FRAUD, SCAMS & INTERNET SAFETY: WHAT EVERY PERSON NEEDS TO KNOW TO STAY SAFE

Presented by Sheffield Lake Police Department

Detectives Buddy Sivert and Miranda Helmick

Agenda

- Sheffield Lake Police Department Overview
- What is Fraud/Scams
- Types of Scams
- How to report suspected fraud/scams?
    - Steps to take when reporting
- Online Safety
- Key Points to Remember
- CodeRED
- Questions/Answers

Sheffield Lake Police Department

Chief Andrew Kory assumed the role of Chief of Police for the Sheffield Lake Police Department In 2021. Chief Andrew Kory has been with the Sheffield Lake Police Department since 2015

Comprised of 13 Full Time Officers and 5 Part Time Officers
Combined 417 years of law enforcement experience

Wellness Checks, Vacation Checks, Safe Drug Turn-in, Safety Town, Transaction Safe Zone, Voluntary Camera Registration, Hiring Off Duty Officers, Do Not Knock Registry, Code Red Alerts, Crash Reports, Vehicle Lockouts





What is Fraud?

Fraud has these elements:

- Misrepresentation
- of a material fact
- with the intent to deceive

All Frauds and Scams have two goals in common:

They want your MONEY
Or
They want the INFORMATION that will get your money

Fraud and Scams

According to the Federal Trade Commission (FTC), 6.5 million Americans reported being the victims of fraud, scams, and identity theft in 2024 alone.

This number is almost certainly underreported, as many victims feel too embarrassed to report the crime. The Department of Justice (DOJ) estimates that only 15% of fraud victims report to law enforcement that they have been scammed.

Anyone can be a victim of a fraud or a scam, although, 9 out of 10 times, elderly persons are targeted because they are more likely to have pensions, savings accounts, money market accounts, jewelry, property, and are usually more trusting.

Perceived financial stability
More trusting of authority
Grew up before digital fraud
Polite generation (scammers exploit that)

Important: Being targeted does NOT mean being gullible

Types of Fraud and Scams

Imposter
Phishing
Identity Theft
Online Shopping
Facebook Marketplace
Blackmail/Extortion/Sextortion
Charity
Tech Support
Lottery and Prize Money
Romance
Grandparent/Family
Skimming
Text/Phone/Email
In Person

Types of Fraud and Scams: Imposter

Imposter scams occur when scammers impersonate trusted individuals or organizations to deceive victims into providing money or sensitive information. These scams can take various forms, including phone calls, emails, or even in-person visits, where the scammer uses tactics to gain the victim's trust.

How to Recognize Imposter Scams

Unsolicited Contact: Be wary of unexpected calls, emails, or messages from individuals claiming to be from government agencies or businesses.

High Pressure Tactics: Scammers often create a sense of urgency, demanding immediate payment or personal information.

Requests for Untraceable Payments: Be cautious of requests for payments via GIFT CARDS, wire transfers or cryptocurrency (Bitcoin).

Poor Communication: Look for unusual grammar or awkward phrasing in written communications, which can indicate a scam.

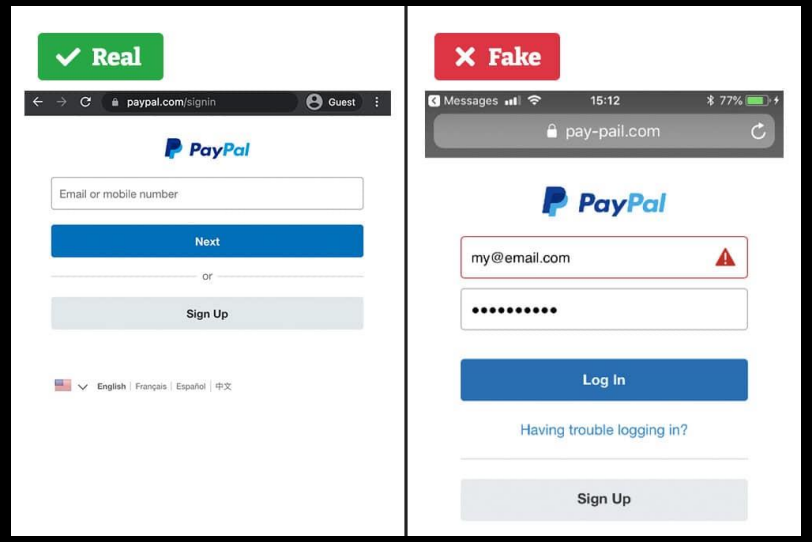
Types of Fraud and Scams: Phishing

Phishing is a type of cyber-attack where scammers impersonate legitimate organizations to trick individuals into revealing personal and financial information and occurs via email, text messages, and phone calls.

