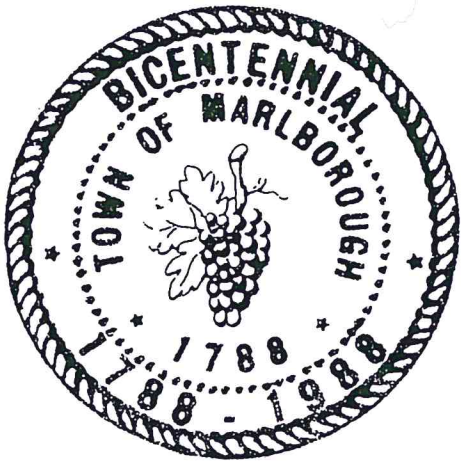
TOP SCAMS AND RESOURCES TO PROTECT YOURSELF



Town of Marlborough

21 Milton Turnpike

P.O. Box 305

Milton, New York 12547

(845) 795-5100 Fax: (845) 795-2031

Chief Gerald T. Cocozza
21 Milton Turnpike
P.O. Box 305
Milton New York 12547
845-795-2181

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

*INFORAMATION AND PHOTOS OBTAINED FROM THE BETTER BUSINESS BUREAU,WESTERN UNION, NEW YORK STATE ATTORNEY GENERAL'S OFFICE, FBI AND THE TOWN OF RAMAPO AND THE TOWN OF RAMAPO POLICE.

Emergency Scams

 Scammers make up an urgent or emergency situation and ask for help. For example—I've been arrested, I've been mugged and I am in the hospital and target friends and family over the telephone with pleas for help and money.

The Grandparent Scam is another version of the emergency scam: A young person poses as a grandchild with an emergency and over the telephone appeals to family members to help them. Don't believe everything you hear, and be sure to verify the emergency situation before you give any contact information or 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 more money from you. Remember, you should **never** wire money to someone that you don't personally know and trust or have not met in person no matter how desperate or sincere they may sound on the telephone or on the computer.

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." See the section on "International Lottery Scams" for more information.

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

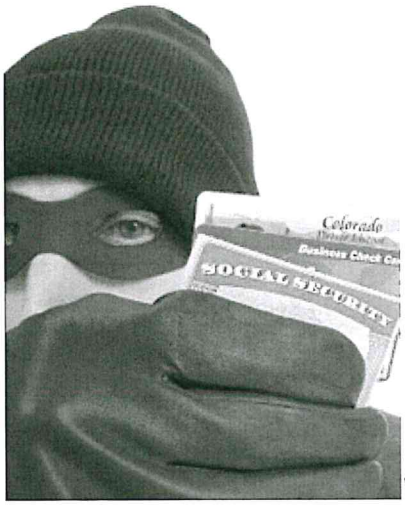
Identity Theft Scams

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, open up credit cards in your name and ruin your credit rating.

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

To protect yourself—**never** ever give your Social Security number /Social Insurance information, bank account or credit card numbers to someone who has contacted you to ask for them.

Phishing Scams



"Phishing" is when you receive an e-mail 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. Up to date virus protection software on your computer can help but the best protection is a good sense of judgment and awareness about the scams used by criminals to take your money.

Legitimate companies and government agencies are not going to ask you to confirm your personal information in this way. Be wary of links on social media sites 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. Do not "click on" or open a link (highlighted text) in an e-mail or webpage if you are not sure what it is.

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. For example—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 resurfacing or resealing. Itinerant contractors move around and keep a step ahead of the law... and angry consumers.

Many Better Business Bureau Accredited Businesses are home contractors who want to make sure you know they are legitimate, trustworthy and dependable. Ask friends and family for a recommendation and always check with the Better Business Bureau and the consumer protection office in your town before hiring a contractor or home improvement company.

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 the Better Business Bureau or other nonprofit consumer organization. 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 and 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 the check officially clears and the funds are on deposit in your bank account. Just because funds are available doesn't mean a check you deposited in your account has cleared. By law, banks must make deposited funds available within a few days but it can take weeks to uncover a fake/fraudulent 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 e-mail addresses rather than specific business e-mail addresses.

