Official

Mobile Phone Upgrade Scam

Published on 8th June 2021
Reference 202104TBC

Mobile Phone Upgrade Scam

CITY OF LONDON POLICE
National Policing Lead For Fraud

Summary

Published on 08/06/2021
Reference 202104TBC

The NFIB are aware of an ongoing scam where consumers are being cold called by individuals impersonating employees of legitimate mobile network operators and suppliers.

Victims are offered early handset upgrades, or new contracts, at significant discounts. Once customers have been convinced that the deals are genuine and agree to proceed, suspects then ask for their online mobile account credentials, including log-ins, address and bank account details.

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

Upon receipt, suspects assure victims that this has been an error and instruct them to 'return' the handset to a different address not affiliated to the mobile company. These addresses are usually residential.

Upon 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.

The NFIB have received over **300** reports since January 2020 with reported losses in excess of **£86,000.**

What you need to do

- Cold calls about mobile upgrades and contracts - 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, 789 for Virgin Mobile and 150 for Sky Mobile.
- 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.

For more information about how to protect yourself online, visit
www.cyberaware.gov.uk and **takefive-stopfraud.org.uk**

Every Report Matters

If you have been a victim of fraud or cyber crime, report it to us at Actionfraud.police.uk, or by calling 0300 123 2040.