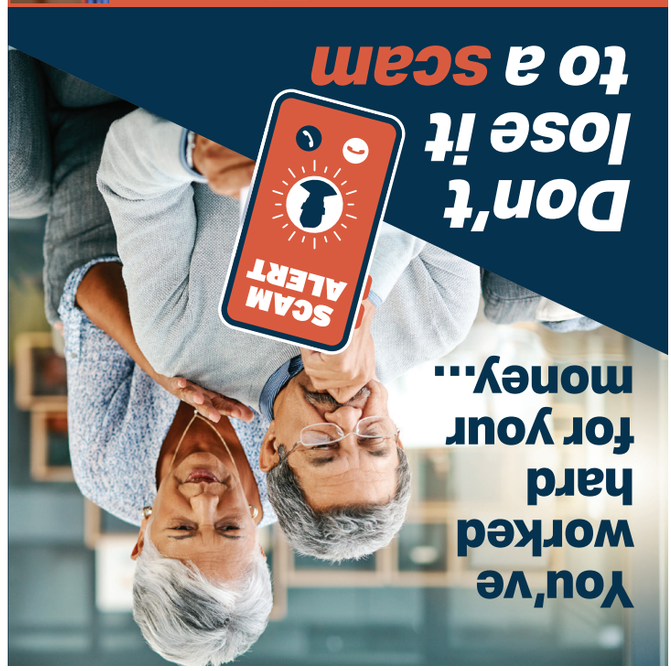
Reporting Fraud

If you were scammed or think you saw a scam, tell the FTC at **ReportFraud.ftc.gov** and report it to your local police and the Federal Bureau of Investigation's Internet Crime Complaint Center at **IC3.gov.**

Assemblyman BRIAN MILLER

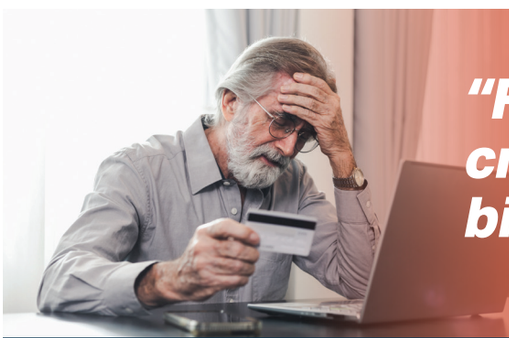
I'm always happy to hear what you think about how I can best serve you in the state Assembly. If you have any comments, questions, or concerns on this or any state issue, please don't hesitate to visit my office or call.
48 Genesee St., New Hartford, NY 13413 • 315-736-3879

A special message from Assemblyman BRIAN MILLER



New York State Assembly
Albany, NY 12248

PRSRT STD.
US Postage
PAID
Albany, NY
Permit No. 75



"FBI warns of rising elder fraud crime rates as scammers steal billions in savings each year[1]"

In the last year...

147,127
Victims over 60[1]

$4.88 Billion
total losses[1]

$83,000
Average dollar loss per victim[1]

46% Increase
from previous year[1]

1. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

How To Protect Yourself Against Common and Emerging Consumer Scams

With technology rapidly changing and expanding, cybercrime experts warn of new covert and alarmingly effective methods criminals are using to target you.

AI-Powered Scams - New technology has made impostor scams even harder to detect. **Voice-mimicking software** (technology that is generated from artificial intelligence, or AI) is used by scammers to clone the voice of someone you know. This is a version of the "grandparent scam" where grandparents are targeted by criminals pretending to be grandchildren in crisis. Voice-cloning tech needs to capture only seconds of audio taken from videos posted online to produce a convincing impersonation.

The latest AI tech can also generate fraudulent videos called **deepfakes,** which impersonate people you know or trust, giving more believability to criminals' deception. **Spoofing numbers** to make it look like you're getting a call, email, text, or social media message from someone you know is also on the rise thanks to the easily available tech.

How to protect yourself against sophisticated AI scams:

- **Never click on a link in an email or text message without confirming it's from a verified source. Scammers have the ability to send messages and fake websites that convincingly mimic real ones.**
- Pick a safe word for your family. If you get a suspicious call from a family member, you can ask for the safe word and if the caller doesn't know it, you can be sure it's a scam.
- Remember, criminals try to scare you into making illogical decisions; if a family member calls in crisis and says their phone is broken so you can't call them back, tell them you want to try to call them back anyway.
- Don't rely on caller ID. When receiving a call from a business, hang up and find their number to call them directly.

Tech Support Scams - Criminals continue to come up with new tactics in tech support scamming, making it one of the most often reported categories of fraud against seniors this year. Many of the devices we use today, such as cell phones and tablets, are technically computers and can be targeted in the same way as a traditional desktop or laptop. In this scam, a pop-up screen will appear on your computer announcing it has been infected with a virus and prompting you to call the provided phone number for help. The "tech support staffer" is actually part of a fraud ring and will use the information you provide to get into your bank account.

How to protect yourself from tech support scams:

- If you can't close a browser window to get rid of a fake virus-warning pop-up, try to reboot your computer. When in doubt, shut it down.
- **Don't ever call the phone number in a pop-up. According to the FTC, legitimate tech companies will never ask you to call a phone number or click a link.**
- Ignore unsolicited calls, emails, or texts telling you there's a problem with your computer. Again, legitimate tech support workers will never contact you unexpectedly.
- Don't trust unknown, unverified people who request remote access to your computer or device.
- Try to stay calm and resist pressure. Scammers pressure their targets to act quickly under the threat of malicious activity on their computers. This is a tactic used to prevent you from having time to think clearly and question the situation.

QR code scam -
QR codes are widely used for various purposes like viewing restaurant menus, paying for parking, accessing events, and boarding flights. However, scammers also use them to steal personal information. Here's what you need to know to stay safe:

Risks

- Spoofed Sites: Scanning a scammer's QR code might take you to a fake site that looks real. If you log in, they can steal your information.

Malware: The QR code could install malware that steals your information.

Scammers' Tactics

- Parking Meters: Scammers cover QR codes on meters with their own codes.
- Text/Email Scams: They send QR codes with fake reasons for you to scan them, such as:
  - Claiming they couldn't deliver a package.
  - Pretending there's a problem with your account.
  - Falsely reporting suspicious activity and urging a password change.

Protection Tips

- Inspect URLs: Before opening a QR code link, check the URL for misspellings or switched letters to ensure it's legitimate.
- Avoid Unsolicited QR Codes: Don't scan QR codes from unexpected emails or texts, especially if they urge immediate action. Contact the company directly using known phone numbers or websites.
- Secure Your Phone and Accounts: Keep your phone's OS updated and use strong passwords and multi-factor authentication to protect your accounts. Scammers hide harmful links in QR codes to steal your information | Consumer Advice (ftc.gov)