FORGE

# The Arkansas Cyber Defense Center

## Phone Spoofing Scams

This type of attack happens when a scammer uses caller ID to make it appear they are contacting you from a trusted source.

**Why be aware of this attack?**

Phone spoofing can be done to attack anybody at any level within an organization. It is easier for a scammer to gain a victim's trust if the caller ID corroborates who they claim to be. Once they gain the victim's trust, scammers have a much easier time getting what they want.

**Common types of phone spoofing scams:**

- "This is Jimmy from tech support. There is a problem on your computer and we need remote access the fix it." The scammer then proceeds to put malware on your computer or steal data.
- "You have won a prize, we just need you to pay to claim the prize."
- "Your loans are being forgiven! (We just need you to make a quick payment."
- "The IRS says you owe them money, and they will come after you if you do not pay."
- A utility company calls and says you need to make a payment or your services will be shut off.

**Red flags:**

- The caller asks for payment in gift cards
- Threatening legal action if you do not pay immediately
- They ask for personal identifiable information (social security number, DOB, etc.)
- The caller ID shows a number that is/close to your number

**Immediate action:**

1. Hang up and block the number.
2. If you have already sent a wire transfer, contact the issuer to see about stopping the transaction.
3. If you have already provided your financial information, contact your financial institution to see about stopping transactions.

POWERED BY SBA U.S. Small Business Administration



REPORT A CYBER INCIDENT:

**forge.institute/acdc**

501-239-9599