An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2412090106

NCSC Advisory

Upgrade Scam targeting Mobile Phone Users

09 December 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP-CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

Subject to standard copyright rules, **TLP-CLEAR** information may be shared without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Description

The NCSC has received reports about a sophisticated scam targeting mobile phone users. Scammers are impersonating mobile phone provider representatives and using deceptive tactics to gain access to your account to order and steal valuable mobile devices.

Here's how the scam works and how to protect yourself.

How the Scam Works

1. **Cold Call**: The scammer calls you, claiming to be from a mobile provider, offering an upgrade on your mobile phone contract or some other offer. At this stage they try to confuse the victim by being unclear about why they are ringing.
2. **Account Access**: While on the call, the scammer uses the “Forgot Password” option on the mobile providers website. This triggers a verification code to be sent to your phone.
3. **Code Request**: The scammer asks you to read out the verification code, claiming it's necessary to process your upgrade.
4. **Account Hacked**: Once the scammer has the code, they reset your online account password and gain full access.
5. **Fraudulent Order**: The scammer orders a high-value phone to be delivered to your address.
6. **Second Call**: After the phone arrives, the scammer contacts you again. When you express confusion or refusal, they offer to "resolve the issue" by collecting the phone and processing a refund.
7. **Collection**: The scammer arranges for the phone to be collected, leaving you without the device and potentially liable for the cost.

How to Protect Yourself

- **Never Share Verification Codes**: No legitimate company will ever ask for a one-time code or password over the phone.
- **Verify the Caller**: If someone claims to be from your mobile provider, hang up and call your provider directly using the official customer service number.
- **Monitor Your Account**: Regularly check your account for unauthorised activity or changes.

- **Use Strong, Unique Passwords**: Avoid using easily guessed passwords and enable additional security features, such as two-factor authentication, if available.
- **Report Suspicious Calls**: If you receive such a call, report it to your mobile provider immediately and to your local Garda station.

What to Do if You're a Victim

1. **Contact Your Mobile Provider**: Inform them immediately to secure your account and report the fraud.
2. **Change Your Passwords**: Reset your account password and any other accounts that use the same credentials.
3. **Report to Authorities**: File a report with your local Garda station.
4. **Contact Your Bank**:If you used a credit or debit card contact your bank straight away.
5. **Be Vigilant**: Keep an eye on your account and credit reports for any further suspicious activity.

Further Advice

- https://www.fraudsmart.ie/
- https://fraudsmart.scamchecker.ie/
- https://www.ncsc.gov.ie/pdfs/NCSC_Quick_Guide_Phishing.pdf
- https://www.ncsc.gov.ie/pdfs/Seasonal_Advisory_2023.pdf
- https://www.ncsc.gov.ie/pdfs/NCSC-MFA-Guide-0723-Final.pdf
- https://n.vodafone.ie/protecting-you.html
- https://www.three.ie/support/online-safety.html