

Office of the New York State Attorney General



Letitia James

New York State Attorney General

Smart Seniors

Smart Seniors

Stay Safe. Take Control. Fight Back.



NYC Parking Ticket Scam

- A new scam in the Hudson Valley. Scammers send deceptive text messages falsely claiming Victims have unpaid parking tickets in New York City that require immediate payment.
 - **Verify:** Check the official NYC parking ticket website or contact the city's parking authorities to verify claims of unpaid tickets.
 - **Be Cautious:** Legitimate institutions do not request **immediate** payments via text messages.
 - **Protect Your Information:** Never share personal or financial information in response to unsolicited messages.
 - Don't wire money, get cash out of a bank, or send a check or money order by overnight delivery or courier.



Leading Scams:

- **Imposter scams.** (\$2.7 billion)
- **Investment scams.** (\$7.7k median)
- **Social media scams.** (\$1.4 billion)
- **Payment methods.** (\$1.86 billion)





TARGET: *Seniors*

- **May be homeowners**
- **Often generous**
- **Often live alone**
- **May have a “nest egg”**
- **Look for affordable solutions**





Fraud and Abuse Against the Elderly

\$3,000,000,000

Americans over 60 are increasingly becoming victims of fraud perpetrated online and over the phone at rates that add up to billions in losses each year



Anatomy of a Scam

1. The Distracting “Hook”

- **Money or Greed**
- **Fear and Desperation**
- **Love, Trust, and Goodwill**

2. A Con Artist Who Seems Trustworthy

3. A Deadline



Financial Fraud & Abuse

7 Top Scams to Watch Out for in 2024:

- 1. Delayed-action sweepstakes scam**
- 2. Check cooking/washing scam**
- 3. The Grandparent Scam**
- 4. Multistage grandparent scam**
- 5. Voiceprint Scams**
- 6. Paris Olympics scams**
- 7. Virtual celebrity scam**



Financial Fraud and Abuse: Prizes and Sweepstakes



- “You’ve won the Canadian Lottery! Here is your first check!”
- “We’re from the National Sweepstakes Bureau.”
- “You might be the next Winner!”

Financial Fraud and Abuse: Prizes and Sweepstakes



- Never Pay to Collect a Prize
- Don't Rely on Caller ID
- Don't buy products you don't want or need.
- Be a Friend

Financial Fraud and Abuse: **Fake Check Scams**



THIS DOCUMENT HAS AN OFFICIAL WATERMARK PRINTED ON THE BACK. THE FRONT OF THE DOCUMENT HAS A MICRO-PRINT. ABSENCE OF THESE FEATURES WILL INDICATE A COPY.

usbank
Five Star Service Guaranteed

FAKE!!!! CHECK

No. 52239085

935-41
920

PAY Eleven Thousand Five Hundred Dollars

DATE:
3/21/12

\$ 11,500.00

TO THE ORDER OF: **Lynn Stewart**

PURPOSE/REMITTER: **MARK VINCIG**

Location: 4937

Issued By: MoneyGram Payment Systems, Inc. P.O. Box 9476, Minneapolis, MN 55480

Andy Johnson
AUTHORIZED SIGNATURE

⑈052239085⑈ ⑆092005411⑆ ⑆0160010698282⑈

Never agree to deposit a check and wire money back to someone you don't know.

Financial Fraud and Abuse: Grandparent Scam

“Grandpa, it’s me.
I need help!”

“... But please don’t tell
Mom or Dad.”



PARIS OLYMPICS SCAMS



- Variation of the “emergency scam”
- Beware of fake tickets



SUMMER TRAVEL SCAMS

- What it can look like:
 - Travel booking site that offers vacation deals **far below market value**
 - Your using a rental app, and the hosts asks you to pay upfront though a means that is **off platform**



SUMMER TRAVEL SCAMS

- **What You Should Do:**
 - **Be skeptical** of steep discounts on travel and accommodations.
 - **Vet travel reservation sites** before you book. Conduct a web search on the company name (along with the word “scam” or “complaint” or “review”) to read about other people’s experiences.
 - When renting a car online, **type in the web address** rather than using a search engine. This will reduce the chance of accidentally landing on a look-alike site.
 - Pay for travel reservations and bookings with a **credit card**, which offers greater protection than other forms of payment.
 - When using a vacation rental app, **be suspicious** if the host wants you to pay off-platform. For example, Airbnb only allows this for certain fees (such as local taxes), and VRBO states that payments outside its checkout form are not eligible for its “Book with Confidence” guarantee.

