

ACT

SPRING – 2022 NEWSLETTER

The Age of Scams

Today's cybercriminals use a variety of increasingly complex tricks and techniques to gain access to personal information. Adults over the age of 65 are often targeted although it is unclear whether older adults actually experience *higher* rates of fraud-scam victimization than other age groups. Older adults represent a distinct demographic group differentiated by a unique set of age-associated fraud-scam vulnerabilities. A large body of research has demonstrated that a decline in a person's cognitive ability and executive functioning are associated with reduced decision-making ability, which is required to actively avoid and resist fraud-scam activities. This decision-making process requires complex, higher-order cognitive functions that decline disproportionately among older adults (Burnes, David et al, 2017).

So, what scams are often used to target the over-65 adult population? Here is a small sampling of the most common:

- **Medicare Card Scams:** scammers are emailing, calling, and even knocking on doors, claiming to represent Medicare, and offering an array of services if you "verify" your Medicare ID number and other personal information.
- **Family Emergency Scams:** Using email, social media or a phone call, the scammer contacts you, posing as a relative or family friend in some sort of trouble and urgently requesting monetary assistance.
- **Telemarketing Fraud:** as a group, seniors make twice as many purchases by phone than the national average, and fraudsters make use of this inclination in several ways, including soliciting for fake charities—especially after natural disasters.
- **Account takeover scam texts:**

Scammers are sending fake text messages claiming that there is an issue with your bank account or shopping order. The urgent-sounding text message may have a real-looking logo and they would like you to click on a link and are then able to capture your information.

What can you do to protect yourself?

- When unknown individuals ask you to verify personal information *of any kind*, hang up the phone, shut the door or delete the email.
- Never open attachments or click on links in emails or texts that you're not expecting or that come from an unknown sender.
- Remember that no *legitimate* government agency, business, or organization will make **unsolicited contact** with you to request that you provide them with your personal information.
- No *legitimate* prize give-away, government grant, lottery or sweepstakes will require you to pay anything up front to claim your winnings.

JUST FOR FUN:

Q: Which days are the strongest?

A: Saturday and Sunday; the other days are "weekdays" (**weak** days).

Send comments or suggestions to:

Roxanne Muiruri

1730 Minor Ave, Suite 1600

Seattle, WA 98101

206-287-2881 or 1-877-879-8757 (Toll Free)

REFERENCES:

<https://www.aarp.org/money/scams-fraud/info-2021/schemes-targeting-older-adults.htm>.retrieved 5/20/21

Burnes D, Henderson CR Jr, Sheppard C, Zhao R, Pillemer K, Lachs MS. Prevalence of Financial Fraud and Scams Among Older Adults in the United States: A Systematic Review and Meta-Analysis. *Am J Public Health*. 2017;107(8):e13-e21. doi:10.2105/AJPH.2017.303821