STAY INFORMED

Confirm a contractor. All contractors who perform at least $5,000 worth of home improvements per year must register with the PA Office of Attorney General. Consumers can verify registration by calling 1-888-520-6680 or at https://hicsearch.attorneygeneral.gov/.

Check with the Better Business Bureau or the Pennsylvania Bureau of Consumer Protection at 1-800-441-2555.

Learn more about fraud schemes and tips to protect yourself and family at the FBI's Common Fraud Schemes webpage: https://www.fbi.gov/scams-and-safety/common-fraud-schemes.

Review the U.S. Senate Special Committee on Aging's fraud book outlining the top ten frauds impacting seniors: https://www.aging.senate.gov/fraudbook/index.html.

I SUSPECT A SCAM!

Scam artists are nearly always friendly and have "honest faces" or pleasant authoritative voices. This is how they gain your trust. If you've fallen victim to fraud, take action quickly. Notify your bank and your credit card company, contact the Social Security Administration about potential identity theft and contact one of the credit-reporting agencies (Equifax, TransUnion or Experian) to place a fraud alert on your file.

CALL THE POLICE TO REPORT THE INCIDENT

If you are suspicious about people in your neighborhood contact your local police department or your local Pennsylvania State Police station.

You can also contact the Pennsylvania Office of Attorney General's Senior Protection Unit at 1-866-623-2137 or seniors@attorneygeneral.gov.

Enhancing Senior Safety
Protect Yourself From Scams

On the street · On the phone
At your door

Senior citizens are a highly targeted population for scams and fraud, and the Commonwealth of Pennsylvania has one of the highest senior populations in the country. This pamphlet is designed to educate seniors and their families about the types of crimes commonly perpetrated against seniors and steps they can take to avoid becoming a victim.

COMMON SCAMS

Schemes against seniors occur *over e-mail, the phone, and even door-to-door*. Scams may take the form of fraudulent credit card offers, charity donation requests, home improvement offers, investment opportunities, banking and wire transfers, insurance offers, fake health/anti-aging products, and sweepstakes and contests, to name a few. The fraudster may employ different tactics. They may be *friendly, sympathetic, and willing to help*, or they may try to create a *sense of urgency and fear* to get you to act quickly.

DOOR-TO-DOOR HOME IMPROVEMENT/CONTRACTOR SCAMS

Never deal with a contractor who shows up unsolicited, offers "left-over materials," or offers significant discounts. Never pay-in-full up-front. Scammers will leave without returning to complete the work, demand additional money once the job is finished, or complete the job with substandard material or workmanship. They may demand immediate payment in cash and may even accompany the victim to the bank. Or, if traveling in pairs, one suspect will divert the homeowner's attention while the second enters the home to steal cash and valuables. Diversion theft is also conducted by utility imposters.

PHONE, EMAIL AND ONLINE SCAMS

Older people are at risk of falling victim to fear-based telephone scams. Unscheduled or unsolicited callers claim to represent a utility company and threaten to cut off service unless an "overdue bill" or "maintenance cost" is paid immediately. The caller may demand payment by wire transfer, cryptocurrency, gift card or cash-reload card. Similar scams include calls from government agencies such as the IRS or police/sheriff's department demanding immediate payment of fines, under threat of arrest.

Computer viruses can be downloaded by clicking an unknown link or opening a malicious email attachment. Viruses can steal user names, passwords, and financial information, and the victim may never know their computer has been infected.

PREVENTION TIPS

Protect Your Physical Security

- Keep your doors locked while at home and always remember to lock up when leaving the house—even for short trips.
- Never allow strangers inside your home.
- Beware of unsolicited home repairmen. Never deal with door-to-door contractors.
- Home repair contracts should include the exact work to be done, the price, start and end dates, and the name and address of the contractor. Be suspicious of contractors that only have a PO Box.
- Don't allow contractors to use urgency or scare tactics to get you to sign a contract.
- Be suspicious of businesses that offer you discount rates due to left over materials from another job or because you are a senior citizen.
- Ask for photo identification from service or delivery people and call the company to verify their identity.
- Be observant. Get a good physical description of individuals and their vehicles.

Protect Your Phone and Electronic Security

- Beware of caller ID. Masked numbers may appear to be from law enforcement, a government agency, or business. Hang up on or do not answer unsolicited calls. Call the agency or business using official telephone numbers posted on websites or utility bills.
- Don't let them scare you. A scammer will try to convince you the lights or water are about to go out or that you could be arrested. If you're actually behind on payments, the utility will send you a delinquent notice in the mail, probably more than once, with a prospective shutoff date.
- Beware of healthcare scams. Never release information to any health service provider that you did not contact directly.
- If you receive a call from someone claiming to be a relative and asking for money, independently call that person at a known phone number to verify their story.
- Do not click on links or open email attachments if you do not know what they are. The email may look like it came from a friend or family member, or even legitimate business but unless you know what it is or are expecting it, delete it without clicking on links or opening attachments.
- Never buy gift cards, cryptocurrency, or cash-reload cards or use wire transfers to pay off a "debt" to individuals who contact you by phone or email.
- Do not provide personal or financial information to an unsolicited caller or visitor.