UGEFCU
UTICA GAS & ELECTRIC FEDERAL CREDIT UNION

215 Old Campion Road
New Hartford, NY 13413
(315) 733-1596
www.ugefcu.com

For more identity theft prevention tips, call or stop by our office UGEFCU today. And if you ever become a victim of identity theft, remember that we're here to help. Call (315) 733-1596 or toll-free 800-990-7499 or visit www.ugefcu.com

REMEMBER: Our credit union will never call you, text you or email you asking for personal account information, because we already have your information on file. Scammers are trying to get your personal information, don't do it!
HANG UP, DON'T OPEN EMAILS

NCUA Adv. #122 - Sept. 2024

TOP TEN OVERALL

Rank	Scam Type	Percentage Total - 2023	% Change (2022-2023)	Median Loss
1	Prizes/Sweepstakes/Free Gifts	28.66%	-5.31%	$1,008
2	Internet: Gen Merchandise	20.39%	-4.73%	$497
3	Phishing/Spoofing	17.31%	-10.83%	$1,615
4	Investments: Other (incl. cryptocurrency)	9.03%	152.25%	$20,000
5	Fake Check Scams	5.41%	-7.34%	$1,718
6	Advance Fee Loans, Credit Arrangers	3.16%	11.52%	$1,225
7	Friendship & Sweetheart Swindles	3.01%	30.33%	$8,000
8	Charitable Solicitations	1.45%	195.57%	$350
9	Family/Friend Imposter	1.42%	-31.96%	$1,040
10	Home Repair	1.05%	17.51%	$2,199

When in Doubt, Report It!

This year's Top Ten Scams report was compiled from more than 2,700 complaints submitted by consumers. No matter what scam a consumer encounters, we always recommend reporting it. Here at Fraud.org, we share complaints with a network of more than 200 law enforcement and consumer protection agency partners. Those partners use complaint data to spot trends, identify gaps in policy, and build cases against scammers.

FCC | CONSUMER CONNECTIONS

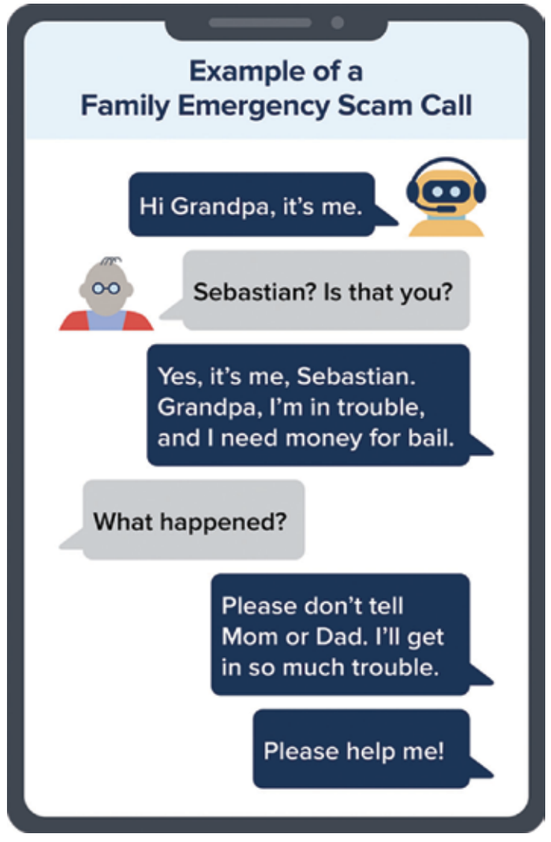
Avoid Spoofing Scams

Phone scammers often disguise their identity by using illegal spoofing techniques to send false information to your caller ID display. To trick you into answering, spoofers may use local area codes and numbers that look familiar. Or they may impersonate a company you do business with, such as a local utility, or even a government agency.

