

Scam Prevention Tips

- If it's free or sounds too good to be true, it probably is.
- <u>SLOW DOWN</u> a scammer doesn't want to give you time to think clearly.
- Bills are <u>NEVER</u> paid with gift cards.
- Verify information independently **<u>BEFORE</u>** sending money. (Hospitals treat first and bill later. If a caller claims a loved one is imprisoned, then they are safe and there is time to address the situation.)
- Check in with elderly relatives routinely and talk about their daily lives. (Scammers target the most vulnerable, including those who are lonely or suffering some degree of cognitive decline.)
- Taxes are NOT paid in advance for lottery / sweepstake winnings.
- Sending compromising photos to romantic partners can provide a scammer an opportunity to blackmail.
- Scammers can find many personal details about people online. Don't trust someone just because they mention a familiar name, place, or have details about your property.
- Double-check email addresses. Ensure the company name after the @ symbol matches the organization from which the email states it came.
- Do NOT click on links or attachments texted or emailed to you from people you don't know.
- STOP THINK VERIFY

Scam Warning Signs

- Someone tells you to keep the conversation confidential and not tell anyone.
- Scammers **pressure** you to act immediately. They may threaten you with arrest or legal action.
- Scammers pretend to be from a familiar organization or government agencies, like the Social Security
 Administration. They may email attachments with official-looking logos, seals, signatures, or pictures of employee
 credentials. Be vigilant.
- Scammers mention a **problem** or a prize. They may say your Social Security number was involved in a crime or ask for personal information to process a benefit.



What to Do If You Are Being Targeted OR You Know Someone Who Is A Victim of Scammers

- Stop communication. Stop cooperating. Keep proof. Contact local police.
- <u>IF YOU DID</u> send money or personal info, report it to the police. **Call 9-1-1**. You can also visit the police department in person.
- IF YOU DID NOT provide any identifying information or money, there is no need to report this to the police. If this happened online, you can report it to the FBI Internet Crime Complaint Center at www.ic3.gov.
- Most companies (banks, credit cards, utilities, IRS) have a scam reporting/ investigation dept. Contact the company directly to learn how to make a report.

RESOURCES

- FBI Internet Crime Complaint Center (IC3) Report internet crimes directly to the FBI, including cases involving elder fraud, ransomware, and compromised business email. https://www.ic3.gov/Home/ComplaintChoice/default.aspx
- USA.gov The federal government has several resources for reporting a variety of scams, including those involving banking and investments. https://www.usa.gov/common-scams-frauds
- PA Department of Banking & Securities, Consumer Services Office 800-PA-BANKS
- PA Attorney General, Consumer Protections Office Email <u>consumers@AttorneyGeneral.gov</u> or 800-441-2555
- PA Public Utility Commission (PUC) Contact the PUC for complaints about energy company sales pitches. The PUC also provides an FAQ with information to help consumers determine which companies are legitimate and which are not. <u>https://www.puc.pa.gov/General/pdf/PAPS-FAQ_Electricity_Shopping.pdf</u>
- National Do Not Call Registry provides an FAQ to help consumers understand this service (and its limitations when it comes to scammers). https://consumer.ftc.gov/articles/national-do-not-call-registry-faqs
- Register to Receive Less Junk Mail Register with the Direct Marketing Association to stop most, but not all, promotional mail. There is a \$5 processing fee, and the registration is valid for 10 years.
 https://www.dmachoice.org
- Stop Credit Card and Insurance Offers Go to <u>www.optoutprescreen.com</u> or call 1-888-5-OPT-OUT (1-888-567-8688).
- Federal Trade Commission Resources to stop junk mail <u>https://consumer.ftc.gov/articles/how-stop-junk-mail</u>