SAFE BANKING FOR SENIORS

Did you know that older Americans lose $2.9 billion each year to fraud?

Our bank is participating in the American Bankers Association Foundation's Safe Banking for Seniors campaign in a nationwide effort to help older customers and their financial caregivers understand the risks of fraud and financial abuse and how to protect themselves and their loved ones.

Financial abuse against older Americans can take many forms, from illegal debits, to third-party scams and even unauthorized withdrawals by an approved financial caregiver.

JOIN US TO LEARN MORE!

Attached, please find the following resources to assist you with avoiding financial abuse:

- What is a Scam?
- 5 Ways to Spot a Lottery Scam
- Don't Fall Victim to the Grandparent Scam
- IRS Imposter Scam
- Social Security Scams
- Tech Support Scams

HATBORO FEDERAL SAVINGS
Established 1941

SAFE BANKING FOR SENIORS
ABA FOUNDATION

For more information and other consumer resources, visit **aba.com/seniors**

What is a Scam?

A scam is a trick a con artist plays on an unsuspecting victim to extort money. If the scam succeeds, the victim's money is gone, and the scammer will move on to the next victim.

A scammer is the ultimate salesperson with a tempting offer or a skilled liar with a plausible story

- Easily pinpoints a victim's vulnerabilities and appeals to emotions: sympathy, fear, loneliness
- Quickly gains trust
- Insist on secrecy
- Shows no mercy, e.g., doesn't take "no" for an answer

Know the Red Flags of a Scam

- Immediate action required
- Insistence on secrecy
- Money needed up front
- Hard-to-track payment methods

Build Your Scam Defenses

- Do not be rushed into any financial decision
- Assume that insistence on secrecy is a ploy to deceive you
- Be suspicious of any situation that requires you to send money up front
- Confirm all stories, offers or charities independently
- Be very cautious about clicking on email links

Block Those Scammers

- Register with National Do Not Call Registry at **www.donotcall.gov** to limit legitimate telemarketing phone calls, making phone scams easier to detect
- Register with **www.DMAchoice.org** to limit legitimate advertising mail, making mail scams easier to detect
- Limit personal information on social media and choose the strictest privacy settings on social media accounts
- Use antivirus software on your computer

What to Do If You Are Scammed

- Don't be embarrassed or afraid
- Tell someone you trust
- Report the scam to your bank immediately to limit losses
- Contact your local police and federal agencies, like the Federal Trade Commission

For more information, visit **aba.com/Seniors**

SAFE BANKING FOR SENIORS®
ABA FOUNDATION

5 Ways to Spot a Lottery Scam

Solicitation scams, commonly referred to as an "advance fee," "lottery" or "sweepstakes" scam, often begin with fraudsters telling the victim they won the lottery or a raffle. The consumer may be issued a check worth more than the amount owed and instructed to pay taxes and fees before receiving a lump sum payment. Unfortunately, the check—in addition to the raffle—is bogus.

1. **Don't be fooled by the appearance of the check.** Scam artists use sophisticated technology to create legitimate-looking counterfeit checks, money orders, and cashier's checks. The company name may be real, but someone has forged the checks without their knowledge.
2. **Never "pay to play."** If someone who is giving you money asks you to wire money back or send more than the exact amount—that's a red flag that it's a scam. If a stranger wants to pay you for something, insist on a cashier's check for the exact amount, preferably from a local bank or one with a local branch.
3. **Verify the requestor before you wire funds or issue a check.** It is important to know who you are sending money to before you make a payment. Confirm the requestor is a trusted source.
4. **Just because the check has cleared does not mean it's good.** Under federal law, banks must make deposited funds available quickly, but it can take days for the bank to learn that a check was bad.
5. **Report suspected fraud to your bank immediately.** Bank staff are trained to spot fraudulent checks. If you think someone gave you a fake check, don't deposit it—report it. Contact your local bank and report it to the Federal Trade Commission at **ReportFraud.ftc.gov**.

