Scammers Calling: How to Prevent Getting Scammed Over the Phone

According to the Federal Trade Commission (FTC) they received more than 2.1 million fraud reports from consumers in 2020, with fraud costing consumers about $3.3 billion. One of the most common types of scams aimed to steal your identity are phone scams.

When a phone scammer gets you on the line, they will likely not hang up until they get your personal data. Common tactics phone scammers use is to claim that they are from the Department of Veterans Affairs (VA) or the Social Security Administration and there is an issue with your social security number, and they will need you to provide the number to them. They often also claim that you have an unpaid debt, taxes, or fines or they would try to make you believe that you have won a large cash prize or a raffle.

Common Tactics Used by Phone Scammers

Scammers are getting increasingly creative in obtaining personal information from you. Below are common tactics that scammers use:

- **Robocalls.** Scammers use spoofing tools to make millions of robocalls a day easily. They call you from a number you may recognize to numbers that appear legitimate to get you to answer the phone. Their goal is to engage with you over the phone and either entice you or scare you into sharing your personal information – social security number, credit card information, address, or other personally identifiable information.
- **Voice Phishing or "Vishing."** Scammers commonly use voice calls or messages to try to get personal information from you. Common vishing tactics include unsolicited loan offers, reports of "compromised" bank or credit accounts or unpaid IRS taxes. Vishing also includes scammers impersonating reputable agencies or individuals to try to obtain your personal information.
- **SMS Phishing or "Smishing."** Scammers are increasingly using text messages to deceive consumers into providing their personal information. Smishing text messages typically request consumers' usernames and passwords, credit card information, PINs, and other categories of data they could use to commit fraud.
- **Phone Hijacking.** Scammers can hijack your phone without physically taking your phone from you. And sadly, it is easier than one would think. Scammers will learn about you online; your name, address and phone number are often used. Then they will contact your phone service provider and request that they transfer the service from an old phone to a new one. They provide the cell company with the identifying information they have on you, and then the cell company ports your number to "your new device." Once that process is complete, the scammer can disconnect your phone number, reset passwords, and access the information on your phone.

VA | U.S. Department of Veterans Affairs
Office of Information and Technology

What to Look For

There are multiple types of phone scams, but scammers use very common tactics, they might attempt to:

- **Seek payment from you.** Phone scammers will try to get you to provide personal financial information. This information could be used to access your accounts; payment via gift card, pre-paid debit card, cash, or wire transfer over the phone; and will not be able to provide you with a safe payment alternative. They may ask you to pay your unpaid bill or raffle entry cost using defined payment such as cryptocurrency or mailing them cash. VA will never request payment by phone.
- **Avoid providing proper identification.** Do not rely on caller ID to verify that the caller is a government employee, as many scammers "spoof" official government numbers. VA will not call you unexpectedly to request information from you.
- **Make vague threats.** Scammers only make money when they receive personal data or payment from you, and they will work hard – even through threats – to get information from you. They may resort to threatening you with arrest, a lawsuit, property liens, or suspending your social security number. VA, other federal agencies, and legitimate businesses will allow you to evaluate your options and avoid high-pressure sales tactics.
- **Offer to provide proof of their legitimacy.** Phone scammers may offer to send official letters or reports by email to convince you they are legitimate employees, but these can easily be faked or spoofed. You can validate if VA is calling you by contacting a VA official using the publicly available contact information.

Don't be a Victim

VA Privacy Service recommends you do the following to prevent phone scammers and fraudsters from stealing your personal information:

- DO NOT provide any personal data or payment details over the phone.
- Sign up for the FTC's Do Not Call Registry (https://www.donotcall.gov/), which will likely not stop robocalls but can limit them.
- Hang up the phone if believe you are being scammed or pressured to provide personal information from someone you do not know.
- Verify the caller's organization. If the scammer claims to be from a legitimate organization, ask for a call-back number, then check to see if the organization's website is professional (typos and bad grammar are red flags); has a privacy policy; and has a verifiable street address. You also can check with the Better Business Bureau or search online to see if complaints have been filed against the business.
- Add known scammers to your blocked contacts list.
- Report the scam to the FTC (https://reportfraud.ftc.gov/#/assistant).

Additional Resources

VA Privacy Services provides a toll-free Identity Theft hotline (1-855-578-5492) and a website to help Veterans protect their data and report identity theft. Learn more about VA Privacy Service (www.va.gov/privacy) or email privacyservice@va.gov.

VA Fraud, Waste and Abuse Initiative:

https://www.va.gov/COMMUNITYCARE/about_us/POI/poi_fwa.asp

VA | U.S. Department of Veterans Affairs
Office of Information and Technology