A Citizen's Guide
To Dangerous Scams
And How to Protect Yourself
Disclaimer

The material herein is accurate to the best of the author’s knowledge. However, the author’s opinions may change. The reader is encouraged to verify the status of those opinions.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

In no event shall Freedom Writers Publishing, Rama Marketing LLC, and/or its agents and affiliates be liable to any party for direct, indirect, special, incidental, or consequential damages of any kind whatsoever arising out of the use of the information contained herein. Freedom Writers Publishing, Rama Marketing LLC and/or its agents and affiliates specifically disclaim any guarantees, including, but not limited to, stated or implied potential profits or rates of return or investment timelines.

The information contained in this kit/book/course and its several complementary guides, is meant to serve as a comprehensive collection of time-tested and proven strategies that the author(s) have deemed successful to meet the intended results. Summaries, strategies, tips and tricks are only recommendations by the authors, and reading this kit does not guarantee that one’s results will exactly mirror our own results. The authors have made all reasonable efforts to provide current and accurate information for the readers of this product. The authors will not be held liable for any unintentional consequences, errors, or omissions that may be found.

The material in this book may include information, products, or services by third parties. Third Party materials comprise of the products and opinions expressed by their owners. As such, the authors of this guide do not assume responsibility or liability for any Third Party Material or opinions.

The publication of such Third Party materials does not constitute the authors’ guarantee of any information, instruction, opinion, products or service contained within the Third Party Material. Use of recommended Third Party Material does not guarantee that your results will mirror our own. Publication of such Third Party Material is simply a recommendation and expression of the authors’ own opinion of that material.

Whether because of the general evolution of the Internet, or the unforeseen changes in company policy and editorial submission guidelines, what is stated as fact at the time of this writing, may become outdated or simply inapplicable at a later date. This may apply to this product, our affiliated website platforms, as well as, the various similar companies that we have referenced in this kit, and our several complementary guides. Great effort has been exerted to safeguard the accuracy of this writing. Opinions regarding similar website platforms have been formulated as a result of both personal experience, as well as the well-documented experiences of others.

No part of this publication shall be reproduced, transmitted or resold in whole or in part in any form, without the prior written consent of the authors. All trademarks and registered trademarks appearing in this kit are the property of their respective owners.
## Contents

Introduction ...............................................................................................................................................5
Adoption Scams .........................................................................................................................................6
Advance Fee Scams ....................................................................................................................................7
Anti-Aging Product Scams ..........................................................................................................................8
ATM Skimmer Scams .................................................................................................................................9
Bankruptcy Scams .......................................................................................................................................11
Business Email Scams ................................................................................................................................13
Cancer Research Scams ............................................................................................................................16
Child Predator Scams ...............................................................................................................................17
Credit and Debit Card Scams ......................................................................................................................19
Debt Relief Scams .......................................................................................................................................21
Disaster Relief Donation Scams ................................................................................................................22
Ebola Scams ................................................................................................................................................24
Foreclosure Scams .....................................................................................................................................26
Funeral Scams .............................................................................................................................................28
Gift Card Scams .........................................................................................................................................30
Grandparent Scams ...................................................................................................................................32
Health Care/Insurance Scams .....................................................................................................................34
Holiday Scams ............................................................................................................................................36
House Stealing Scams ...............................................................................................................................37
Investment Scams .......................................................................................................................................39
IRS Scams ..................................................................................................................................................42
Jury Duty Scams ..........................................................................................................................................44
Letter of Credit Scams ...............................................................................................................................46
LinkedIn Support Scams ............................................................................................................................47
Lottery Scams ...............................................................................................................................................49
Mass Marketing Scams ..............................................................................................................................51
Mystery Shopper Scams ............................................................................................................................53
Nigerian Letter Scams ..................................................................................................................................55
Online Auction Scams ..............................................................................................................................57
Online Automobile Auction Scams ...........................................................................................................59
Online Dating Scams ............................................................................................................................. 61
Online Rental Housing Scams ............................................................................................................. 63
Phishing Scams ..................................................................................................................................... 65
Ponzi Scams ........................................................................................................................................... 67
Prime Bank Note Scams ....................................................................................................................... 69
Pump-and-Dump Stock Scams ............................................................................................................. 71
Pyramid Scams ....................................................................................................................................... 73
Ransomware Scams .................................................................................................................................. 75
Redemption/Strawman/Bond Scams ...................................................................................................... 77
Scareware Scams ................................................................................................................................... 79
Senior Citizen Scams ............................................................................................................................ 81
Shared Community Scams ...................................................................................................................... 83
Smishing Scams ...................................................................................................................................... 85
Social Security Card Scams .................................................................................................................... 87
Soldier Love Scams ............................................................................................................................... 89
Spear Phishing Scams ............................................................................................................................. 91
Sports Memorabilia Scams .................................................................................................................... 93
Staged Auto Accident Scams .................................................................................................................. 95
Surrogacy Scams .................................................................................................................................... 97
Tech Support Scams .............................................................................................................................. 99
Telemarketing Scams ............................................................................................................................ 101
Telephone Denial of Service Scams ...................................................................................................... 103
Timeshare Scams ................................................................................................................................... 105
Vishing Scams ....................................................................................................................................... 107
Work at Home Scams ........................................................................................................................... 109
Introduction

Every year, Americans lose billions of dollars to scams conducted by criminals who work full time to steal the hard-earned dollars of innocent victims.

To make matters worse, rapid advances in technology – including the Internet, the World Wide Web, email, smartphones, SMS text messaging, chat rooms and social media applications – help crooks spread their scams globally while also making it easier for them to hide from the police.

If it seems like the “bad guys” are winning, it’s because they are.

Realistically, the police can’t possibly keep up with the growing number of scams and the majority of criminals conducting scams and fraud against Americans are never caught or prosecuted.

The truth is, for scammers, crime really does pay.

In fact, while they rarely admit it publicly, prosecutors have “prosecutorial thresholds” that prevent them from prosecuting cases involving scammers unless the dollar value lost by the victim is over a certain “threshold” amount.

Depending on the jurisdiction, the threshold can be tens of thousands of dollars.

So even if the police track down a crook who scams you – a long shot at best – the odds of that scammer being prosecuted are infinitesimally small.

So what can be done to combat scams? How can you avoid being ripped off?

The best defense is knowledge.

The best defense against scams is knowledge of the types of scams attacking Americans combined with an understanding of how those scams are conducted.

This guide, *A Citizen’s Guide to Dangerous Scams and How To Protect Yourself*, provides you with that important knowledge and it will empower you to recognize scams in real-time so that you can avoid becoming a victim.

As you learn about the different scams covered in this guide, you will learn of the common traits that many scams have and, in so doing, learn to recognize the warning signs of a possible scam.

And if you learn nothing else, always remember that if an offer appears too good to be true, it probably is. So be suspicious and proceed with caution.

Welcome to *A Citizen’s Guide to Dangerous Scams and How To Protect Yourself!*
Adoption Scams

While all scams are wrong, it's hard to imagine a scam that is more painful on an emotional level than the Adoption Scam.

For example, according to the FBI at least six couples in the Midwest were victimized by adoption fraud schemes in recent years...cases where birth mothers promised their unborn children to more than one couple or who weren't even pregnant...where couples did business with phony domestic adoption agencies or facilitators...or where the international adoptions weren’t sanctioned by the home country or even involved kidnapped children.

"It's really awful. These con artists feed on their victims' hopes and then they get crushed,' says Special Agent Patrick B. Sullivan, who worked an adoption fraud case out of Florida.

"In the Florida case, a woman contacted over a dozen victims through an Internet site for people wanting to adopt. She claimed she knew women about to give birth, then asked for either small administrative fees or for money to help the birth mother with expenses. ‘She milked them along, raking in the money, until they figured out they were being taken,’ Sullivan said."

In an Indiana case, “Victoria Farahan approached the director of a new local adoption ministry and said she could provide healthy newborns from Hospital 31 in Moscow. She provided pictures of the babies—which turned out to be pictures of her own children. She also sent the victims e-mails during her “trips” to Russia. ‘Farahan was very good at sprinkling in little bits of truth,' said Special Agent Steven T. Secor, who led the investigation. ‘She was very convincing. And she was dealing with couples that wanted babies and were willing to overlook some things.' She eventually duped six couples out of a total of $97,500.”

The Do’s and Don’ts to Avoid Adoption Scams:

- Check for licensing. Most states require agencies and facilitators to be licensed.
- Don’t rely solely on the Internet for research.
- Meet the agency or facilitator in person.
- Ask for documentation and references.
- Be skeptical if agencies or individuals say they have shortcuts.
- Hire your own social worker to interview the birthmother.
- For international adoptions, check with the U.S. Department of State for more information.
Advance Fee Scams

An Advance Fee Scam happens when a victim pays money in advance because they believe they will receive something of greater value—such as a loan, contract, or gift. But they end up with nothing or something of little value once the scam is completed.

The range of Advance Fee Scams is endless. Often, they involve the sale of products, services, investments, lottery winnings, or many other attractive offerings.

In a typical example, scammers will offer to find financing arrangements for “clients” who pay a “finder’s fee” in advance. The client is told by the scammer that they are required to sign a contract obligating them to pay an advance fee.

After paying the advance fee or finder’s fee, the victim is told they are ineligible or unqualified for the financing they believed they would receive.

The Do’s and Don’ts to Avoid Advance Fee Scams:

- Know who you are dealing with. If you haven’t done business with the person or company, investigate their background and reputation.
- Visit the business location.
- Check with the Better Business Bureau, your bank, or the police to see if they have heard of the business offering the products, services, or investments.
- Make sure you completely understand the terms of any contract or agreement. Have the contract or agreement reviewed by an attorney.
- Be suspicious of businesses or individuals that only provide a post office box for an address.
- Be suspicious when dealing with individuals who don’t have a direct telephone contact number or are never available when you call.
- Be suspicious of contracts or agreements that require non-disclosure agreements that prevent you from independently checking the background and reputation of the individual or business you are dealing with.
- Be suspicious of any agreement or contract that includes a non-circumvention agreement that threatens a civil law suit if losses are reported to the police.
Anti-Aging Product Scams

Perhaps it is human nature, but it seems that most of us want to avoid growing “old.”
And we’ve all seen products offered that promise to make us “look and feel younger.”
In fact, it’s hard to avoid these types of advertisements for anti-aging products as the ads are everywhere – on the TV, radio, newspapers, magazines and the Internet.
For those reasons, scam artists are constantly trying to take advantage of the marketplace for anti-aging products by offering “miraculous,” “secret formula” “breakthrough” anti-aging products.
Unfortunately, many of these products or treatments are nothing more than scams designed by con artists to steal your hard-earned money.

The Do’s and Don’ts to Avoid Anti-Aging Product Scams:

- If it sounds too good to be true, it probably is.
- Be suspicious of “secret formulas” or “breakthrough” products.
- Don’t be afraid to ask questions about the product. Find out exactly what it should and should not do.
- Research a product thoroughly before buying it. Call the Better Business Bureau to find out if other people have complained about the product or the company/individual offering the product.
- Be suspicious of products that claim to cure a wide variety of illnesses - particularly serious ones - that don’t appear to be related.
- Be aware that testimonials and/or celebrity endorsements are often paid for and misleading.
- Be suspicious of products that are marketed as having no side effects.
- Question products that are advertised as making visits to a physician unnecessary.
- Always consult your doctor before taking any dietary or nutritional supplement.
ATM Skimmer Scams

If there was ever a scam that comes close to the equivalent of printing money, it’s the ATM Skimmer Scam.

Have you ever looked closely at the device you slide your ATM, debit, or credit cards into when withdrawing cash from an ATM? Probably not. Most of us don’t. We just assume that the device is legitimate and as long as we get our cash, we’re happy.