Always Do Your Research:

- Be wary of businesses that operate using a post office box, don't have a street address and only communicate with customers by e-mail. Do not underestimate the power of the "Google" search engine. Type in the name, e-mail address, telephone number, etc. in the Google search box on your computer and see what comes up. You may be very surprised at what you find!

- 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, Attorney General's Office, local consumer protection 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 office.

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 deposited check 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 do it and terminate the transaction. Scammers pressure people to use wire transfer services because the money is picked up in cash and impossible to trace afterward. Always think in terms of creating a **"paper trail"** when making a purchase or engaging in a financial transaction. By creating a paper trail—both investigators and yourself can trace the transaction from start to finish.
- 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 the money is actually in your account. Remember, banks must make deposited funds available within a few days but it can take weeks to uncover a fake or fraudulent 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 for criminals to steal your money. For 100 years, the Better Business Bureau has been advising consumers:

IF IT SOUNDS TOO GOOD TO BE TRUE, IT PROBABLY IS.

High-pressure sales tactics, "limited time offers" and prices that seem too low are all 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 professional looking e-mails, websites and online "job applications" that look authentic. 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, bank account number, mother's maiden name and place of birth or other personally identifiable information. 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. AT&T says DO NOT CALL BACK telephone numbers with area codes 809, 284, 784, 264, 473, 268 or 876.

2. Area code 809 is being distributed all over the United States. The caller leaves a message and gets you to call them back 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 or a sum of money. 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.

3. If you call back you will be charged up to **$2,425.00 per minute**. They will keep you on the phone as long as possible to increase the charges.

4. If you complain to your local and long distance carriers they will not get involved because they are just providing the billing for the foreign telephone company. The 809 area code is located in the Dominican Republic. The toll charge is legal because it is billed at international rates.

IRS SCAM:

The IRS is warning the public about a phone scam that targets people across the country. 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.

Some tactics used by the callers are:

1. Use of common names (Mr. Smith or Ms. Jones) and fake badge numbers
2. They sometimes 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 a second time claiming to be the Police or DMV

**Caller ID spoofing* *is the practice of causing the telephone network to indicate to the receiver of a call that the originator of the call is a station other than the true originating station. For example, a Caller ID display might display a phone number different from that of the telephone from which the call was placed. The term is commonly used to describe situations in which the motivation is considered malicious by the caller. Caller ID spoofing is generally illegal in the United States. The relevant federal statute, the Truth in Caller ID Act of 2009, does make exceptions for certain law-enforcement purposes. Callers are also still allowed to preserve their anonymity by choosing to block all outgoing caller ID information on their phone lines.*

Truth of the Matter:

1. IRS will contact you by mail not the telephone about unpaid 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 the IRS directly at 1-800-829-1040
5. If you don't owe taxes report the incident to the U.S. Treasury Council for Tax Administration at 1-800-366-4484
6. You can also file a complaint with the Federal Trade Commission (FTC)

INTERNATIONAL LOTTERY SCAMS

> Congratulations! You may receive a certified check for up to $400,000,000 U.S. CASH!
> One Lump sum! Tax free! Your odds to WIN are 1-6.
> "Hundreds of U.S. citizens win every week using our secret system!
> You can win as much as you want!"

Sound great right? In reality—it's a fraud.

Scam operators often based in Canada and other countries are using the telephone and direct mail to entice U.S. consumers to buy chances in high-stakes foreign lotteries from as far away as Australia, Nigeria, Mexico and Europe. These lottery solicitations violate U.S. law which prohibits the cross-border sale or purchase of lottery tickets by phone or mail.

Still, federal law enforcement authorities are intercepting and destroying millions of foreign lottery mailings sent or delivered by the truckload into the U.S. and consumers, lured by prospects of instant wealth, are responding to the solicitations that do get through at an estimated loss of $120 million a year; according to the U.S. Postal Inspection Service.

The Federal Trade Commission (FTC) the nation's consumer protection agency, says most promotions for foreign lotteries are likely to be phony.

