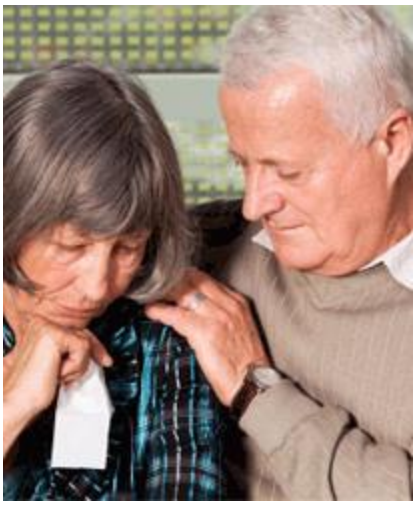
This booklet is provided by the Town of Ramapo and the Town of Ramapo Police Department. Provided within this booklet are the top scams identified by the Better Business Bureau, Western Union, The New York State Attorney General's Office and the FBI. We have also provided numerous resources that can help you combat these scams and identity theft. If you believe you are a victim of a scam, do not hesitate to call your local Police Department.

*INFORMATION AND PHOTOS OBTAINED FROM BETTER BUSINESS BUREAU, WESTERN UNION, NEW YORK STATE ATTORNEY GENERAL'S OFFICE AND FBI

TOP SCAMS AND RESOURCES TO PROTECT YOURSELF

TOWN OF RAMAPO
237 Route 59
Suffern, New York 10901
(845) 357-5100 Fax: (845) 357-3877

Emergency Scams

 Scammers make up an urgent situation—I've been arrested, I've been mugged, I'm in the hospital—and target friends and family with pleas for help, and money.

The Grandparent Scam is one version of the emergency scam: A young person poses as a grandchild with an emergency and appeals to family members to help them immediately. Don't believe everything you hear, and be sure to verify the emergency situation before you give them any contact information, and especially before you send any money.

Another variation is the relationship scam. You meet a great person online, everything seems to be going great but you aren't able to meet yet for any variety of reasons (distance, military deployment, work travel, etc.). Suddenly your online love interest has an emergency and needs you to wire money, and as soon as you do, he or she will continue to find more reasons to ask for money from you. Remember, you should never wire money to someone that you don't personally know or trust or haven't met in person.

Sweepstakes & Lottery Scams

Lottery or prize scams follow two similar patterns:

1. Victims get an unsolicited phone call, email, letter or fax from someone claiming to work for a government agency or representing a well-known organization or celebrity, notifying them that they've won a lot of money or a prize. The scammer gains their trust and explains that, in order to collect the winnings, they first have to send a small sum of money to pay for processing fees or taxes. Following these instructions, victims immediately wire the money, but never get their "winnings." And they're out the money they paid for "fees and taxes."

2. Victims get an unsolicited check or money order and directions to deposit the money, and immediately wire a portion of it back to cover processing fees or taxes. Soon after this, victims learn that the checks are counterfeit, but have already wired the money to cover the "taxes" and can't get it back. And they're on the hook to pay their banks back for any money they withdrew.

Identity Theft Scams

There are a million ways to steal someone's identity and once thieves have your personal information, they can max out your credit cards, drain your bank account, and ruin your credit rating.

Identity theft scams come in all shapes and sizes—friends or grandchildren "stranded" in a foreign country, the hotel front desk "verifying" your credit card in the middle of the night, "charity" solicitations from groups you've never supported in the past.

Never, ever give your Social Security/Social Insurance, bank account or credit card numbers to someone who has contacted you to ask for them.

Phishing Scams

"Phishing" is when you receive an email telling you that you've won a contest or that a company needs to verify personal information. Links in the email can take you to a site that downloads a virus on your computer to hunt for your sensitive data. Virus protection software on your computer can help, but the best protection is a good sense of judgment.

Legitimate companies and government agencies are not going to ask you to confirm your personal information in this way. Be wary of links in social media, too. Some apps, humorous websites, contests or links to shocking videos are just distractions to get you to click on something that downloads malware onto your computer.

Home Improvement Scams

Look out for home improvement contractors who leave your home worse than they found it. They usually knock on your door with a story or a deal—the roofer who can spot some missing shingles on your roof, the paver with some leftover asphalt who can give you a great deal on driveway resealing. Itinerant contractors move around, keeping a step ahead of the law... and angry consumers.

