TIP FROM SARATOGA COUNTY SHERIFF MICHAEL H. ZURLO:

MEDICARE SCAMS

Someone may contact you claiming to be a Medicare representative who can help you save money by getting some form of additional coverage. The caller might ask for personal information or checking account numbers and even have some information about you. If you get a Medicare-related call, email or text, **ignore it**. If you have questions about your health coverage, **contact Medicare directly**.

You've worked hard for your money...

DON'T LOSE IT TO A SCAM

A SPECIAL MESSAGE FROM

ASSEMBLYWOMAN *Mary Beth* **WALSH**

New York State Assembly
Albany, NY 12248

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

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**.

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.

CRYPTOCURRENCY-ROMANCE SCAMS

- Anti-fraud experts have tracked this as one of the top emerging scams in 2023. This scheme combines cryptocurrency scams with the age-old romance scam, where the scammer poses as an internet love interest to persuade the target into investing money in fake crypto accounts. The fake website or app will display data that shows your wealth growing, meanwhile, the criminals are taking your money.

How to avoid the crypto-romance scam:

- Don't think it can't happen to you. According to the FTC, crypto fraud has skyrocketed with annual losses increasing more than 20 times in the last three years.
- Scammers follow trends and headlines, and with cryptocurrency in the news, it's important to carefully scrutinize any investment opportunity and keep your guard up.

For more information on this or any other state issues, please contact Assemblywoman Mary Beth Walsh at:
199 Milton Avenue, Suite 2, Ballston Spa, NY 12020 518-884-8010 · walshm@nyassembly.gov