

Recent Phone Spoofing Scam Advisory

Dover – The Delaware State Police are issuing the following advisory in response to a recent phone scams involving a “spoofed phone number”.

The Delaware State Police were made aware of multiple incidents in which individuals received a phone call advising that they were under investigation. The caller asked the individuals to verify all of their information, and threatened to “put a hold on their Social Security number” if they did not comply. The call is appearing on caller ID as a Delaware State Police issued phone number. The caller suggested to the victims to look up the phone number in which they are calling from so that the victims would see that it is in fact a Delaware State Police issued phone number.

A second scam incident was also reported today in which the caller identified themselves as the “Delaware State Police Alliance” requesting donations on behalf of the Delaware State Police. The call appears on caller ID to be originating from a Frankford area phone number.

Caller ID spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Spoofing is often used as part of an attempt to trick someone into giving away valuable personal information so it can be used in fraudulent activity or sold illegally.

The Federal Communications Commissions has provided the following tips to avoid spoofing scams:

You may not be able to tell right away if an incoming call is spoofed. Be extremely careful about responding to any request

for personal identifying information.

- Don't answer calls from unknown numbers. If you answer such a call, hang up immediately.
- If you answer the phone and the caller – or a recording – asks you to hit a button to stop getting the calls, you should just hang up. Scammers often use this trick to identify potential targets.
- Do not respond to any questions, especially those that can be answered with “Yes” or “No.”
- 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.
- Use caution if you are being pressured for information immediately.
- If you have a voice mail account with your phone service, be sure to set a password for it. Some voicemail services are preset to allow access if you call in from your own phone number. A hacker could spoof your home phone number and gain access to your voice mail if you do not set a password.
- Talk to your phone company about call blocking tools they may have and check into apps that you can download to your mobile device to block unwanted calls. Information on available robocall blocking tools is available at [fcc.gov/robocalls](https://www.fcc.gov/robocalls).

<https://www.comparitech.com/blog/vpn-privacy/robocalls-analysis/>

[s/](#)

This information was provided through the Federal Communications Commissions website located at:

<https://www.fcc.gov/consumers/guides/spoofing-and-caller-id>

Many of these scams are difficult to investigate. They will target persons of all age groups. The Delaware State Police is asking citizens to remember the tips previously mentioned in order to not become a victim of one of these scam artists.

If you suspect you have been a victim of this scam, please contact your local law enforcement agency. Information may also be provided by calling Delaware crime stoppers at 1-800-TIP-3333 or via the internet at <http://www.delaware.crimestoppersweb.com>

You can follow the Delaware State Police by clicking on:

[Delaware State Police Official Web Site](#)

[Facebook](#)

[Twitter](#)

[Nextdoor](#)

Please tell us how we're doing via our [Citizen Satisfaction Survey](#).

*Presented by Public Information Officer, Master Corporal
Melissa Jaffe*

Released: 020119 1251

-End-