Information about common scams:

IRS

The IRS will never:

- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer. Generally, the IRS will first mail a bill to any taxpayer who owes taxes.
- Threaten to immediately bring in local police or other law enforcement groups to have the taxpayer arrested for not paying.
- Demand that taxes be paid without giving taxpayers the opportunity to question or appeal the amount owed.
- Call unexpectedly about a tax refund.

Social Security

Social Security will never:

- Threaten you with arrest or legal action because you don't agree to pay money immediately.
- Suspend your Social Security number.
- Claim to need personal information or payment to activate a cost-of-living adjustment (COLA) or other benefit increase.
- Pressure you to take immediate action, including sharing personal information.
- Ask you to pay with gift cards, prepaid debit cards, wire transfers, cryptocurrency, or by mailing cash.
- Threaten to seize your bank account.
- Offer to move your money to a "protected" bank account.
- Demand secrecy.
- Direct message you on social media.

Warrant for arrest

- You will never receive a phone call that tells you there's a warrant issued for your arrest.
- The court will always send a jury summons by U.S. Mail.
- The court and law enforcement will never demand payment over the phone.
- The court and law enforcement will never demand a gift card number to satisfy an obligation.
- Warrants are typically served in person by a uniformed officer.
- Never, ever agree to meet someone at a strange address, especially someone who calls and demands cash payment.

Hostage

- You receive a call (possibly from spoofed family members phone number on the caller ID) – hear screaming, then silent or fades away, then someone comes online and demands immediate payment "or else"
- Usually demand P2P payments such as CashApp or VenMo; wire transfer, etc
- Try to contact your allegedly kidnapped relative by other means while the scammers are on the line

Grandparent

- The scammers call and impersonate a grandchild – or another close relative –“Hello Grandpa??” in a crisis situation, asking for immediate financial assistance.
- Sometimes these callers “spoof” the caller ID to make an incoming call appear to be coming from a trusted source.
- Always use caution if you are being pressured for information or to send money quickly. Scammers often try to bully victims into transferring money through a mobile payment app, by wiring money, or by purchasing gift cards or money orders. Some may even request to meet to receive money in person. If you get a call like this, hang up and report it immediately to local law enforcement

Tech Support

- You get a Phone Call, Pop-Up, or Email telling you there's a problem with your computer
- The scammers may pretend to be from a well-known tech company, such as Microsoft. They use lots of technical terms to convince you that the problems with your computer are real. They may ask you to open some files or run a scan on your computer — and then tell you those files or the scan results show a problem…but there isn’t one.
- Ask you to give them remote access to your computer — which lets them access all information stored on it, and on any network connected to it

They may also:

- Try to enroll you in a worthless computer maintenance or warranty program
- Install malware that gives them access to your computer and sensitive data, like user names and passwords
- Ask for credit card information so they can bill you for phony services or services available elsewhere for free
- Try to sell you software or repair services that are worthless or available elsewhere for free
- Direct you to websites and ask you to enter credit card, bank account, and other personal information

Investment

- Investment fraud happens when people try to trick you into investing money.
- They might want you to invest money in stocks, bonds, notes, commodities, currency, or even real estate. A scammer may lie to you or give you fake information about a real investment. Or they may make up a fake investment opportunity.
- Always a promise of a ton of money fast.

Steps to take if you paid a scammer

Did you pay with a credit card or debit card?	Contact the company or bank that issued the credit card or debit card. Tell them it was a fraudulent charge. Ask them to reverse the transaction and give you your money back.
Did a scammer make an unauthorized transfer from your bank account?	Contact your bank and tell them it was an unauthorized debit or withdrawal. Ask them to reverse the transaction and give you your money back.
Did you pay with a gift card?	Contact the company that issued the gift card. Tell them it was used in a scam and ask them to refund your money. Keep the gift card itself, and the gift card receipt.
Did you send a wire transfer through a company like Western Union or MoneyGram?	Contact the wire transfer company. Tell them it was a fraudulent transfer. Ask them to reverse the wire transfer and give you your money back. • MoneyGram at 1-800-926-9400 • Western Union at 1-800-448-1492 • Ria (non-Walmart transfers) at 1-877-443-1399 • Ria (Walmart2Walmart and Walmart2World transfers) at 1-855-355-2144
Did you send a wire transfer through your bank?	Contact your bank and report the fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.
Did you send money through a money transfer app?	Report the fraudulent transaction to the company behind the money transfer app and ask them to reverse the payment. If you linked the app to a credit card or debit card, report the fraud to your credit card company or bank. Ask them to reverse the charge.
Did you pay with cryptocurrency?	Cryptocurrency payments typically are not reversible. Once you pay with cryptocurrency, you can only get your money back if the person you paid sends it back. But contact the company you used to send the money and tell them it was a fraudulent transaction. Ask them to reverse the transaction, if possible.
Did you send cash?	If you sent cash by U.S. mail, contact the U.S. Postal Inspection Service at 877-876-2455 and ask them to intercept the package. To learn more about this process, visit USPS Package Intercept: The Basics. If you used another delivery service, contact them as soon as possible.

If You Gave a Scammer Your Personal Information

Did you give a scammer your Social Security number?	Go to IdentityTheft.gov to see what steps to take, including how to monitor your credit.
Did you give a scammer your username and password?	Create a new, strong password. If you use the same password anywhere else, change it there, too.

If a Scammer Has Access to Your Computer or Phone

Does a scammer have remote access to your computer?	Update your computer's security software, run a scan, and delete anything it identifies as a problem. Then take other steps to protect your personal information.
Did a scammer take control of your cell phone number and account?	Contact your service provider to take back control of your phone number. Once you do, change your account password. Also check your credit card, bank, and other financial accounts for unauthorized charges or changes. If you see any, report them to the company or institution. Then go to IdentityTheft.gov to see what steps you should take.