From the desk of
Michael Aliperti
MS-ISAC Chair

6 Common Elderly Scams to Watch Out For and How to Stay Safe

A scam can be initiated via the computer (email, internet, social media), text, postal mail, in person, or a phone call. No matter the origin of the scam, the characteristics are the same:

- First, there is something to pique your interest – someone in trouble, big discount offers, lottery win.
- Second, the individual contacting you seems trustworthy, super friendly, and seems to care about you.
- Third, there's a deadline associated with the offer – act fast, act now.

There will always be scams, particularly those targeted at seniors. This month's newsletter identifies some common scams and some tips to help you take control of the situation and stay safe and stay in control.

Grandparent Scam

One of the most common scams presented to seniors is the Grandparent Scam. The caller claims to be a relative, a grandson or granddaughter, and the call is urgent. Typically, the grandchild is out of town and is in trouble, needs money fast for some emergency, and doesn't want the rest of the family to know. The caller may have bits of information, some of which could be collected from sources like social media, and prompts the senior to provide more information, making the call appear genuine.

- **This is not a legitimate call**. Hang up the phone and contact your family or the authorities.

Sweepstakes Scam

In this case, the scammer would send their target a check or something else of value, whether in the mail, email, text or phone call, that indicates the recipient won something. In order to claim the "prize," the recipient may have to send a check or money order to cover taxes and fees, and may be asked for banking information to deposit the winnings, or to buy something to enter the contest. This is so the scammer can obtain private banking information. The name of the sweepstakes may seem familiar – quite often scammers will do this to make it recognizable.

- **Legitimate contents do not ask for money or financial information up front.** Do not respond to these messages with a check, money order or cash. It is always best to never provide identifying information to anyone over the phone, text, or email especially your bank account information.

Home Improvement Scam	Scammers target seniors by providing home improvement services in order to gain access to their home, belongings, and personal information. They will arrive at their target's house, offer free inspections, or offer services to fix something they deem "needs work". Scammer will pretend to be working for the local town or county to appear more legitimate. The homeowner should stay in control of the situation and not be intimidated by the person at their door. • Never let them in your home. • Be suspicious of unsolicited offers, and ask for identification. • If work does need to be done, ask friends and neighbors who they would recommend. Be sure to get references, and only used licensed contractors. • Never pay the full amount up front. Pay as the work is completed according to a contract.
Telemarketer Scam	Scammers will target seniors in an effort to obtain financial information by claiming to be from an important institution such as a credit card company, Microsoft, Social Security Administration, Internal Revenue Service, phone company, power company, and so on. **Never feel pressured to commit to anything over the phone.** • Don't rely upon caller ID to let you know who the call is coming from. Technology today allows for calls to be masked and appear to be from a number you know or can associate with, but it is not. • Never give out personal information to an unsolicited caller. Never provide birthday, social security number (even the last 4 digits), your mother's maiden name, pet's name, bank account information or anything that can be used as password or identifying information. • Hang up and contact the company the caller claims to be with directly if you feel you need to talk to them. Refer to your copy of your phone bill, power bill, or the number on the back of your credit card or bank card to initiate contact.
Internet Scams	There are many ways scammers are using technology to take advantage of seniors. Whether it is a special offer via email, attempts to acquire your user name and password via a scheme, or skimming of information while shopping online, there are ways you can be in control and keep your information safe. If you are computer-savvy, keep these tips in mind to keep your information safe: • Never click on links in emails. • Don't open attachments for special offers. • Be careful of free offers over holidays. • Watch for malicious adds and popups. • Don't shop over public wi-fi. • Be suspicious of gift card scams –buy from trusted sources.

	• Know what your product costs. • Make sure the site is secure – look for the “lock” icon and “https” on your browser address bar when shopping. • Make sure all computer anti-virus, malware, and security software is up to date. • Don’t save credit card information online; check out as guest if offered on the site.
Charities	While there are many charities that are worthy of your donations, be sure you know who you are donating to. • Always verify the charity before making any donation by checking with your Attorney General’s office. • Know what the charity is doing with your contribution. • Avoid charities that will not answer your questions or provide written information about their programs or finances. • Talk with family, friends, or trusted sources before giving to charity. • Do not give on the spot before doing research on the charity • Never give cash or purchase gift cards for payment.

If you feel you have been scammed, or are concerned that you are a victim of fraud, contact your local law enforcement immediately. Remember to keep a close eye on bank and credit card statements, and report any unusual activity. Stay informed. Remember, you are in control!

Additional Resources	https://ag.ny.gov/sites/default/files/smart_seniors.pdf https://www.cisecurity.org/newsletter/how-to-spot-and-avoid-common-scams/ https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud https://www.pa.gov/guides/cybersecurity/ https://www.guidestar.org/ https://www.charitynavigator.org/
MS-ISAC Multi-State Information Sharing & Analysis Center STOP | THINK CONNECT™	The information provided in the MS-ISAC Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes. Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.