Some of the most common types of vishing methods used by cyber criminals:

AI Deepfake Voice Attacks: Using AI, attackers clone the voices of executives, managers, or relatives, demanding urgent fund transfers or sensitive data.

Wardialing: Attackers use automated systems to call large volumes of numbers within specific area codes, often pretending to be local banks or law enforcement. These calls typically contain pre-recorded messages designed to instill fear and prompt victims to share personal information like Social Security numbers or banking details.

VoIP (Voice over Internet Protocol): Cyber criminals leverage VoIP technology to mask their identities and scale attacks by generating thousands of fake phone numbers. These calls often appear as legitimate local or toll-free numbers, making them harder to detect.

Caller ID spoofing: Scammers manipulate caller ID systems to display trusted names like "IRS" or "Police Department." This tactic creates a sense of legitimacy and urgency, increasing the likelihood that victims will comply with requests for sensitive information.

Tech support scams: Fraudsters impersonate representatives from well-known companies like Microsoft or Apple, claiming there's an issue with the victim's device. They may request remote access or personal credentials under the guise of resolving the problem.

Voicemail phishing: In this method, attackers leave urgent voicemails impersonating banks or government agencies, asking victims to call back. When victims return the call, they're connected with scammers who attempt to extract sensitive data.

Dumpster diving: This unconventional approach involves searching through physical trash from businesses to obtain documents containing personal data, such as employee names or account details. The gathered information is then used to craft persuasive vishing attacks.

Each type of vishing underscores the importance of vigilance and verification when responding to phone calls or voicemails requesting sensitive information.

How to Prevent Vishing

Stay informed and educated: Regular training and awareness programs are crucial for both individuals and organizations. Educating employees helps them recognize and report vishing attempts, reducing the risk of successful attacks.

Verify caller identities: If a caller requests sensitive information, hang up and contact the institution directly using a verified number. Verify the caller's position, purpose, and organization to ensure legitimacy.

Use multifactor authentication (MFA): Implement MFA on all sensitive systems to add an extra layer of security, making it harder for attackers to bypass security measures.

Be cautious with unsolicited calls: Ignore calls from unknown numbers and let them go to voicemail. If necessary, call back using a verified number from the organization's official website.

Watch for pressure tactics: Scammers typically use urgency and fear to manipulate victims. Be wary of requests for immediate financial transactions or sensitive information.

Register with do not call lists: Enroll in the National Do Not Call Registry to reduce unsolicited calls, making it easier to identify potential scams.

While telecoms have systems in place to flag suspicious calls, relying solely on these systems is insufficient. By strategically adopting these tactics, individuals and organizations can significantly reduce their vulnerability to vishing attacks.