For more information, visit **aba.com/Consumers**

SAFE BANKING FOR SENIORS®
ABA FOUNDATION

Don't Fall Victim to the Grandparent Scam

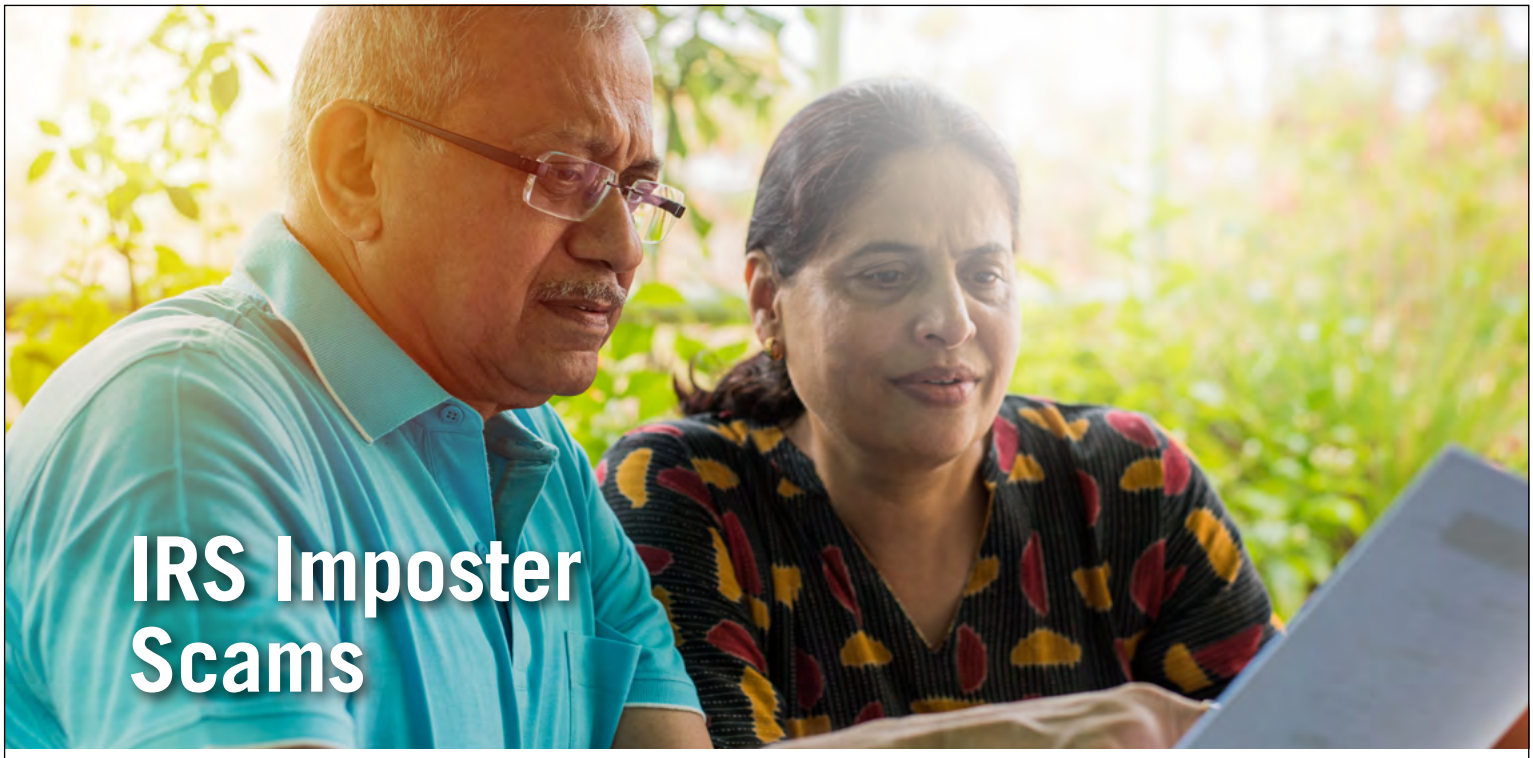
A grandparent scam is a type of impostor scam. Fraudsters call claiming to be a family member who needs money immediately for an emergency. They may have information about you, including your name and where you live. They'll claim to be stranded, in jail, or require help paying medical bills.

Scammers will beg you for money, ask you to keep it a secret, and urge you to act quickly. Usually, they will tell you to wire money, pay with gift cards, or send cryptocurrency. Stop! Don't pay—it's a scam! If you send money, you won't be able to get it back.

- **Confirm the caller.** Fraudsters are using social networking sites to gain the personal information of friends and relatives to carry out their crimes. Verify who's calling by contacting the person directly on a known number, or consult a trusted family member.
- **Don't be afraid to ask questions.** Fraudsters want to execute their crimes quickly. In this type of scam, they count on fear and your concern for your loved one to make you act before you think. The more questions you ask, the more inclined they will be to ditch the scam if they suspect you're on to them.
- **Never give personal information to anyone over the phone** unless you initiated the call and you trust the other party.
- **Never rush into a financial decision.** Don't be fooled—if something doesn't feel right, it may not be right. It's not rude to say no and get more information, or decline to act.
- Report it to the Federal Trade Commission at **ReportFraud.ftc.gov**.

