Federal Bureau of Investigations (FBI)
857-386-2000

US Securities & Exchange
1-800-732-0330
www.sec.gov or www.investor.gov

Block unwanted robo-calls:
www.nomorobo

Opt out of unsolicited mail:
www.dmachoice.org
Direct Marketing Association
PO Box 643
Carmel, NY 10512

Serving the Health Insurance Needs of Everyone (S.H.I.N.E)
1-800-243-4636
1-800-AGE-INFO

Long Term Care Ombudsman Program
1-800-243-4636
Executive Office of Elder Affairs
1-617-727-7750

MassOptions
Service of the MA Executive Office of Health & Human Services
1-844-422-6277

MA Attorney General
Elder Hotline
1-888-243-5337

Norfolk District Attorney
Michael W. Morrissey
Crime Prevention Unit
Senior Programming
781-830-4920

Norfolk County Sheriff
Michael G. Bellotti
Senior Programs
781-751-3516

FTC Consumer Protection
Consumer.gov

Spot & Stop Scams

The common goal of all scams :
to obtain your personal, confidential and financial information
You can protect yourself by knowing what to watch out for and by sharing the information with others.

Now, when we receive an email, text or telephone call, we question if it is a scam - - and rightfully so!

There are countless variations of scams out there, and new scams are born daily. Scams evolve over time, but typically have the same ingredients, as scammers tend to use the same methodology and simply change the pitch. Scams come in many different forms: from getting personal, confidential and financial information the "old fashioned way" by "dumpster diving" or rummaging through trash, to emails, phone calls and text messages to phish for personal and financial information under the guise of a trusted source, like a bank or utility company.

Why do scams work? Because they are often plausible. Many people find it believable that they missed a deadline, forgot to pay a bill or misfiled their tax returns.

Scammers exploit the vulnerable. For many reasons, elders are targeted more often; the number of reported elderly scam victims reflects that. Those raised to be polite and trusting are particularly vulnerable. It is important to be less trusting and more self-protective. Knowledge is power and vigilance is their number one weapon against scams.

An understanding of the recipe for a scam can help you spot and stop them. Here are some of the ingredients to a scam recipe:

- Most scammers use pushy techniques and persuade their victims by appealing to their emotions. They prey on their fear, excitement and sadness – and they are good at it!

HELPFUL RESOURCES

AARP ElderWatch
1800-222-4444, Option 2
www.aarpelderwatch.org

Annual Credit Report
1-877-322-8228
www.annualcreditreport.com

Better Business Bureau
www.bbb.org/scam-stopper

Consumer Financial Protection Bureau
1-855-411-2372
www.consumerfinance.gov

Eldercare Locator
1-800-677-1116
www.eldercare.gov

Equifax
1-888-766-0008
www.equifax.com

Experian
1-888-397-3742
www.experian.com

Federal Trade Commission (FTC)
1-877-438-4338
www.ftc.gov

Financial Industry Regulatory Authority
1-800-289-9999
www.finra.org

FTC Do Not Call Registry
1-888-382-1222
www.ftc.gov/donotcall

Massachusetts Do Not Call Registry
1-866-231-2255

Opt Out of Credit Card Offers
1-888-5-OPTOUT

Contractor License Information
www.mass.gov/dps

MA Attorney General
1-617-727-2200
www.mass.gov/ag

Social Security Administration
1-800-269-0271
www.ssa.gov

US Postal Inspector General
1-888-877-7644 or 877-876-2455

TransUnion
1-800-680-7289
www.transunion.com

Medicare
1-800-Medicare (800-633-4227)
www.medicare.gov

MA Senior Medicare Patrol
1-800-892-0890
www.masmp.org

Internal Revenue Service (IRS)
1-800-908-4490

National Fraud Information Center
1-800-876-7060

National Fraud Information Hotline
1-800-876-7060

Prescription Advantage
1-800-243-4636

MassHealth and Medicaid
1-800-841-2900
www.mass.gov/masshealth

Medicare Advocacy Project
1-800-323-3205
www.gbls.com

Fraud Tips Hotline
Health and Human Services
Office of the Inspector General
1-800-HHS-TIPS

