February 2025
A Safer Naper --- Scam Awareness

This month, the Naperville Police Department aims to make our community "A Safer Naper" by alerting you to the warning signs of scams and how to protect yourself from becoming an unsuspecting victim.

In 2024, Naperville residents reported losing more than $5.5 million to scams! Victims ranged in age from 15 to 91, emphasizing the need for everyone to pay attention to the red flags of various scams. The most common scams reported in 2024 were tech support, online resale commerce (e.g., Facebook Marketplace), fake warrants, phishing, and investment scams. Investment scams resulted in the highest monetary loss. Learn more about those common scams here.

Scammers are always changing their tactics and looking for new victims. However, while scams can take many forms, here are some warning signs that are present in most scams and tips on how to protect yourself.

SECTION 1: Four Signs It's a Scam

1. Scammers **PRETEND** to be from an organization you know.
   Scammers often pretend to be contacting you on behalf of the government. They might use a real name, like the FTC, Social Security Administration, IRS, or Medicare, or make up a name that sounds official. Some pretend to be from a business you know, like a utility company, a tech company, or even a charity asking for donations. They use technology to change the phone number that appears on your caller ID. So, the name and number you see might not be real.

2. Scammers say there's a **PROBLEM** or a **PRIZE**.
   They might say you're in trouble with the government. Or you owe money. Or someone in your family had an emergency. Or that there's a virus on your computer. Some scammers say there's a problem with one of your accounts and that you need to verify some information. Others will lie and say you won money in a lottery or sweepstakes but have to pay a fee to get it.

3. Scammers **PRESSURE** you to act immediately.
   Scammers want you to act before you have time to think. If you're on the phone, they might tell you not to hang up so you can't check out their story. They might threaten to arrest you, sue you, take away your driver's or business license, or deport you. They might say your computer is about to be corrupted.

4. Scammers tell you to **PAY** in a specific way.
   They often insist that you can only pay by using cryptocurrency, wiring money through a company like MoneyGram or Western Union, using a payment app, or putting money on a gift card and then giving them the numbers on the back of the card. Some will send you a check (that will later turn out to be fake), then tell you to deposit it and send them money.

Source: Federal Trade Commission
https://consumer.ftc.gov/articles/how-avoid-scam

SECTION 2: Common Scam Scenarios

Here are a few common scenarios that can help tip you off to a scam.

- **Someone promises a high returns on a cryptocurrency investment.** Consumers should be cautious of investing in cryptocurrency, which is highly volatile and largely unregulated. If a cryptocurrency investment seems too good to be true, it probably is. Be aware that you will not be able to reverse a cryptocurrency transaction and get your money back.
- **A pop up appears on your computer indicating there is a virus.** Do not attempt to click on any part of the pop-up or follow the instructions contained within it (such as to call a phone number). Close your browser and run a full scan with your legitimate antivirus software to check for actual infections. Never provide personal information, call numbers or click links in a suspicious pop-up, or allow anyone remote access to your device.
- **Someone calls saying they are from a government agency, threatens you or demands money to satisfy a warrant, a fine, or to post bond for a relative in jail.** The government doesn't call to ask for money, nor do they take cryptocurrency or gift cards for payment.
- **Scammers pose as both fake sellers and fake buyers on online resale commerce platforms to steal your money.** Scammers pretend to make fake payments, sell fake items, ask for deposits, and request personal information. Personal information such as your phone number or email address could be used to steal your identity, hack your email or computer, or access your peer-to-peer (Zelle/Venmo) payment account.
- **You get an email, text, or call asking to verify your credit card, bank account, or Social Security Number.** Never click on any links or give that information to anyone who contacts you and asks for it. Always independently verify with your own records the contact information for any business or government entity if you think there is an issue.
- **Someone says you can "only" pay in a specific way such as cryptocurrency or a gift card.** No legitimate business or government agency is going to direct you to pay in this form.

SECTION 3: What You Can Do to Avoid a Scam

Block unwanted calls and text messages. Take steps to block unwanted calls and to filter unwanted text messages.

Don't give your personal or financial information in response to a request that you didn't expect. Honest organizations won't call, email, or text to ask for your personal information, like your Social Security, bank account, or credit card numbers. If you get an email or text message from a company you do business with and you think it's real, it's still best not to click on any links. Instead, contact them using a website you know is trustworthy. Or look up their phone number. Don't call a number they gave you or the number from your caller ID.

Resist the pressure to act immediately. Honest businesses will give you time to make a decision. Anyone who pressures you to pay or give them your personal information is a scammer.

Know how scammers tell you to pay. Never pay someone who insists that you can only pay with cryptocurrency, a wire transfer service like Western Union or MoneyGram, a payment app, or a gift card. And never deposit a check and send money back to someone.

Stop and talk to someone you trust. If you're being pressured to send money or personal information, tell someone — a friend, a family member, or a neighbor – before you do anything else. Talking about it could help you realize it's a scam.

Keep up with the latest. Sign up for FTC consumer alerts at ftc.gov/ConsumerAlerts to get email updates on recent scams, announcements, and advice.

Share what you know. Awareness is your best defense against falling for a scam, so share what you know with friends, family members and neighbors. You could help prevent someone from losing money to a scammer.

Just remember the saying … If it sounds too good to be true, it probably is.

SECTION 4: What To Do if You've Been Scammed

Here's what to do if you find that you've been the victim of a scam:

- If you paid the scammer with a gift card, wire transfer, credit or debit card, or cryptocurrency, contact the company or your bank right away. For additional information for what to do based upon how you paid the offender, click here for guidance from the FTC.
- Close out any fraudulent accounts.
- Contact the fraud department at the three major credit bureaus – Equifax, Experian and Trans Union – to block or freeze your accounts and obtain a current credit report and review it.
- Make a report with the Naperville Police Department, either online, in person at the police department (1350 Aurora Ave., Naperville) or by calling (630) 420-6666 to request to have an officer come to you.
- Make a report with the Federal Trade Commission at https://reportfraud.ftc.gov.
- Tell others what happened to you to help them from becoming a victim of a scam.
- Keep a log of all you do and BE PERSISTENT!!!