vishing

WHO'S **REALLY** ON THE LINE?

Sometimes the best answer is **not** to answer.

Voice + Phishing = Phone Fraud

Vishing (voice phishing) is a type of fraud carried out over the phone. Attackers typically attempt to steal money or gain access to sensitive information in order to commit identity theft.

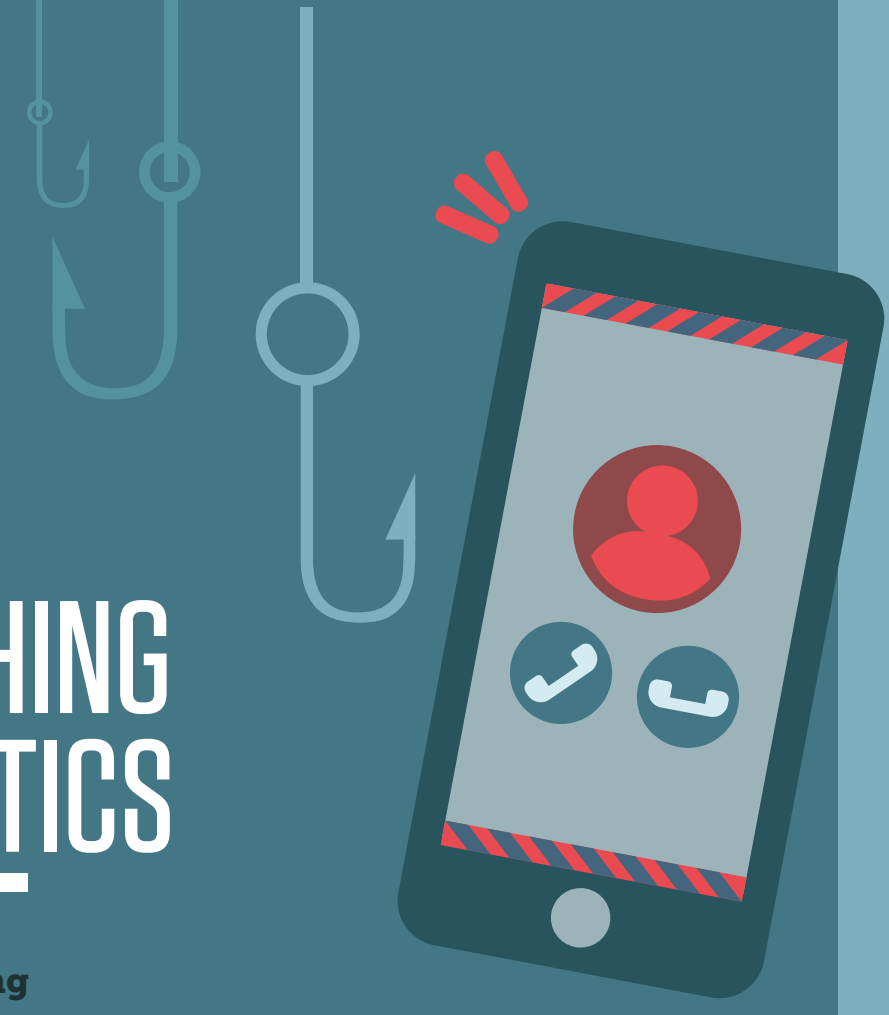
But threat actors also use vishing attacks as stepping-stones, gathering information about an organization and its employees as part of a sophisticated, targeted cyberattack.

A Social Engineering Attack

In faceless attacks like vishing, it's easy for attackers to pretend to be someone they're not. Callers use "social engineering" techniques to manipulate emotions and coerce people into making bad decisions.

These techniques are highly effective, and attackers are constantly looking for ways to make vishing seem more credible.

Bottom line: If something doesn't feel right, simply disconnect!



VISHING TACTICS

Pretexting

Pretexting is a lie or a misleading motive. Attackers may impersonate people and organizations you know, or that you've worked with in the past. This tactic is often used in highly targeted "spear vishing" attacks, in which threat actors do advanced planning and research before making a call.

Spoofing

Spoofing techniques disguise a caller's identity, and can make the call appear to be coming from a trusted source.

TTY (teletype) relay

The hearing-impaired often use TTY relay services, where an operator relays a typed message to a person or business. Attackers also use these services to avoid direct conversations and thoroughly disguise their identity and their location.

Deepfakes

These calls use sophisticated artificial intelligence to impersonate someone's voice—usually a high-ranking executive or authority figure. While rare, deepfake vishing calls do happen, and are likely to become more common.

Robocalls

These automated messages can reach thousands of individuals, and claim to come from any number of sources (including law enforcement, tax agencies, and charitable organizations).

Planted phone numbers

In some cases, victims are tricked into initiating a vishing call. Attackers plant fraudulent phone numbers in phishing emails, voicemail messages, social media posts, and web search results … then wait for unsuspecting people to call.

COMMON THEMES

Many vishing calls follow well-established patterns. Be very suspicious if you receive a call that presents one of the following scenarios.

Urgent payment request

A caller may claim to be a representative from a company that you normally deal and insist you make a payment immediately to avoid termination of service.

Financial account security

Banking and credit card scams are common, with callers asking you to "confirm" your personal information for security purposes.

Legal or tax trouble

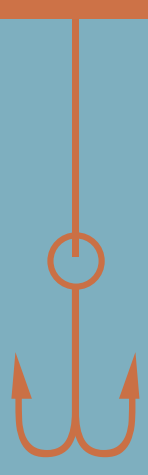
Attackers often pose as government officials and claim you must make a payment immediately to avoid being arrested.

Tech support issues

An attacker may claim they need to help you update your computer software to avoid harm to your device.

A valuable opportunity

You might be offered the chance to invest in an exciting venture, or be told you have won a free vacation or prize. The catch? You have to pay a small upfront fee ... right now.



Suspect a vishing attack?

Report suspicious calls at work to your security team and manager.

Follow local or regional recommendations for reporting fraudulent calls received at home.

STOP THOSE VICIOUS VISHES!

Always be wary of unsolicited and unusual phone calls and voicemail messages. Be especially careful if you feel pressured to:

- Make an immediate payment you weren't expecting
- Provide personal information about yourself; your boss; your coworkers; or your organization's vendors, customers, or operations
- Act quickly to take advantage of a special offer
- Pay for products or services via gift card, wire transfer, or Bitcoin

Remember: With vishing attacks, you are in control, because **you can disconnect.**