# Vishing and Smishing: What You Need to Know

It would be great if technology could solve all of our cybersecurity problems. We rely on security systems such as antivirus software, firewalls, and software updates to protect our devices and data. However, at the end of the day it all comes down to people. According to the Verizon 2022 Data Breach Investigations Report, 82% of breaches involved the Human Element, including Social Engineering Attacks, Errors, and Misuse.

Phishing e-mails continue to be one of the most popular methods of attack used by cybercriminals, but they are not the only method. Let's review some additional types of social engineering attacks and what you can do to protect yourself.

## Voice Phishing (Vishing) and SMS Phishing (Smishing)

- **Vishing.** In vishing attacks, scammers use phone calls or voice messages to impersonate legitimate businesses and trick you into giving them money or revealing personal information. Sometimes these fraudulent calls are made by actual people; other times they are done via robocalls. Worse yet, the scammers may spoof phone numbers that belong to real companies or individuals to deceive you.
- **Smishing.** In smishing attacks, scammers send phishing messages via text messages or messaging apps to your smart phone or tablet. Like phishing e-mails, you are prompted to open a link to access a website or app. The link may take you to a login page to enter your username and password, a form to provide your personal information, or a malicious app that infects your device.

## Common Vishing and Smishing Scams

Below are examples of common Vishing and Smishing Scams to look out for.

- **Demands for payment**. The scammer pretends to work for a government agency such as the IRS and tells you that you owe money. They may threaten that you will be fined or even arrested if you do not pay.
- **Account verification.** The scammer poses as an employee of your bank or credit card company and states that they noticed unusual activity on your account. You are asked to provide personal information to verify your account.
- **Program enrollment.** The scammer represents themselves as a representative of a government program such as Medicaid and offers to help you with your benefits. You are asked for your personal or financial information to complete enrollment.

- **Order/shipping confirmation.** The scammer sends you a link to track a package or confirm your order, even though you did not order anything recently. The link may ask for your username and password or install malicious software on your device.
- **Winning a prize.** The scammer informs you that you won a contest. From there, they may ask for personal information or walk you through accessing your bank account so you can receive a deposit.
- **Tech support.** The scammer offers to fix a computer problem that you didn't even know you had. They may ask you to visit their support website, install software to give them remote control, or provide them with your accounts and passwords.

## How to Protect Yourself from Vishing and Smishing Scams

Here are some tips to help protect yourself from both vishing and smishing scams.

- **Pause, think, and act.** Scammers will stress a sense of urgency to trick you into doing what they want. Don't take the bait. Take time to think about what you are being asked to do and why before you take any actions. Think twice before clicking on links in text messages. Instead, visit the organization's website directly to ensure you are communicating with the real business.
- **Do not answer the phone or respond to texts from unknown numbers.** If the scammers can't reach you, they can't trick you. If you do answer the call, hang up immediately.
- **Keep your personal information private.** Never give out personal information such as account numbers, Social Security numbers, passwords, or Multi-Factor Authentication (MFA) codes to unknown people.
- **Verify the source.** If you receive a message from someone who says they represent a company or a government agency, hang up and contact them by using the contact information posted on the organization's website.
- **Enable strong security on your accounts.** Creating strong and unique passwords is still a security best practice for protecting your personal and financial information. If you have difficulty creating unique passwords for each of your accounts, consider using password generators and managers to develop more complex passwords and store them securely as well. Enable MFA when available as an added layer of protection for your online accounts.

## Additional Resources

- FCC: Caller ID Spoofing
- CISA: Avoiding Social Engineering and Phishing Attacks

MS-ISAC®
Multi-State Information Sharing & Analysis Center®
STOP | THINK CONNECT™

The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.