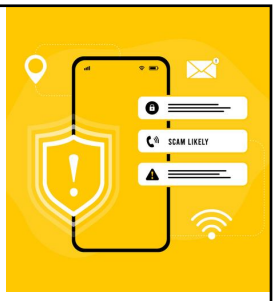
Everyday Fraud

Tips for avoiding scams

Vanessa VanderWeele
Community Development Specialist



What is the impact of fraud and scams?

Stand up for your response!

How many people reported being scammed to the FTC in 2024?

A. 780,000
B. 1.6 million
C. 2.6 million

Answer: The FTC received 2.6 million fraud reports in 2024

How much money was lost to scams?

A. $5.8 billion
B. $12.5 billion
C. $34 billion

Answer: There was $12.5 billion in reported losses to fraud

What was the top scam reported?

A. Online Shopping
B. Investments
C. Imposter

Answer: The top scam was Imposter Scams

What do they want?

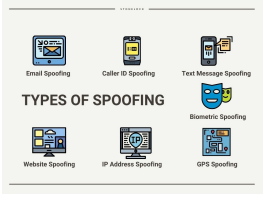
- Identifying information
- Passwords and log-ins
- Access to your cash
- **They don't want to steal it, hack in or break in; they want you to freely give it to them!**

Impersonation Scams

- A scammer pretends to be someone you trust to convince you to send them money or information
  - Law enforcement
  - Family member
  - US government
  - Geek Squad
  - Microsoft
  - MacAfee or Norton Anti-Virus
  - Employers
  - Online Dating
  - Utility company
  - Retail- Amazon, Costco
  - Investment services/crypto/gold
  - PayPal and payment apps
  - Banks and Credit Unions
  - Giveaways, contests, prizes
  - Celebrities
  - Farmers market and craft fair organizers

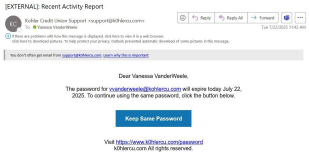
What's Spoofing?

- Easiest way to impersonate a trusted person/ organization
- ***Free, fast and easy to do with AI (Artificial Intelligence)!***



Email Scams

- Missing package
- Order confirmation
- Request for information
- Plan will auto renew

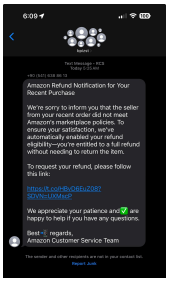


- What to do?
  - Don't click links or attachments
  - Check the real email address

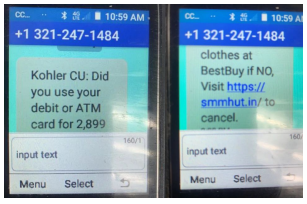
Text Scams

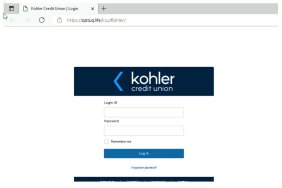
- Missing package
- Order confirmation
- Tolls or fees
- Account compromised

- What to do?
  - Don't click links!
  - Verify with a trusted number



Text Scams

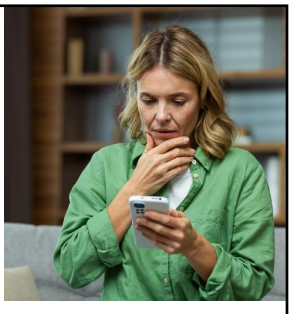




Phone Scams #1

A Call for Help

- What happens?
  - They say your loved one was in an accident and is either at risk of jail or is in the hospital.
  - A lawyer, nurse or other official will ask for payment to bail them out or pay for medical care
  - They want you to panic and worry about them



Phone Scams #2

Financial institution calls

- What happens?
  - Someone acting as your financial institution will call, saying that your accounts are hacked
  - They are trying to get additional sensitive information
  - Or encourage you to move your money somewhere "safer", such as a wire transfer, cash or cryptocurrency

Phone Scams #3

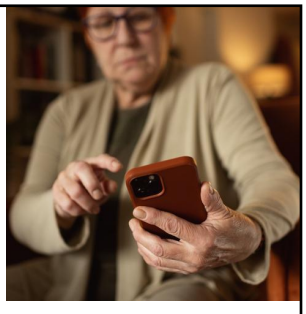
Medicare/Medicaid calls

- What happens?
  - Ask you to verify your information, update your card
  - Upgrade your plan to provide better benefits/ save money
  - Give payment information
  - Promise to mail you a new card
  - Instead- they steal your identity or your payment information

Phone Scams

What should you do?

- Avoid answering if you can
- Don't trust caller ID
- Create a family password or question
- Set your voicemail as generic
- Hang up and call a number you trust to verify before sharing personal information



Investing Scams

- Often starts as a business proposal, a friendship or relationship
- Show off their wealth and say they can help you too!
- Give fake screenshots that show your "investment" growing
- Scammers say you need to act fast or risk missing out on the next big thing

Check Cashing Scams

- Scammer offers to pay you with a check, and have you send a wire transfer, crypto or gift cards back
- Check bounces, you own the cost of what you sent plus fees
- **Common themes include:**
  - Romantic- "I've lost access to my bank account, can you cash this check then send me gift cards to keep my phone on?"
  - Services/Jobs- "I need a pet sitter for a month. I'll send you a check for supplies, then send me the rest back"

Government Scams

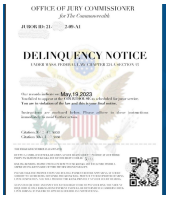
- You receive an email or a phone call from your local government office. The sender says you have unpaid invoices or bills, and you are in trouble
- Another common scam is impersonating the IRS or Social Security, requesting updated payment or contact information

Law enforcement Scams

- Police and sheriff officers, detectives are trusted officials
- Easy to impersonate
- Strong emotions: Embarrassed, afraid, urgency, panic, guilt and shame
- You are a good person and want to avoid getting in trouble!