Unfortunately, scammers have figured out that they can use the machines to their advantage. According to experts, here’s how ATM (and other bank card) skimmers work.

The devices planted on ATMs are usually undetectable by users – the makers of this equipment have become very adept at creating them so that they blend right into the ATM and appear legitimate. The specific device used is often a realistic-looking card reader placed over the factory-installed card reader. Customers insert their ATM card into the phony reader, and their account info is stolen and stored on a small attached device or sent wirelessly to the criminals waiting nearby.

Often, skimming involves the use of a hidden camera, installed on or near an ATM, to record customers’ entry of their PINs into the ATM’s keypad. There have also been cases where scammers attach a false keypad on top of the real keypad, thereby recording the PINs as they are entered by the customer.

Skimming devices are usually installed for a short period of time so they may be attached in a very flimsy fashion. But recently, far more sophisticated devices have been created that are almost impossible to detect.

Once the customers’ account information and PINs are stolen, it can be downloaded and encoded onto blank ATM cards and used to make withdrawals from the victims’ accounts at other ATMs.

ATM Skimmer Scams have included:

- A Romanian gang charged with fraud and identity theft after they made and placed skimming devices on ATMs in Florida.
- Another Romanian gang that stole account information from nearly 400 bank customers through the use of skimming equipment installed on ATMs in Atlanta.
- A Serbian who was caught trying to purchase an ATM skimming device with plans to steal account information from ATM users in Chicago.
- A scam that used sophisticated skimming devices on ATMs in New York City that resulted in the theft of over $1.8 million from at least 1,400 customer accounts.
Remember: ATMs aren’t the only target of skimmers. They are also used on gas pumps and any other point-of-sale location where customers swipe debit or credit cards through a device to make their transaction.

The Do’s and Don’ts to Avoid ATM Skimmer Scams:

- Inspect the ATM, gas pump, or credit card reader before using it.
- Be suspicious if you see anything loose, crooked, or damaged, or if you notice scratches or adhesive/tape residue.
- When entering your PIN, block the keypad with your other hand to prevent possible hidden cameras from recording your number.
- If possible, use an ATM at an inside location (because there’s less access for criminals to install skimmers).
- Be suspicious of ATMs in areas that attract tourists. They are popular targets of skimmers.
- If your card isn’t returned after the transaction or after hitting “cancel,” immediately contact the financial institution that issued the card.
Bankruptcy Scams

Bankruptcy can be a legitimate legal process for individuals and companies that have no ability to pay off their debts due to a wide-range of reasons including unemployment, a medical crisis, divorce, and disability.

However, there are those who use the bankruptcy process to scam and defraud individuals and companies by not paying debts they owe even though they have the money to pay off their debts.

For that reason, it is important to understand how bankruptcy scams work and to report individuals and businesses to the police if you suspect they are attempting to scam or defraud you through the bankruptcy process.

According to law enforcement sources, bankruptcy scams typically involve small business owners, corporate CEOs, real estate agents, politicians, and bank loan officers. Cases involving the participation of bankruptcy attorneys and bankruptcy document preparers are not unheard of and involve criminal behavior that defrauds debtors and creditors in otherwise legitimate bankruptcy proceedings.

The most common types of bankruptcy scams and fraud include people who lie under oath or provide false documentation during bankruptcy proceedings. Additionally, they may conceal or transfer their financial assets, or commit tax fraud. Other schemes include using false identities to file for bankruptcy multiple times in multiple locations, bribing a bankruptcy trustee, and intentionally running up credit card bills with no intention of paying them off.

Bankruptcy scams and fraud are often involved with other crimes like credit card fraud, identity theft, mortgage fraud, money laundering, and mail and wire fraud.

Here’s a typical case as reported from the files of the United States Attorney for the Southern District of Illinois.

Stephanie Reeves, 35, of Belleville, Illinois, entered a plea of guilty in federal district court to committing bankruptcy fraud by falsely claiming that she was in bankruptcy in order to stop collection efforts by a business to which she owed money. At her plea, Reeves admitted that she utilized the bankruptcy documents of another person by placing her name on the court forms and then sending them to a lender in order to gain benefit of an automatic bankruptcy stay to which she was not entitled.

In a case from Massachusetts, John Pregent, “aka” Jack Pregent, 61, pleaded guilty before United States District Judge George A. O’Toole to one count of bankruptcy fraud.
According to the U.S. Attorney, “Pregent owned the precision machine part manufacturing business Technical Fabrications, Inc. ("TechFab") which operated in Newburyport until it filed for bankruptcy in July 2010. Pregent engaged in a scheme to defraud TechFab’s creditors, bankruptcy trustee and the bankruptcy court by transferring certain TechFab assets, including equipment and ongoing business, to a newly formed company. Pregent arranged for that new company to pay compensation for TechFab's assets directly to himself, then filed a Chapter 7 bankruptcy for TechFab to discharge its debts all while concealing the pre-bankruptcy transfer of assets and the agreement to pay compensation for those assets to Pregent. Furthermore, Pregent failed to disclose the transfers and compensation agreement in TechFab’s bankruptcy pleadings and during his testimony before a meeting of creditors.”

And in a third case, the former CEO of Worldwide Financial Resources, a New Jersey-based mortgage origination firm, received 63 months in prison in connection with an $11 million fraudulent loan scheme.

According to the U.S. Attorney for New Jersey, David Findel, 45, “admitted he prepared and sold fake mortgage loans from 2008 through September 2009. Specifically, after Worldwide had originated a mortgage loan and sold that loan to a third-party lender, Findel would create a second set of fraudulent loan documents for the same property. He would then sell the second set of fraudulent loan documents to another third-party lender, even though the actual mortgage loan for that property already had been sold. As a result of these fake mortgage loans, Findel received over $11 million in illicit proceeds, which he used, in part, to maintain his lavish lifestyle—including his multi-million-dollar home in Colts Neck, exotic travel, and exclusive seating at a major New Jersey professional sports arena.”

The Do’s and Don’ts to Avoid Bankruptcy Scams and Fraud:

- Know who you are dealing with. If you haven’t done business with the person or company, investigate their background and reputation.
- Check with the Better Business Bureau, your bank, or the police to see if they have heard of the business offering the products, services, or investments and whether the individual or company have any lawsuits or bankruptcy proceedings.
- Perform an Internet search looking for any negative information or complaints about the individual or business.
- Check all financial statements from an individual or business closely and on a monthly basis. Watch for any transactions that don’t make sense or that are out of the ordinary course of business.
- Ask questions about any financial transactions you don’t completely understand. Be certain the answer makes sense and if it is complicated seek outside advice and counsel from an accountant or attorney of your choosing.
Business Email Scams

According to law enforcement experts at the internet Crime Complaint Center (IC3), the Business Email Scam targets businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. Formerly known as the Man-in-the-E-mail Scam, the Business Email Scam was renamed to focus on the “business angle” of this scam and to avoid confusion with another unrelated scam. The fraudulent wire transfer payments sent to foreign banks may be transferred several times but are quickly dispersed. Asian banks, located in China and Hong Kong, are the most commonly reported ending destination for these fraudulent transfers.

The Business Email Scam is a global scam with subjects and victims in many countries. The IC3 has received complaint data from victims in every U.S. state and 45 countries. The FBI assesses with high confidence the number of victims and the total dollar loss will continue to increase.

The Business Email Scam is linked to other forms of fraud, including but not limited to: romance, lottery, employment, and home/vacation rental scams. The victims of these scams are usually U.S. based and may be recruited as unwitting “money mules.” The mules receive the fraudulent funds in their personal accounts and are then directed by the subject to quickly transfer the funds using wire transfer services or another bank account, usually outside the U.S. Upon direction, mules may sometimes open business accounts for fake corporations both of which may be incorporated in the true name of the mule.

The victims of the Business Email Scam range from small to large businesses. These businesses may purchase or supply a variety of goods, such as textiles, furniture, food, and pharmaceuticals. This scam impacts both ends of the supply chain, as both supplies and money can be lost and business relations may be damaged.

It is still largely unknown how victims are selected; however, the subjects monitor and study their selected victims prior to initiating the scam. The subjects are able to accurately identify the individuals and protocol necessary to perform wire transfers within a specific business environment. Victims may also first receive “phishing” e-mails requesting additional details of the business or individual being targeted (name, travel dates, etc). Some victims reported being a victim of various Scareware or Ransomware cyber intrusions, immediately preceding a scam request.

Based on IC3 complaints and other complaint data received since 2009, there are three main versions of this scam:
Version 1 - A business, which often has a long standing relationship with a supplier, is asked to wire funds for invoice payment to an alternate, fraudulent account. The request may be made via telephone, facsimile or e-mail. If an e-mail is received, the subject will spoof the e-mail request so it appears very similar to a legitimate account and would take very close scrutiny to determine it was fraudulent. Likewise, if a facsimile or telephone call is received, it will closely mimic a legitimate request. This particular version has also been referred to as “The Bogus Invoice Scheme,” “The Supplier Swindle,” and “Invoice Modification Scheme.”

Version 2 - The email accounts of high-level business executives (CFO, CTO, etc) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is normally responsible for processing these requests. In some instances a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank “X” for reason “Y.” This particular version has also been referred to as “CEO Fraud,” “Business Executive Scam,” “Masquerading,” and “Financial Industry Wire Frauds.”

Version 3 - An employee of a business has his/her personal e-mail hacked. Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee’s personal e-mail to multiple vendors identified from this employee’s contact list. The business may not become aware of the fraudulent requests until they are contacted by their vendors to follow up on the status of their invoice payment.

The IC3 has noted the following characteristics of Business Email Scams:

- Businesses and personnel using open source e-mail are most targeted.
- Individuals responsible for handling wire transfers within a specific business are targeted.
- Spoofed e-mails very closely mimic a legitimate e-mail request.
- Hacked e-mails often occur with a personal e-mail account.
- Fraudulent e-mail requests for a wire transfer are well-worded, specific to the business being victimized, and do not raise suspicions to the legitimacy of the request.
- The phrases “code to admin expenses” or “urgent wire transfer” were reported by victims in some of the fraudulent e-mail requests.
- The amount of the fraudulent wire transfer request is business specific; therefore, dollar amounts requested are similar to normal business transaction amounts so as to not raise doubt.
- Fraudulent e-mails received have coincided with business travel dates for executives whose e-mails were spoofed.
- Victims report that IP addresses frequently trace back to free domain registrars.
The Do’s and Don’ts to Avoid Business Email Scams:

- Avoid Free Web-Based E-mail: Establish a company web site domain and use it to establish company e-mail accounts in lieu of free, web-based accounts.
- Be careful what is posted to social media and company websites, especially job duties/descriptions, hierarchal information, and out of office details.
- Be suspicious of requests for secrecy or pressure to take action quickly.
- Consider additional IT and Financial security procedures and 2-step verification processes.
- Significant Changes: Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via their personal e-mail address when all previous official correspondence has been on a company e-mail, the request could be fraudulent. Always verify via other channels that you are still communicating with your legitimate business partner.
Cancer Research Scams

Unfortunately, most of us have had a family member or friend who has been impacted by cancer. Our natural desire for a cure to a disease that kills millions can make us easy targets for scammers.

Often, the scam is about an amazing breakthrough in cancer research. In a typical case scenario, the FBI reports:

“A woman claiming to have a master’s degree in clinical nutrition was successfully marketing a full-body “electrotherapy cancer machine” across the United States.

“She said it was a breakthrough development by a London-based team of doctors, lab technicians, and physicists from the combined research fields of electromagnetic field therapy, radio frequency therapy, crystal healing therapy, and “human energy” healing.

“The machine had been tested on local cancer patients in London who were now cured, and a European company had promised to buy the machine for millions of dollars. Money was needed to complete the project...and the return on investors’ money would be at least 50% and likely much more.”

Of course, none of this was true.