Here are some good ways to avoid being spoofed:

- ☑ Don't answer calls from unknown numbers.
- ☑ If you answer and it's not who you expected, don't hang on, hang up.
- ☑ If a caller asks you to hit a button to stop getting calls, just hang up.
- ☑ Never assume an unexpected call is legitimate. Hang up and call back using a number you can verify on a bill, a statement, or an official website.
- ☑ Be suspicious. Con artists can be very convincing: They may ask innocuous questions, or sound threatening, or sometimes seem too good to be true.
- ☑ Don't give out personal information – account numbers, Social Security numbers or passwords – or answer security questions.
- ☑ Use extreme caution if you are being pressured for immediate payment.
- ☑ Ask your phone company about call blocking tools for landlines or apps for mobile devices.
- ☑ Report spoofing scams to law enforcement, the FCC and the FTC.

FCC Learn more at fcc.gov/spoofing

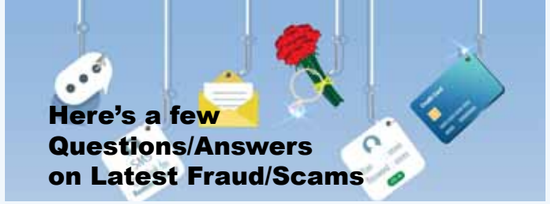


HANG UP!

Don't fall for this scam, no one in your family is going to call you like this. Verify that your family is okay.

DON'T OPEN EMAIL!

Don't fall for this scam, someone pretending to be an email from your family/friend with photos. Contact your family and let them know they been hacked into!



Here's a few Questions/Answers on Latest Fraud/Scams

Q: *What is the federal website for scams?*
A: The power of ReportFraud.ftc.gov
Your report is shared with more than 2,800 law enforcers. We can't resolve your individual report, but we use reports to investigate and bring cases against fraud, scams, and bad business practices.

Q: *What are the latest phone scams?*
A: The 12 Latest Scams You Need To Know
- The "pig butchering" scam.
- Damaged used cars sales.
- Work-from-home scams.
- Student loan forgiveness scams.
- Google Voice verification code scams.
- Amazon imposter scams.
- Zelle, Venmo, and Cash App Scams.
- Robocalls attempting to steal 2FA codes.

Common types of scam apps used by fraudsters include:
- Phishing apps: Mimics legitimate services to trick users into providing highly sensitive information, like passwords and credit card numbers.
- Fleeceware: Offers free trials and charges exorbitant subscription fees once the trial period ends.

Q: *How do you find out if you are talking to a scammer?*
A: If you think you're dealing with a scammer, stop communicating with them immediately. Go to Google and do a reverse image search of their profile picture. If it's associated with other names or comes up on a stock image site, it's a scam.

Q: *What are three excuses a scammer uses?*
A: They come up with various reasons, such as emergencies, medical expenses, or travel costs. Never send money to someone you've only met online.

Q: *What numbers should you avoid answering?*
A: Things You Should Know
Ignore calls from 3-digit international area codes that are likely to be scams, including 232, 268, 284, 473, 664, 649, 767, 809, 829, 849, and 876. Be wary of calls from unknown numbers with your own area code. These may be international caller ID spoof scams that appear local.

Q: *Do banks refund scammed money?*
A: While banks are generally obligated to refund money lost to fraud, they may deny the refund if you were negligent or involved in the scam.
Below are common warning signs of a phone scam:
1. A claim that you have been specially selected.
2. Use of high-pressure sales tactics and "limited-time" offers.
3. Reluctance to answer questions about the business or the offer.
4. Request that you "confirm your personal information"

Q: *What is Cash App method scamming?*
A: Cash App explains, Scammers might send you a payment 'by accident' and ask for you to send the payment amount back to them. The amount you send them back is from your account funds. These scammers will dispute the payment with their bank or credit card after you've sent the funds back.

Q: *What is the app that identifies scammer numbers?*
A: Stop scammers in their tracks with Truecaller, a handy app that helps detect which calls are from a legitimate source, and which should get a one-way ticket to the "end call" button.

Q: *What are the red flags of a scammer?*
A: Unsolicited offers: Don't respond to unsolicited cold calls, emails, junk mail, late-night commercials or infomercials, or social media posts that are either overly attractive or fear-inducing. These are all common tactics scammers use to entice you to engage.

Q: *What happens if you call back a spam number?*
A: You're playing directly into the scammer's hands. You could expose sensitive data on the call or make yourself a target for further scam attempts.

