**VISHING**

THE VOICE PHISHING SCAM
ADVICE FOR CORPORATE EMPLOYEES

A fraudulent practice where verbal communication technology (e.g. VOIP or telephone) is used by an unauthorised entity pretending to be a reputable company. The aim is to manipulate individuals into revealing financial or personal information, or into providing unlawful access to their corporate networks.

**BE AWARE OF THE SCAM - HOW TO RECOGNISE THE CALL?**

- **Generic greeting.** The attacker rarely knows your name.
- **Sense of urgency due to different reasons:** detected unsecure systems, bank account problems, package delivery, etc.
- **Impersonation of a trusted third party,** such as banks, technological or telecommunications companies, courier, etc.
- **Reference to personal information available on public corporate websites or social media profiles.**

**WHAT CAN YOU DO?**

**During the call**

- Try to verify the identity of the caller.
- Avoid giving any information such as your contact details, your company’s organisational structure, etc.
- Avoid performing any action you may be requested: configuration change, sending an email, clicking on a link, etc.

**After the call**

Report to your corporate Helpdesk:
- The date and time of the call
- The originator’s phone number
- Any other data provided by the attacker
- Any action you may have been requested to perform

**HOW TO AVOID BECOMING A VISHING TARGET?**

- Limit the amount of personal information you share online.
- Avoid providing your corporate contact details (email, phone number, etc.) to external websites unless there is a business need.

*Created by Europol*