“Thanks to an alert local bank investigator who was suspicious of an account suddenly receiving massive numbers of wire transfers [the FBI] opened a case and turned two undercover agents into wannabe investors. It was just a matter of time before a joint investigation with our local Florida police partners turned up hard evidence that the full-body “electrotherapy cancer machine” was a complete fraud...to the tune of $2.5 million illegally raked in.

The Do’s and Don’ts to Avoid Cancer Research Scams:

- If the research or treatment sounds too good to be true, it probably is.
- Be suspicious if you’ve never heard of the research or treatment.
- Be suspicious if you can’t easily find reputable reports, articles and information from legitimate medical journals or websites about a “miracle” cure.
- Discuss any information about research or treatments with a reputable doctor.
- Be suspicious of any “advance fee” required to “invest” in research.
Child Predator Scams

It’s hard to imagine a more disgusting scam than the Child Predator Scam.

After all, the scam relies on scaring parents and concerned community members into thinking that a child predator may be roaming their neighborhood.

According to experts, here’s how the Child Predator Scam works.

“This phishing scam preys on a parent’s fear. The scam email looks like a warning for parents about a child predator that moved into their zip code area, but it’s a really low phishing scam.”

“You receive an email with a subject line like: “Alert: There is a child predator living near you!” This information is based on your “local area zip code.” But you don’t remember signing up for such a service.”

“When you open the email, it "warns" you that a predator has moved into your area and it provides a link for more information. As you by now know, clicking the link infects your computer with malware that will try to steal your passwords, credit information, your passwords up to and including your identity.”

According to experts, in some cases, “If you click on the link, you are redirected through several sites to land on the Kids Live Safe website, which is a service that sells localized reports on sex offenders. But this phishing attack is not from that website, it just sends victims there to try to look credible and distract your attention from the fact your computer is now infected with malware.”

Here’s an example of the text that may be contained in the email (remember, the text in any one scam email may be different. This is just one example.):

“Neighborhood Safety Warning”

“You are receiving this email because we have detected Sex Offender activity in your area. If you would like to know who they are, where they live and how you can protect your family from sexual predators please click here.”

“NOTE: the website you are about to access contains actual sex offender information. Please use extreme caution when utilizing this service. Learning the truth about who lives near your family can be shocking and disturbing. By proceeding you agree to utilize Kids Live Safety solely for informational purposes and to protect your children and loved ones.”

If you click on any links in the email, your computer will be infected with malware.
The Do’s and Don’ts to Avoid Child Predator Scams:

- Keep in mind that reputable agencies like Kids Live Safety will not email you in an unsolicited fashion or require you to click links to learn important information.
- If in doubt about any specific email, contact the agency directly but don’t use the phone number or links contained in the email as they may be fraudulent and direct you to scammers or download malware. Obtain the phone number or website from a source, directory or document you’ve used before.
- Use a phishing filter that most web browsers and email programs have installed or available as plug-ins.
- Never follow a link to a supposedly secure site from an email. Always enter the URL for the website manually or from a previously used and trusted bookmark.
- Stay abreast of the latest scams so you won’t be fooled when you receive a scam like the Child Predator Scam.
Credit and Debit Card Scams

Credit and Debit Card Scams can be involved in almost every other type of scam discussed in this guide. (Debit cards are also known as check cards or bank cards)

For that reason, you should keep the following list of do’s and don’ts in mind whenever making a purchase using a credit or debit card to make a purchase.

In fact, these do’s and don’ts apply to many types of transactions and serve as a good scam avoidance reference list to review from time to time.

The Do’s and Don’ts to Avoid Credit and Debit Card Scams:

- Don’t give out your credit card number online unless the site is secure and reputable. Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. This icon is not a guarantee of a secure site, but provides some assurance.
- Before using the site, check out the security/encryption software it uses.
- Make sure you are purchasing merchandise from a reputable source.
- Do your homework on the individual or company to ensure that they are legitimate.
- Obtain a physical address rather than simply a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.
- Send an e-mail to the seller to make sure the e-mail address is active, and be wary of those that utilize free e-mail services where a credit card wasn’t required to open the account.
- Consider not purchasing from sellers who won’t provide you with this type of information.
- Check with the Better Business Bureau from the seller’s area.
- Check out other websites regarding this person/company.
- Don’t judge a person or company by their website. Flashy websites can be set up quickly.
- Be cautious when responding to special investment offers, especially through unsolicited e-mail.
- Be cautious when dealing with individuals/companies from outside your own country.
- If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong.
- Make sure the transaction is secure when you electronically send your credit card number.

[19]
Keep a list of all your credit cards and account information along with the card issuer’s contact information. If anything looks suspicious or you lose your credit card(s), contact the card issuer immediately.
Debt Relief Scams

As always happens when financial times are difficult, a growing number of scammers are targeting consumers with significant credit card debt.

In Debt Relief Scams, the scammers claim – in fact, guarantee – they can lower a victim’s monthly credit card and loan payments.

But what they really do is charge those cash-strapped victims large up-front fees and then they fail to help them settle or lower their debts.

In fact, in many cases, they don’t provide any service of any kind.

They either make excuses as to why the victim’s debt couldn’t be lowered or disappear altogether – along with the fees the victim paid.

And what about those phone calls promising to help with your debt?

If you hear a recorded sales message and you haven’t given your permission to get calls from the company on the other end, the pitch may be a scam.

Hang up and don’t press 1 to speak to a live operator or press any other number because, if you do, you may just be in for more phone calls.

The Do’s and Don’ts to Avoid Debt Relief Scams:

- Be suspicious of any company that charges fees before settling your debts.
- Be suspicious of any company that guarantees it can make your unsecured debt go away.
- Be suspicious of any company that tells you it can stop all debt collection calls and lawsuits.
- Be suspicious of any company that won’t send you free information about its services unless you provide personal and financial information, like your credit card and bank account numbers.
- If the debt relief offer comes from an unsolicited communication and sounds too good to be true, then it’s probably a scam.
Disaster Relief Donation Scams

Some types of scams are so prevalent and damaging, there are entire agencies within the federal government that are designated to combat the scams.

This is the case when it comes to Disaster Relief Donation Scams.

The National Center for Disaster Fraud (NCDF) was established by the Criminal Division of the United States Department of Justice in the fall of 2005 in the wake of Hurricane Katrina. The NCDF is located in Baton Rouge, Louisiana.

Its purpose is to receive and screen reports from the public about possible fraud relating to disasters of all types, and to refer those reports to the field offices of appropriate federal law enforcement agencies.

Unfortunately, every time there is a natural disaster of any size in the United States, scammers design schemes to tug on the heart strings of generous Americans and then steal their money.

Here are two documented examples of how natural disasters – that bring out the best in most Americans – can bring out the worst of scammers.

A Louisiana fire chief, who had no previous criminal record, volunteered to organize medical relief efforts in Baton Rouge shortly after Hurricane Katrina devastated the Gulf Coast.

He then proceeded to steal and sell nearly $500,000 worth of government-owned defibrillators.

When the theft was discovered and an investigation was begun, the fire chief tried to hire a hit man to kill a witness that could link him to the scam.

In the second example, a Texas man was spotted beating his pickup truck with an empty propane tank shortly before Hurricane Ike made landfall. The scammer told a friend he planned to report the battered truck as having been storm-damaged so he could collect an insurance settlement.

As you can see, Disaster Relief Donation Scams – and all other natural disaster related scams – can run the gamut from scams involving hundreds of thousands of dollars to scams that may only involve a few hundred dollars, or less.

But, every year Disaster Relief Donation Scams and disaster related scams cost victims and taxpayers millions of dollars.
And in most cases, those scammed dollars are money that would have gone to assist those who are truly in need following a natural disaster.

The Do’s and Don’ts to Avoid Disaster Relief Donation Scams:

- Watch for media reports of Disaster Relief Donation Scams that develop in the wake of a disaster.
- Investigate and research any organization or individual that seeks a donation following a natural disaster.
- Be suspicious of any organization or individual that you’ve never heard of and that doesn’t have an independently verifiable and established history of disaster aid.
- To be safe, only donate to well-known, national organizations with a long track record of providing relief following natural disasters.
Ebola Scams

When Ebola began to spread across several African countries in 2014, and a number of cases popped up around the globe, scammers and other assorted crooks began creating Ebola Scams.

That’s because scammers prey on our fears during events that contain dangerous circumstances like natural disasters.

The Ebola crisis is no different and scammers are on the prowl.

Specifically, according to scam experts and law enforcement agencies that monitor and combat scams, the U.S. Food and Drug Administration has seen and received “consumer complaints about a variety of products claiming to either prevent the Ebola virus or treat the infection.”

Despite these claims, “…there are no approved vaccines, drugs, or investigational products specifically for purchase on the Internet.”

And the Council for Responsible Nutrition, a trade association for the dietary supplement industry, warns consumers that there are currently no supplements that can prevent or cure Ebola.

So even though others claim differently, and everyone has the right to decide what may or may not be the best way to protect themselves from Ebola and other diseases, the federal government is warning that Ebola Scams are prevalent and the majority of claims and products being offered are nothing more than scams.

The Do’s and Don’ts to Avoid Ebola Scams:

- Be suspicious of online offers for an Ebola cure or special “natural” or “dietary” methods to alleviate or prevent symptoms.
- Be suspicious of email scams with alarming messages like "Ebola update" or “Ebola Pandemic” which may include links that release computer viruses.
- Delete any suspicious emails without opening or clicking on any links.
- Be suspicious of sales of "personal protection kits" at low prices to provide supposed “infection defense.”
- Watch out for charity scams claiming to help victims or fight the disease.
- Ask how donations will be spent and check a charity’s registration before providing any money.
- Watch out for potential stock investment scams involving companies that say they are involved in the development of products that will prevent the spread of viral diseases like Ebola.
- Never provide your personal or financial information to companies you don’t know.
Foreclosure Scams

Since the onset of the Great Recession, Foreclosure Scams have increased to a degree never before seen in history.

One of the most effective ways to defend yourself against Foreclosure Scams is through awareness of how a typical Foreclosure Scam works.

Here’s an example of an actual Foreclosure Scam as publicized by law enforcement authorities.

Jeff McGrue, owner of a Los Angeles-area foreclosure relief business, was sentenced to 25 years in prison for defrauding people who were at the end of their rope. Even the federal judge who sentenced him called him “heartless.”

It all started when McGrue - and several other conspirators who have pled guilty - orchestrated the scam primarily through his company Gateway International.

McGrue paid unwitting real estate agents and others to serve as “consultants” to recruit customers who were facing foreclosure or were “upside-down” on their mortgages - meaning they owed more than their homes were worth. Many of the customers didn’t understand English or the contracts they were signing.

How did the Foreclosure Scam work?

McGrue and his associates told the homeowners that “bonded promissory notes” drawn on a U.S. Treasury Department account would be sent to lenders to pay off mortgage loans and stop foreclosure proceedings. Further, he told them that lenders were required by law to accept the notes and that homeowners could buy their homes back from Gateway and receive $25,000, regardless of whether they decided to re-purchase.

In return, McGrue demanded that the homeowners pay an upfront fee ranging from $1,500 to $2,000, sign over the titles of their homes to Gateway, and pay Gateway half of their previous mortgage amount as rent for as long as they lived in the house.

Of course, it was all part of a Foreclosure Scam.

McGrue didn’t own any bonds or have a U.S. Treasury account, plus the Treasury doesn’t even maintain accounts that can be used to make third-party payments.

Lenders weren’t legally obligated to accept bonded promissory notes, which were worthless anyway.

And Gateway International had no intention of selling back the properties to the homeowners.
Finally, evidence shown at McGrue’s trial revealed that it was his intent to re-sell the homes, once they were titled in Gateway’s name, to unsuspecting buyers.

Meanwhile, the victims who trusted McGrue were scammed for thousands of dollars they couldn’t afford to lose and, to make matters worse, they were no closer to getting out from under an upside-down mortgage.