Spoofed Emails: Scammers often send emails that look like they are from trusted companies, such as banks or online services. These emails may say they contain urgent messages, prompting the recipient to click on a link or provide personal information.

Fake Websites: Links in phishing emails often lead to spoofed websites that closely resemble legitimate sites.

** How To Tell If It Is Fake: Look for poor grammar or spelling errors, low quality images, extra words or hyphens in the URL, lack of contact information, or requests personal information like SSN or credit card details or passwords, especially if it seems unnecessary for the service being offered. **



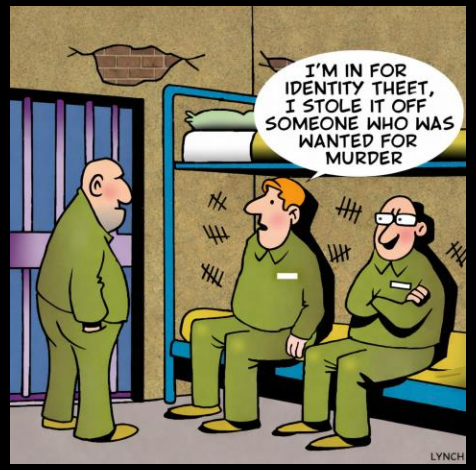
Personalization: Some phishing attacks are highly targeted, using information about the victim to make the scam more convincing. This can include referencing real colleagues or recent events.

Types of Fraud and Scams: Identity Theft

What is Identity Theft? Identity theft occurs when someone uses your personal or financial information without your permission. This can include your name, SSN, bank account details, and other sensitive information. Scammers can obtain this information through phishing emails, social medial, or even physical theft.

Common Types of Identity Theft Scams

Account Takeover Fraud – Criminals use stolen credentials to hijack bank accounts, credit cards, or social media accounts, preventing the rightful owner from accessing them.
Online Shopping Fraud – Scammers use stolen credit card information to make unauthorized purchases.
Mail Identity Theft – Thieves steal personal information from your mailbox, such as bank statements or credit card offers.



Warning Signs of Identity Theft

- Unexplained charges on your bank or credit card statements.
- Receiving bills or collection notices for accounts you did not open.
- Your credit report shows accounts you do not recognize.
- You are denied credit unexpectedly.

Types of Fraud and Scams: Online Shopping

Common Types of Online Shopping Scams

Fake E-commerce Sites: Scammers create websites that mimic legitimate retailers, often using slightly altered URLs. These sites may offer popular items at steep discounts.
Auction and Peer-to-Peer Scams: Fraudsters often pose as sellers on auction sites or peer-to-peer platforms and they may request payment through unprotected methods, making it difficult for victims to recover their funds.
Phishing Scams: Scammers send emails or messages that appear to be from well known retailers or payment platforms, tricking users into providing personal or financial information.
Counterfeit Goods: Some scams involve selling counterfeit or substandard products, leaving consumers dissatisfied and out of pocket.

Red Flags to Watch For and Tips for Safe Online Shopping

- Watch for Too Good To Be True offers – Research before you buy
- Unusual Payment Methods – Be cautious of sellers who request payments through wire transfers or gift cards
- Use secure payment methods that offer buyer protection
- Keep Software Updated
- Monitor Your Accounts
- Check Seller's Review History

Types of Fraud and Scams: Facebook Marketplace

Payment App Scams: Scammers often request payment through apps like Venmo, Zelle, or CashApp, which offer little to no buyer protection. They may claim the payment didn't go through or ask for additional payments, tricking users into sending more money without receiving their items.

Overpayment Scams: In this scam, a buying sends a check for more than the agreed price and asks the seller to refund the difference. The check eventually bounces, leaving the seller out of pocket.

Fake Listings: Scammers may list items at prices that are too good to be true, often for high demand items or events. Scammers may often list animals that do not exist and ask for payment for the animal/transportation before you even see the animal.

Shipping Scams: Buyers may be pressured to pay for items before they are shipped, with scammers providing fake tracking information to make it seem like the item was sent.

