

## Scam support calls (CSS fraud)

- Criminals may phone you purporting to be a technical support service or your computer, phone, app or Internet provider (ISP).
- They will claim that they have identified problems with your computer, phone or tablet or issues with your Internet, which need fixing immediately.
- They can be extremely convincing and manipulative and may try to entice, scare or bully you into acting quickly without taking the time to consider your actions.
- You may be asked to change settings, press certain keys or download an app or other software. Doing so will help criminals gain access to your device or data.
- They will often direct you to fake technical information, logs or errors on your screen to try and convince you to follow the instructions they give.
- No genuine company or organisation will call you unexpectedly about technical faults they have identified or ask for access to your computer or online accounts.
- Never give any caller your password, PIN or other on-screen codes or details.
- Pop-up messages or alerts may appear on your device, claiming to have detected viruses or other security issues with instructions to call a fake service line for support, or to purchase unnecessary subscriptions or software.

## What should I do if I receive a scam support call?

- If you receive one of these calls – hang up immediately.
- Report it to Action Fraud – Tel: 0300 123 2040
- If you have made any changes to your device or downloaded an app or other software as a result of a call or pop-up, contact a reputable computer support service or talk to someone you trust, to check the device fully before reusing it.

For further cyber safety resources and advice contact:

**CyberProtect@northants.police.uk**



**NorthantsCyber**



**Northamptonshire Police**

Fighting crime, protecting people