The Do’s and Don’ts to Avoid Foreclosure Scams:

- Be suspicious of offers that guarantee to get you a loan modification or stop the foreclosure process.
- Be suspicious of loan modification offers that instruct you not to contact your lender, lawyer, or a housing counselor.
- Be suspicious of loan modification businesses that request upfront fees before providing you with any services.
- Be suspicious of loan modification businesses that encourages you to transfer your property deed or title to them.
- Be suspicious of loan modification businesses that accepts payment only by cashier’s check or wire transfer
- Be suspicious of loan modification businesses that pressures you to sign papers you haven’t had the chance to read thoroughly or that you don’t understand.
Funeral Scams

It takes an especially evil scammer to conduct a fraud that takes advantage of victims making funeral arrangements or planning what will happen with their remains when they die.

But evil scammers do exist.

And Funeral Scams also exist.

Here’s a real Funeral Scam as uncovered and reported by law enforcement authorities.

Six scammers created a Ponzi-like (see Ponzi Scams) prepaid funeral scam that victimized some 97,000 customers in more than 16 states.

The scheme caused more than $450 million in losses, smaller or non-existent death benefits for families at their most vulnerable, and huge profits that lined the pockets of the scammers.

According to law enforcement, the scammers devised and ran a scam to defraud purchasers of prearranged funeral contracts. Also victimized were funeral homes that did business with the scammers, financial institutions that served as trustees of the prearranged trusts established by the scammers for their “customers,” and state insurance guarantee associations.

To carry out the scam, after discussing what the customer wanted, a price would be agreed upon and payment accepted. The scammers would make arrangements with the customer-designated funeral home. In accordance with state law, the funds would be placed with a third party - depending on the state, that third party would be a financial institution that would put the funds into a trust that could be only used for safe investments (like government-backed securities) or a life insurance company that would put the funds into a life insurance policy in the name of the customer.

What the scammers didn’t tell the customer victims is that the scammers didn’t put all of the funds from customers into a trust or life insurance policy, but instead brazenly altered application documents (changing deposit amounts, naming itself as a beneficiary, converting whole life insurance policies to term life) and used the money for unauthorized purposes like risky investments, payments for existing funeral claims, and personal enrichment.

In some instances, the scammers even removed money previously placed in trusts and life insurance policies all while lying to state regulators.
In the end, the victims were scammed out of what they believed they’d purchased in advance of their death – a funeral.

The Do’s and Don’ts to Avoid Funeral Scams:

- Know what you are paying for. Are you buying a casket and vault or are you purchasing funeral services as well?
- Know what happens to the money you’ve prepaid. States have different requirements for handling funds paid for prearranged funeral services.
- Know what happens to the interest income on money that is prepaid and put into a trust account.
- Know what happens if the firm you dealt with goes out of business.
- Know whether you can cancel a contract and get a full refund if you change your mind.
- Know what happens if you move to a different area or die while away from home. Some prepaid funeral plans can be transferred, but often at an added cost.
- Be sure to tell your family about the plans you’ve made and where your documents are located.
Gift Card Scams

You’ve probably received an email very similar to this one that purports to be from the well-known online retailer, Amazon.

It reads:
----- (start of email)

Subject: Amazon Survey for Rewards
Complete the Amazon Survey!
Claim Your $25 Amazon Gift Card!

Are you ready for the extra deals and savings at Amazon? Will you be shopping online or in-store? Share your opinions and experiences by completing the survey and claim your Amazon gift card!

All you need to do is complete the quick survey to claim your free gift!
START NOW! >

If you wish to no longer receive emails about this offer please follow this
----- (end of email)

In the actual email, all of the words that are underlined are hot links that will take you to a website if you click them. But, as part of the scam, if you click any of them you will download malware to your computer that is designed to steal information from your compute and/or turn your computer into a botnet that will churn out more scam emails that will be sent to others around the world.

While the example above purports to come from Amazon, these Gift Card Scams are designed with variations that impersonate almost every major retailer you can name.

In the example above, by hovering a cursor over one of the hotlinks, the URL that someone clicking on the hot link would be sent to was easily detectable as not belonging to Amazon.

But in many cases, Gift Card Scams can have hot linked URLs that may closely match the company that purportedly sent the email.

The Do’s and Don’ts to Avoid Gift Card Scams:
• Be suspicious of unsolicited web ads, emails or text messages that offer gift cards simply for providing some personal information, filling out a survey or making a small purchase.
• If the offer comes from unsolicited communication and sounds too good to be true, then it’s probably a scam.
• Never give out personal or financial information in exchange for a gift card. That’s a good sign it could lead to identity theft or malware.
Grandparent Scams

Sadly, one of the most prevalent scams today is the Grandparent Scam. Grandparent Scams are designed to take advantage of the natural love and desire to help that most grandparents have when it comes to their grandchildren.

While the Grandparent Scam has been around since at least 2008, the scam and scam artists have become more sophisticated. By using the Internet and social networking sites, criminal can often locate personal information about their targets. This personal information makes the impersonation of the grandchild more believable.

For example, a real grandson may state on his social networking site, like Facebook, that he’s a photographer who often travels to Europe. When contacting the grandparents, the scam artist who is impersonating the grandson will say he’s calling from a country in Europe, where someone stole his personal belongings camera equipment and passport and he needs money to get home.

Or, the impersonator may say he’s been arrested and needs bail money as quickly as possible – preferable wired immediately.

A typical Grandparent Scam often happens like this:

The grandparent receives a phone call or an e-mail from someone who identifies himself as the grandparent’s grandson.

The “grandson” states, “I’ve been arrested while traveling in Germany [or any other country name the scam artist uses] and need money wired quickly to pay my bail. Please don’t tell my parents because they’ll get upset.”

According to law enforcement sources, frequently used Grandparent Scams include:

- A grandparent receives a phone call or an e-mail from a “grandchild.” If it is a phone call, it’s often late at night or early in the morning when most people aren’t thinking that clearly. Usually, the “grandchild” claims to be traveling in a foreign country and has gotten into a bad situation, like being arrested for drugs, getting in a car accident, or being mugged. The “grandchild” claims to need money wired immediately and want his or her parents told.

- Sometimes, instead of the “grandchild” making the phone call, the scam artist impersonates a police officer, lawyer, doctor at a hospital, or some other person who is calling to assist the “grandchild” who is in trouble or having a crisis.

- In more sophisticated scams, the “grandchild” will talk first and then hand the phone to an accomplice acting as a police officer, lawyer, doctor at a hospital, or
some other person who is calling to assist the “grandchild” who is in trouble or having a crisis.

- Military families have also been victimized by this scam. After reviewing a soldier’s social networking site, a scam artist calls the soldier’s grandparents claiming that a problem came up during military leave requiring that money be immediately wired or delivered to an account or location.

- Variations of the grandparent scam include criminals claiming to be family friends or other family relatives.

The Do’s and Don’ts to Avoid Grandparent Scams:

- Don’t succumb to any calls that pressure you to immediately send money.
- Try to contact the grandchild or another family member directly through a phone number you know to be accurate to determine whether or not the call is legitimate.
- Most important, never wire money overseas based on a demand made by phone or e-mail. Once you wire money, you can’t get it back.
Health Care/Insurance Scams

Almost without exception, everyone will need medical care during their lifetime.

Additionally, the overwhelming majority of patients will have some form of private or government provided health insurance.

In fact, the health care system makes up almost 20 percent of the economy of the United States.

With that much money flowing through a complicated health care system, criminals (including those who may appear to be legitimate health care providers) are always creating new scams designed to steal money from anyone and everyone involved in the system.

How much money is involved with Health Care/Insurance Scams?

Well, according to law enforcement experts:

“Health care fraud costs the country tens of billions of dollars a year. It’s a rising threat, with national health care expenditures estimated to exceed $3 trillion in 2014 and spending continuing to outpace inflation.

“Recent cases also show that medical professionals continue, and may be more willing, to risk patient harm in furtherance of their schemes.”

Health Care/Insurance Scams include:

Medical Equipment Scams: Equipment “manufacturers” offer “free” products to individuals. Insurers are then charged for products that were not needed and/or may not have been delivered.

Rolling Lab Scams: Unnecessary and sometimes fake tests are given to individuals at health clubs, retirement homes, or shopping malls and billed to insurance companies or Medicare.

Services Not Performed Scams: Customers or providers bill insurers for services never rendered by changing bills or submitting fake ones.

Medicare Scams: Medicare scams can take the form of any of the health insurance frauds described above. Senior citizens are frequent targets of Medicare scams, especially by medical equipment manufacturers who offer seniors free medical products in exchange for their Medicare numbers. Because a physician has to sign a form certifying that equipment or testing is needed before Medicare pays for it, con artists fake signatures or bribe corrupt doctors to sign the forms. Once a signature is in place,
the manufacturers bill Medicare for merchandise or service that was not needed or was not ordered.

The Do’s and Don’ts to Avoid Health Care/Insurance Scams:

- Never sign blank insurance claim forms.
- Never give blanket authorization to a medical provider to bill for services rendered.
- Ask your medical providers what they will charge and what you will be expected to pay out-of-pocket.
- Carefully review your insurer’s explanation of the benefits statement. Call your insurer and provider if you have questions.
- Do not do business with door-to-door or telephone salespeople who tell you that services or medical equipment are free.
- Give your insurance/Medicare identification only to those who have provided you with medical services.
- Keep accurate records of all health care appointments.
- Know if your physician ordered equipment for you.
Holiday Scams

When the holidays roll around, so do the scam artists and fraudsters. For every holiday we celebrate, scammers are busy creating scams to try to trick folks into downloading malware, spyware and other computer viruses that steal personal and financial information.

Further, scammers try to take advantage of our natural desire to send and receive holiday greeting cards by email – known as eCards – as a means of tricking people into clicking on links in those eCards that contain malicious software.

Specifically, experts warn that whether you shop online or in a store, scammers are looking to hook you.

You may be tempted by great Internet deals, but beware of copycat sites mimicking well-known retailers.

If you do make a lot of online purchases, keep track of what will be delivered to your house.

Package delivery hoaxes are all too common during the holidays – either by phone or email with a malware link.

So when the holidays roll around, be extra vigilant and on the lookout for potential scams that take advantage of festive times of the year.

The Do’s and Don’ts to Avoid Holiday Scams:

- Don’t click on a link from an email or social media site unless you are absolutely sure the message is from a legitimate business.
- Before making a purchase, do an online search for the “vendor name + scam”.
- When shopping at brick-and-mortar stores, use your credit card instead of your debit card for better protection.
- Don’t open eCards if the sender is from someone you don’t know, the URL looks odd, or your name is misspelled.
- Keep your antivirus software up-to-date.
- Look for a confirmation code accompanying the eCard, which usually takes you to the website issuing the card.
- Only deal with organizations and people you know when opening unsolicited emails.
- Don’t provide personal or financial information.
House Stealing Scams

You may be surprised, but there are scams that can involve your home. While not as common as some other scams, it does happen.

According to law enforcement sources, here’s how the House Stealing Scam works.

The scam artists pick the house they’re targeting.

They then commit identity theft by finding the name and personal information (often easily located on the Internet) and using that information to create fake driver’s licenses, social security cards and other forms of “official” identification.

They then obtain standard property transfer forms that are available on the Internet and at many office supply stores.

After forging your signature and using the fake IDs, they file the fraudulently created deeds with the county clerk or other appropriate agency.

Now, on paper, the house “belongs” to the scam artist.

Believe it or not, once they “own” the house, the scam artists can sell it or obtain money through fraudulent financing schemes using the house as collateral.