Gift Card and Wire Transfer Scams: Scammers may insist on payment via gift cards or wire transfers, which are nearly impossible to reverse once sent. Legitimate transactions should always use secure payment methods that offer buyer protection.

Safety for Online Transactions

Sheffield Lake Police Department and Police Departments in the surrounding communities offer a Transaction Safe Zone. This area is located at the front of our Police Department and is designated for completing online transactions. This initiative aims to make local buying and selling safer by providing a safe and secure area to conduct these transactions.

Types of Fraud and Scams: Blackmail/Extortion/Sextortion

Social Media Account Takeover Blackmail – One of the most common online extortion methods. Attackers often begin with phishing links that appear to be Instagram, Facebook, or other social media login pages. Once victims enter their credentials, the attackers quickly lock them out. From there, the blackmail begins. Victims are told they must pay to regain access or else their private messages and photos will be leaked. In some situations, attackers impersonate the victim and send messages to friends or relatives, attempting to persuade them with send money or other compromising material.

Sextortion – A crime where scammers threaten to share private sexual images, videos, or personal information unless you meet their demands. These demands often include paying money, buying gift cards, or performing other actions you do not want to do. Anyone can be a target, even if you've never shared an intimate photo. Criminals are incredibly skilled and can use sophisticated tools like Artificial Intelligence (AI) to create convincing fake images or videos.

How to Respond

1. Don't Pay - Scammers often send these messages in bulk. If you pay once, you'll likely be targeted again.
2. Don't Reply - Responding only confirms you saw the message — and makes you more of a target
3. Change your passwords - Especially if they include an old one in the message. Use strong, unique passwords and enable two-factor authentication.
4. Report the message - To your local law enforcement, the FBI's Internet Crime Complaint Center (IC3.gov) or the FTC. You can also report emails as spam or phishing in your email provider.
5. Talk to someone - These scams are designed to isolate you. If you're scared, talk to a trusted friend or a professional. You're not alone and you're not the only one getting these messages.
6. Cover your Webcams - Going forward it will be obvious the sender is lying about the message if the camera couldn't have recorded any footage.

Types of Fraud and Scams: Charity

Scammers create fake charities or impersonate legitimate ones, often using emotional appeals to solicit donations. Commonly, scammers may use emails, fake websites, and caller ID spoofing to reach victims.

Signs of Fraud: Be wary of charities that pressure you for immediate donations or lack transparency about how funds are used.

How to Protect Yourself: Research charities before donating, check their legitimacy through resources like the Better Business Bureau, and be cautious of unsolicited requests. If you do donate, use a secure payment method.

In December 2024, the most trusted charity categories were: veterans organization (28%), non-profit hospitals (27%), religious organizations (26%), animal welfare organizations(26%), and social service charities (25%) such as homeless shelters, family counseling centers, and services for the elderly.

8 Most Common Types of Charity Scams

Disaster Relief Scams
Veteran, Military, Firefighter and Police Scams
Animal Welfare Scams
Health Related Scams
International Aid Scams
Impersonations of well-known charitable organizations
IRS Scams
Crowdfunding and Social Media Scams

Types of Fraud and Scams: Tech Support

In these scams, criminals pose as technical or customer support/service

How the Scam Works

Scammers—some working out of fraudulent call center across the globe—pose as representatives from legitimate companies, such as financial institutions, utility companies, or cryptocurrency exchanges.

They tell you that there's some sort of issue with your device or account. They try to reach you in a number of ways, including:

Unsolicited phone calls or text messages claiming to be from tech support
Internet pop-up windows telling you to call a tech support number
Websites or online ads advertising a tech support number
financial institutions, utility companies, or cryptocurrency exchanges

However the scammer gets your attention, they'll inform you that they can fix the issue for you—for a fee—and that you have to act fast. Scammers may ask you to wire cash, send a gift card, or even transfer cryptocurrency as payment. Once you grant the scammer remote access to your computer or your account, they'll steal your personal information and/or money.

Unfortunately, many people in this situation don’t realize they're being scammed until it's too late.

Types of Fraud and Scams: Lottery/Prize Money

You get a call, email, or letter saying you won a sweepstakes, lottery, or prize — like an iPad, a new car, or something else. But you know it's a scam because of what they do next: they ask you to pay money or give them your account information to get the prize. If you pay, you'll lose your money and find out there is no prize.