Many BBB Accredited Businesses are home contractors who want to make sure you know they are legitimate, trustworthy and dependable. Find one at the Better Business Bureau search page.

Advance Fee/Prepayment Scams

 In challenging economic times, many people are looking for help getting out of debt or hanging on to their home. Scammers pose as representatives from phony loan companies and use authentic-looking documents, emails and websites to fool consumers into parting with their money. Some sound like a government agency, or even part of BBB or other nonprofit consumer organizations. Most ask for an upfront fee to help you deal with your mortgage company, creditors or the government (services you could do yourself for free), but leave you in more debt than when you started.

They all have a common theme: Victims pay a smaller amount of money in anticipation of something of greater value, but then you receive nothing in return. You should not send a wire transfer to receive a loan or a credit card.

Here are some tips from Western Union to help you avoid advance fee scams:

Be skeptical of any offer where you have to pay money up front. Walk away if you're asked for money immediately, especially if it's for "insurance," "processing," or "paperwork."

- Never send money from a deposited check until it officially clears. Just because funds are available doesn't mean a check has cleared—by law, banks must make deposited funds available within a few days, but it can take weeks to uncover a fake check.

- If you're communicating with anyone by email, check for common red flags like poor grammar, misspellings, character/spacing mistakes, and excessive capitalization. Look for use of generic email addresses rather than specific business email addresses.

Do your research.

- Be wary of businesses that operate using a post office box and don't have a street address.

- Check out the company that contacted you with local law enforcement or a consumer protection agency like the Better Business Bureau, the Federal Trade Commission, your State Attorney General's Office, or other trusted sources.

- Check the company out independently by getting its phone number from a phone book or directory assistance and calling to confirm they are who they say they are.

- If you're checking out a lender or loan broker, they're required to register in the state where they do business so contact your State Attorney General's office or your state's department of banking or finance regulation.

Overpayment and Fake Check Scams

With overpayment scams, fraudsters play the role of buyer and target consumers selling a product or service. It usually works this way: The buyer "accidentally" sends you a check for more than the amount they owe you. They ask you to deposit it into your bank account and then wire them the difference. A deposited check can take several days or more to clear. When the original check turns out to be a fake and bounces, the victim is still on the hook to pay the bank back for any money withdrawn.

Fake checks can be used for any type of scam, so always wait for a deposit to clear before writing checks against the funds.

Western Union has these recommendations:

- Know who you're doing business with; independently confirm your buyer's name, street address, and telephone number.
- Don't accept a check or money order for more than your selling price. If the name on the check doesn't match the name of the person you're dealing with, immediately end the transaction.
- Consider dealing in cash and in-person with local buyers. If this isn't feasible, ask for a check drawn on a local bank so you can visit a local branch or office to determine if the check is legitimate. Or, consider an alternative method of payment like a trusted escrow service or online payment service.
- If a buyer insists that you wire money, don't. Scammers pressure people to use wire transfer services because the money's picked up in cash and impossible to trace afterward.
- Fake checks or money orders play a starring role in overpayment scams, advance fee and prepayment scams, mystery shopping scams, lottery prize scams, and more. Don't use these funds until your bank officially clears them, and remember Banks must make deposited funds available within a few days but it can take weeks to uncover a fake check.
- Resist pressure from a buyer to act immediately. If the buyer's intentions are good, he or she will wait for the check to clear to finish the transaction.
- If you're communicating with anyone by email, check for common red flags like poor grammar, misspellings, character/spacing mistakes, and excessive capitalization.

Sales and Rental Scams

Sales scams are as old as humanity, but the Internet has introduced a whole new way to rip people off. For 100 years, BBB has been advising consumers: If it sounds too good to be true, it probably is.

High-pressure sales tactics, "limited time offers," prices that seem too low—all are tip-offs that something may not be quite right. Be especially wary of products that claim to help you lose weight without trying, settle a debt, make you rich, look younger, etc.

Another variation is rental or vacation properties advertised online; sometimes the property isn't what it looks like in the pictures, and sometimes it doesn't even belong to the person who just collected your deposit or rental fee. The owner says the place is yours if you wire money to cover an application fee, security deposit, etc. Once you wire the money, you never hear from the "owner" again.

