

## Top 10 Tips to Avoid Becoming a Fraud Victim

1. **DO NOT** respond to unsolicited phone calls, texts, emails, social media messages, mailings, or letters from someone you do not know and trust.
2. **DO NOT** give personal or financial/banking information to anyone you do not know or trust.
3. **KEEP** your debit/credit cards safe. Don't store or write down your PIN codes or passwords. Protect your cards as you would cash.
4. **HANG UP** the phone if someone you don't know or trust acts suspicious or asks you for money or threatens you with arrest if you do not comply with their demands.
5. **DO NOT** trust caller ID functions. A phone number can be altered to look like a legitimate number when it is not.
6. **RED FLAGS** include anything that sounds too good to be true. Get rich quick schemes such as being told you can make a thousand dollars a week stuffing envelopes from home or cheap travel offers should be considered a red flag.
7. **CHECK** your credit card statements upon receipt and check your credit rating periodically.
8. **DO NOT** let anyone pressure you, bully you, or threaten you.
9. **PROTECT** your PC, laptop, tablet or smartphone with strong passwords and security programs and only download files or software from trusted sources.
10. **TALK** with a trusted family member or friend for assistance.

## *Have you been a victim of identity theft, fraud or a scam?*

- Notify your financial institutions, including banks and credit card companies.
- Report the incident to the police. Pennsylvania State Police at 570-253-7126.
- Notify credit reporting agencies:

### **Equifax**

888-766-0008

[Equifax.com/personal/credit-report-services/](https://www.equifax.com/personal/credit-report-services/)

### **Experian**

888-397-3742

[Experian.com/fraud/center/html](https://www.experian.com/fraud/center/html)

### **TransUnion**

800-680-7289

[TransUnion.com/Fraud-Alerts](https://www.transunion.com/Fraud-Alerts)



**MORAVIAN MANOR  
COMMUNITIES**

300 W. Lemon Street

Lititz, PA 17543

717-626-0214

[moravianmanorcommunities.org](https://www.moravianmanorcommunities.org)

This brochure is for general informational purposes only, and is not intended to serve as professional advice or as a substitute for seeking professional guidance. Information in the brochure may not constitute the most up-to-date information or cover all types of scams or new scams. If you suspect you have been a victim of fraud, always contact the proper authorities.

## Protecting Yourself from Scams & Fraud



**MORAVIAN MANOR  
COMMUNITIES**

*Connecting community and offering  
services that enrich the journey of aging*

# Trending Scams and How to Avoid Them

## Grandparent Scam

Scammers call and pretend to be a grandchild. When you answer, they will say something like “Hi grandma, do you know who this is?” If you go along with it, the fake grandchild will ask for money for overdue rent, car repairs, or bail money. They often ask that it be sent via a prepaid card.

*Hang up, and immediately confirm with family that an actual crisis is happening.*

## Home Improvement Scam

Scammers often target older adults convincing them of unnecessary repairs. Once paid a deposit for the work, the victim never sees the perpetrator again.

*Always use a licensed contractor that was referred to you by someone you trust. When in doubt, get a second opinion before hiring someone or giving a deposit.*

## Lottery Scam

Phone calls or texts claiming you won a foreign lottery are always a scam. The scammer will state that you have won and need to pay a small handling fee in order to claim your big prize. They will ask funds be wired or prepaid cards sent or payment in bit coin.

*If contacted about winning a foreign lottery, contact the FTC at 202-326-2222.*



## Computer Virus Scam

Criminals pose as tech support specialists offering to fix computer issues that don't exist. Or they may try to sell you anti-virus protection programs. They will ask for access to your computer, and then install malware instead of anti-virus software, giving them long-term access to your personal and financial information.

*Do not respond to high pressure, unsolicited sales pitches and offers. Hang up.*

## Inheritance Scam

With this type of scam, you are contacted by someone claiming to be an attorney in another country who says you have a relative who left you an inheritance. That “lawyer” requests a fee for you to claim it.

*Hang up, and contact family members to confirm if it's legitimate. Never send funds or prepaid cards to people you do not know or trust.*

## Social Security Scam

Scammers may impersonate Social Security Administration (SSA) employees requesting personal and banking information. They may threaten you, stating benefits will end if information is not provided.

*Hang up the phone and call your local social security administration office, as they do not request personal and banking information in this manner.*

## Telemarketing Scam

Telemarketing remains one of the most popular forms of scamming people.

*Do not fall for offers that sound too good to be true. Do not respond to unsolicited calls or offers!*

## Romance Scam

Criminals sometimes pose as interested romantic partners on social media or other dating platforms, capitalizing on the need for companionship.

*Never send money to someone you only know through the internet. If meeting in person, make sure family knows where you are going or bring a family member with you.*

## Medicare Fraud

Scammers can alter their phone number to appear on your caller ID as someone you know, such as a doctor's office. They will ask you to confirm or supply your Medicare number. Your Medicare number can then be used to order durable medical equipment or supplies and submit fraudulent claims.

*Hang up the phone! Call the number on the back of your insurance card to report. If the scammers manipulated caller ID to reflect someone you trust such as your doctor, call them as well to verify it was a scam call.*

## Fake Shipping Notification Scam

Scammers send fake package shipment and delivery notifications via text or email. The message might say you missed a delivery and to click a link to re-schedule or update shipping preferences. The link takes you to a fake site and it will capture all the personal information you enter.

*If you get a link, don't click it. If you think it might be a legitimate message, contact the shipping company using a phone number or email address you know is real. If you are expecting a package, go to the site where you purchased it and look up shipping/delivery status there.*

