# What is voice phishing (vishing)?

CANADIAN CENTRE FOR CYBER SECURITY

July 2022 | ITSAP.00.102

Vishing is a type of social engineering technique that leverages voice communication technology. In a vishing attack, threat actors or "vishers" use fraudulent phone numbers, voice altering software, and other social engineering tactics to entice people to divulge personal and sensitive information over the phone. Advanced vishing attacks exploit Voice over Internet Protocol (VoIP) technology to create fake phone numbers and spoof the caller ID so that the call appears to be from legitimate companies or institutions. VoIP makes it easy for vishers to automate hundreds of scam calls over the internet and these numbers are hard to trace.

## How Does a Vishing Scam Work

### 1. Data collection

Vishers will use different techniques to collect a list of phone numbers for indiscriminate mass vishing attacks. In some cases, vishers will research and collect specific information about their victims (individuals or organizations) to create a tailored vishing attack.

**Dumpster diving**
Vishers retrieve lists of phone numbers that a bank or organization has disposed of in the trash.

**War dialing**
Vishers use this technique to automatically call every number in a specific area code to look for active phone numbers.

**Internet search**
Vishers scours the Internet (YouTube, social media platforms) to obtain voice samples of a high-value target (e,g, company CEO).

**Data breach**
Vishers may obtain stolen phone number lists sold by other scammers from a data breach.

### 2. Voice manipulation

Vishers uses machine learning, a subset of Artificial Intelligence (AI) technology, to create a simulation of a person's voice. This technique called **voice cloning**, is used to add realism to the vishing attack by disguising the voice and impersonating someone the victim knows or trusts (for example a colleague, or their boss).

### 3. Fraudulent call

Vishers spoof their caller ID and call as many numbers as possible and leave a prepared voicemail message for callback. In an advanced attack, vishers use **voice synthesis** software to hide their identity (accent, gender or age) or control the cloned voice of the high-value target during the call.

## Examples of vishing scams

Vishing aims to convince the victim to disclose confidential information, such as a PIN, Social Insurance Number (SIN), credit card information, or account passwords. This information can be used for identity fraud, to conduct unauthorized financial transactions, or to gain access to corporate or personal accounts. The list below provides some examples of common vishing scams :

**Credential vishing.** Vishers use this method to gain access to banking and credit card information. They will use these compromised credentials to login into your account, access funds, or make unauthorized purchases.

**Government impersonation.** Vishers pose as government employees, most frequently from departments dealing with taxes and personal finance. They will use scare tactics to convince you to pay for items like overdue or unpaid taxes, or face legal consequences.

Vishers also pose as members of law enforcement organizations and request your personal information which they can use for identity fraud.

**Corporate extortions.** Posing as the boss, or company CEO, vishers will convince you to comply with your boss' request (e.g. releasing funds, authorizing approvals for access to sensitive systems).

**Telemarketing scams.** Posing as a telemarketer or representative of a company, vishers will congratulate you on winning a contest and then ask for you to pay a redemption fee or provide your credit card information to reserve your prize.

**Technical support scams.** Posing as technical support employees for various organizations, vishers will often ask for personal or employment information to verify your identity.

Vishers may even ask for your permission to access your device remotely to help install software. While doing so they can download malicious software on your device that can trigger pop-up warnings that encourages you to call a number to fix a technical or security issue.

Communications Security Establishment | Centre de la sécurité des télécommunications



Canada

# What is voice phishing (vishing)?

CANADIAN CENTRE FOR CYBER SECURITY

July 2022 | ITSAP.00.102

## Tips for spotting and avoiding vishing scams

- **Be suspicious of callers that want sensitive information.** Do not give personal information like your username, password, or banking information over the phone, unless you are certain it is a legitimate institution. Ask the institution for a contact name and reach the organization via an official channel (their publicly listed phone number or website).
- **Be wary of calls from unknown numbers or automated calls**. Let the call go to voicemail if you do not recognize the number. Avoid using your phone's callback function or phone numbers provided by the caller. Communicate with the site or service through a trusted contact method.
- **Beware of scare tactics.** Vishers try to catch you off guard and make you feel you have no other options but to provide the requested information. Some may use threatening language to get you to act quickly. For example, they may say you must provide your information to avoid having your account from being deactivated.
- **Be on guard for calls with poor audio quality** or with a robotic tone or an unnatural rhythm to their speech. Hang up and let the call go to voicemail if they call back.
- **Be proactive and train your staff on vishing** attacks and how to respond appropriately. Create a process for your staff to report incidents easily and quickly. Consider including a formalized authentication process for employee-to-employee communications made over the phone where authentication is required before sensitive information is discussed.
- **Be informed that most-smartphones have built-in spam protection features** that can filter, block or report spam calls. Check your smartphones manual on how to enable these features.

**Scammer are After Your :**

**Identity—Passwords—Money**

Vishing can be part of a larger phishing attack, another social engineering technique, to steal money or data from individuals or organizations.

To learn more info about phishing refer to Don't Take the Bait: Recognize and Avoid Phishing Attacks (ITSAP.00.101) on our website.

## STIR/SHAKEN

STIR stands for **Secure Telephone Identity Revisited**. SHAKEN stands for **Signature-based Handling of Asserted Information using toKENs**. As of November 30, 2021, the Canadian Radio-television and Telecommunications Commission (CRTC) required all telecommunications providers in Canada to implement this new technology to authenticate and validate VoIP voice calls.

### What does this mean?

Once your phone company implements STIR/SHAKEN they will be able to determine if a call is from a legitimate source and better inform customers of spam calls. This will enable you to make an informed decision about whether to respond to the unknown caller.

As more phone companies implement STIR/SHAKEN, there should be a reduction in the volume of spam calls made over VoIP.

## How to recover from a vishing scam

Take the following actions if you have been a victim of a vishing scam.

**Notify all your financial institutions** related to the compromised accounts. Ask if the fraudulent transactions can be cancelled and block future charges.

**Change your passwords immediately** for all affected accounts as well as other accounts that used the same compromised passwords.

**Monitor your financial accounts.** Consider signing up with a credit monitoring service to alert you of potential fraudulent activity, especially if you have concerns that you've been a victim of identity theft.

**Report the scam to the Canadian Anti-Fraud Centre (CAFC).** Document the phone number of the scammer as well as any websites you were asked to visit and provide this info to CAFC (antifraudcentre-centreantifraude.ca).

**Report the incident to your organization's IT administrator** if you think you might have revealed sensitive corporate information. Follow your organization's protocol for reporting cyber incidents.

Communications Security Establishment | Centre de la sécurité des télécommunications



Canada