****PUBLIC SERVICE ANNOUNCEMENT****

Town of Gordonsville Police Department

Authorities from the Town of Gordonsville Police Department, are warning residents about an influx of phone calls from scammers.

Police want to warn residents of the following scams:

The Neighbor Spoofing Scam: A form of subterfuge that has grown exponentially in the past year, this trick involves "spoofing" (faking) the caller ID information that is displayed when crooks call or text you. Knowing that people are more likely to trust a call that comes from an individual or business in their area, criminals use special software to change the number that appears on your screen to one with your area code and prefix (the first three digits of a seven digit number). Not only are you more likely to pick up the phone when it rings, but the fake phone number makes it more difficult for authorities to track. Because it's easy for the scammer to get around call blocking, it's generally best not to answer calls from unknown numbers like these. Also, watch out for calls from your own number. Scammers may use it hoping your curiosity will override any reasonable caution.

The New Medicare Card Ploy: While con artists have been impersonating representatives from Medicare for years, the roll out of new Medicare cards between April 2018 and April 2019 gives them a brand new opportunity to exploit. So what's the problem with the new Medicare cards? Nothing, they've actually been created to provide better protection against fraud and identify theft and have a unique 11-character code as an identifier instead of a social security number. But it's important to guard yourself or your loved ones against the possibility that criminals may use them as an excuse to contact Medicare beneficiaries for a variety of nefarious purposes. Callers may claim that they must verify a Social Security number or other sensitive information in order to issue the new card, or they may insist on payment for it via money wire, credit card or gift card. Be aware that there is no fee for the new Medicare card and no action that beneficiaries need to take to receive them. Furthermore, a legitimate Medicare representative will never ask for personal information via phone or email, and official correspondence from Medicare is sent via mail.

The Smishing Attack: The mobile phone version of an email phishing scam, "smishing" (SMS phishing) occurs when an attacker contacts you by text to acquire financial information or other personal data by posing as a trustworthy entity such as your financial institution. In many cases, they'll tell you that there is a problem with your account in order to get you to reveal sensitive banking details such as your account number, password or PIN. For example, you might be asked to provide certain details in order to unlock your account or told to call their fraud prevention hotline, which will of course be answered by the fraudster. These texts may also prompt you to click on a link to a fraudulent website. As with your email, don't assume that a text message is authentic, and be aware that financial institutions like credit unions and banks will never ask you to reveal security details such as your PIN or password over the phone or via text. Even if a caller is appearing to be calling you from a legitimate number, keep in mind that it could be spoofed. To check the status of your account and any possible fraudulent activity, call the number on the back of your card right away. You should also check online for unauthorized transactions, but be sure to type the web address of your financial institution directly into your browser.

The Jury Duty Scare: Although scams in which callers attempt to shake down law-abiding citizens with threats of an arrest for failure to show up for jury duty are not new, they are still being

effectively used throughout the country. Typically, scammers tell potential victims that they have a summons to appear in court for missed jury duty or a warrant for an arrest, and that they must pay a fee immediately to avoid being arrested. They may also claim to need your personal details in order to cancel an arrest warrant. In another twist on this scam, they call with a seemingly innocuous request of verifying your information for future jury duty. In all of these scenarios, they may manipulate the number that displays on your phone or caller ID to make it look as though the courthouse or police agency is calling.

For those of us who are civilians, keep in mind that **no member of a law enforcement agency** will contact you by phone to demand money and they don't provide a warning by phone about an impending arrest. The only time a courthouse employee might contact you by phone is if a jury duty summons was returned to the sender as undeliverable. And if the courts do reach out to you by phone, they won't ask that you reveal sensitive information like your Social Security number or birth date. Regardless of how much the caller persists, refuse to give out this information, and of course, hang up immediately. If you're concerned about jury duty, contact the courts directly.

A Word About Tax Scams: We can always count on plenty of imposters looking to cash in on taxpayer dollars and this year promises to be no different. Tax scams take various forms from criminals who acquire private information in order to file fraudulent tax returns to intimidating calls from IRS agent impersonators demanding immediate payment for back taxes supposed owed. Just remember that the IRS will not call you with a demand for immediate payment, and they won't demand a specific form of payment to settle your debt or ask for financial information over the phone. Also be aware that tricksters may try to convince that they had previously attempted to contact you by mail but that their correspondence was returned. If you get a call like this, hang up the phone. You can report the incident to the Treasury Inspector General for Tax Administration (TIGTA) at http://bit.ly/IRSImpersonationScamReport, or call their hotline at 800-366-4484.

Police want to remind residents:

1. The real IRS does not call people.
2. The IRS does not accept payment via Walmart or Rite Aid.
3. The IRS does not call police departments directly and say go arrest *your name here*

Quick Tips for Reducing Unwanted Calls and Dealing with Phone Scams

Of course, one of the best ways to fend off phone scams and unwanted phone solicitations is simply not to answer calls from numbers that you don't recognize. But again, remember that it's easy for scammers to fake a phone number. If you answer the phone and the caller seems suspicious, just say, "No thanks," and hang up right away.

If you have questions or concerns, please do not hesitate to call the Gordonsville Police Department at (540) 832-2234, physical address 112 South Main Street, Gordonsville, VA.