SECURITY-MINDED

Practical security wisdom for daily life.

# WHO'S CALLING?

## Don't Be a Victim of Vishing Scams

Every day, criminals use malicious phone calls and voicemails to acquire confidential information—a type of attack known as "vishing."

Unsolicited phone calls and robocalls are often an annoyance, whether they're asking for contributions or trying to sell you something. While some of these calls are legitimate, scams and swindles are all too common.

Some phone-based attacks focus on stealing your financial details, access credentials, or other sensitive information. These are known as *vishing attacks*. "Vishing" comes from combining the words "voice" and "phishing." The term refers to criminal phone fraud, initiated via a voice-to-voice exchange or a malicious voicemail message.

### Persuasion + Pressure = Problem

Vishing calls attempt to manipulate people through tactics known as *social engineering*. These psychological tricks often create a sense of urgency or fear that's intended to pressure you into doing what the attacker wants.

Another social engineering tactic is to build familiarity and trust. For example, an attacker or social engineer could start by researching your organization to gather convincing details. Then, they could call an employee and use those details to persuade them to transfer money into the attacker's account.

Unfortunately, you can't rely on caller ID alone to avoid vishing. In fact, attackers have tools that let them display a fake name or number. And once you're on the phone, a skillful social engineer can apply their powers of persuasion. The voice-to-voice, personal connection can make vishing attacks seem more believable.

### Vishing in the Workplace

Many vishing calls try to defraud consumers. But some are targeted, coordinated attacks against a specific individual or organization. For example, attackers may contact several people within an organization to gather small pieces of valuable information from different sources. If one of these vishing calls is successful, it can become a stepping-stone to more criminal activities.

Vishing can also be highly targeted, with attackers researching a specific person before they call. Frequent targets include managers, financial professionals, and customer service representatives, due to their access to valuable information, systems, and physical assets.

# SECURITY TIPS FOR FAMILY AND FRIENDS

**Many scammers target consumers, rather than organizations. You may have already experienced a vishing call on your home or cell phone. Here's some good advice to share with family and friends on how to avoid falling victim to vishing calls:**

1. **Avoid the call –** Whenever possible, avoid answering calls from unknown numbers.
2. **Don't interact with calls –** If you accidentally answer a robocall, hang up. Any interaction—even to remove yourself from a call list—can lead to more robocalls.
3. **Terminate the call –** If a call is confusing or seems suspicious, hang up.

## Warning Signs

Beware of callers who:

- Claim to be from a tax, government, or law enforcement agency, and use threatening language (these are almost always fraudulent)
- Request payment for products or services via gift card or wire transfer
- Ask for authentication information, such as one-time verification codes
- Present offers that seem too good to be true

## Common Vishing Varieties

### Imposter Scams

An attacker could pretend to be someone you trust, like a friend or family member. Or, they could claim to be from a tax, government, or law enforcement agency. An attacker could also pose as technical support, calling to solve a problem with your computer or device. Falling for such an attack could give cybercriminals access to your organization's network, systems, and confidential information.

### Charity Scams

Scammers often pose as charities and call to request donations for disaster relief efforts. Resist any pressure to give immediately over the phone. Instead, take time to investigate a charity, then contact them directly if you wish to donate.

### Prize Scams

Many attacks use "too good to be true" offers and prizes as lures to get you to act quickly, without thinking. The caller might congratulate you on winning a prize … but you'll need to pay some sort of fee to claim it. Even if you pay, you'll probably never receive a prize. Similar scams offer free or low-cost vacations or cruises, or the opportunity to buy something rare.

*Source: Federal Trade Commission, Consumer Information.*

## Activity Corner // An Interesting Call

Hello! It's **1.**_____, lead singer of the band "The **2.**_____ **3.**_____." You have won a cash prize from **4.**_____, and I'm calling to announce your winnings of $**5**_____. **6.** _____! But before the funds are transferred, we will need some more information. Don't be alarmed! We only ask for common things, like your **7.**_____ home address, the year you graduated from **8.**_____ and your **9.**_____ account number. And hurry! This prize needs to be collected before **10.**_____ or we will have to give it to the runner up, **11.**_____. Please call us back at 1-800- **12.**_____ or press "one" to be connected with an operator.

1. Celebrity
2. Color
3. Plural noun
4. Local radio station
5. Number
6. Exclamation
7. Family member
8. Name of a school
9. Name of a bank
10. Time of day
11. Someone you dislike
12. Noun