February 2019 "A Safer Naper" Website Content

Scam Presentations

The Naperville Police Department is hosting two scam awareness presentations as part of this month's A Safer Naper campaign. Learn more about fraud, the types of scams being reported in Naperville, and how to protect yourself. Most importantly, have all your questions answered in person!

- Tuesday, Feb. 26, from 1 to 2 p.m. at the 95th Street Library, 3015 Cedar Glade Drive
- Wednesday, Feb. 27, from 6:30 to 7:30 p.m. at the Municipal Center, 400 S. Eagle Street

---

February – Scam Prevention

A scam is a fraudulent or deceptive act, and in 2017, Americans were defrauded of $905 million. A surprising trend is that more young people are falling victim to fraud and scams than older people. A recent Better Business Bureau (BBB) report shows that Americans ages 18 to 34 were more susceptible to scams (43.7% were victims) than Americans 55 and older (27.6% were victims). However, while occurrences are fewer for older Americans, seniors still lose more money in scams than younger victims.

<u>Common Scams</u>

Grandkid Scams:
You get a call: "Grandma, I need money for bail." Or money for a medical bill. Or some other kind of trouble. The caller says it's urgent — and tells you to keep it a secret. But is the caller who you think it is? Scammers are good at pretending to be someone they're not. They can be convincing: sometimes using information from social networking sites, or hacking into your loved one's email account, to make it seem more real. And they'll pressure you to send money before you have time to think. The caller instructs you to either wire the money or purchase prepaid cards and give them the PIN number on the card. Do not act on the caller's directions before talking with a family member to verify the claim.

Internal Revenue Service / Social Security / Government Scams:
You get a call from someone who says she's from the IRS. She says that you owe back taxes. She threatens to sue you, arrest or deport you, or revoke your license if you don't pay right away. She tells you to put money on a prepaid debit card and give her the card numbers.

The caller may know some of your Social Security number. And your caller ID might show a Washington DC area code. But is it really the IRS calling? No. The real IRS won't ask you to pay with prepaid debit cards or wire transfers. They also won't ask for a credit card over the phone. And when the IRS first contacts you about unpaid taxes, they do it by mail, not by phone. And caller IDs can be faked.

"You've Won" Scams
You get a card, a call or an email telling you that you won! Maybe it's a trip or a prize, a lottery or a sweepstakes. The person calling is so excited and can't wait for you to get your winnings.

But here's what happens next: they tell you there's a fee, some taxes, or customs duties to pay. Then they ask for your credit card number or bank account information, or they ask you to wire money. Either way, you lose money instead of winning it. You don't ever get that big prize. Instead, you get more requests for money and more promises that you won big.

Imposter Scams

February 2019 "A Safer Naper" Website Content

You get a call or an email from a government official or someone you know – your grandchild, a relative or a friend. Or maybe it's from someone you *feel* like you know, but you haven't met in person – say, a person you met online who you've been writing to. Whatever the story, the request is the same: wire money to pay taxes or fees, or to help someone you care about.

But is the person who you think it is? Is there an emergency or a prize? Judging by the complaints to the Federal Trade Commission (FTC), the answer is no. The person calling you is pretending to be someone else.

Utility Scams
Someone claiming to be with your local utility company calls saying you owe money and threatening to shut off your utility unless you make a payment by wiring the money or using a prepaid card. Or during an outage, someone knocks on your door and offers to reconnect your service for a cash payment.

The problem is, once you wire money or use a prepaid card, your money is gone for good. And if you paid cash to restore your utility, your cash will be gone and your utility will still be out.

Real utility companies will not direct you to pay with prepaid debit cards or wire transfers. They also won't ask for a credit card over the phone, and they will never ask for cash to restore your connection.

Money Wiring Scams
Wiring money is like sending cash. Do not wire money to people you do not know. A scammer might use different ways to convince you to wire money. The scammer might say:

- You won a prize or inherited money, but you have to pay fees first
- You won the lottery, but you have to pay some taxes first
- A friend or family member is in trouble and needs you to send money to help
- You need to pay for something you just bought online before they send it
- You got a check for too much money and need to send back the extra

These are all tricks. When you hear stories like these, you have spotted a money wiring scam.

