

What is Vishing?

May 19, 2024 • vajiramandravi.com



About Vishing

- It is a short form of **voice+phishing**, carried out through a **call on a mobile phone or landline**.
- It's a technique wherein a threat actor calls the victim over the phone and tries to trick him/her into **clicking on malicious files** or emails, which can then take one to a legitimate-looking website asking to **share personal information**.
 - In other cases, the attacker can solicit sensitive information from the victim.
 - It can be so tricky that the caller might appear as the manager or colleague of the victim, enticing her to share sensitive information, at times using urgency as the tactic.

How to spot a vishing scam?

- **A pre-recorded message:** On many occasions, a vishing call starts with an automated call claiming there's an urgency related to financial or other matters, making you click a few numbers or take certain actions.
- **Pretending to be a government official:** There's a very slim chance that a government official would directly call you or even email or text. And if you get a call from somebody claiming to be a government official, chances are high that it's not legitimate.

- **Using fear and urgency tactics:** In case of a vishing attack, chances are that the scammer would stoke a sense of urgency using threat or fear.
 - **Poor audio quality:** If in doubt, also pay attention to the call's audio quality and any background noises. At times, there could be robotic-sounding voices, which could mean that it's a **robocall**.
-

Q1: What is Ransomware?

Ransomware is a malware designed to deny a user or organization access to files on their own computer.

Source: [Beware of vishing: How not to fall prey to voice call frauds](#)

Source: <https://vajiramandravi.com/current-affairs/what-is-vishing/>

© Vajiram & Ravi. For personal use only.