Many scam operators don't even buy the promised lottery tickets. Others buy some tickets, but keep the "winnings" for themselves.

In addition, lottery hustlers use victims' bank account numbers to make unauthorized withdrawals or their credit card numbers to run up additional charges.

The FTC has these words of caution for consumers who are thinking about responding to a foreign lottery:

- If you play a foreign lottery, through the mail or over the telephone, you are violating federal law.
- There are no secret systems for winning foreign lotteries. Your chances of winning more than the cost of your tickets are slim to none.
- If you purchase one foreign lottery ticket, expect many more bogus offers for lottery or investment "opportunities." Your name will be placed on "sucker lists" that fraudulent telemarketers buy and sell.
- Keep your credit card and bank account numbers to yourself. Scam artists often ask for them during an unsolicited sales pitch.

The bottom line, according to the FTC: Ignore all mail and phone solicitations for foreign lottery promotions. If you receive what looks like lottery material from a foreign country, give it to your local postmaster and report it to the FTC.

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.

***YOU CAN MONITOR YOUR CREDIT THROUGHOUT THE YEAR BY PLACING A FRAUD ALERT ON YOUR CREDIT REPORT TO EACH CREDIT REPORTING AGENCY EVERY 120 DAYS. You will receive a free credit report from each agency if requested.**

EXAMPLE: Equifax: 1-800-525-6285 in January

Experian: 1-800-397-3742 in May

TransUnion: 1-800-680-7289 in September

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 your telephone number(s) from their call lists. The Do Not Call Registry is managed by the FTC.

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

Federal Trade Commission

877-FTC-HELP (382-4357); 9:00 am to 8:00 pm Eastern Standard Time, Monday through Friday. Address: Federal Trade Commission 1 Bowling Green, New York, N.Y. 10004

Deter Identity Thieves by Safeguarding Your Information:

SHRED financial documents, pre-opened credit card applications and paperwork with personal information before you discard them.

PROTECT your Social Security number. Don't carry your Social Security Card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.

DON'T GIVE OUT personal information on the phone, through the mail, or over the internet unless you know who you are dealing with.

NEVER CLICK on links sent in unsolicited emails; instead, type in a web address you know. Use firewalls, anti-spyware, and ant-virus software to protect your home computer; keep them up to date. Visit **OnGuardOnline.gov** for more information.

DON'T USE an obvious password like your birth date, your mother's maiden name, or the last four digits of your Social Security number.

KEEP your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.

A WORD ABOUT SENIOR CITIZENS

Senior citizens are clearly in the crosshairs of scam artists and financial predators and the exploitation runs from the subtle to the most brazen types of financial abuse. Telemarketers sell Auto Club memberships to seniors who do not drive or are blind, caregivers who are asked to help with financial transactions withdraw cash for their own personal use, adult children who hold power of attorney drain retirement savings for personal use and/or pressure a parent(s) to change their will for their own benefit. The statistics illustrate only a fraction of the problem because most senior financial abuse goes unreported. Moreover, seniors may be reluctant to report they have been scammed because they are embarrassed, afraid they will be deemed no longer capable of managing their own finances or unwilling to expose a family member who has been stealing their money.

Last year, eighteen states passed legislation or resolutions relating to financial crimes against seniors and the North American Securities Administrators Association formed a committee focused on senior investors' issues. A top priority is to draft model rules that will give financial brokers and investment advisers guidance on dealing with senior clients who have diminished capacity.

To stay abreast of the latest trends and scams perpetrated against seniors, take a moment and check out AARP's newly launched Fraud Watch Network at www.aarp.org/fraudwatchnetwork. The site offers an interactive map showing law-enforcement warnings from your state, scam prevention tips and an option to sign up for e-mail alerts on the latest scams.

The Fraud Watch Network is **free of charge** for everyone – members, non-members, and people of all ages. Register to download the free e-book, *Protecting Yourself Online for Dummies*. You'll learn how to shop and bank safely, create strong passwords, protect yourself from identity theft and scams, and use social media risk-free.