TN Department of Finance & Administration | Strategic Technology Solutions

Spoofed phone calls

Vishing

Vishing — or “voice phishing” — is phishing via phone call. Vishing scams commonly use Voice over IP (VoIP) technology like we have in state government.

Vishing attacks are sometimes called “social engineering attacks.” While 96% of phishing attacks arrive via email, criminal hackers can also use social media channels to trap you. Regardless of how the attack is delivered, the message will appear to come from a trusted sender.

Like targets of other types of phishing attacks, the victim of a vishing attack will receive a phone call (or a voicemail) from a scammer, pretending to be a trusted person who’s attempting to elicit personal information such as credit card or login details.

We have had a small number of reports of attempts to spoof the STS Customer Care Center with the actual phone number (615) 741-1001.

So how do the hackers pull this off? They use a range of advanced techniques, including:

Faking caller ID, so it appears that the call is coming from a trusted number
Using synthetic speech and automated call processes

A vishing scam often starts with an automated message, telling the recipient that he or she is the victim of identity fraud. The message requests that the recipient call a specific number. When doing so, they are asked to disclose personal information. Hackers then may use the information to gain access to other accounts or sell the information on the Dark Web.

How to Identify a Vishing Attack

We can categorize vishing attacks according to the person the attacker is impersonating: Businesses or charities — Such scam calls may inform you that you have won a prize, present you with you an investment opportunity, or attempt to elicit a charitable donation. **If it sounds too good to be true, it probably is.**

Banks — Banking phone scams will usually incite alarm by informing you about suspicious activity on your account. Always remember that banks ***will never*** ask you to confirm your full card number over the phone.

Government institutions — These calls may claim that you are owed a tax refund or required to pay a fine. They may even threaten legal action if you do not respond.

Tech support — Posing as an IT technician, an attacker may claim your computer is infected with a virus. You may be asked to download software (which will usually be some form of malware or spyware) or allow the attacker to take remote control of your computer.

How to Prevent Vishing Attacks

The key to preventing vishing attacks is security training.

Training can help ensure all employees are familiar with the common signs of phishing and vishing attacks which could reduce the possibility that they will fall victim to such an attack.

But, what do you do if you receive a suspicious message?
The first rule is: don't respond.

If you receive a text requesting that you follow a link, or a phone message requesting that you call a number or divulge personal information — ignore it, at least until you've confirmed whether or not it's legitimate. The message itself can't cause damage, but acting on it can.

If the message appears to be from a trusted business, search for their phone number and call them directly. For example, if a message appears to be from your phone provider, search for your phone provider's customer service number and discuss the request directly with the operator.

If you receive a vishing at work or on a work device, make sure you report it to your IT or security team.

Unfortunately, we can’t block these types of call, but we would like to remind you that spoofed calls can come from any familiar number including the Service Desk.

For more info: https://www.fcc.gov/spoofed-robocalls

You are a part of Cyber Security.

Cyber security is how we protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: confidentiality, integrity, and availability.

Cyber security is achieved through implementing technical, management, and operational controls designed to protect the confidentiality, integrity and availability of information. Your continued investment in participating in this year’s information security training class, will help drive the actions and activities that will help to sustain a culture of cyber security here at the state.

If you *think* you are being spoofed with a unsolicited call from the STS Customer Care Center at 615-741-1001, hang up and call them back directly.

Remember: always trust your instincts. If an email, phone call or an attachment seem suspicious, don't let your curiosity put your computer at risk! If you see or hear something cyber suspicious, please contact the STS Customer Care Center at 615-741-1001.

Best regards to all,

Curtis Clan | Chief Information Security Officer