February 2024
A Safer Naper --- Scam Awareness

This month, the Naperville Police Department aims to make our community "A Safer Naper" by educating you about common scams, the warning signs that can help identify one, and how to protect yourself from becoming an unsuspecting victim.

Consumers reported losing almost $8.8 billion to scams and fraud in 2022, up 30 percent over 2021's losses, according to the Federal Trade Commission (FTC). The rising cost of these crimes is staggering, considering that in 2020 Americans lost only $3.5 billion to fraud, including identity theft.

Naperville is not immune to these trends. Naperville Police Department's Financial Crimes Unit, which is composed of a sergeant and six detectives, reviews an average of 70 financial crime reports each month, making this a relevant topic that everyone should be aware of!

And while the national number of scam reports last year was actually down — to 2.4 million, from 2.9 million in 2021 — individual victims lost far more than ever before: In 2022, the median loss from fraud was $650, up from $500 in 2021. Some scams proved much more lucrative for criminals than others, according to these numbers, which are based on reports submitted to the FTC's Consumer Sentinel Network directly by consumers, or through law enforcement and other organizations.

In terms of the number of fraud reports received nationally, the most common are:

1) Imposter Scams
2) Online Shopping
3) Prizes, Sweepstakes, and Lotteries
4) Investments
5) Business and Job Opportunities

Scammers are always changing their tactics and looking for new victims. However, while scams can take many forms, here are some warning signs 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: 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. Before you do anything else, tell someone — a friend, a family member, a neighbor — what happened. Talking about it could help you realize it's a scam.

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

SECTION 3: Common Scams

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

- Someone promises you a job – if you pay them. Never pay anyone who promises to get you a job, or a certificate that will get you a job.

- Someone calls saying they are from a government agency and threatens you and demands money. The government doesn't call to ask for money nor do they take prepaid cards for payment.
- You get a call or email saying you won the lottery or a raffle that you never bought a ticket for. Except there's a fee? Never pay for a prize.
- A caller offers to help you get back some money you lost. No government agency or legitimate business will call and demand money to help you get money back.
- You get a check from someone who asked you to give them part of the money back. Never give someone money in return for a check. Fake checks can look real and fool the bank. You'll have to pay back all the money.
- A caller tells you that there is a virus on your computer and instructs you to allow them remote access. Don't respond to phone calls about your computer asking for remote access – hang up.
- You get an email, text, or call asking to verify your credit card, bank account, or Social Security number. Never give that information to anyone who contacts you and asks for it.
- Someone says you can "ONLY" pay by wiring money, putting money on a gift card or loading money on a cash reload card? No legitimate company or government agency is going to direct you to pay in this form.

Familiarize yourself with some of the more common scams that have been reported in our area by visiting www.naperville.il.us/fraudscam.

SECTION 4: Reporting a Scam

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!!!