

OFFICIAL



## **Home working and coronavirus scam emails**

**18 March 2020**

As more businesses encourage their staff to start working from home the National Cyber Security Centre (NCSC) has launched new guidance to help prepare your workforce.

Home working brings its own cybersecurity challenges that organisations must manage including possibly setting up new accounts, using new video conferencing facilities and document sharing.

The new guidance from NCSC includes:

- recommended steps to take if your organisation is introducing (or scaling up the amount of) home working
- tips on how individuals can spot the typical signs of phishing emails

Cybercriminals are always looking for opportunities to develop different ways to exploit the general public for their own gain and these phishing emails are designed to trick people into clicking on bad links that will take users to dodgy websites which will then download malicious software or steal data including passwords.

To read this new NCSC guidance please visit [www.ncsc.gov.uk/guidance/home-working](http://www.ncsc.gov.uk/guidance/home-working) and remember, if you are the victim of a cyber-attack please report it to Police Scotland by calling 101.

*This alert was sent out for your information by Police Scotland Safer Communities  
Cybercrime Prevention Unit - [SCDCyberPreventionNorth@Scotland.pnn.police.uk](mailto:SCDCyberPreventionNorth@Scotland.pnn.police.uk)  
All information was correct at time of distribution.*

OFFICIAL