What is Vishing (Voice Phishing)?

Vishing is voice phishing carried out over the phone. Attackers use calls to trick victims into handing over sensitive details such as login credentials, banking info, or personal data.

How It Works

Impersonating Trusted Sources

Scammers often pose as IT staff, banks, or even managers. They use authority and urgency to pressure you into complying on the spot.

Tip: *Hang up immediately if someone pressures you to act quickly.*

The Rise of AI Voice Cloning

With modern AI tools, attackers can clone real voices, making it sound like your boss, coworker, or family member is on the line. This increases believability and makes scams harder to detect.

Tip: *Verify suspicious requests by calling the organisation back using a trusted number.*

Phoney Security Checks

Vishers may claim they need your password, PIN, or MFA code to “secure your account.” In reality, they’re stealing your access.

Tip: *Remember, Banks and IT staff will never ask for full passwords or MFA codes over the phone.*

Reporting Matters

The quicker vishing attempts are reported, the less chance they have to succeed. Sharing what happened helps protect others.

Tip: *Report suspicious calls to your bank, IT team, or security team immediately.*