Q: *Is it best to block a scammer?*
A: Scammers don't care if you're on the National Do Not Call Registry. That's why your best defense against unwanted calls is call blocking and call labeling.

Q: *What information does a scammer need to access my bank account?*
A: The easiest way to become a victim of a bank scam is to share your banking info — e.g., account numbers, PIN codes, social security number — with someone you don't know well and trust. If someone asks for sensitive banking details, proceed with caution.

Q: *Can a scammer get into your bank account with your phone number?*
A: If scammers have access to your phone number, they could potentially use it to hack into your online accounts — including your email, social media, and even your bank account.

Q: Can police track a scammer?
A: While agencies can't always track down perpetrators of crimes against scammers, they can utilize the information gathered to record patterns of abuse which may lead to action being taken against a company or industry.

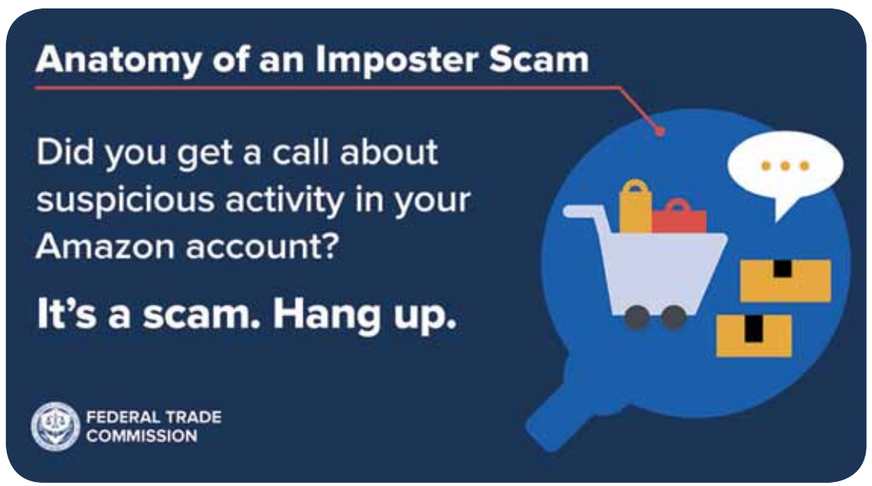
Q: *What are the symptoms of your phone being hacked?*
A: Here are the main signs of a hacked phone:
• It's running slower than usual • Your phone feels hot. • The battery is draining faster than usual. • You notice service disruptions. • Strange pop-ups appear. • Websites look different. • New apps appear. • Apps stop working properly.

Q: *Can someone tell if you are using your phone?*
A: There is a way someone can monitor your mobile phone without ever touching the actual device. **Spyware** (a portmanteau of 'spying software) and stalkerware can be installed on a phone without the owner's knowledge, allowing an attacker to steal information, track activity, and more.

Q: *What not to do if a scammer calls you?*
A: Hang up right away. If you think scammers are targeting you, hang up before they can record your voice or get any information.

FRAUD!ORG
a project of the National Consumers League

Report scams to the National Fraud Information Center/ Internet Fraud Watch at fraud.org. Sign up for email scam alerts and read more scam articles.



Data breaches are unfortunately a new way of life.

If you have ever used a credit or debit card in the United States, chances are pretty good you've been involved in a data breach. In recent years, hackers have compromised data gathered and stored by major retailers including Target, Home Depot, T-mobile, Neiman Marcus, and hundreds more — as well as government agencies and other major institutions. When a data breach occurs, hackers gain access to personally identifiable information that can be sold to criminals and used to commit identity fraud. Consumers whose data is exposed typically become aware of the breach via a letter or other communication from the organization that was breached. Many breached organizations offer free credit monitoring service, advise consumers to check their credit reports and keep an eye out for suspicious activity on their bank and credit card accounts.

(by Fraud.org)

Become a smarter consumer and avoid fraud:

• **Know who you're dealing with.** In any transaction you conduct, make sure to check with your state or local consumer protection agency and the Better Business Bureau (BBB) to see if the seller, charity, company, or organization is credible. Always call the number found on a website's contact information to make sure the number legitimately belongs to the entity you are dealing with.

