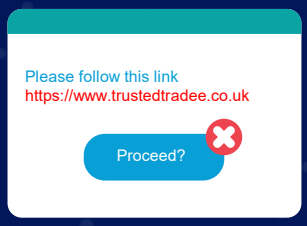
Government Security



Malware

Cyber criminals use malicious software, or 'Malware', to infiltrate or corrupt systems to change, destroy, or steal information — often delivering it via spam emails.

Devices can become infected by accidentally downloading an email attachment that contains malware, or by plugging in a USB stick that is already infected. You can even get infected by visiting a dodgy website.

For these reasons, it's important that you always use antivirus software on your personal laptops and PCs. Smartphones and tablets don't need antivirus software, provided you only install apps and software from official stores such as Google Play and Apple's App Store.

If you receive a phone call offering help to remove viruses and malware on your computer, hang up immediately (this is a common scam).

Whilst at work think about the emails you receive. Never reply to messages, click on links or open attachments immediately, even if there is a sense of urgency, unless you are certain of its authenticity.

If you think you may have clicked on a malicious link don't panic, follow your local security reporting procedures. Reporting incidents like these enables security professionals to act promptly to rectify any problems and prevent future incidents from occurring.

For more advice on how to stay secure online visit the National Cyber Security Centres **Cyber Aware** pages

Always report any unusual activity within your work accounts or devices by following your department's security protocols.