FRAUD ALERT

February 2020

Who's Really Calling? Beware of Growing Government Impostor Phone and Email Scams

How the Imposter scams work:

Have you received the fake call(s) "from the Social Security Administration?" Did you know that older adults and people with disabilities are often singled-out and targeted, oftentimes receiving multiples calls like these every day?

Scammers are increasingly using phone calls, emails, and even text messages to impersonate government officials in an attempt to steal money and personal information.

The plan is simple for these "impostor scams." They call, email, or text claiming to represent a government agency such as the Social Security Administration (SSA), Internal Revenue Service (IRS), or Department of Health and Human Services (HHS). Some even "spoof" their phone number or email address so that it looks like the call or email is coming from a legitimate government phone number or e-mail address. They lure victims by telling them they've "won the lottery" sponsored by the federal government or "owe a debt" to the IRS that must be paid back immediately. They may even claim that a person's social security number has been linked to criminal activities and suspended, and all they have to do to reactivate it is to "just confirm" the social security number. They will often use threats of arrest or harsh legal action to create a sense of panic, and demand payment via wire transfer or gift card (so the payment cannot be traced).

One of the best protections against this and other scams is knowledge. When people are familiar with these scams, they are less likely to lose money. Telling others about these scams may help stop the scammers and the harm they cause.

Reporting the scam calls matters!

What you should know:

- **The government will never call out of the blue and ask for a social security number.**
- **The government will never ask for payment by gift card or wire transfer.**
- **Social security numbers cannot be suspended.**

How to Respond:

- If you are ever suspicious about a call, hang up immediately.
- Never click on an e-mail link or attachment unless you fully trust the sender.
- Never pay someone you do not know well via gift card or wire transfer.
- Always be cautious about giving out your personal or financial information, including your Medicare or Social Security numbers, or any banking information.
- Sign up for the National Do Not Call Registry.

REPORT all scams to the Arkansas SMP — 866-726-2916

The Arkansas SMP (Senior Medicare Patrol) is a grant program administered by the Department of Human Services Division of Aging & Adult Services. This publication was paid for by a grant from the Administration for Community Living, Administration on Aging (AoA). Points expressed herein do not necessarily reflect official AoA policy.