• **Pay the safest way.** Credit cards are the safest way to pay for online purchases because you can dispute the charges if you never get the goods or services or if the offer was misrepresented. Federal law limits your liability to $50 if someone makes unauthorized charges to your account, and most credit card issuers will remove them completely if you report the problem promptly.

• **Guard your personal information.** Crooks pretending to be from companies you do business with may call or send an email, claiming they need to verify your personal information. Don't provide your credit card or bank account number unless you are actually paying for something and know who you are sending payment to. Your social security number should not be necessary unless you are applying for credit. Be especially suspicious if someone claiming to be from a company with whom you have an account asks for information that the business already has.

• **Stay safe online.** Don't send sensitive information such as credit card numbers by email because it's not secure. Look for clues about security on Web sites. At the point where you are asked to provide your financial or other sensitive information, the letters at the beginning of the address bar at the top of the screen should change from "http" to "https" or "shttp." Your browser may also show that the information is being encrypted, or scrambled, so no one who might intercept it can read it. But while your information may be safe in transmission, that's no guarantee that the company will store it securely. See what Web sites say about how your information is safeguarded in storage.

• **Be cautious about unsolicited emails.** They are often fraudulent. If you are familiar with the company or charity that sent you the email and you don't want to receive further messages, send a reply asking to be removed from the email list. However, responding to unknown senders may simply verify that yours is a working email address and result in even more unwanted messages from strangers. The best approach may simply be to delete the email.

• **Resist pressure.** Legitimate companies and charities will be happy to give you time to make a decision. It's probably a scam if they demand that you act immediately or won't take "No" for an answer. Some scammers may also demand you pay off a loan immediately or damaging consequences may occur, always take time to look into who is requesting the money before you pay up.

• **Don't believe promises of easy money.** If someone claims that you can earn money with little or no work, get a loan or credit card even if you have bad credit, or make money on an investment with little or no risk, it's probably a scam. Oftentimes, offers that seem too good to be true, actually are too good to be true.

• **Fully understand the offer.** A legitimate seller will give you all the details about the products or services, the total price, the delivery time, the refund and cancellation policies, and the terms of any warranty. Contact the seller if any of these details are missing, if they are unable to provide the details, it may be a sign that it's a scam.

• **Get off credit marketing lists.** Credit bureaus compile marketing lists for pre-approved offers of credit. These mailings are a goldmine for identity thieves, who may steal them and apply for credit in your name. Get off these mailing lists by calling 888-567-8688 (your social security number will be required to verify your identity). Removing yourself from these lists does not hurt your chances of applying for or getting credit.

• **Check your credit reports regularly.** If you find accounts that don't belong to you or other incorrect information, follow the instructions for disputing those items. You can ask for free copies of your credit reports in certain situations. If you were denied credit because of information in a credit report, you can ask the credit bureau that the report came from for a free copy of your file. And if you are the victim of identity theft, you can ask all three of the major credit bureaus for free copies of your reports. Contact the credit bureaus at: Equifax, 800-685-111; Experian, 800-311-4769; TransUnion, 800-888-4213.

• **Everyone can request free copies of their credit reports once a year.** In addition to the rights described above, a new federal law entitles all consumers to ask each of the three major credit bureaus for free copies of their reports once in every 12-month period. Go to www.ftc.gov/credit or call 877-382-4357 for more details and to see when you can make your requests. You don't have to ask all three credit bureaus for your reports at the same time; you can stagger your requests if you prefer. Do not contact the credit bureaus directly for these free annual reports. They are only available by calling 877-322-8228 or going to www.annualcreditreport.com. You can make your requests by phone or online, or download a form to mail your requests.

• **Be cautious about offers for credit monitoring services.** Why pay extra for them when you can get your credit reports for free or very cheap? Read the description of the services carefully. Unless you're a victim of serious and ongoing identity theft, buying a service that alerts you to certain activities in your credit files probably isn't worthwhile, especially if it costs hundreds of dollars a year. You can purchase copies of your credit reports anytime for about $9 through the bureaus' Web sites or by phone: Equifax, 800-685-111; Experian, 800-311-4769; TransUnion, 800-888-4213.