For more information, visit **aba.com/Consumers**

SAFE BANKING FOR SENIORS®
ABA FOUNDATION



IRS Imposter Scams

Scammers claiming to work for the Internal Revenue Service (IRS) may reach out via phone, email, or text to say you owe money to the government. Look out for any of these scenarios:

- **Taxes** – The fraudsters will say you owe taxes and demand that you pay right away. They usually require payment through a wire transfer, a prepaid debit or gift card, or funds via a mobile payment app. Often, the criminals will threaten arrest or deportation if you don't pay.
- **Information Verification** – The scammer will send you an email or text message that asks you to confirm or authenticate your personal information. The messages often include a link to click or another feature that connects you to a fraudulent form or website.

Don't Be a Victim

- Be wary of anyone claiming to be from the IRS. The IRS will always contact you via postal mail before making a call about unpaid taxes.
- The IRS won't threaten to arrest you for not paying a bill.
- If the IRS does contact you, they will offer you time to submit an appeal.
- Scammers can spoof caller ID and change the name that appears on your phone, so don't trust the caller just because it shows up as "IRS."
- If you think you owe back taxes, you can check with the IRS by calling **1-800-829-1040**.

Report the Scam

If you think you've been scammed, report the incident to the IRS at **phishing@irs.gov**.

For more information, visit **aba.com/Consumers**

SAFE BANKING FOR SENIORS®
ABA FOUNDATION

Social Security Scams

Americans have lost millions of dollars from Social Security scams. Fraudsters reach out to unsuspecting victims to steal benefits and to obtain personal information. Victims are often exploited through two common scenarios:

Phone Call

For many, it starts with an unsolicited phone call:

An individual impersonating a government official tells the victim that their Social Security number has been suspended or linked to criminal activity.

The victim is asked to confirm the Social Security number for security purposes.

The fraudster then offers to issue a new number or reactivate the old one for a fee.

In complying, the victim shares everything that the fraudster needs to steal the victim's identity.

Office Closures

A fraudulent letter threatening to suspend or discontinue Social Security benefits due to office closures amid a crisis is sent to the victim.

The letter instructs the victim to call a number.

Once the victim makes the call, fraudsters will manipulate callers into sharing personal information and/or remitting payment via gift cards, wire transfers, cryptocurrency or cash.

Recognize the Signs

The best way to protect yourself is to recognize the signs of a scam and remember not to engage with scammers.

- If you receive an unsolicited call, email or text asking for your Social Security number, be suspicious and don't share it.
- Fraudsters try to incite fear, encourage secrecy and make you act before you can think. Don't be afraid to hang up.
- **The Social Security Administration will never:**
  - Threaten you with benefit suspension, arrest or other legal actions unless you pay a fine
  - Require payment via gift card, cash, wire transfer, cryptocurrency or prepaid debit card

If you have questions, always confirm by calling the Social Security Administration directly at **1-800-772-1213**.

For more information, visit **aba.com/Consumers**

SAFE BANKING FOR SENIORS®
ABA FOUNDATION

Tech Support Scams

Tech support scams often begin with a phone call or a pop-up window displaying a fake error message with a number to call. Scammers often impersonate representatives from a tech company—such as Apple, Google or Microsoft—to persuade victims to provide remote access to their computers to "repair" an issue, such as malware.

If the victim provides access to the device, criminals will scan the computer to "troubleshoot the problem" and offer fake solutions. They may install dangerous computer applications or encourage the victim to pay for a phony subscription. In the process, the scammers steal the victim's money and identity.

Don't Be a Victim

- Hang up the phone if you receive an unsolicited call from someone who says there's something wrong with your computer.
- Be suspicious of pop-up warnings. Security pop-ups from real tech companies will not ask you to call a phone number.
- Do not give access to your computer or share passwords with anyone who contacts you.
- Keep your computer's security software up to date.

If Scammed

- Contact your bank to report fraud and check your statements.
- Change passwords to your computer, bank accounts and other sites.
- Scan your computer for viruses and call your security software company for help.
- Report it to the Federal Trade Commission at **ReportFraud.ftc.gov**.

For more information, visit **aba.com/Consumers**

SAFE BANKING FOR SENIORS®
ABA FOUNDATION