The following examples of this scam have been reported to law enforcement agencies:

- Scam artists look for a vacant house—typically a vacation home or rental property—and do a little research to find out who owns it. Then, they steal the owner’s identity, go through the same process of transferring the deed, put the empty house on the market, and pocket the profits.
- The crooks steal a house an individual or family is still living in and then find a buyer (often on the Internet) who “buys” the house without the real owner(s) ever knowing. Meanwhile, the real owner(s) are still paying the mortgage for a house they no longer “own.”

In an actual case that was prosecuted, a real estate business owner in Los Angeles, California pled guilty to a scam that defrauded more than 100 homeowners and lenders out of more than $12 million. The real estate agent promised to help homeowners by refinancing their loans. Instead, she and her accomplices used stolen identities and/or paid people for the illegal use of their personal information to purchase the homes. They then pocketed the money they borrowed without ever making any mortgage payments. The actual homeowners lost the title to their homes and the banks who provided the financing lost their money to the scam artists.
The Do’s and Don’ts to Avoid House Stealing Scams:

- First and foremost, always be on the lookout for anything that comes by mail or email that involves your property. Don’t assume it’s just spam. Read it closely for any signs that a transaction involving your home may be underway.
- If you receive a payment book or information from a mortgage company that’s not yours, whether your name is on the envelope or not, don’t just throw it away. Open it, figure out what it says, and follow up with the company that sent it.
- On an annual basis, check all information pertaining to your house through the county office where your deed is recorded. If you see any paperwork you don’t recognize or any signature that is not yours, investigate it.
Investment Scams

Investment Scams are one of the largest categories of scams that victimize Americans every year.

Throughout this guide, there are several individual scam topics that fall under the broader heading of Investment Scams.

Perhaps the best way to develop an understanding of the range of scams that are contained within the broader category of Investment Scams is to look at actual scams that were uncovered as part of Operation Broken Trust, a massive law enforcement operation undertaken a few years ago by law enforcement agencies across the United States.

The following scenarios come directly from the files of Operation Broken Trust. All involved Investment Scams.

$485 Million Dollar Ponzi Scam: Joseph Blimline pleaded guilty for his role in one of North Texas’ largest oil and gas investment Ponzi schemes defrauding 7,700 investors of more than $485 million. Blimline was a majority owner of Provident Royalties, an investment company. Beginning in 2006, Blimline and others involved at Provident Royalties made false representations and failed to disclose other material facts to their investors to induce the investors into providing payments to Provident. The investors were not told that Blimline had received millions of dollars of unsecured loans and had been previously charged with securities fraud. Blimline issued approximately 20 oil and gas offerings, and used a significant amount of the money raised in these offerings to purchase oil and gas assets from earlier offerings and to pay dividends to earlier investors in order to facilitate the scheme. Blimline also pleaded guilty to charges related to a separate, but similar oil and gas scheme based in Michigan that defrauded investors out of $50 million.

FOREX Trading Scam Targeted Members of Christian Faith: Eldon A. Gresham Jr. was indicted on 10 counts of mail fraud in connection with a foreign currency exchange (FOREX) trading scam. Gresham solicited at least 90 individuals to invest in his FOREX trading business, the Gresham Company. Gresham falsely represented to potential investors that he generated consistent returns on investments of up to 10 percent per month. In fact, Gresham was actually losing money on his FOREX trading. Gresham also concealed from investors that he used their investment funds for personal reasons or as payments to earlier investors. Over the life of the scheme, Gresham obtained nearly $15.8 million from unsuspecting victims. Gresham used contacts from the Texas area and beyond to locate investors and targeted members of the Christian faith, who were elderly and particularly vulnerable to Gresham’s inducements. Gresham often told
potential investors that he believed his success in FOREX trading was a blessing and gift from God, and Gresham considered his investment business to be “his ministry.” Gresham also encouraged people to invest by telling them that investors could use their investment gains to “further God’s work.”

**Ponzi Scam Victimizing Elderly Italian Immigrants:** Frank Castaldi operated a Ponzi scheme that resulted in more than $30 million in losses to hundreds of victims, including many elderly Italian immigrants. As part of his scam, Castaldi guaranteed investors that he would pay them annual returns between 10 and 15 percent. He made false representations to most investors about investing their principal in his various businesses, and about the source of the funds that he used to make their interest payments. Castaldi used new investors’ principal payments to make interest payments to other investors, without disclosing the true source of the interest payments. Castaldi also lost investors’ money by funding a failed banquet hall and other failing businesses, and by purchasing stocks.

**Scam Targeted Elderly and Victimized 800 Individuals throughout the U.S. and Canada:** Four individuals pleaded guilty for their roles in A&O entities, a group of businesses that acquired and marketed life settlements to investors. The defendants defrauded investors by making misrepresentations about such things as A&O’s prior success, its size and office locations, its number of employees, the risks of its investment offerings, and its safekeeping and use of investor funds. Their fraud scheme involved more than 800 victims throughout the U.S. and Canada, many of whom were elderly.

**Internet-Based Fraud Targeted the Deaf Community:** The SEC obtained a temporary restraining order and emergency order freezing the assets of Imperia Invest IBC. According to the SEC’s complaint, Imperia solicited investors through the Internet, claiming it would use the investor funds to purchase Traded Endowment Policies (TEPs), the British term for viatical settlements. Imperia falsely promised to pay investors—the majority of whom are members of the deaf community—a guaranteed return of 1.2 percent per day. The SEC alleged that Imperia’s website said that investors could only access their profits by purchasing a Visa debit card from Imperia, but Imperia has no relationship with Visa and was using the Visa name without authorization. Through its website and a series of offshore PayPal style bank accounts, Imperia raised in excess of $7 million from at least 14,000 investors worldwide, including 6,000 investors in the U.S. who have invested in excess of $4 million with Imperia.

**Haitian-Americans Victimized in $14 Million Ponzi/Affinity Scam:** Ronnie E. Bass Jr. was convicted in the Southern District of Florida for his participation in a Ponzi scam. Bass and his coconspirators engaged in a classic affinity scam which sought to exploit the common interests and trusts of a certain group of individuals. Bass and others solicited and targeted members of the Haitian community to invest in Homepals LLC. Homepals offered investments in “unsecured notes” sold by the defendants that promised to
double investor funds in 90 days. Eventually, Homepals could not generate enough investor funds to pay off the existing investors. The scam led to an estimated loss of $14.3 million to 500 victims.

Owners of Trading Company Allegedly Scammed Investors: Craig Karlis and Ahmet Devrim Akyil were charged with wire fraud and tax crimes. The indictment alleges that Karlis and Akyil founded Boston Trading and Research (BTR) and recruited customers to open accounts with BTR to trade in the foreign currency exchange market. Karlis and Akyil allegedly made a series of misrepresentations to customers about how BTR operated and about what they did with customer money. They allegedly diverted millions of dollars from BTR customer accounts to pay BTR's business expenses and their personal expenses, such as houses, cars and jewelry. Karlis and Akyil told customers that BTR employed strategies to reduce risk, when in fact they did not. Eventually, BTR had approximately 1,200 customers and more than $35 million under management.

Oil and Gas Investment Scam Victimizes Blind Man: The SEC filed a lawsuit alleging that Jason A. Halek of Southlake, Texas, and two companies he owns and controls—Halek Energy LLC and CBO Energy Inc.—fraudulently sold investments in Texas oil and gas projects. The complaint alleges that Halek, Halek Energy and CBO Energy raised approximately $22 million from at least 300 investors nationwide by making materially false and misleading statements about the risks of the oil and gas projects, the use of investor funds, and potential returns from the investments. Victims of the scam included a financially unsophisticated 24-year old blind man.

As you can see, there is almost no end to the types of investment scams. As always, if an investment sounds too good to be true, it usually is.

The Do's and Don’ts to Avoid Investment Scams:

- Be suspicious of any investment opportunity that makes exaggerated earnings claims, especially during a short period of time.
- Ask for written information about the investment, such as a prospectus, recent quarterly or annual reports, or an offering memorandum.
- Consult an unbiased third party, like an unconnected broker or licensed financial advisor, before investing.
- Don't be fooled into believing an investment is safe just because someone you know is recommending it. So-called “affinity scams” are one of the favorite methods used to lure people in.
- If you feel you are being pressured into investing, don’t do it.
- Be suspicious of people you meet on social networking sites and in chat rooms, where investment fraud criminals have been known to troll for victims.
- If it sounds too good to be true, it is.
IRS Scams

One of the fastest growing and most nefarious types of scams in recent years are the IRS Scams where the scammer impersonates the IRS.

For example, according to law enforcement sources, in the IRS Telephone Scam the victim receives a phone call in which the caller purports to be an Internal Revenue Service (IRS) representative.

Using intimidation tactics, the caller tries to take control of the situation from the beginning.

The caller advises the victim of the call that the IRS has charges against them and threatens legal action and arrest.

If the victim questions the caller in any way, the caller becomes more aggressive.

The caller continues to intimidate by threatening to confiscate the victim’s property, freeze bank accounts, and have the victim arrested and placed in jail. The alleged charges include defrauding the government, money owed for back taxes, law suits pending against the victim and nonpayment of taxes.

The victims are advised that it will cost thousands of dollars in fees/court costs to resolve this matter. The caller creates a sense of urgency by saying that being arrested can be avoided and fees reduced if the victim purchases moneypak cards to cover the fees within an hour.

Sometimes the caller provides specific instructions on where to purchase the moneypak cards and the amount to put on each card. The caller tells the victim not to tell anyone about the issue and to remain on the telephone until the moneypak cards are purchased and the moneypak codes are provided to the caller.

The caller states that if the call is disconnected for any reason, the victim would be arrested. Some victims have reported that once the caller obtained the moneypak codes, they were advised that the transaction took too long and additional fees were required.

Many victims, who are often immigrants, report that the callers spoke with broken English or stated the caller had an Indian accent.

Another type of IRS Scam is the IRS Refund Scam. The IRS Refund Scam is when an identity thief uses your personal information to file a tax return in your name as a scam to get a tax refund check.
Dan, a victim of this type of IRS Refund Scam reports that this is what happened to him:

“I received a notice from the IRS that my refund could not be direct deposited so my refund would be mailed within the next 4-6 weeks. One problem, though; I have not yet filed my 2013 returns! All the IRS will tell me is that a return has been filed utilizing my name and SSN so I now have to jump through all sorts of hoops and will have to file a paper return, waiting up to 6 months for any refund that might be due me. According to them, this could also affect my future filings.”

Another victim of the IRS Refund Scam, Steve, reports:

“Steve Bryant here…I think I may have come across a new scam or something of a twist on old theme. On March 24, 2014, I received a CP53 Notice from the IRS concerning my 2013 1040. The notice indicates that my refund check will be mailed to me since my financial institution rejected the direct deposit request. The notice was post dated April 7, 2014. The interesting issue here is that I HAVE NOT FILED MY TAXES for 2013 at this point.”

The Do’s and Don’ts to Avoid IRS Telephone and Refund Scams:

- Beware of any individual who calls and claims to be from the IRS or any other government or law enforcement agency.
- Specifically, the IRS does not require specific payment methods such as a moneypak cards or wire transfers.
- Beware of refund notices that don’t correspond precisely with a tax return you filed.
- The IRS would never demand that payment be made immediately or the same day.
- The IRS would never threaten arrest during a first contact phone call.
- If you receive a call from someone purporting to be from the IRS, ask for their name and the specific location they are calling from. Tell the “agent” you will call back on a number that you will independently obtain and verify from a phone directory or web search.
- If you feel you are being threatened or harassed, hang up and call your local police.
Jury Duty Scams

We’ve all had that sinking feeling when we open our mail and find a jury duty summons. While most of us are more than happy to perform one of our civic obligations, by taking time away from our daily routine, it always seems that a jury summons arrives when it will be most inconvenient.

And, truth be told, more than a few of us have tossed the jury duty summons in the trash either intentionally or having mistaken the envelope for junk mail.