3 Signs of a Prize Scam

1. If you have to pay to get your prize, it's a scam
2. If you have to pay to increase your odds of winning, it's a scam
3. If you have to give your financial or personal information, it's a scam

How Scammers Try to Trick You

1. Scammers say they're from the government when they're not
2. Scammers use names of organizations you might recognize
3. Scammers send you a message (via text, email, or social media) to get your personal information
4. Scammers make it seem like you're the only person who won a prize. But the same text, call, email, or letter went to lots of people
5. Scammers say you've won a foreign lottery or say you can buy tickets for one
6. Scammers pressure you to act now to get a prize, or to hurry up and pay or give them information
7. Scammers send you a check and ask you to send some of the money back
8. Scammers tell you to pay a specific way (wire money via Western Union, gift cards, or cryptocurrency)

Types of Fraud and Scams: Romance

Romance Scams occur when a criminal creates a fake online identity to gain a victim's affection and trust, often claiming to be in love or seeking a relationship. Scammers my propose marriage, express strong emotions quickly, or claim to be abroad for work, military service, or other reasons that prevent in-person meetings. Once trust is established, they request money, gifts, or personal information, often citing emergencies, travel expenses, medical bills, or investment opportunities as reasons for payment.

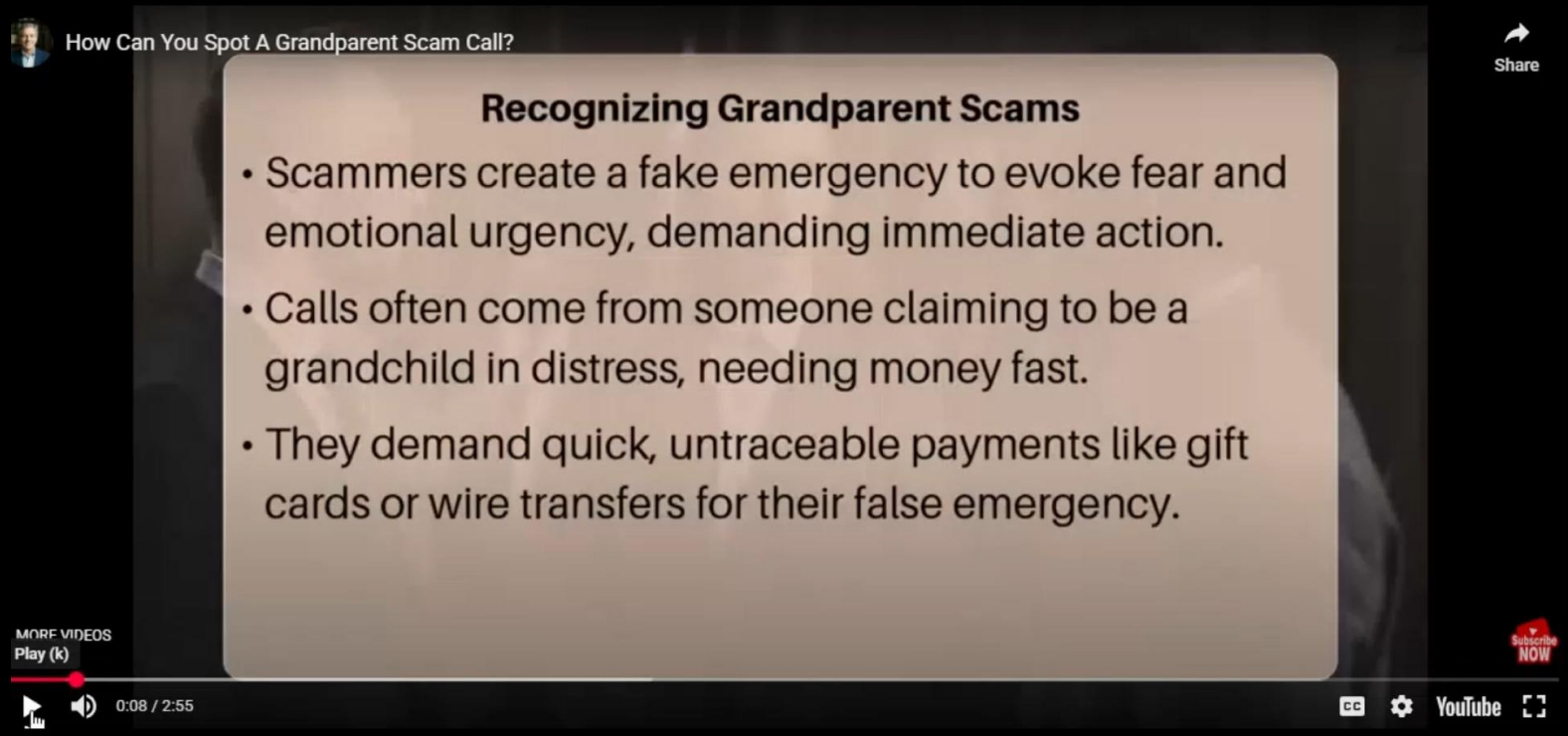
While anyone can be targeted, older adults, especially those aged 50-64, are disproportionately affected. Research shows nearly 1 in 10 adults over 50 have been asked for money or cryptocurrency in a supposed romantic connection, with 16% reporting a financial loss. (AARP)

