

VISHING

Vishing is short for “voice phishing”, and refers to phonecall scams, including robocalls and any other fraudulent activity that might trick someone into divulging personal information.



WHAT CAN YOU DO?

- ➔ Beware of unsolicited telephone calls.
Remember that modern scammers can make robocalls from numbers similar to yours. Inspect the caller ID first, but remember that called ID can be spoofed. If you don't know them or weren't expecting the call, send the call to voicemail.
- ➔ Take the caller's number and advise them that you will call them back.
- ➔ In order to validate their identity, look up the organization'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.