<u>Steps to Avoid Scams</u>

There are thousands of new scams every year, and you can't keep up with all of them. We know … we try! But if you can just remember these ELEVEN THINGS, you can avoid most scams and help protect yourself and your family.

- **Never send money to someone you have never met face-to-face.** Seriously, just don't ever do it. And really, really don't do it if they ask you to use wire transfer, a prepaid debit card or a gift card (those cannot be traced and are as good as cash).

- **Don't click on links or open attachments in unsolicited email.** Links can download malware onto your computer and/or steal your identity. Be cautious even with email that looks familiar; it could be fake.

- **Don't believe everything you see.** Scammers are great at mimicking official seals, fonts and other details. Just because a website or email looks official does not mean that it is. Even caller ID can be faked.

- **Don't buy online unless the transaction is secure.** Make sure the website has "https" in the URL (the extra s is for "secure") and that there is a small lock icon on the address bar. Even then, the site could be shady, but it's a start. Check out the company first. Read reviews about the quality of the merchandise

and make sure you are not buying cheap and/or counterfeit goods.

- **Be extremely cautious when dealing with anyone you've met online.** Scammers use dating websites, Craigslist, social media and many other sites to reach potential targets. They can quickly feel like a friend or even a romantic partner, but that is part of the con to get you to trust them.

- **Never share personally-identifiable information** with someone who has contacted you unsolicited, whether it's over the phone, by email, on social media or even at your front door. This includes banking and credit card information, your birthdate and Social Security/Social Insurance numbers.

- **Don't be pressured to act immediately.** Scammers typically try to make you think something is scarce or a limited time offer. They want to push you into action before you have time to think or to discuss it with a family member, friend or financial advisor. High-pressure sales tactics are also used by some legitimate businesses, but it's never a good idea to make an important decision quickly.

- **Use secure, traceable transactions** when making payments for goods, services, taxes and debts. Do not pay by wire transfer, prepaid money card, gift card or other non-traditional payment method. Say no to cash-only deals, high pressure sales tactics, high upfront payments, overpayments and handshake deals without a contract.

- **Whenever possible, work with local businesses** that have proper identification, licensing and insurance, especially contractors who will be coming into your home or anyone dealing with your money or sensitive information. Check them out to see what other consumers have experienced.

- **Be cautious about what you share on social media** and consider only connecting with people you already know. Be sure to use privacy settings on all social media and online accounts. Imposters often get information about their targets from their online interactions and can make themselves sound like a friend or family member because they know so much about you.

- **Sign up for free scam alerts from the FTC at ftc.gov/scams.**

Online Identity Theft Resources:

- Call the FTC at (877) 438-4338.
- Go to the Federal Trade Commission website or to sign up for FTC Consumer Alerts, https://www.consumer.ftc.gov/features/scam-alerts
- Check out the Better Business Bureau, https://www.bbb.org/us/news/scams
- Report identify theft and get help with a recovery plan at the Federal Trade Commission's IdentityTheft.gov site.

Don't Be Scammed - FTC Videos & Games

- PLAY - Grand Scam Challenge: Fact or Fiction https://www.consumer.ftc.gov/sites/default/files/games/off-site/grandscam/factfiction.html
- PLAY - Phishing Scams https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

February 2019 "A Safer Naper" Website Content

- PLAY - Spam Scam Slam
  https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_spam-scam-slam.html
- WATCH - Family Emergency Imposter Scams
  https://www.consumer.ftc.gov/media/video-0117-family-emergency-imposter-scams
- WATCH - How scammers make you pay
  https://www.consumer.ftc.gov/blog/2018/01/how-scammers-make-you-pay
- WATCH - IRS Imposter Scams
  https://www.consumer.ftc.gov/media/video-0118-irs-imposter-scams
- More Videos & Games
  https://www.consumer.ftc.gov/media