How to Protect Yourself

- Never send money or gifts to someone you haven't met in person
- Verify identities using reverse image searches or online research (often use stolen photos of celebrities)
- Keep communication on reputable platforms (will often ask to switch over to WhatsApp)
- Discuss new relationships with trusted friends and family
- Use strong privacy settings on social media and limit personal information shared publicly

Types of Fraud and Scams: Grandparent/Family

Grandparent scams are a type of fraud where scammers impersonate family members, often grandchildren, to create a sense of urgency and fear. They may claim to be in trouble, such as an accident or arrest, and ask for money to resolve the situation. These scams can be very convincing, especially when the scammers use voice cloning technology to imitate the victim's voice.



Recommendation:

Come up with a code word that only your family member would know. Try to avoid common phrases or personal details that could be easily guessed by scammers.

Types of Fraud and Scams: Skimming

Skimming occurs when devices illegally installed on or inside ATMs, point-of-sale (POS) terminals, or fuel pumps capture card data and record cardholders' PIN entries. Criminals use the data to create fake payment cards and then make unauthorized purchases or steal from victims' accounts

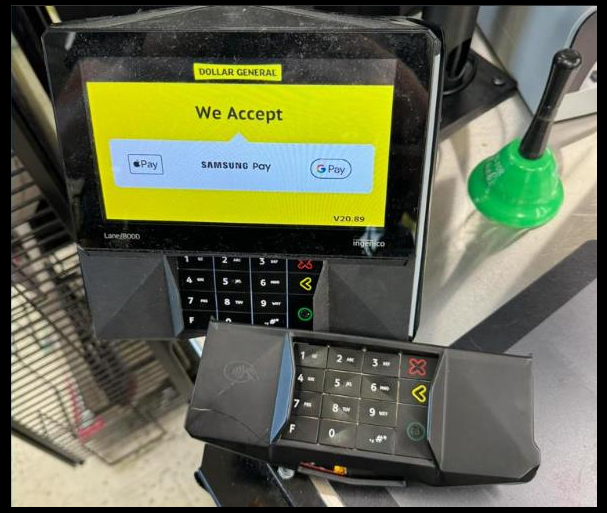
It is estimated that skimming costs financial institutions and consumers more than $1 billion each year.

Protect Yourself

- Inspect ATMs, POS terminals, and other card readers before using. Look for anything loose, crooked, damaged, or scratched. Pull at the edges of the keypad before entering your PIN.
- When possible, use debit and credit cards with chip technology. There are fewer devices in the U.S. that steal chip data than magnetic strip data.
- Routinely monitor your credit card, bank, and EBT or other benefits accounts to promptly identify any unauthorized transactions. If possible, set email or text-message alerts to notify you of card or account transactions.
- Proactively review the account-security options available for any payment cards you use. These options can include multi-factor authentication of transactions or freezing an account between your own transactions.
- Contact your financial institution immediately if the ATM doesn't return your card after you end or cancel a transaction. This may suggest the presence of a foreign device in the card reader.

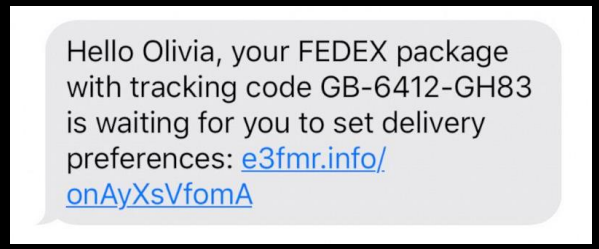
- If you receive a call, text message, or email asking for your PIN, never provide it.
- Always use a strong PIN. Avoid using PINs that may be easily guessed, such as strings of the same or consecutive numbers.

