FS-ISAC

Security Tips Newsletter

5 July 2024 | Issue No. 11

Security is Everyone's Responsibility

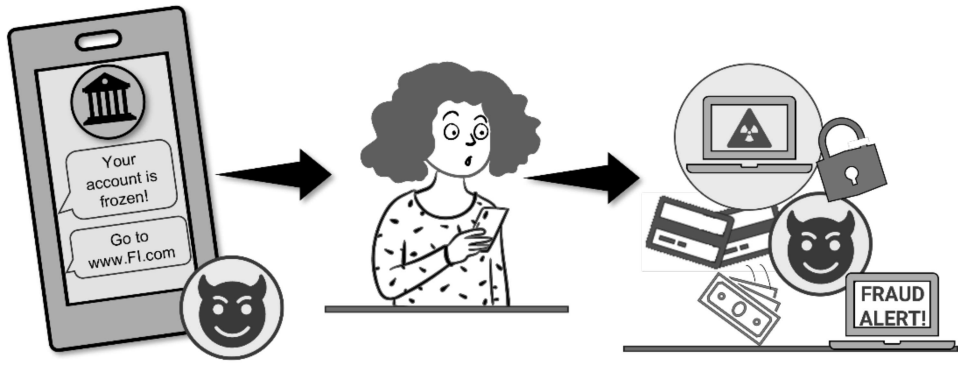
Keeping an Eye Out for Telcom Attacks

Summary

Voice Over Internet Protocols (VoIP) is one-way threat actors attempt to trick unsuspecting consumers into sharing their confidential information, such as user names, passwords, bank account information, and the like. These actors frequently use "ID Spoofing" as vehicles in their attack campaigns.

ID Spoofing is when a caller deliberately falsifies the information transmitted to a caller ID display to disguise their identity. Scammers often use "neighbor spoofing" so it appears that an incoming call is coming from a local number, or spoof a number from a company or a government agency that the victim probably knows and trusts. Then they use scam scripts to try to steal money or valuable personal information that can be used in fraudulent activity.

Smishing is a similar form of social engineering fraud, but it exploits SMS, or text, messages rather than VoIP. In a smishing scheme, the scammer purports to be a known entitity and texts a link to such things as webpages, email addresses, or phone numbers that, when clicked, automatically open a browser window or email message or dial a number. This integration of email, voice, text message, and web browser functionality increases the likelihood that users will fall victim to engineered malicious activity.



The scammer sends a seemingly real message, but it contains a malicious link.

The user opens the text, clicks on the link, and then provides the account information.

The information is used by the attacker to commit fraud or make a profit.

Red Flags

- Demands for payment
- Program enrollment
- Winning a prize
- Account verification
- Order/shipping confirmation
- Tech support

Tips To Help You Remain On Guard

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in a text or email, and do not respond to email solicitations for this information. This includes following links sent in a text or email.
- Don't send sensitive information over the internet without checking a website's security.
    - Pay attention to the Uniform Resource Locator (URL) of a website. Look for URLs that begin with "https" - an indication that sites are secure - rather than "http."

Resources

If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to IC3.gov, and the police, and file a report with the Federal Trade Commission.

Getting Help

If you identify suspicious activity involving your [Institution] account, contact us immediately.

