AVOID **SCAMS** AND PROTECT WHAT IS **YOURS**

In 2023 alone, the FBI estimated more than $12.5 billion* was lost to cybercrime in the United States. Vulnerabilities in technology and lack of sufficient attention to security by users provide cybercriminals with low-risk, high-reward opportunities for illicit gain. Through research and personal experience, we hope to help you be better prepared to protect yourself from possible attacks.

*Figure sourced from the FBI 2023 Internet Crime Report

Call Us With Questions
603 294 4121

SAGE WEALTH PARTNERS

Visit Our Website
sagewpartners.com

Four Signs That 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, 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.

- There is usually an "important reason". They might say you're in trouble with the government, you owe money, someone in your family had an emergency, there's a dangerous virus on your computer, etc.
- Some scammers might say there's a problem with one of your accounts and that you need to verify your information.
- Others will lie and say you won money in a lottery or sweepstakes but you have to pay a fee to claim it.

3 Scammers PRESSURE you to act immediately.

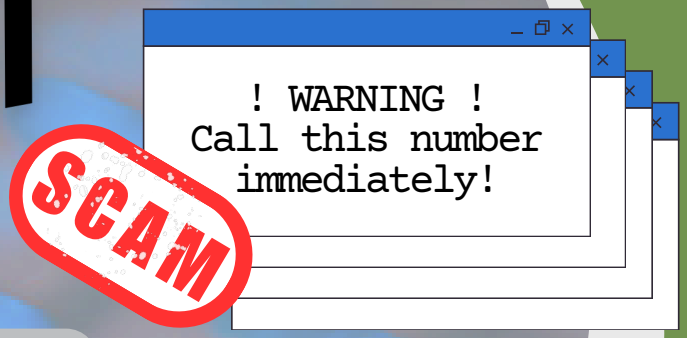
- Scammers want you to act before you have time to think. If you're on the phone, they might tell you not to hang up so you can't fact check their story.
- They might threaten to arrest you, sue you, take away your driver's or business license, or deport you. They might say your computer is about to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

4 Scammers tell you to PAY in a specific way.

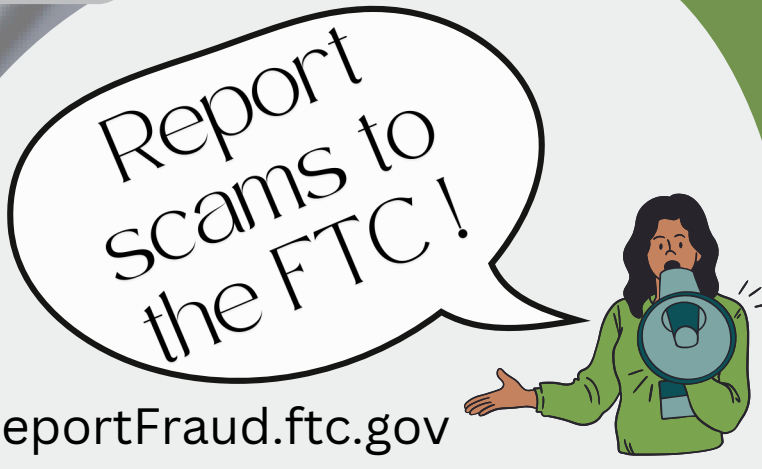
- They often insist that you can only pay using cryptocurrency, using a payment app, wiring money to an unknown account, or putting money on a gift card and then giving them the card number.
- Some may send you a fake check, then tell you to deposit it and send them money.

information sourced from https://consumer.ftc.gov/

How to Avoid a Scam



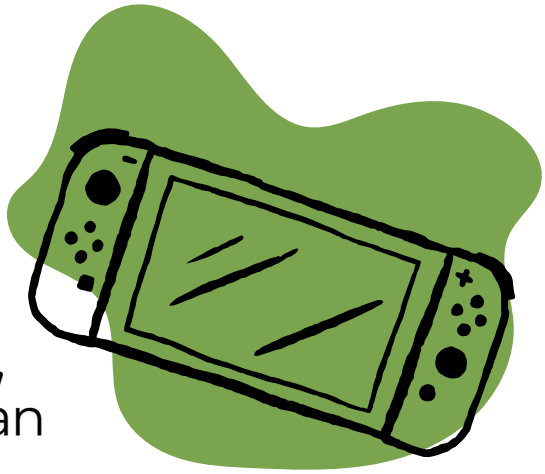
- BLOCK UNWANTED CALLS TEXTS AND POP-UPS
- DO NOT GIVE FINANCIAL OR PERSONAL INFORMATION WHEN REQUESTED UNEXPECTEDLY
- RESIST THE PRESSURE TO ACT IMMEDIATELY
- NEVER PAY SOMEONE THROUGH UNCONVENTIONAL METHODS
- NEVER DEPOSIT A CHECK OR ONLINE PAYMENT AND SEND THE MONEY BACK TO SOMEONE.
- ***STOP AND TALK TO SOMEONE YOU TUST***



ReportFraud.ftc.gov

An unexpected package from an unknown sender arrives in your name. You open it and find a note that says it's a gift, but it doesn't say who sent it. The note also says to scan a QR code to find out who sent it — or to get instructions on how to return it. Did someone really send you a gift? Or is it an attempt to steal your personal information?