Types of Frauds and Scams: Skimming

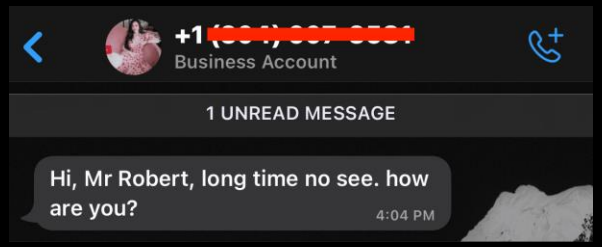


Types of Fraud and Scams: Text/Phone/Email

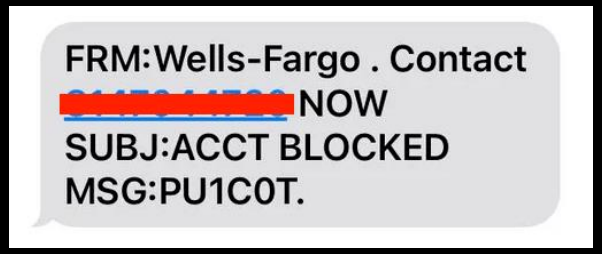
- Fake Delivery Problems: Scammers impersonate delivery services to trick you into providing personal information or pay a fee. Don't click on the link in the text. Instead, go to the official website for the delivery service.



- "Is this you?" Messages: Scammers are hoping that they can convince you that this message is from someone you know and may ask for money or other favors. Do not respond if you do not recognize the number

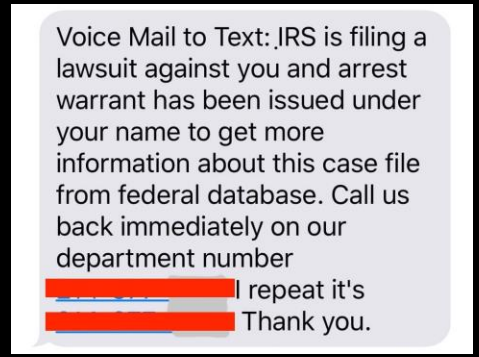


- Text Claiming Your Bank is Closing Your Account or Debit/Credit Card Has Been Locked: Scammers will claim your account has been locked or closed and to restore access, you will be asked to follow a link or call a phone number. Don't respond to the text. Instead, contact your bank via official channels to confirm the status of your account(s).



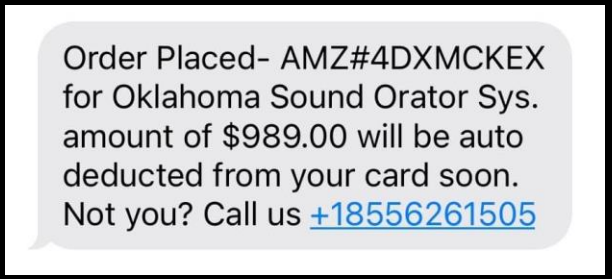
Types of Fraud and Scams: Text/Phone/Email

- IRS/Other Government Agencies: Scammers may tell you that you have a warrant out for your arrest due to tax evasion or you must pay a "fee" to accept your tax refund or benefits. The IRS will not contact you through text



- Texts claiming that your payment for subscription services didn't go through (Netflix, HBO, ect): The scammer's goal is to get you to click on the link and enter payment information. Log into your account directly through the company's website and check your payment history.

- Texts about purchases you didn't make: Scammers will often provide you a phone number to call and then you'll be prompted to "verify" your information, such as your credit card number. Do not click the link or call the phone number. If you're concerned about a fraudulent purchase, contact your bank directly.



Types of Fraud and Scams: Text/Phone/Email

- Unpaid Toll Fees: Scammers claim you owe a small toll fee and must pay it immediately to avoid penalties. The Ohio Turnpike does NOT send text messages requesting payment for unpaid tolls. They will notify you through US Mail.

- 2,695,229,046. That's the number of spam messages that scammers send out *every week*

- On iPhone: Go to Settings > Messages > then scroll down to Message Filtering > Toggle on "Filter Unknown Senders."
- On Android: Go to Messages > then navigate to Settings > Click on Spam Protection and enable it

How to Keep Yourself Safe

Avoid giving out your phone number to strangers or posting it to your social media accounts.
Never provide personal information over a text or phone call unless you know for certain whom you're speaking with.
Don't share your temporary credentials like 2-factor verification, account numbers, or any personal identifying information.

