.uk/a-z-of-fraud/online-shopping-fraud>



Online shopping fraud

- If you're purchasing goods and services from a company or person you don't know and trust, carry out some research first. Look up reviews of the company and ask trusted friends and family members if they have heard of it before.
- Be wary of unsolicited emails and texts offering questionably good deals, and never respond to messages that ask for your personal and financial details.
- Avoid paying for goods and services by bank transfer as that offers you little protection if you become a victim of fraud. Instead, use a credit card or payment service such as PayPal if possible.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

2) Be wary of cold calls or unsolicited emails offering you help with your device or to fix a problem

<https://www.actionfraud.police.uk/a-z-of-fraud/computer-software-service-frauds>



Computer Software Service Fraud

| Spot the signs |

Unsolicited calls
Unsolicited calls purporting to be from well known companies, such as your Internet Service Provider (ISP), or Microsoft, offering to provide technical support for a fee.

Software installation
The caller instructs you to install certain software, or asks you to visit a particular website, so that they can gain remote access to your computer and "fix" the problem.

Your information
The caller may already know some of your details (full name or address), and use that to gain your confidence and extract further personal and financial information from you.

Browser pop-ups
Pop-ups purporting to be from well known companies, such as your ISP, or Microsoft, offering technical support and providing a number for you to call.

CITY OF LONDON POLICE
ActionFraud
National Fraud & Cyber Crime Reporting Centre
www.actionfraud.police.uk

3) A number of #COVID19 related phishing emails have been reported to Action Fraud. These emails attempt to trick you into opening malicious attachments which could lead to fraudsters stealing your personal information, logins, passwords, or banking details.

<https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march>

How to deal with scam texts and emails

Don't click on the links or attachments in suspicious emails, and never respond to messages that ask for your personal or financial details.



For more information, visit [actionfraud.police.uk/cybercrime](https://www.actionfraud.police.uk/cybercrime)

4) Wash your hands of coronavirus scams! The Friends Against Scams training has been updated to include information on coronavirus scams – complete it here:

<https://www.friendsagainscams.org.uk/training/friends-elearning> #Coronavirus

#ScamAware



Protect your loved ones from coronavirus scams.

Have a look at the updated Friends training for information.

www.friendsagainscams.org.uk/training/friends-elearning

