1. VISHING (VOICE PHISHING)

Vishing = voice phishing, where attackers make scam calls pretending to be trusted sources.

The goal is to extract sensitive information or pressure the victim into taking urgent actions that benefit the attacker.

Common vishing scenarios include:

* IT support calling about a “security issue” and asking for credentials

* Banks requesting verification of account details or transactions

* HR or Payroll impersonators asking for personal information

* Government agencies claiming urgent legal or tax matters

* Delivery companies saying there’s an issue with a package and requesting payment or details

These calls often create a sense of urgency or fear to manipulate the victim into responding without verification.

VISHING

- IT support
- Banks
- HR/Payroll
- Government
- Delivery companies

Goal: extract info or push victim to act urgently

Scenario: Maryam Gets a Fake “IT Support” Call

Maryam receives a call from someone claiming to be IT support.
The caller says, “Ma’am, we detected unusual login attempts on your account. Please tell me your OTP so we can block them.”
The call sounds urgent and convincing, and Maryam almost shares her one-time password.
However, legitimate IT support never asks for OTPs or passwords over the phone. The attacker’s goal is to gain immediate access to her account.

Lesson: Never share OTPs, passwords, or sensitive information over the phone. Always verify unexpected calls by contacting the official support channel directly.

VISHING

“Ma’am, we detected unusual login attempts from your account. Please tell me your OTP so we can block them.”

Maryam almost shares it — but IT never asks for OTP

Tactics Used by Vishing Attackers

- Spoofed caller ID
- Scary urgent language
- “I’m from your bank; fraud detected”
- Asking for OTPs or passwords
- Pretending call is being recorded for “security”

Red Flags

- Asking for sensitive info
- Asking you to install software
- Caller becomes pushy
- Claims of “immediate account closure”

Prevention Tips

- Never share OTPs
- Hang up & call back using official number
- IT department NEVER asks for passwords
- Treat unknown calls as suspicious