Types of Fraud and Scams: In Person

In-person fraud involves criminals physically interacting with victims to steal money, personal information, or assets, often using fake identities or impersonation tactics.

In person fraud occurs when scammers meet victims face to face or arrange transactions to commit theft or deception. Unlike online scams, these crimes rely on direct interaction, often exploiting trust, urgency, or fear to manipulate victims into handing over money, valuables, or sensitive information. Common target include bank accounts, credit cards, medical insurance, and personal property.

- Courier or Pickup Scams – Scammers instruct victims to hand over valuables to a courier or at a public location, claiming it is for safekeeping or verification or to solve an issue.
- Check Fraud – Stolen checks and identifying documents are obtained by theft from a residence, vehicle or mail and then sold to scammers to commit financial fraud.
- Rental Property Fraud – Scammers pose as landlords to exploit prospective tenants. These scammers create fake listings for properties that do not exist or are not available for rent. They then ask for upfront payments such as application fees, deposits, and/or first month's rent before the prospective tenant has even seen the property. Sometimes scammers hijack real listings and change the contact information to their own.

How to Report a Fraud/Scam

Federal Trade Commission (FTC) – The FTC collects reports about scams, fraud and bad business practices. You can submit a report online at www.ReportFraud.ftc.gov

Better Business Bureau (BBB) – The BBB Scam Tracker allows you to report scams such as fake job offers, counterfeit products, investment fraud, or identity theft. www.bbb.org/scamtracker

Internet Crime Complaint Center (IC3) - For cyber enabled crimes, including online scams, phishing, or hacking, file a report with the IC3, run by the FBI. www.ic3.gov

USA.gov Scam Reporting Tool – If you are uncertain which agency to contact, USA.gov provides a tool to help identify the correct organization for your scam report. www.USA.gov

FBI and Local Law Enforcement – For serious scams, especially those involving threats, extortion, or immediate danger, contact your local police and/or the FBI.

How to Report a Scam: Steps to Take When Reporting

1. Document everything: Keep emails, receipts, screenshots, and any communication with the scammer.

2. Report promptly: Use the appropriate platform (FTC, BBB, IC3, or local authorities).

3. Protect your information: Change passwords, monitor bank accounts, and consider credit monitoring if personal data was compromised. Another option is to freeze your credit temporarily and to put an alert on your bank accounts.

Equifax	Experian	Transunion
Fraud alert • Security freeze • 1-800-525-6285	Fraud alert • Security freeze • 1-888-397-3742	Fraud alert • Security freeze • 1-800-916-8800

4. Warn others: Sharing your experience on platforms like BBB Scam Tracker helps prevent others from falling victim.

Online Safety Tips

Don't Overshare Information – This info can lead to identity theft and crime. Think About What You Post

Passwords are important! Stats show that over 50% of Internet users use the same password for all or most of their accts/sites

Guard Personal Information

Don't accept friend requests from people you do not know or have never met

Use a secure website used for banking and online shopping. Should start with "https:" and have a  icon in URL field

Make sure your connections are secure at home and on your devices. Refrain from using "free" wifi at locations

Summary: Key Points

1. Do NOT pay anyone with Apple Giftcards or Cryptocurrency (ie Bitcoin)! No reputable agency or company will ask for payment in this way

2. Do NOT disclose account numbers or personal identifying information to anyone that you do not know or recognize. When in doubt, call the number on the back of your card or go to your local bank branch.

3. Law Enforcement will NEVER call you and tell you that you or a family member has a warrant and you need to pay money for bond.

4. NEVER install an app when a supposed technical support or banking individual who has reached out to you first, sends a link or points you to a website.

5. Your bank or credit card company will NEVER call and ask for security credentials, have you transfer money or change your account.

6. Refrain from using communication applications such as WhatsApp unless you know the person in real life.

Emergency Alerting Information - CodeRED

This Service will provide residents with essential notifications during emergencies

ONSOLVE™
CODERED

Text “LORAINCO” to 24639
https://loraincountyohio.gov/777/Emergency-Alerting-Information

CodeRED Sign Up Step by Step Instructions Available Online

SHEFFIELD LAKE POLICE