

## Phone Contract Scam

Avon and Somerset Police are seeing an increase in scams where fraudsters are making cold calls, impersonating employees of legitimate mobile network operators and suppliers. The National Fraud Intelligence Bureau (NFIB) have issued the following warning regarding this type of scam.



Victims are offered early upgrades, or new contracts, at a discounted price. Once victims agree to proceed, suspects then ask for their online mobile account credentials, including logins, address and bank account details.

Suspects then place orders with genuine companies on behalf of victims, selecting a different handset to that requested and have it shipped to the victim's address.

When received, the fraudsters tell victims that there has been an error and instruct them to 'return' the handset to a different address not affiliated to the mobile company.

After intercepting the 'returned' handsets, the suspects cease contact, and victims find themselves stuck with no phone and liable for the entirety of a new contract taken out in their name.

### **What you need to do**

- If you're unsure that the person calling you is an official representative of the company they claim to be from, hang up and do not reveal any personal information.
- Only contact your mobile network provider on a number you know to be correct. For example, 191 for Vodafone customers, 150 for EE customers, 333 for Three customers, 202 for O2 customers, 4455 for Tesco Mobile, and 789 for Virgin Mobile. Or attend the store and speak to someone in person.
- If you receive a device that you did not order or expect, contact the genuine sender immediately. The details for this will be within the parcel.
- NEVER post a device directly to a given address. All genuine Mobile Network Operators would send out a jiffy bag for you to return without you incurring additional cost.
- Don't disclose any of your personal or bank account information, including your PIN or One Time Passcode (OTP).