That’s why Jury Duty Scams often work.

According to the FBI, here’s how a typical Jury Duty Scam usually unfolds:

“The phone rings, you pick it up, and the caller identifies himself as an officer of the court. He says you failed to report for jury duty and that a warrant is out for your arrest. You say you never received a notice. To clear it up, the caller says he’ll need some information for “verification purposes”—your birth date, social security number, maybe even a credit card number.”

Of course, if the individual was truly from the “court,” they’d already have the information they need to identify you and there would be no reason for you to verify that information.

Further, there is no circumstance that will result in a “court officer” calling you because you didn’t appear in response to a jury duty summons. It just doesn’t happen that way.

Most important, the first rule of avoiding all scams is to never give any personal or biographical information over the phone. That is particularly true in the case of someone calling and saying they are from your local courthouse. If you have any reason to believe they are being truthful, ask them for where they can be located in the courthouse and that you will come see them in person. At that point, a scam artist will usually hang up the phone.

Unfortunately, as law enforcement reports, jury scams have been around for years and they are very effective. Communities across the country have found it necessary to routinely issue public warnings about calls from people impersonating court officials as a means of stealing personal information from unsuspecting citizens. That stolen information is often used for identity theft and other scams that can steal money from your bank account.

Interestingly, it’s the scam’s simplicity may be what makes the jury duty scam so effective. As with a number of other types of scams, the threat of arrest knocks victims off guard and may induce them to provide with some information to defuse the situation.
“They get you scared first,” says a special agent with the FBI. “They get people saying, ‘Oh my gosh! I’m not a criminal. What’s going on?’” That’s when the scammer dangles a solution – a fine, payable by credit card that will clear up the problem.

Plus, with enough information, scammers can assume your identity and empty your bank accounts.

According to the FBI agent, “It seems like a very simple scam.” The trick is putting people on the defensive, then reeling them back in with the promise of a clean slate. “It’s kind of ingenious. It’s social engineering.”

Because the Jury Duty Scam is tried so often by criminals and identity thieves, federal courts have had to issue warnings about the scam. The courts encourage people to call their local court office if they receive suspicious calls. You can even contact the local FBI field office if you suspect a Jury Duty Scam is underway.

Remember, as a rule, court officers will never ask for confidential information over the phone. They will almost always contact prospective jurors by mail.

The Do’s and Don’ts to Avoid Jury Duty Scams:

- First and foremost, always be on the lookout for anything that comes by mail or email that involves jury duty.
- Never give out personal information when you receive an unsolicited phone call.
- If you receive a call from someone claiming to be a “court officer” demanding payment for a missed jury duty summons, tell them you are calling the police and FBI.
- Do contact the police or FBI if you have any questions about a jury duty call.
Letter of Credit Scams

While not as well-known and not as prevalent as other “investment” scams, Letter of Credit Scams can inflict serious financial damage to victims.

In fact, because it is less well-known and relatively rare, it’s all the more important to understand this scam because knowledge is always the best method of avoiding a scam.

According to the experts who investigate and track Letter of Credit Scams:

“Legitimate letters of credit are never sold or offered as investments. They are issued by banks to ensure payment for goods shipped in connection with international trade. Payment on a letter of credit generally requires that the paying bank receive documentation certifying that the goods ordered have been shipped and are en route to their intended destination. Letters of credit frauds are often attempted against banks by providing false documentation to show that goods were shipped when, in fact, no goods or inferior goods were shipped.

“Other letter of credit frauds occur when con artists offer a “letter of credit” or “bank guarantee” as an investment wherein the investor is promised huge interest rates on the order of 100 to 300 percent annually. Such investment “opportunities” simply do not exist.”

This scam is similar to the Prime Bank Note Scam also discussed in this guide.

The Do’s and Don’ts to Avoid Letter of Credit Scams:

- Do not invest or attempt to “purchase” a “letter of credit.” Such investments simply do not exist.
- Do not invest in anything unless you understand the deal. Scammers rely on complex transactions and faulty logic to “explain” fraudulent investment schemes.
- Be wary of any investment that offers the promise of extremely high yields.
- Independently verify the terms of any investment that you intend to make, including the parties involved and the nature of the investment.
- If an “opportunity” appears too good to be true, it probably is.
LinkedIn Support Scams

LinkedIn is one of the most popular social media platforms for connecting professionals and others who are looking to network based on similar job skills and interests.

Unfortunately, because of the fact that millions of people around the world use the service, LinkedIn is also a target for scammers.

According to experts, “scammers are attacking people on LinkedIn with phishing e-mails claiming to be a LinkedIn Tech Support message. In these fake e-mails it is stated that "irregular activities" are happening on your LinkedIn account which require a mandatory security update of your account.”

“Obviously this is all a scam, and the purpose of the emails is to get you to fill out an attached HTML form which is a spoofed LinkedIn login page. What you fill out does not get you logged into the site but it gets sent to the bad guys who then own your account.”

According to experts, in many cases “You can recognize this scam because the email uses a lowercase "i" instead of a capital "I" when spelling “LinkedIn.”

The text of the scam email usually reads something like this (also notice the bad English and grammar which can be a sign of a scam email):

“Due to irregular activities your Linkedin account has been subjected to compulsory security update. Linkedin may sometimes deny logins in cases where we believe the account could have been compromised.”

“To do this we developed a new secure way that keeps your account safe. We have attached a form to this email to complete the process. Please, download the form and follow the instructions on your screen.”

“LinkedIn Support”

The scam email will have an attachment. If you open the attachment and fill it out, you will be potentially be providing the scammers personal and financial information that they can then use for identity theft and other forms of fraud.

The Do’s and Don'ts to Avoid LinkedIn Support Scams:

- Turn on and use LinkedIn’s two-factor authentication security system.
- Keep in mind that reputable companies like LinkedIn don’t request personal information via email.
- If in doubt about a specific email that claims to be from LinkedIn, contact LinkedIn directly. But, don’t use any links or phone numbers contained in the suspect email as that may be fraudulent and direct you to the scammers. Obtain the website or phone number from a source, directory or document you’ve used before.
- Use a phishing filter that most web browsers and email programs have installed or available as plug-ins.
- Never follow a link to a secure site like LinkedIn from an email. Always enter the URL for the website manually or from a previously used and trusted bookmark.
- Stay abreast of the latest scams so you won’t be fooled when you receive a Phishing Scam email like the LinkedIn scam.
Lottery Scams

As a rule of thumb, most scams strike the potential victim as “too good to be true” the moment they learn the details of what is being offered or provided.

That’s how scams work, they appeal to our natural desire to get a great bargain or “something for nothing.”

This is especially true of lottery scams. Especially foreign Lottery Scams.

Take this example:

“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!”

That’s just one example of a seemingly never-ending stream of lottery scams that swamp Americans every day.

It sounds too good to be true because it is. International scam artists use lottery scams like the one above to defraud Americans out of more than $120 million a year.

$120 million per year!

What that means is, sadly, many Americans fall for these Lottery Scams.

So here’s what you need to know.

Federal law prohibits the cross-border sale or purchase of lottery tickets by phone, mail or email. That means, by definition, if you receive an invitation to participate in a lottery from another country – it is illegal. More important, it’s almost definitely a scam.

And if you fall for the scam, the Lottery Scam artists will most likely drain your bank account or steal the money you sent to pay for the tickets, duties, and taxes that they will insist you pay in order to receive your “prize.”

Common Lottery Scams:

- You receive a call, an e-mail, or a letter telling you that you’ve won a large sum of money in a foreign lottery you don’t remember entering. To claim your “winnings,” you’ll have to provide your bank account number so your winnings may be deposited into your account.
- You’re told you’ve won a sizeable lottery and are asked to wire a few thousand dollars to a “customs agent” to cover duties and taxes. But after wiring the money, you’re contacted again and told you must send even more money to collect your prize.
You receive a congratulatory letter in the mail along with a check for $5,000. You’re instructed to cash the check, then wire a portion of the funds to a foreign address to cover taxes and fees, keeping the remaining money as your “lottery winnings.” A few days after doing so, your bank notifies you that the check was counterfeit and you now must repay it the $5,000.

The Do’s and Don’ts to Avoid Lottery Scams:

- Don’t respond to calls, e-mails, or mailings promoting foreign lotteries.
- Remember, foreign lotteries are illegal so any offer is illegitimate and almost definitely a scam.
- If you receive a phone call from someone claiming you’ve won a foreign lottery, just hang up or tell them you will contact the FBI to determine if the lottery is legitimate.
- If you think you or a loved one have become a victim of a lottery scam, contact the FBI or your local police.
Mass Marketing Scams

As with everything else in modern life, Mass Marketing Scams have gone hi-tech.

In one variation of a Mass Marketing Scam, Shirley reports:

“I received a postcard telling me I would be given a necklace worth $50 for FREE and all I would have to do is pay the $8.95 shipping cost. I was to call a phone number to get the information. When I called I was told it was from a jeweler who considered me a good customer and described the necklace as pearl with real red gems on it. I was to give them a credit card # to pay the shipping. This raised a red flag in me. They would accept a check if I gave my check bank number to them, I asked to give the money direct to the jeweler and they wouldn't name the jeweler. So I told them I wasn't interested under those conditions. Then I emailed two jewelers I had purchased some jewelry from: Stauer and Natures Jewelry and asked if they were the ones who made the offer. Both emailed right back and said they never do business that way.”

In other Mass Marketing Scams, instead of just relying on the postal system or telemarketers, scam artists and other criminals can target potential victims across the globe by transmitting spam e-mails by the millions and setting up fraudulent but realistic-looking websites to entice potential victims.

Specifically, according to scam experts, Mass Marketing Scams attempt to trick victims into handing over money or personal information for the promise of future prizes, products, or services that never materialize.

Mass Marketing Scams can encompass a range of scams – some of which are discussed individually in this guide – like:

- Charity Scams
- Credit & Loan Scams
- Foreign Lotteries & Sweepstakes
- Nigerian Letter Scams
- Overpayment Scams

Some scenarios involved in Mass Marketing Scams include:

- Individuals from overseas contact U.S. businesses or individuals and ask them to perform work. The overseas firm overpays the retainer fee via check and asks that the remaining funds be wired back overseas. Almost always, the check is counterfeit.
- In online rental schemes, scammers forward a counterfeit check to the property owner for more than the amount of the rent and then ask for the difference to be
wired back. They also duplicate postings from legitimate online real estate sites and when contacted over e-mail by interested renters, ask the interested party to send money.

- Unsolicited e-mails that are supposedly from the FBI, IRS or other government law enforcement agencies that ask for money or personal information.
- Unsolicited emails asking for help to transfer funds out of a foreign country for a share of the money.

The Do’s and Don’ts to Avoid Mass Marketing Scams:

- Don’t believe everything you are told. If something sounds too good to be true, it probably is.
- Be suspicious of unsolicited offers.
- Avoid being taken by high pressure sales. Take the time to research offers before deciding whether or not to participate.
- Don’t do business with anyone who solicits your money in advance of awarding a prize.
- Inspect all representatives’ credentials carefully.
- Get all offers in writing and keep a copy for your records.
- Don’t deposit checks sent by companies that claim the check is being sent to pay fees or taxes on lottery winnings.
- Never provide personal information over the telephone.
- If you think you’ve been victimized, report the crime to the police of the FBI immediately. That way you’ll have a better chance of getting your money back.
Mystery Shopper Scams

According to scam experts and regulatory agencies that monitor mystery shoppers, some retailers do indeed hire companies to evaluate the quality of service in their stores. And to conduct those evaluations they often use mystery shoppers.

They instruct a mystery shopper to make a particular purchase in a store or restaurant, and then report on the experience.

Typically, the mystery shopper is reimbursed and can keep the product or service.

Sometimes the shopper receives a small payment, as well.

But, while there are legitimate mystery shoppers, there are also Mystery Shopper Scams.

