

# VISHING CALLS

## Infographic

### VISHING CALLS

Vishing (a combination of the words Voice and Phishing) is a phone scam in which fraudsters trick you into divulging your personal, financial or security information or into transferring money to them.



#### WHAT CAN YOU DO?

- > **Beware** of unsolicited telephone calls.
- > **Take the caller's number** and advise them that you will call them back.
- > In order to validate their identity, **look up the organisation's phone number** and contact them directly.
- > **Don't validate the caller using the phone number they have given you** (this could be a fake or spoofed number).
- > Fraudsters can find your basic information online (e.g. social media). **Don't assume a caller is genuine** just because they have such details.
- > **Don't share** your credit or debit card PIN number or your online banking password. Your bank will never ask for such details.
- > **Don't transfer money** to another account on their request. Your bank will never ask you to do so.
- > If you think it's a bogus call, **report it to your bank and let your phone operator know**.
- > **Block unknown and unwanted calls** - ask your phone operator about available blocking tools.



**#TelecomFraud**


#TelecomFraud



EN [VISHING CALLS](#) [210.26 KB]

CRIME AREAS

[Cybercrime](#)

TARGET GROUPS

[General Public](#) • [Law Enforcement](#) • [Academia](#) • [Professor](#) • [Students](#) • [Researcher](#) •

[Press/Journalists](#) •

[Other](#)

ENTITIES

[European Cybercrime Center \(EC3\)](#)

---

**Source URL:** <https://www.europol.europa.eu/publications-documents/vishing-calls>