Types of phone and email scams

Smishing: Con artists send text messages that ask you to verify personal information like Social Security and credit card numbers. Contact your bank or credit card company directly and don't respond to the text.

Tax return: Scammers impersonate tax return websites to get information such as your name and Social Security number in order to file fraudulent tax returns.

Robocalls for medical devices: Hang up on prerecorded messages when asked to press 1 for a free device or to press 5 to opt out of future calls. Pressing it alerts scammers that they have a working number to keep calling.

Grandparent scam: Scammers obtain personal information through social networking sites and internet searches. These scams involve either a grandchild asking to have money wired in an emergency situation (or a person who says they are acting on behalf of a relative). In these instances, confirm the caller's identity and don't act rashly.

Online dating: Beware of scammers who send small gifts to express affection building up to their eventual request for a large sum of money, usually in the form of a wire transfer. Very often these scammers are not even in the U.S.

Jury duty: You receive a phone call for failure to report for jury duty and the caller tries to scam you into paying a fine by credit card or to provide your Social Security number.

IRS impostors: These scammers try to get you to use prepaid debit cards or wire transfers to pay debts owed to the IRS. The IRS does not request information through email nor will they ask for credit card numbers over the phone.

Visa applicant scams: Persons posing as immigration officials call and demand your personal information such as your passport number or claim that there's a new fee for visas. Resist high-pressure tactics and call U.S. Citizenship and Immigration Services at 800-375-5283 to determine whether the call was legitimate.

Fake debt collectors: Consumers receive phone calls and voicemails from scammers threatening legal action to collect money that isn't actually owed. Don't provide any information. Check to find out if the agency is real by asking for the caller's name, company address and telephone number. Then hang up and verify that information. You can also check your credit report for free at www.annualcreditreport.com.

For more information

NYS Attorney General Consumer Helpline
800-771-7755
www.ag.ny.gov

Federal Trade Commission
Consumer Response Center
877-FTC-HELP (877-382-4357)
www.ftc.gov

NYS Department of State, Division of Consumer Protection Helpline
800-697-1220
www.dos.ny.gov/consumer-protection

Do Not Call Registry
Free to register by calling
toll-free: 888-382-1222
TTY: 866-290-4236
www.donotcall.gov

Please contact my office if you have questions or concerns about this or any other matter.

Speaker of the Assembly
Carl E. Heastie

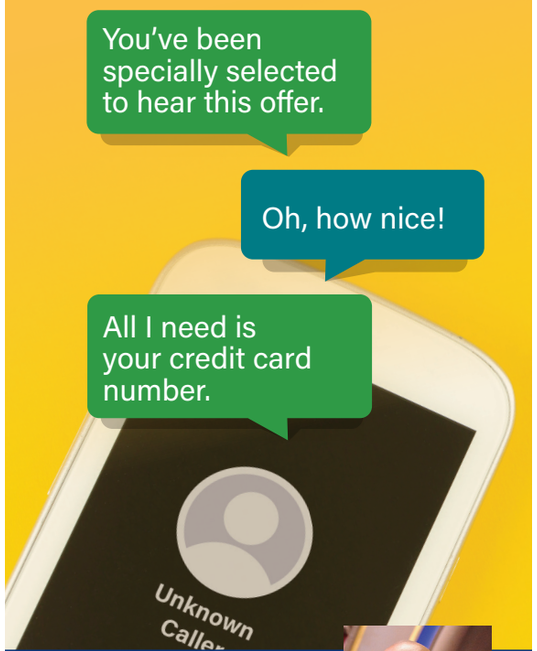
District Office
250 Broadway, Suite 2301
New York, NY 10007
212-312-1400

Albany Office
Room 932, LOB
Albany, NY 12248
518-455-3791

speaker@nyassembly.gov

Updated 2/22

BEWARE OF PHONE AND EMAIL SCAMS



Important information from
Speaker of the Assembly
Carl E. Heastie

What you should know about telemarketing scams

While most telemarketing pitches are made on behalf of legitimate companies offering products and services, many sales calls are fraudulent. According to the Federal Trade Commission, consumers lose billions annually to telemarketing fraud.

These scams range from fraudulent charity appeals and bogus vacation and prize awards, to small cash "deposits" and shady investment lures.

Committing telemarketing fraud is easy for unscrupulous promoters, since they have access to telephone directories, mailing lists and "sucker lists," which include consumers who have been scammed before.

For example, cybercriminals often know some personal information about you and may gain your trust by guessing which computer operating system you have. Once they have your trust, they may ask for your username and password or ask you to install software so they can fix a problem. Do not trust unsolicited phone calls and never install or purchase software or services in this way.

How you can find out if the call is legitimate

To verify the legitimacy of the promoter, contact your local Better Business Bureau, the state attorney general's office, the New York State Department of State's Division of Consumer Protection or your local consumer protection agency.

The telemarketing sales rules

- Telemarketers may only call between 8 a.m. and 9 p.m.
- They must tell you that they are selling something and who they represent before they make their pitch.
- It's illegal for a telemarketer to call you back after you've told them not to call.
- Before you pay for any products or services, you must be told of their total cost and restrictions.
- It's illegal for telemarketers to block their identification on your caller identification service.
- Telemarketers cannot call consumers on the Do Not Call Registry to schedule an appointment for a face-to-face sales presentation.

Do Not Call Registry stops unwanted sales calls

Consumers can stop most unsolicited sales calls by putting their home and cellphone numbers on the free National Do Not Call Registry. Companies that illegally call numbers on the National Do Not Call Registry can currently be fined up to $43,792 per call.

If you were already listed on the New York State Do Not Call Registry, you were automatically registered on the National Do Not Call Registry when it was established in 2003.

To register your phone number on the National Do Not Call Registry, verify a previous registration or report an unwanted call, visit www.donotcall.gov.

What you can do to avoid being scammed

- Never send money or give out personal information like your credit card or checking account numbers to anyone through text or email.
- Ask the telemarketer to send additional written information about the company, its products and services to you. Take the time to thoroughly investigate the company before responding to any unsolicited offer.
- Proceed with caution if the caller uses high-pressure language, such as "act now," "send your money today" or "we need your credit card or bank account number right away."
- Don't answer calls from unidentified phone numbers. If it's legitimate, the caller will leave a voicemail. Don't call back one-ring calls.
- The government will never call you and ask you for money. Never.
- No government office or legitimate business will ever ask you to pay them using a prepaid card or money transfer.
- Report suspected scams to law enforcement.
- Report questionable telemarketing companies to the Better Business Bureau and send a detailed complaint to the Federal Trade Commission.
- If you are not interested in the offer, interrupt the caller and say you are not interested. Ask the caller to take your name off his or her list if you don't want to be called again.
- Don't be intimidated by the caller, and don't be afraid to hang up the telephone.
- Don't click on email and text links or open attachments if the source of the text or email is unknown.

Anyone...

can be a victim of phone fraud. Con artists don't care about your age, the color of your skin or your religion. However, older people and non-native English speakers are frequently targeted.