In a Mystery Shopper Scam, dishonest “promoters” use newspaper ads and emails to create the impression that mystery shopping jobs are a gateway to a high-paying job with reputable companies.

They often create websites where you can “register” to become a mystery shopper, but first you have to pay a fee – for information about a certification program, a directory of mystery shopping companies, or a guarantee of a mystery shopping job.

You should know that it's unnecessary to pay anyone to get into the mystery shopper business. The certification offered by the “promoter” is usually worthless.

Lists of companies that hire mystery shoppers are available for free and legitimate mystery shopper jobs are listed on the Internet for free.

Unfortunately, if you fall for a Mystery Shopper Scam and then try to get a refund from the promoters, you will be out of luck.

Either the business won't return your phone calls, or if it does, it’s to try another pitch in an attempt to scam you again.

Also, there is a variation on the Mystery Shopper Scam that is exceptionally dangerous for victims.

In this variation, the victim is hired as a “mystery shopper” and told that their first assignment is to evaluate a money transfer service, like Western Union or MoneyGram.

The shopper receives a check with instructions to deposit it in a personal bank account, withdraw the amount in cash, and wire it to a third party. The check is a fake.
By law, banks must make the funds from deposited checks available within days, but uncovering a fake check can take weeks.

It may seem that the check has cleared and that the money has posted to the victim’s account, but when the check turns out to be a fake, the victim who deposited the check and wired the money will be responsible for paying back the bank.

The Do’s and Don’ts to Avoid Mystery Shopper Scams:

- Be suspicious of advertisements for mystery shoppers in a newspaper’s ‘help wanted’ section or by email.
- Be suspicious of mystery shopper firms that require you to pay for “certification.”
- Be suspicious of anyone who guarantees a job as a mystery shopper.
- Be suspicious of anyone who charges a fee for access to mystery shopping opportunities.
- Be suspicious of anyone who sells directories of companies that hire mystery shoppers.
- Be suspicious of anyone who asks you to deposit a check and wire some or all of the money to someone.
Nigerian Letter Scams

Perhaps the best known and most prolific scam that still victimizes thousands of individuals every year is the Nigerian Letter Scam along with scams originating in other countries that use similar tactics and scenarios.

The letter is often delivered by email.

According to fraud experts, Nigerian Letter Scams combine the threat of Imposter Scams with a variation of an Advance Fee Scam in which a letter mailed or emailed from Nigeria offers the recipient the possibility of sharing in a percentage of millions of dollars that the letter's author – a self-proclaimed government official – is trying to transfer illegally out of Nigeria.

The recipient of the correspondence is encouraged to send information to the author, such as blank letterhead stationery, bank name and account numbers, and other identifying information using a fax number or email account provided in the letter or email.

The scam is dependent on convincing an often willing victim to send money to the author of the letter in Nigeria (or another country) in several installments of increasing amounts for a variety of reasons.

The letters and emails are often long and very detailed. Payment of taxes, bribes to government officials, and legal fees are often discussed at length.

The scam always includes a promise that all expenses will be reimbursed as soon as the funds are spirited out of Nigeria (or another named country).

In reality, the promised funds don’t exist and the victim will eventually end up losing a considerable amount of money.

Additionally, when the victim stops sending money, the scam artists have been known to use the personal information and checks that they received to impersonate the victim, draining bank accounts and credit card balances.

While this type of scam is easily detected and rejected by the majority of individuals who receive these letters and emails, millions of dollars in losses are caused by these scams every year.

Some victims have even been convinced to travel to Nigeria, where they have been imprisoned against their will along with losing large sums of money. The Nigerian government is not sympathetic to victims of these schemes, since the victim actually conspires to remove funds from Nigeria in a manner that is contrary to Nigerian law. So
while the true criminal is the Nigerian (or citizen of another country) conducting the scam, it is the victim who may end up behind bars in a foreign country.

The Do’s and Don’ts to Avoid Nigerian Letter Scams:

- If you receive a letter from Nigeria (or another foreign country) asking you to provide personal or banking information, do not reply in any manner. Contact your local FBI office or the U.S. Secret Service or the U.S. Postal Service.
- Be suspicious of individuals representing themselves as Nigerian or foreign government officials asking for your help in placing large sums of money in overseas bank accounts.
- Do not believe the promise of large sums of money for your cooperation.
- As always, never provide any personal or financial information by mail, email or over the phone.
- If you know someone who is corresponding in one of these schemes, encourage that person to contact the FBI or the U.S. Secret Service as soon as possible. Tragically, this scam victimizes thousands of Americans every year.
Online Auction Scams

With the rapid growth of the Internet and World Wide Web, online auctions have enabled individuals to buy and sell merchandise on a much larger scale than ever before.

But that benefit has also attracted scam artists.

Name the item and it is probably available as part of an online auction. In fact, millions of items are legitimately offered every day by means of online auctions.

Unfortunately, a small by significant number of those items are being offered by scam artists and crooks.

In fact, Online Auction Scams are one of the most frequent complaints to the Internet Crime Complaint Center (IC3).

According to scam and fraud experts, these are some of the most frequent Online Auction Scams:

- **The Overpayment Scam.** A legitimate seller advertises a high-value item – like a car or computer – on the Internet. A scammer contacts the seller to purchase the item, then sends the seller a counterfeit check or money order for an amount greater than the price of the item. The purchaser asks the seller to deposit the payment, deduct the actual sale price, and then return the difference to the purchaser.

- **The Wire Transfer Scam.** This scam begins with fraudulent and misleading ads for the sale of high-value items being posted on well-known online auction sites. When victims contact the “seller,” they are instructed to wire money to the “seller” (in reality the scammers) using a money transfer company. Once the money is provided, the buyer is unable to contact the “seller.”

- **The Second-Chance Scam.** This scam involves scammers offering losing bidders of legitimate online auctions the chance to buy the item they wanted at a reduced price. The scammer then requires the buyer (victim) to send payment through money transfer companies. Once again, the “seller” is never heard from again and there is no delivery of the purchased item.

While Online Auction Scams are usually conducted by individual criminals, there is evidence that organized criminal syndicates operating from West Africa are involved in Overpayment Scams that are often a part of Online Auction Scams. Similarly, Romanian crime syndicates have been implicated in second-chance scams.
The Do’s and Don’ts to Avoid Online Auction Scams:

- Ask the seller for a phone number and verify it.
- Beware of buyers who insist on wire transfers as the only form of payment they’ll accept.
- For big-ticket items, use a legitimate online escrow service that will hold the payment until you receive what you’ve ordered.
- If you receive an overpayment as a seller, don’t cash it but instead ask for the exact purchase price. The overpayment check is probably counterfeit.
- Don’t ever give out your social security or driver’s license number—a legitimate seller wouldn’t ask.
- Be skeptical if the price sounds too low.
- As always, if it sounds too good to be true, it is.
Online Automobile Auction Scams

While they can be considered a subset of Online Auction Scams, Online Automobile Auction Scams are so prolific and so financially devastating to the victim, they merit individual attention.

Every year, victims lose millions of dollars to Online Automobile Auction Scams.

According to scam experts, here is how a basic Online Automobile Auction Scam works. Remember, there can be variations of this basic version of the scam.

A potential car buyer finds a vehicle they like for what seems like a below-market price on a legitimate auction website. The buyer contacts the “seller” (the scammer), usually through an e-mail address in the ad, to indicate interest in the vehicle. The seller responds via e-mail, often with a hard-luck story about why they want to sell the vehicle and at such a good price.

In the e-mail, the “seller” asks the buyer to transfer the transaction a different company’s website – purportedly for security reasons – and then offers a buyer protection plan in the name of a major Internet company like eBay. Through the new website, the buyer receives an invoice and is instructed to wire the funds for the vehicle to an account number that is provided by the “seller.” To add the sense of legitimacy, the scammers may pose as company representatives in a live chat to answer questions from the buyer.

Once the funds are wired, the buyer may be asked by the “seller” to fax a receipt to show that the transaction has taken place. And then the “seller” and buyer agree upon a time and place for the delivery of the vehicle.

Unfortunately for the buyer, the ad the buyer responded to is a scam that is either a completely fraudulent ad or was duplicated from another website. The buyer is asked to move from a legitimate website to a spoofed (fraudulent) website, where it’s easier for the scammer to carry out the scam. The buyer protection plan offered as part of the deal is a fraud and is part of the scam. Once the buyer send the “seller” proof of the transaction, the scammers know they’ve successfully stolen the buyer’s money.

By the time the buyer realizes he’s been scammed, the crooks and the money are nowhere to be found.

The Do’s and Don’ts to Avoid Online Automobile Auction Scams:

- Be suspicious of cars that are advertised at too-good-to-be true prices.
• Be suspicious of sellers who want to move transactions from the original website to another website.
• Be suspicious of sellers who claim the buyer’s protection program offered by a major Internet company (like eBay) covers an automobile transaction conducted outside that company’s website.
• Be suspicious of sellers who refuse to meet in person or allow potential buyers to inspect the car ahead of time.
• Be suspicious of sellers who say they want to sell the car because they’re in the U.S. military and are about to be deployed, are moving, the car belonged to someone who recently died, or a similar story.
• Be suspicious of sellers who ask for funds to be wired ahead of time.
Online Dating Scams

Depending on when you came of age, you might be surprised to learn that millions of Americans use online dating websites every year. In fact, whether you know it or not, it’s a safe bet that you have friends or even family members who’ve done so – even if they never mentioned it to you.

And, truth be told, many folks who use online dating websites have had wonderful experiences. A growing number even find a mate and marry. So, there are many wonderful success stories.

But, as with all relationships where emotion can lead us astray, online dating websites attract scam artists looking for easy prey.

According to experts, these scammers are often criminals living overseas who falsely claim that they are Americans working or traveling outside of the country.

Often, they target women over the age of 40 who are divorced or widowed.

Still, it’s important to understand that men and women of all ages have been victims of Online Dating Scams – sometimes with tragic outcomes like the loss of large amounts of money.

Authorities who’ve studied Online Dating Scams say that a typical scam works like this:

The victim is contacted online by a prospective “date” who pretends to be attracted to the victim. The “dates” online profile has pictures and a description or profile that seems real enough.

The victim and prospective “date” begin corresponding and an emotional connection begins to be established. The victim may even receive gifts from this person who is slowly becoming a love interest.

And then it happens. This new love interest asks for money.

The alarm bells should sound, but some victims fall prey to the scam and start sending money because they want believe they have found someone with whom they can be in love.

The requests for money, based on a range of reasons that sound dire, keep coming.

By the time the victim realizes they’ve been scammed – usually because they can no longer reach their new love interest – it’s too late. The money is gone and will never be recovered because the victim doesn’t really know who they were dealing with and the money may have been sent out of the country.

[61]
As part of the scam, everything the victim believes to be true is actually false.

The pictures that were sent to the victim are fakes – often copied from other websites. The online dating profile is also bogus and is often created to specifically attract the victim based on the victim’s personal likes and dislikes located on their profile.

The Do’s and Don’ts to Avoid Online Dating Scams:

- Be suspicious if someone you’ve just connected with on an online dating site immediately claims they have fallen in love with you.
- Be suspicious if you receive a photograph from your prospective “date” that looks like a professional photograph from a magazine or website.
- Be suspicious if the prospective “date” asks for money for any of a variety of reasons including, but not limited to, travel, medical emergencies, hotel bills, or because they’ve been a victim of crime.
- Don’t ever provide money to a “prospective “date.”
- Be suspicious if a prospective date claims to be traveling or working overseas and is therefore unavailable to meet – but still makes demands of you.
- Be suspicious if the prospective “date” plans to meet you but then cancels because of an “emergency.”
- Use reputable and well-known online dating sites. Don’t be scammed into communicating away from the website until you’ve had plenty of time to get to know your prospective date.
Online Rental Housing Scams

With the growth of online real estate websites, Online Rental Housing Scams are becoming very common.