Talk to your kids about protecting their personal information. Tell them not to share their Social Security numbers, account numbers, and passwords. Watching out for "free" stuff. Free Apps, games, ring tones, or other downloads can hide malware.



Is it Phishing? Phishing is when scam artists send fake text, email, or pop-up messages to get people to share their personal and financial information. Criminals use the information to commit identity theft. Don't reply to text, email, or pop-up messages that ask for personal or financial information. Be cautious about unknown links, attachments or downloading any files from emails you receive, **regardless of who sent them**.

PREVENTING IDENTITY THEFT

PROTECT YOUR PERSONAL INFORMATION

- Don't carry your social security card. The key to identity theft is your social security number.
- Don't provide your social security number to anyone unless there is a legitimate reason. These include: Applying for employment; opening a financial account; getting a credit check; checking or freezing your credit reports.

PROTECT YOUR DOCUMENTS

- Shred your sensitive trash with a cross-cut, micro-cut or diamond-cut shredder.
- Don't leave outgoing mail with personal information in your mailbox for pickup.

BE VIGILANT AGAINST TRICKS

- Never provide personal information to anyone in response to an unsolicited request.
- Never reply to unsolicited emails from unknown senders or open their attachments.
- Don't click on links in emails from unknown senders.

PROTECT YOUR COMMUNICATIONS

- Keep your computer and security software updated.
- Don't conduct sensitive transactions on a computer that is not under your control.
- Protect your Wi-Fi with a strong password and WPA2 encryption.

PROTECT YOUR DIGITAL WORLD

- Use strong passwords with at least twelve characters.
- Use different passwords for your various online accounts.
- Consider using password management programs

YOU CAN FREEZE YOUR CREDIT BY MAIL, PHONE OR ONLINE

CREDIT REPORT BUREAUS

Experian
(888) 397-3742
www.experian.com/freeze

Equifax
(800) 685-1111
www.equifax.com/personal/credit-report-services

Innovis
(866) 712-4546
www.innovis.com/personal/SecurityFreeze

Trans Union
(888) 909-8872
www.transunion.com/credit-freeze

"If they have my Social Security Number, what can they do?"

- New account fraud - meaning they can open credit cards, bank accounts and take out loans in your name.
- File state and federal tax returns in your name.
- File for social security benefits in your name (if you're eligible), or redirect your current benefits to their accounts.
- Receive medical care or prescription drugs in your name.

YOU ARE ALLOWED 4 FREE CREDIT REPORTS EACH YEAR

Go to
www.annualcreditreport.com or
call 877-322-8228
for more information

TAX REFUND FRAUD

Criminals can file tax returns using your identity. When this happens, you won't be able to file your tax return. Check with your state authorities to see what methods they use to help prevent fraud. For federal taxes you might be able to get a PIN number from the IRS to prevent fraud. For more information, go to www.irs.gov

MEDICAL FRAUD

If a ciminal used your identity to receive medical services, not only does it defraud the insurance provider or Medicare, but it could create entries in your permanent medical record for procedures you did not receive and conditions you have never had.

Check your health insurance statements carefully and let providers know right away if you have been a victim of identiry theft.

SOCIAL SECURITY BENEFITS FRAUD

With your social security number, a criminal can sign-up for social security benefits in your name or re-direct existing benefit payments to their bank account.

If you are 62 years of age or older and have not created your online social security account, prevent the criminal from doing it before you. Sign-up at www.ssa.gov

TITLE FRAUD

Criminals use your identity to forge documents to transfer your real-estate into their name. Although the transfer is not legitimate, it is possible they could sell the property before the fraud is discovered. Your best defense is to routinely monitor your property records with the county and request automatic notifications for any record changes.

STEPS TO TAKE IF YOU ARE A VICTIM OF IDENTITY THEFT

1. Notify all four major credit agencies.
2. Call your local police and file a report.
3. Call the Social Security Administration's fraud hotline at 800-269-0271.
4. Contact the Internal Revenue Service at 800-829-0433.
5. Notify any organization that had your money, including your financial advisor.
6. Notify your medical insurance providers.
7. Review all recent account statements for unauthorized activity and report any suspicious transactions.

DO YOUR PART TO BE CYBER SMART

SHOW STRENGTH
Form a strong password or “passphrase” of three random words, and at least one number & symbol.

GET CREATIVE
Use seperate passphrases for each of your online accounts.

GO THE EXTRA STEP
Turn on two factor Authentication & sign-in alerts.

GET PICKY
Confirm authenticity. Don’t open messages or click on links from vague emails or texts.

BE DILIGENT
Keep security software up to date and schedule routine anti-virus scans.

HAVE A SAFETY NET
Regularly backing up your storage protects your files and important information, incase they become inaccessible or corrupted.

SAGE WEALTH PARTNERS

603-294-4121 sagewpartners.com

The financial advisors at Sage Wealth Partners are registered representatives with, and securities and advisory services are offered through LPL Financial, a registered investment advisor, Member FINRA/SIPC