Area IV Agency on Aging 1(800)551-3191

February 2020

'Care Share

10 TIPS TO HELP KEEP YOU SAFE FROM COMMON SCAMS

1. Write the full year 2020 on your checks, contract agreements or any legal docs so people can't change them to a future or past year.

2. Medicare only pays for lab tests or supplies that are medically necessary and are ordered by your doctor. Don't accept unnecessary supplies and report to your local SMP at 800-551-3191 if you see charges on your MSN's, including genetic test kit scams.
***MSN is the Medicare Summary Notice**

3. If you receive an unsolicited call, NEVER give your Medicare number, bank account numbers or any personal info if asked.

4. Social Security will never:

   - Suspend your card
   - Threaten you with arrest unless you pay a fine
   - Require a payment by gift cards, etc. ***No one legitimate will ask for this**
   - Email you with or without attached letters.

5. If an email seems odd, hover over the address to make sure it's actually from the sender BEFORE you open it and delete if not. Do not click on links unless you know the sender. Don't be afraid to check with sender by phone first if you're not sure.

6. Thieves "phish" for your personal and bank info by tricking you into clicking on a link in an email or text. They often send very legitimate looking emails or text messages. See #5

7. Caller ID spoofing is how crooks make a phone call or email look legitimate. It can look like any number they want it to, including a local one even when they're actually calling from outside of the country. See #3.

   Do not answer your phone if you don't recognize the number. If it's important, they will leave a message. If it's not someone you know well, independently look the number up before calling them back.

   It could be a robocall that is created electronically. If you answer you will be logged as a "live line" and will stay on rotation. Don't answer, block the calls, and over time you will receive less calls.

   The "Your grandchild is in jail" robocall is never true. If you answer, hang up immediately. Then call your grandchild or a family member to be assured your loved one is safe.

8. Do not let personal information be visible on your luggage tags when traveling.

9. Shred all papers with your personal information on them.

10. Report scams to AARP Fraud Watch if you think you might be a victim.

11. Call 877-908-3360 and a trained volunteer will help direct your next steps. Find info about the latest scams on www.aarp.org/fraudwatchnetwork.

Fraud Avoidance for Veterans

Over the past four years, there has been a **4x increase in fraudulent activity against Veterans, their survivors, and dependents.** VA is actively working to prevent these incidents, but the best line of defense against this criminal activity is you!

Here are some tips about being contacted regarding your Veterans Affairs (VA) benefits:

1. If you receive correspondence from VA concerning a claim, and you don't remember filing a claim, contact VA directly at **1-800-827-1000** to confirm details.

2. VA will **never charge you for processing a claim** or request a processing fee prior to releasing benefit payments.

3. VA will **never ask for your personal information via email.** This includes verification of your SSN, address, and/or bank information. VA only addresses personal information via mailed letters.

4. VA may check in with you by phone, email, or text message. If you are unsure about any call, email, or text, confirm details with VA directly at **1-800-827-1000.**

5. VA **does not threaten** claimants with jail or lawsuits.

6. **Be cautious of telephone numbers** on your caller ID. Scammers can change the telephone number (spoofing) to make a call appear to come from a diffferent person or place.

7. **When in doubt, hang up** and call VA directly at 1-800-827-1000, or call your Power of Attorney representative (DAV, VFW, etc).

8. If you receive an email or letter from VA notifying you that your direct deposit information was updated, or that your eBenefits account information was updated, and you don't remember doing so — immediately contact VA at 1-800-827-1000. **Do not ignore the email or letter.** It could be your first sign that your information has been compromised.

VA | U.S. Department of Veterans Affairs

To learn more about protecting yourself from fraud, and how to report it, visit **https://www.va.gov/oig/hotline/default.asp**, or go to **VA.gov** and search "**Office of Inspector General**". For more details on how to avoid scams, go to **https://www.fcc.gov/veterans-targeted-benefits-scams**. Download free financial scam awareness resources at **https://www.consumerfinance.gov/about-us/blog/helping-prevent-scams-targeted-veterans/**