Don't Become a Scam Victim

Harpswell Aging at Home

Scams targeting people 60 and older caused $3.4 billion-plus in losses in 2023, and the average victim lost $33,915. To avoid becoming a victim:

Understand common scams

Type of scam	What to do
Gift Cards - Someone you don't know calls or emails, asking you to buy a gift card for them and to provide the card number and PIN. They extract the money you've loaded onto the card.	**IGNORE THE REQUEST.**
Phony Tech Support - Someone contacts you, saying they're a technician and your computer has viruses.	If you didn't contact a computer service, **HANG UP** and **TURN OFF YOUR COMPUTER!**
Banking - Someone claiming to be from your bank calls and asks you to verify your account number or personal information, or to wire money.	**HANG UP**, but if you think the call may be legitimate, contact your bank to verify.
Social Security/Medicare/IRS - Someone contacts you, saying they're from one of these agencies and asking for personal information. Such agencies only contact people by postal mail for official business.	**HANG UP** or **DELETE THE EMAILS** immediately.
Romance - Someone contacts you on social media, expressing interest in getting to know you. They later ask for your phone number and address so they can "call" or "write." They intensify the courtship, then start asking for money; for example, for plane fare to visit you.	**DO NOT SEND MONEY!**
Fake Grandchild - A stranger calls and says your grandchild needs money, to pay for medical bills, bail, a lawyer. The caller warns you not to tell anyone. They may seem legit, if they know something about your grandchild from his or her social media. They may even say they're a lawyer or a policeman.	**STOP, and check it out.** Ask a family member if your grandchild really is in trouble.
Home Repair - Someone calls or knocks on your door, offering to tackle handyman projects for you. They pressure you to act quickly, and might ask you to pay cash upfront. Or they may offer to get you financing. They'll run off with your money, never make the repairs, or do shoddy work. They might even get you to sign a bad financing agreement that puts your house at risk.	**DON'T FALL FOR IT!**
Facebook - Scammers post ads on Facebook's side panel designed to trick you into clicking on a malicious link or providing personal information.	**DON'T CLICK**, if there's no customer service number displayed, or if the ad has spelling and grammar mistakes.

If a scammer targets you, alert friends and neighbors. You'll help them avoid being scammed.

Know how scammers get in touch

Contact Method	What to do
Links or Attachments	Whether a link or attachment arrives by email, text message, or direct message, never click on it unless you know it's legitimate. If the sender claims to be from a company or government agency, don't call the number provided. **LOOK UP THE REAL NUMBER, AND CALL TO CLARIFY WHETHER THE LINK OR ATTACHMENT IS SAFE.**
Phone Calls	If caller ID shows an unfamiliar number, let it go to voicemail. If you answer by mistake and it's a spam call, never say "Yes," and **HANG UP IMMEDIATELY. DON'T CALL ANY NUMBER PROVIDED. Look up the organization they claim to be from, and call them yourself.** Also: **NEVER GIVE OUT YOUR SOCIAL SECURITY NUMBER** unless you know the request is legitimate.
Email	Scammers are getting better at fooling people with official-looking logos and graphics in their emails. Examine the sender's email address. If the address doesn't look real, or the email message contains spelling and grammar mistakes, it's likely an attempted scam. **DON'T REPLY TO THE EMAIL OR OPEN ANY LINKS OR ATTACHMENTS IN IT.**

Take action if you get scammed

If you've been scammed, despite your best efforts, don't be ashamed! Instead, **tell a trusted relative right away.** They can guide you through the following steps, which can help limit the damage the scam inflicts and protect you from being victimized further:

1. **Report the scam and scammer** by calling the FCC at (877) 382-4357 or going to reportfraud.ftc.gov. As applicable, notify your bank, credit card company, social media platform, phone carrier, or the United States Postal Service (USPS).
2. **File a police report** with Cumberland County Sheriff's Department: (207) 774-1444. They might help with recovering money or personal information the scammer took.
3. **Run an antivirus scan on your electronic devices to check for malware** if you clicked on a link or attachment. Need help? Call the town office and ask for a Harpswell Aging at Home tech referral at (207) 833-5771 x108.
4. **Change your passwords** on accounts using a password the scammer might know. Create strong passwords or use the new password-less option Passkey, available on some websites.
5. **Lock down your credit** if you gave the scammer personal information or you're worried. Consider adding fraud alerts and security freezes to your credit reports from Equifax or Transunion. These are free and can help stop scammers from opening accounts using your personal information.

As scammers grow increasingly sophisticated, the battle to protect ourselves against them has become tougher. But by understanding how scams work, how scammers target their victims, and what to do if you get scammed, you'll be in the best possible shape to protect yourself.

Harpswell Aging at Home

Please visit our website **www.hah.community** or email us at **hah@hah.community** to learn more about HAH.

Email: hah@hah.community | **Phone:** (207) 833-5771 x108 | **Mailing:** P.O. Box 25, Harpswell, ME 04079

Rev. 01/13/2025