NEWS

NCSC issues guidance as home working increases in response to COVID-19

Advice to help organisations manage the cyber security challenges of increased home working.

Organisations are being urged to follow cyber security best practice guidance to help prepare for an increase in home and remote working in the wake of the coronavirus (COVID-19) outbreak.

The National Cyber Security Centre (NCSC) has today published advice for UK companies to reduce the risk of cyber attack on deployed devices including laptops, mobiles and tablets, and tips to help staff spot typical signs of phishing scams.

Working from home is new for a lot of organisations and employees. Even if home working has been supported for some time, there may suddenly be more people working from home than usual, some of whom may not have done it before.

The NCSC has outlined recommended steps for organisations in:

- Preparing for home working
- Setting up new accounts and accesses
- Controlling access to corporate systems
- Helping staff to look after devices
- Reducing the risk from removable media

Within the guidance there is advice on dealing with suspicious emails, as evidence emerges that criminals are exploiting the coronavirus online by sending phishing emails that try and trick users into clicking on a bad link. If clicked, these links could lead to malware infection and loss of data like passwords. The scams may claim to have a 'cure' for the virus, offer a financial reward, or be encouraging you to donate.

The guidance offers advice on spotting those emails, as well as on how to respond in the event of falling victim to a scam.

For official information about coronavirus, please refer to trusted resources such as the Public Health England or NHS websites.

PUBLISHED

17 March 2020

NEWS TYPE

General news

WRITTEN FOR ⓘ

Small & medium sized organisations

Large organisations

Public sector

Cyber security professionals