Financial Fraud and Abuse:

Telephone Safety



- Telemarketers are regulated
- Caller ID (name and number) can be manipulated
- Don't give out personal information
- Don't give out security information
- Don't commit on the phone

Financial Fraud and Abuse

Take Control



National Do Not Call Registry

888-382-1222 or

www.donotcall.gov

Opt Out of credit cards and insurance offers

888-567-8688 or

www.optoutprescreen.com

Direct mail

www.dmachoice.org

Common scams:

Romance



- Seniors collectively lost over a billion dollars in these scams in 2023.
- For example, a recently widowed senior repeatedly sent tens of thousands of dollars to someone she had fallen in love with to pay for their nonexistent medical procedure.
- Familiar fact pattern: the scammer cultivates a relationship over time before asking to “borrow” \$\$\$, while avoiding and rescheduling any in person meetings.

Time Share Fraud



- Cartel employees posing as sales representatives call up timeshare owners, offering to buy their investments back for generous sums. They then demand upfront fees for anything from listing advertisements to paying government fines.
- The representatives persuade their victims to wire large amounts of money to Mexico — sometimes as much as hundreds of thousands of dollars — and then they disappear.

Financial Fraud and Abuse Home Improvement Contractors

Recommendations and References

- License?
- Get It In Writing
- Permits and Insurance
- Don't pay the full amount up front!



WATCH OUT!



Unfortunately, bad actors can now use artificial intelligence technology, commonly known as AI, and a short audio or video clip to "clone" a loved one's voice.

Internet Safety



Smart Seniors

1. Don't click on links in emails **or text messages** from unfamiliar senders. Be wary of any strange or unexpected messages, even if it's from someone you know.



2. Don't open any attachments unless you know the sender and were expecting them to send it.



3. Ignore unsolicited phone calls and “robocalls.”



4. Don't respond to or click on pop-up windows on your phone or computer.



5. Don't conduct any transaction involving personal information while using a public (or unsecured) network.



Internet Safety

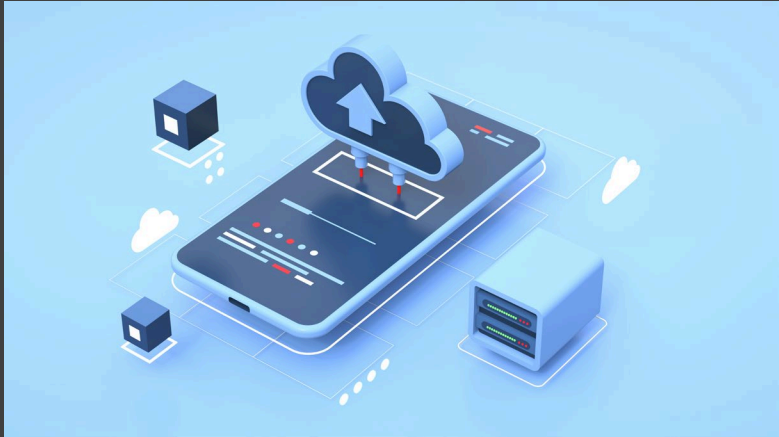
Use Strong Passwords



- Wireless Internet
- Each Computer,
Each Account
- Email



Internet Safety Social Media





Internet Safety Security Measures

Internet
Safety
Gone
Phishing



- *Social Security Number*
- *Credit Cards*
- *Identity*
- *Bank Accounts*
- *Email Addresses*
- *Passwords, Pins, or Codes*





Gift Cards ---> *Cryptocurrency*

Did someone
send you to a
Bitcoin ATM?
-- It's a scam





Identity Theft

- Safeguard
- Review
- Destroy

Internet Safety **Identity Theft**



Free Credit Reports

www.annualcreditreport.com

1-877-322-8228

If Someone You Care About Paid A Scammer, Here's How To Help

- **Lead with empathy.** Respond with kindness and concern instead of criticizing or expressing disappointment. Scams can happen to anyone.
- **Let them tell their story.** Talking about the scam helps both of you spot it in the future.
- **Validate their story.** Ask them not to blame themselves and, instead, blame the scammer.
- **Ask what we can do next together.** See if there was a potential for identity theft and if they might want to report the scam.



Charitable Giving



Tips for Charitable Giving



Know the Charity

Know the Program

Know that is Registered

www.charitiesnys.com

Tips for Charitable Giving

Be Careful How You Give

- Telemarketer
- Unsolicited Email
- Social Media
- Fake Invoices
- No cash



Latest News You Can Use:

The following are the top **10 most common** types of consumer complaints received by OAG:



1. Retail Sales
2. Landlord/Tenant
3. Automobile
4. Credit, Banking, and Mortgages
5. Consumer Services
6. Internet
7. Utilities
8. Home Repair/Improvement
9. Travel
10. Entertainment