

Daily Union Article

Saturday, January 21, 2017

Title: Don't Be A Target

I recently received a phone call from a Geary County resident who is approaching their 65<sup>th</sup> birthday. She shared that she is receiving a significant amount of mail regarding her upcoming qualification for Medicare. Her question is "How do I know what mail and emails are legitimate and what is a scam?"

That is a common and relevant question I get about Medicare. In my SHICK training class, the speaker told us that approaching the age of 65 puts a target on your back. You become the target for advertisements, a target for credible insurance providers supplement plans, and a target audience for receiving communications from Social Security and Medicare. However, you also become the target of scammers who are trying to get your personal information for illegal purposes. Even those who have already transitioned to Medicare continue to be targeted by these audiences – including scammers.

Social Security recently reported of a scam where individuals were posing as Social Security employees who would call and ask for personal information, like your name, Social Security number and bank account information. The caller alleges that Social Security needed this information so that they could issue additional funds or rebates or they allege that because of a computer glitch your personal information has been lost.

Another scam used an email that was designed to look like it came from Social Security. It provided information about the annual cost-of-living-adjustment (COLA) and directed email recipients to a website designed to look like Social Security's site so people could "update their information" – providing valuable information for identity thieves and criminals.

Why are senior citizens especially targeted for scams? The FBI's Common Fraud Schemes website offers the following reasons:

- Senior citizens are most likely to have a "nest egg," to own their home, and/or to have excellent credit—all of which make them attractive to con artists.
- People who grew up in the 1930s, 1940s, and 1950s were generally raised to be polite and trusting. Con artists exploit these traits, knowing that it is difficult or impossible for these individuals to say "no" or just hang up the telephone.
- Older Americans are less likely to report a fraud because they don't know who to report it to, are too ashamed at having been scammed, or don't know they have been scammed. Elderly victims may not report crimes, for example, because they are concerned that relatives may think the victims no longer have the mental capacity to take care of their own financial affairs.
- When an elderly victim does report the crime, they often make poor witnesses. Con artists know the effects of age on memory, and they are counting on elderly victims not being able to supply enough detailed information to investigators. In addition, the victims' realization that they have been swindled may take weeks—or more likely,

months—after contact with the fraudster. This extended time frame makes it even more difficult to remember details from the events.

- Senior citizens are more interested in and susceptible to products promising increased cognitive function, virility, physical conditioning, anti-cancer properties, and so on. In a country where new cures and vaccinations for old diseases have given every American hope for a long and fruitful life, it is not so unbelievable that the con artists' products can do what they claim.

What should you do? First, do not give them your personal information. Social Security will NOT send you an email asking you to give them your personal information, such as your Social Security number, date of birth, or other private information.

Instead of responding, call our local Social Security Office in Manhattan, Kansas (1-877-810-5741) or the national Social Security Administration office (1-800-772-1213). Do not use any phone numbers or email addresses provided in the communication you received unless you are confident that it is legitimate. If you use the contact information listed in the email or letter, you'll be directed back to the scammer who will proceed by attempting to convince you that they are legitimate.

Here are some clues that an email is a phishing scam: 1) The email went to your junk folder, 2) When you hover the cursor over the link, it doesn't have a .gov extension (it likely has a .com extension). 3) Check for grammar – many scam emails generate from other countries and often contain subtle grammatical errors.

The postal carrier will bring a lot of mail to your box as you approach 65. These pieces of mail can be difficult to sort through as well. Insurance companies are looking for your business by signing on for a Medicare Supplement plan. Before you pick up the phone to call the company, do your research. Check the Kansas Insurance Commissioner's website for the list of companies approved to sell Medicare supplemental insurance in our state (<http://www.ksinsurance.org/healthlife/medicare/med-supp.php> )

If you planning to enroll in a Part D prescription plan, check out the plan finder on the Medicare.gov website to see what plans are available in your area ([www.medicare.gov/find-a-plan](http://www.medicare.gov/find-a-plan)). If you are uncomfortable in using a computer yourself, you can call me at the Geary County K-State Research & Extension office 785-238-4161 for an appointment to help you navigate the process. I have been trained by the Kansas Department for Aging and Disability Services as a SHICK counselor to help Medicare beneficiaries with the Part D enrollment process. I can also help field some general questions about Medicare Supplement insurance and how Medicare Part A & B work for beneficiaries.

Staying ahead of scams is difficult, so approach with caution. As a rule, "if it sounds too good to be true, it probably is." Until next time, keep living resourcefully!