Employment Scams

Employment scams generally start with a too-good-to-be-true offer—work from home and earn thousands of dollars a month, no experience needed—and end with the consumer out of a "job" and out of money. Whether it's a secret shopper scheme, work-from-home scam, or a phony offer of employment, job-related scams are the worst because they can dash your hopes and steal your money or your identity.

It's easy for scammers to create email, websites and online "job applications" that look very professional. Be cautious of anyone who wants to interview you only over the phone, who asks you to wire money for supplies or other upfront expenses, or who asks you to fill out an online form that asks for personal data like your Social Security Number or bank account. Be especially cautious of offers that claim you can make big money with no experience necessary. And, never wire money to secure a job offer.

(809) Area Code scam:

1. Someone calls and says sorry I missed your call get back to us as soon as you can.

2. AT&T says DO NOT CALL BACK area codes 809, 284, 784, 264, 473, 268 or 876.

3. 809 is being distributed all over the US. They get you to call by telling you that they have information about a family member who has been ill, arrested or died. Sometimes they say you have won a prize etc. The other area codes have also been linked to these scams and the one ring scam where the phone rings once and hangs up hoping you will call back and get charged at the international rate.

4. If you call you will be charged $2425.00 per minute. They will keep you on the phone as long as possible to increase the charges.

5. If you complain to local and long distance carriers, they will not get involved because they are just providing the billing for the foreign company. 809 area code is located in the Dominican Republic. This charge is legal because it is billed as international rates.

IRS SCAM:

The IRS is warning the public about a phone scam that targets people across the Nation. Callers claiming to be from the IRS tell intended victims that they owe taxes and must pay using a prepaid debit card or wire transfer.

Callers use:

1. Common names and fake badge numbers
2. Know the last 4 digits of your social security number
3. Make caller ID appear as if the IRS is calling
4. Send bogus IRS emails to support the claim
5. Call second time claiming to be the Police or DMV

Truth of the Matter:

1. IRS will contact you by mail not phone about taxes
2. IRS will never ask you to pay using a prepaid debit card or wire transfer
3. IRS will not ask you for a credit card number over the phone.
4. If you think you owe taxes call IRS at 1-800-829-1040
5. If you don't owe taxes report incident to Treasury Council for Tax Administration at 1-800-366-4484
6. You can also file a complaint with the FTC (Federal Trade Commission)

RESOURCES:

Free credit report: www.annualcreditreport.com or 1-877-322-8228

Everyone is entitled to a free copy of their credit report each year. You can get yours by registering at this website or calling this toll free number.

If you see accounts or inquiries that you did not initiate or you don't recognize, it may indicate that someone else is using your identity.

Do Not Call Registry: 1-800-382-1222 or www.donotcall.gov

You can place your telephone number (both landline and cell phone numbers can both be registered) on the Do Not Call Registry. Within 31 days of when you register your number, telemarketers — with certain exceptions — must remove you from their call lists.

Unsolicited credit and insurance offers: 1-888-5-OPT-OUT (1-888-567-8688)

www.optoutprescreen.com

This service is run by the four major consumer credit reporting companies. When registering you will be asked to provide your home phone number, name, date of birth and Social Security number. This information will be kept confidential.

New York State Attorney General's Charities website: www.charitiesnys.com

This website provides information on the fundraising firms that charities use, and how much of the money raised actually goes to the charity.

Medicaid Fraud Control Unit: call the Attorney General's Hotline

1-800-771-7755 or file a complaint online: www.ag.ny.gov/comments-mfcu

Pearl River Regional Office: 845-732-7500

The Medicaid Fraud Control Unit is an important part of the Attorney General's office that targets large-scale frauds involving overbilling, kickbacks, substandard drugs and medical equipment, and "Medicaid mills" run by organized criminals. It also safeguards elderly and disabled New Yorkers from abuse and neglect in nursing homes and other health care facilities.

Better Business Bureau

newyork.bbb.org or **upstateny.bbb.org**

Mid Hudson Office: (914) 333-0550

NYS Department of Financial Services

877-226-5697 or www.dfs.ny.gov

New York State Office for the Aging

2 Empire State Plaza

Albany, New York 12223-1251

Help Line: (800)342-9871

General Assistance: 800-342-9871

U.S. Dept. of Health and Human Services

Administration on Aging

Public Inquiries: (202) 619-0724

Eldercare Locator (to find local resources): 800-677-1116