Tips to help you avoid falling for scams:

- Never give out PII – personal identity information over the phone, text or email.
- Never reveal your bank account numbers or other account numbers to anyone over the phone or that comes to your door.
- Carefully read contracts before signing and have someone you trust look it over. Do not feel pressured to sign.
- Never sign power of attorney to someone you don't know well or trust well. Never sign power of attorney
- It is safe to assume a stranger who says he is representing a charitable organization is a scammer at your door on one the other end of the phone. Do your homework before donating your money.
- Be wary of who is at your door trying to sell you products/ services. It is best to never answer the door to strangers.
- It is safe to assume any phone calls that do not come from family and friends are likely telemarketers or scammers. Voicemail can be a helpful tool in screening calls.
- Do not carry your Medicare or Social Security card with you.

If you receive an email, call or text asking for money or personal information, **STOP!** Don't click on the link, don't engage with the caller, and, above all, don't rush into a decision.

What to do if you have been scammed?

- Immediately contact the money transfer service to report it. If the money has not been picked up yet, you can retrieve it.
- Contact the police
- Contact the Internet Crime Complaint Center (www.ic3.gov).
- File a report with the Federal Trade Commission at 1-877-438-4338 or www.ftc.gov.

For example, in the grandparent scam, the caller claims to be a grandchild in need of immediate cash for an emergency. This sense of urgency results in the victim reacting quickly, based on emotions instead of rational thinking.

- Scammers will use any tactic to build trust. They gain the victim's trust by seeming to care, by being attentive, and available. They ask questions about their health and family and make small talk. This approach works best on elders who may be lonely.

- Scammers masquerade as lawyers, law enforcement, federal agents, non-profit organizations, or real businesses. To look official, scammers employ caller ID spoofing apps or software to manipulate caller IDs to read whatever name and number they choose.

- Scammers know they need to distract you from your common sense. They want to get your personal information or money as quickly as possible. They try to make you act before you can ask questions, verify their credentials, confirm the reason for their call or think rationally. Scammers may demand to stay on the phone with you while you go to the store to purchase gift cards or wire money for payment. They advise you not to tell anyone anything.

- The scammer informs payment can **only** be by wiring money, gift card or loading money on a cash-reload card? Scammers want payment that is hard or impossible to trace and impossible to recover. Scammers know that wired money is like cash payment. No legitimate government agency or business will ever ask for payment by gift cards, cash reload cards or wiring money, nor will they demand payment in an hour with the threat of arrest.

IRS/Tax scams: Someone claiming to be from the IRS calls to say you owe back taxes. The caller threatens to arrest you if you do not pay immediately, usually by money transfer or prepaid debit card. The caller ID is spoofed so that the call appears to be from a government agency or the police. **How to tell it's a scam:** The IRS never calls.

Debt collection scam: Someone calls claiming you have an unpaid debt and threaten wage garnishment, lawsuits, or jail time if you don't pay immediately. The scammer often spoofs the phone number of a government agency or law enforcement. **How to tell it's a scam:** Debtors have rights and the caller may be breaking them. Be sure to know your rights.

Sweepstakes, prizes and gifts scam: You receive a call, letter, or email announcing you've won a prize. However, in order to receive the prize, you must pay tax, delivery or processing fee. **How to tell it's a scam:** If you never entered the contest. You should never have to pay money to claim a prize.

Tech scam: Callers claiming to be Microsoft that have detected a virus on your computer promise to correct the problem remotely for a fee. They want to steal money or use your computer password to steal your information or install malware in your system. **How to tell it's a scam:** You haven't had computer problems. If you do, take it to a trusted repair shop.

Government grants scam: You receive a call, email, or letter saying that you qualify for a government grant. In order to receive the grant, however, you are told to pay a processing or delivery fee by wire transfer or prepaid debit card. **How to tell it's a scam:** The government won't hand out free money you haven't applied for.

Social media scam: They come in many varieties, but are usually shopping for too-good-to-be-true deals on hot item. **How to tell it's a scam:** If it looks too good to be true, it probably is.

