# Vishing Attacks

## Vishing= Voice+Phishing

### Five tips to help protect yourself from Vishing attacks

- **Don’t answer calls from unknown numbers** — Let calls from unknown numbers go to voicemail. Many Vishing scams will also leave a pre-recorded voicemail message, which will give you a chance to properly vet whether the caller is from a legitimate source

- **Be suspicious** — Most successful Vishing calls appear to come from a company you know and trust. Bank fraud Vishing attempts are among the most prevalent, claiming fraud or suspicious activity. Banks will never ask you for private information over the phone — so don’t give it out

- **Don’t be pressured** — Some Vishing scams attempt to create a sense of urgency and fear. For example, claiming that you owe back taxes. Government institutions like the IRS almost exclusively communicate by mail.

- **Never provide user names or passwords** — Most Vishing attempts try to convince the victim to give up PIN numbers, Social Security Numbers, credit card security codes, passwords, or other personal details. Reputable sources will never ask for these

- **Beware of “no hang up” technique** — While you may believe the call ended, the fraudster will maintain the connection while producing a faked dial tone. When you call the provided number, or your bank, you are instead speaking to another scammer and potentially giving away valuable information

**If you suspect you’ve been a victim of Vishing, report it immediately to the Federal Trade Commission.**

1. .
2. .
3. 
4. .
5. .