Law Enforcement Scams

- Donations to a national law enforcement charity
- Texts about unpaid tickets
- Missed jury duty or other court proceeding
  - Urges you to pay before there is legal action, vehicle repossession, greater fines or arrest


OFFICE OF JURY COMMISSIONER
for The Commonwealth

DELINQUENCY NOTICE

May 19 2023

Red flags

- Payment isn't possible at police station
- Requesting wire transfer, gift cards, cryptocurrency or cash picked up by an "agent"
- They negotiate the "bond" or fine down if you can't afford it
- They want to keep you on the phone
- May send a (fake) warrant by text or email

Law Enforcement Scams

- Hang up
- Call non-emergency number
- Or go in person to the station
- Verify if you have any outstanding issues
- Donate to local law enforcement groups directly

Why cryptocurrency?

- Cryptocurrency, like Bitcoin, is one of the fastest growing ways for scammers to request cash
- **Bitcoin "ATMs" or kiosks are in at least 700 locations in Wisconsin so far**
- Investigations have shown that more than 9 in 10 uses of crypto kiosks are fraudulent
- **In Wisconsin, over $5.4 million lost in 2025**
- Scammers might call them:
  - "Official Payment Stations"
  - "Police Certified Repayment"

Wisconsin is fighting back!

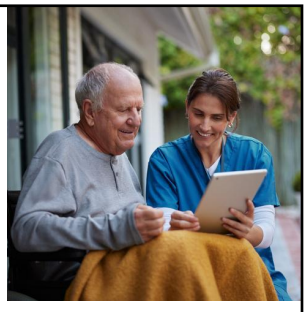
- **As of April 10th, Wisconsin Law- Act 226 imposes new regulations on virtual currency kiosks to prevent fraud**
- **Under the new law:**
  - Operators must be licensed by the state and notify local law enforcement of locations
  - They may not be within 5 feet of an ATM, and can't function as both
  - Customers using the machines must have their identity verified with photo and ID
  - Limit of $1,000 in transactions per day
  - Operators must refund the full transaction amount including fees if a customer reports a fraudulent transaction to the operator and to law enforcement within **30 days**.

Caregiving and Scams

- **Money represents a form of security and independence**
- **Common aspect of Alzheimer's or other dementia, signs include:**
  - Uncharacteristic spending patterns
  - Inability to manage a budget
  - Unopened bills
  - Giving money to telemarketers or soliciting companies
  - Unexplained withdrawals from the person's bank account

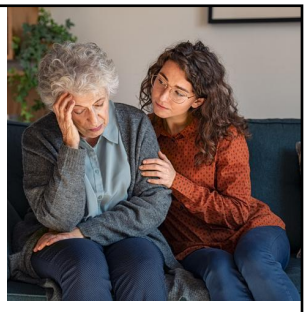
Caregiving and Scams

- **Connect with financial institutions to put alerts on accounts**
- Financial power of attorney
- **Signing up for the "Do Not Call" list at DoNotCall.gov**
- Setting up auto-pay for bills instead of paying them by check
- **Reduce credit card limits**
- If you are concerned that they don't have the ability to care for themselves, report to the local ADRC



Chronic Scam Victims

- The person is being targeted by sophisticated techniques designed to stimulate their emotions in ways that prevent rational thinking
- **Victims often have intense unmet needs that the scammer is tapping into**
- Understand it's not you against the victim; it's you against the criminal who's in the ear of the victim



Prevention Steps

- **Focus on working together vs. taking over accounts**
- Set healthy boundaries
- **Be an example of awareness**
- Build a support network
  - Friends, family, neighbors
  - Community resources
  - Businesses you trust
- **AARP and FTC have great resources**

Protecting yourself

- Always be aware that emails, texts, and phone calls **may not be from who they say they are**
- Keep trusted contact numbers to verify the situation
- **Google your name** and find out what is publicly available!

Protecting yourself

Freezing credit

- A credit freeze restricts access to your credit report preventing identity thieves from opening new accounts in your name
- **It is a free, secure, and reversible measure that does not affect your credit score**
- Call the three credit bureaus or go online
  - Equifax **1-888-Equifax (1-888-378-4329)**
  - Trans Union **800-916-8800**
  - Experian **1-888-Experian (1-888-397-3742)**

What if I was Scammed?

- The FTC has a full guide on what to do if you've been scammed based on what happened
- **Contact your bank/credit union within 24 hours**
- Update your passwords
- **Check your devices for malware and keylogging**
- IdentityTheft.gov has steps to monitor your credit
- **Ask for help!**

Thank You!

For free scam education resources, visit the Resources tab on kohlercu.com!

Vanessa VanderWeele
Community Development Specialist
vvanderweele@kohlercu.com