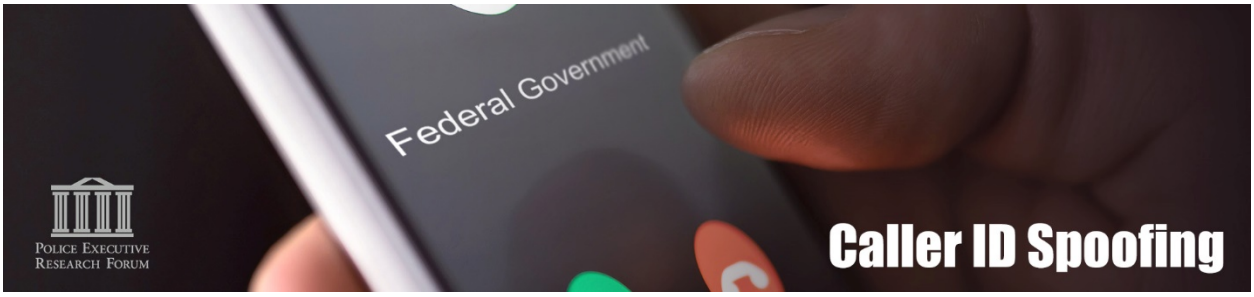

What is Spoofing?

Spoofing is a very common type of scam carried out by cybercriminals. According to the FBI, spoofing is when a criminal "disguises an email address, sender name, phone number, or website URL—often just by changing one letter, symbol, or number—to convince you that you are interacting with a trusted source."[1]

Caller ID spoofing

According to the Federal Trade Commission (FTC), caller ID spoofing is specifically when "a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity."[2] These scammers frequently try to gain their victims' trust by using "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] may already know."[3] Once the victim answers the phone, the scammer will attempt to try and gain personal information or request money to carry out fraudulent activities.[4]

[1] https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing
[2] https://www.fcc.gov/consumers/guides/spoofing-and-caller-id
[3] Ibid.
[4] Ibid.

Source: https://www.consumer.ftc.gov/articles/caller-id-spoofing-infographic

In 2019, the Federal Trade Commission received more than 3.2 million fraud reports. Of these reports, caller ID spoofing was the primary method used by scammers, resulting in an average loss of $1,000 per victim.[5]

According to a recent Consumer Reports survey, 70% of consumers do not answer incoming calls from an unknown number.[6] As a result, many scammers utilize caller ID spoofing to appear as a recognizable number to get potential victims to answer the phone. In First Orion's analysis of scam calls, they found that 83% of all scam callers featured a familiar phone number, with either a familiar area code or business name used to lure the intended victim into answering their phone.[7]

Spoofing of Law Enforcement Agencies' Phone Numbers

Scammers will often spoof law enforcement agencies' phone numbers to target victims into thinking the police, a trusted source, is calling them. There are several examples of this spoofing scam happening to police departments across the country.

For example, in December 2020, the Herndon (VA) Police Department had their non-emergency phone number spoofed. Victims received calls from an individual claiming to be a lieutenant with the department, who asked for money and other personal information.[8]

In October 2020, the Sommerville (MA) Police Department's non-emergency number was spoofed. The scammer, claiming to be a law enforcement officer investigating criminal cases involving the resident, attempted to solicit personal information such as social security numbers, date of birth, and bank information.[9]

In April 2020, the Salem (OR) Police Department's non-emergency line was spoofed. The scammer, claiming to be a sergeant with the department, attempted to collect money from people by telling them they had outstanding arrest warrants, but they could pay a fine to him to avoid arrest.

Even the FBI has been a victim of spoofing scams. In January 2020, the FBI put out a release warning that scammers were spoofing the FBI Headquarters' phone number. In the scam, cybercriminals were posing as FBI agents, providing a fake name and badge number, and then informing victims that their Social Security number had been suspended. The "scammer tells the victim that in order to get their Social Security number reinstated, they must purchase gift

[5] https://www.consumer.ftc.gov/blog/2020/01/top-frauds-2019
[6] http://firstorion.com/wp-content/uploads/2019/07/First-Orion-Scam-Trends-Report_Summer-2019.pdf
[7] Ibid.
[8] https://www.facebook.com/Herndonpolicedepartment/posts/4038519279511274
[9] https://www.cambridgema.gov/News/detail?path=%2Fsitecore%2Fcontent%2Fhome%2Fcpd%2Fnewsandalerts%2Farchives%2F2020%2F10%2Fcityofcambridgewarnsresidentsofphonescamspoofingcambridgepolicenumber

card(s), put money on the card(s), and call the scammer back and provide the gift card number(s)."[10]

These types of spoofing scams are a serious issue. According to the Internet Crime Complaint Center (IC3), "13,873 people reported being victims of government impersonation scams in 2019, with losses totaling more than $124 million."[11]

Caller ID Spoofing Mitigation

The FCC highlights several actions steps to protect someone from falling victim to a caller ID spoofing scam:

- Do not answer calls from unknown or strange numbers.
- Hang up the phone once you recognize it may be a scam.
- Never give out personal information such as account numbers, Social Security numbers, mother's maiden names, passwords or other identifying information in response to unexpected calls or if you are at all suspicious.
- If you get an inquiry from someone who says they represent a company or a government agency, hang up and call the phone number on your account statement, in the phone book, or on the company's or government agency's website to verify the authenticity of the request. You will usually get a written statement in the mail before you get a phone call from a legitimate source, particularly if the caller is asking for a payment.
- Talk to your phone company about call blocking tools and check into apps that you can download to your mobile device.[12]

Victims of caller ID spoofing scams should file a complaint with the FCC, at https://consumercomplaints.fcc.gov/hc/en-us, or a complaint with the FTC, at https://reportfraud.ftc.gov/#/.

Resources for law enforcement:

- Check out the FBI's article on *Investigating Scam Phone Calls* for information on steps to take to identify the scammer.
- Educate the community on spoofing scams, including how to identify when a call is a scam. Emphasize that a police agency would never call someone asking for money or personal information.
- If your agency has become the victim of a spoofing scam, inform the community via a press release, social media, etc. to make them aware and alert of the scam.

[10] https://www.fbi.gov/contact-us/field-offices/washingtondc/news/press-releases/fbi-warns-of-scammers-spoofing-fbi-phone-number-in-government-impersonation-fraud
[11] Ibid.
[12] https://www.fcc.gov/consumers/guides/spoofing-and-caller-id

Example of social media outreach from the Herndon (VA) Police Department's Twitter to inform their residents of a spoofing scam in December 2020:

[13]

Conclusion

As technology continues to advance, cybercriminals are finding new ways to carry out cybercrimes. Cybercriminals utilize caller ID spoofing to appear as a trusted caller and take advantage of unknowing victims. As the frequency of these crimes continue to rise, it is vital to be informed on how to spot and react to caller ID spoofing scams.

[13] https://twitter.com/HerndonPolice/status/1334914551998013445?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1334914551998013445%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fpatch.com%2Fvirginia%2Fherndon%2Fherndon-police-warn-town-residents-telephone-scam