The Equifax data breach

In September, 2017, Equifax, one of the nation's three major credit bureaus, announced a data breach that compromised the personal information of nearly 150 million Americans, roughly 2 out of 3. Though this doesn't mean you will become a victim of identity theft, vigilance is key. To find out if the breach affected you, visit **www. equifaxsecurity2017.com**. Be sure to type in the website address carefully, as there are scam sites that look authentic.

By law, you are entitled to one free report from each of the credit reporting agencies yearly. Monitor them regularly at www. annualcreditreport.com. Don't order all three reports at the same time – spread them out over the year to keep closer tabs on any suspicious activity.

Consider placing a freeze or lock on your credit to prevent identity thieves from opening a new account in your name. You will have to request to lift the freeze when you apply for credit.

The information that was gathered may be sold to scammers, resulting in an increase in scam calls. Because the hackers have the dates of birth of the consumers, the information can be used to target elders. If you receive a phone call from Equifax asking to verify your personal information to see if you are on the impact list, it is a scam. Equifax will not call you out of the blue.

Be wary of any emails appearing to come from Equifax. They may be from scammers trying to get additional information.

Help protect your family and friends from falling victim to scams by sharing this information.

Lottery/winnings scam: You receive a call, letter, or email saying you've won money in a foreign lottery. Though, in order to collect it you need to pay upfront for taxes and fees. **How to tell it's a scam:** Such lotteries are illegal. If you receive a check as partial payment, it is counterfeit.

Dating scam: These scams start with fake online dating profiles. The scammer builds a relationship with the target, exchanges photos, messages and even calls. Then comes: "I need money to see you." After money is sent, they're never heard from again. **How to tell it's a scam:** Watch out if they want to: use personal email /text; make spelling/grammar errors; professes love quickly; currently overseas and asks for money.

Medicare Scams Medicare beneficiaries are getting calls claiming to be from Medicare asking that they pay for or verify their Medicare number before their new Medicare number can be issued. **How to tell it's a scam**: Medicare will NEVER call you to verify your number and the new card is free.

Reverse mortgage scam: Unlike official refinancing schemes, unsecured reverse mortgages can lead property owners to lose their homes when perpetrators offer money or in exchange for the title to the property. **How to tell it's a scam:** It is complicated even for well-educated people in the mortgage business.

Phishing Via Text/Email Scam: Scammers try to get you to share information through legitimate-looking e-mail and text messages from what appears to be a bank, federal agency or service provider requesting that you "verify" personal information. **How to tell it's a scam:** They will not ask to verify it by text or email. They already have it.

Loan application scam: While researching loans, you see an enticing ad. You click and, after filling out the application, you receive an email or call saying your application has been approved, but you must first send money for a processing fee or insurance payment. Not only is there no loan, but if you follow the instructions, you'll share personal information, opening yourself up to identity theft. **How to tell it's a scam:** Hover your mouse over the link before clicking; often the name doesn't match the company advertising the loan. If you get scammed, lock your credit to prevent new accounts in your name.

Credit card scams: A scammer calls as your credit card issuer saying you qualify for lower interest rates or to verify a recent transaction. The caller asks for your credit card number and security code to "confirm your account." Then the data is used to steal your identity. **How to tell it's a scam:** Your credit card company knows your number.

Work-from-home scams: You answer an online ad offering to pay you big bucks to work from home. In fact, it's a front for stealing your personal information from your resume or employment form. **How to tell it's a scam:** If it sounds too good to be true, it probably is.

Fake check/money order scam: Someone pays you more than you are owed for goods/services and asks you to deposit the check and wire the difference. The check is a fake and when it bounces, you're out the money *and* the fee. **How to tell it's a scam:** The only reason for someone to ask you to be like a bank is to extract money from you.

Jury Duty Scam: Scammers posing as marshals or sheriffs (sometimes using names and numbers of legitimate officials) call people and demand immediate payment or face arrest for missing jury duty they were never scheduled for. **How to tell it's a scam**: Government officials will never call and threaten arrest or demand payment.