According to scam experts and law enforcement sources, the scam often works like this:

You can’t believe your good fortune – you locate a rental home in a nice area through a Craigslist classified ad (or some other online site advertising rental properties) at an unbelievably low rate. The landlord – who had to leave the country and travel to Nigeria (or any other country or location that makes the landlord “unavailable” to meet you at the property) – asks that you wire him two months’ rent. You arrive at what you believe will be your new home on the agreed-upon date, but there’s a problem – the house is not actually for rent and its owners know nothing about your agreement.

You’ve just fallen prey to the Online Rental Housing Scam.

If this seems similar to the Nigerian Letter Scam, it is. In fact, some experts believe that this scam originated from Nigeria. But no matter where it originated, in recent years it has tricked many folks looking to secure rental housing – especially when they need to move quickly or a significant distance.

According to authorities, here’s how the Online Rental Housing Scam works.

The scammers research websites like Craigslist that list homes for sale or rent. They take the info in those ads, duplicate it and post it with their own email address in an ad on Craigslist (or other online site advertising rental properties) in the housing rentals category. To make the ad more attractive, the homes are usually posted with below-market rental rates.

An interested renter contacts the “homeowner” via email. The “owner” makes excuses about having to be outside of the United States on an emergency or because of work in a foreign country. The prospective renter is then told to wire money (usually enough to cover two months of rent) overseas. Once the money is wired, it is almost impossible to get it back and the renter will never hear from the “homeowner” again.

To add insult to injury, prospective renters are often instructed to fill out credit applications that include questions for credit, bank and employment history along with social security numbers. The scammers then use this information for identity theft.

In a worst case scenario, the prospective tenant now has nowhere to live and is also a victim of identity theft which can make using credit cards and bank accounts difficult – at least for a period of time.
As you can see, Rental Housing Scams can inflict a lot of damage on an unsuspecting victim.

The Do’s and Don’ts to Avoid Online Rental Housing Scams:

- Only deal with landlords or renters who are local.
- Be suspicious if you’re asked to only use a wire transfer service.
- Beware of e-mail correspondence from the “landlord” that’s written in poor or broken English.
- Research the average rental rates in that area and be suspicious if the rate is significantly lower.
- Don’t give out personal information, like social security, bank account, or credit card numbers.
Phishing Scams

There are many varieties of Phishing Scams and several of the more prevalent varieties are discussed throughout this guide.

But at their core, all Phishing Scams work in a similar fashion because, as defined, Phishing is an email (or other method of communication) scam method in which the scammer sends out legitimate-looking email in an attempt to gather personal and financial information from victims.

In a typical Phishing Scam, the victim gets an email that looks like it's from their bank or another trusted business or financial institution. However, the email is really a way to scam the victim into providing personal and financial information such as PINs, social security numbers, credit card information, and account numbers.

For example, Rich was almost a victim of Phishing Scams where the crooks were impersonating Bank of America. According to Rich:

“I received email from Bank of America a few days ago requesting information because my Bank of America Visa Card may have been compromised by someone. It stated, if I don’t fill out the information my charge card would be cancelled as of a date. The information they wanted was my name, date of birth and password. No mistakes on the email, it was very professional, looked official, the logo was 100% and no misspelled words. I called Bank of America and they told me they never send for information, as they have it all and they never threaten to cancel someone’s account. I sent a copy to Bank of America fraud office. I’m in my seventies which I know they go for. I have received a few of these over the years. I went from four charge cards to one and always check my account on the computer. Only got hit once and this is when the wife was on a cruise ship. It had to have been done from the ship. I found the fraud on my home computer and notified Bank of America. They wanted to cancel the card right then, but I talked to the person in charge and they allowed to keep the card active until the wife hit the states in three days. The wife called me when she arrived and I immediately cancelled the card. Maybe it is a good idea to have two cards in case you have to cancel one of them.”

In another actual case of an organized Phishing Scam that law enforcement authorities investigated, scammers working primarily out of Romania - known as the “suppliers” - went “phishing” and obtained thousands of credit and debit card accounts and related personal information by sending out masses of spam phishing emails.

The “suppliers” then sent the stolen data to their partners in the U.S. - so-called “cashiers” - through Internet chat and email messages.
By using some readily available software and technologies, the cashiers manufactured their own credit, debit, and gift cards encoded with the stolen information, giving them unfettered access to large amounts of money via ATMs and point-of-sale terminals.

Before these cards were used, “cashiers” directed “runners” to test the cards by checking balances or withdrawing small amounts of money from ATMs. Then, these “cashable” cards were used on the most lucrative accounts.

Once the “cashable” cards were used to obtain cash, the “cashiers” wired a percentage of the stolen money back to the “suppliers.”

There in a nutshell, illustrated by an actual Phishing Scam, is a real-world demonstration of how an innocent looking email that a victim believes is from their bank or other reputable company can be the first step in a Phishing Scam that eventually drains money from the victim’s bank and credit card accounts.

Every year, billions of dollars are lost to scammers conducting Phishing Scams.

And, every year the Phishing Scams become more and more sophisticated by using better crafted and more official looking emails that direct the victims to better crafted and better looking (but phony) websites designed to replicate the websites of the businesses and financial institutions being impersonated.

The Do’s and Don’ts to Avoid Phishing Scams:

- Keep in mind that reputable companies, banks, agencies, and other firms don’t request personal information via email.
- If in doubt about a specific email, call the sending institution but don’t use the phone number contained in the email as that may be fraudulent and direct you to the scammers. Obtain the phone number from a source, directory or document you’ve used before.
- Use a phishing filter that most web browsers and email programs have installed or available as plug-ins.
- Never follow a link to a secure site from an email. Always enter the URL for the website manually or from a previously used and trusted bookmark.
- Stay abreast of the latest scams so you won’t be fooled when you receive a Phishing Scam email.
Ponzi Scams

This scam is named after its creator, the infamous Charles Ponzi. In the early 1900s, Ponzi created a scam guaranteeing “investors” (actually, victims) a 50 percent return on their investment.

Although Ponzi paid the initial investor victims, the scam collapsed when he was unable to pay later investor victims.

According to the experts who investigate and prosecute Ponzi Scams, the scam almost always promises high financial returns or dividends not available through traditional investments.

The scam is the fact that instead of actually investing the funds of victims, the scammer pays “dividends” to initial investor victims using the funds of subsequent investor victims.

The scheme almost always collapses when the scammer takes off with the money after enough new investor victims can’t be enrolled in the scam so that the scammer can continue to pay the fraudulent “dividends.”

Here's how an actual Ponzi scam of recent vintage worked according to the FBI.

“He was living the high life - taking up residence in a Miami Beach mansion worth more than $5 million, cruising around in a million-dollar yacht and his leased Mercedes-Benz, shelling out more than $400,000 for floor seats at Miami Heat basketball games, and donating thousands of dollars to the athletic program of a local university (the school was so appreciative it named a student athlete lounge after him).

“But it all came crashing down on Florida businessman Nevin Shapiro, when he was charged with orchestrating a multi-million-dollar Ponzi scheme involving about 60 victims throughout the United States.”

Over a period of four years, “Shapiro raised more than $880 million from his investors. These individuals thought they were investing in his wholesale grocery distribution business - Capitol Investments, a Florida corporation with offices in Miami Beach that Shapiro owned and ran as CEO.”

“In reality, there was no grocery distribution business. Shapiro allegedly used new investor money to fund principal and interest payments to existing investors - a textbook Ponzi scheme - while at the same time, taking tens of millions of dollars for his own use.”
How did he pull it off? By using fake documents and other scam tactics, including:

- Financial statements claiming that the business generated millions of dollars in annual sales.
- Shapiro’s personal and business tax returns (also fraudulent).
- Phony invoices revealing transactions that Shapiro’s business had supposedly entered into with other businesses.
- Promissory notes reflecting the amount of the victims' investment, along with a schedule for a payment of interest (at anywhere from 10 to 26 percent on an annual basis) and the return of their principal.

Of course, as with all Ponzi scams, the fraud eventually imploded and defrauded investors out of at least $80 million.

The Do’s and Don’ts to Avoid Ponzi Scams:

- Be careful of any investment opportunity that makes exaggerated earnings claims.
- Exercise due diligence in selecting investments and the people with whom you invest. Do your own research.
- Consult an unbiased third party - like an unconnected broker or licensed financial advisor - before investing.
Prime Bank Note Scams

While not as well-known as other “investment” scams, Prime Bank Note Scams can inflict serious financial damage to victims.

In fact, because it is less well-known, it’s all the more important to understand this scam because knowledge is always the best method of avoiding a scam.

According to the experts who track Prime Bank Note Scams:

“International fraud artists have invented an investment scheme that supposedly offers extremely high yields in a relatively short period of time. In this scheme, they claim to have access to “bank guarantees” that they can buy at a discount and sell at a premium. By reselling the “bank guarantees” several times, they claim to be able to produce exceptional returns on investment. For example, if $10 million worth of “bank guarantees” can be sold at a two percent profit on 10 separate occasions—or “tranches”—the seller would receive a 20 percent profit. Such a scheme is often referred to as a “roll program.”

“To make their schemes more enticing, con artists often refer to the “guarantees” as being issued by the world’s “prime banks,” hence the term “prime bank guarantees.” Other official sounding terms are also used, such as “prime bank notes” and “prime bank debentures.” Legal documents associated with such schemes often require the victim to enter into non-disclosure and non-circumvention agreements, offer returns on investment in “a year and a day”, and claim to use forms required by the International Chamber of Commerce (ICC). In fact, the ICC has issued a warning to all potential investors that no such investments exist.

“The purpose of these frauds is generally to encourage the victim to send money to a foreign bank, where it is eventually transferred to an off-shore account in the control of the con artist. From there, the victim’s money is used for the perpetrator’s personal expenses or is laundered in an effort to make it disappear.

“While foreign banks use instruments called “bank guarantees” in the same manner that U.S. banks use letters of credit to insure payment for goods in international trade, such bank guarantees are never traded or sold on any kind of market.”

The Do’s and Don’ts to Avoid Prime Bank Note Scams:
Think before you invest in anything. Be wary of an investment in any scheme, referred to as a “roll program,” that offers unusually high yields by buying and selling anything issued by “prime banks.”

As with any investment, perform due diligence. Independently verify the identity of the people involved, the veracity of the deal, and the existence of the security in which you plan to invest.

Be suspicious of business deals that require non-disclosure or non-circumvention agreements that are designed to prevent you from independently verifying information about the investment.
Pump-and-Dump Stock Scams

You may have heard about Pump-and-Dump Stock Scams in the news or seen one of these scams as part of the plot in a film about organized crime.

But do you really know how a Pump-and-Dump Stock Scam works well enough to avoid falling for the scam?

According to scam experts and law enforcement authorities, a Pump-and-Dump Stock Scam typically begins with a glowing press release about a company. The release will trumpet the financial health of the company or some new product or innovation the company has created.

At the same time, emails, newsletters, and “experts” that supposedly offer unbiased recommendations start touting the company as the latest “hot” stock. Messages in chat rooms and bulletin board postings may urge you to buy the stock quickly or to sell before the price goes down. Or you may even hear the company mentioned by a radio or TV analyst.

Unsuspecting investors start purchasing large amounts of the stock, pumping up the price. Once the price has been pumped up, the scammers sell their shares (dump) at the peak and immediately stop hyping the stock. The price of the stock craters and the innocent investors lose their money.

In an actual case that law enforcement code named “Operation Shore Shells”:

“The ringleaders created shell companies whose penny stock (worth less than $5 a share) was traded on the OTC Bulletin Board (not on the more widely known New York Stock Exchange or NASDAQ). They secretly issued most of the shares for themselves in fictitious names, then touted their companies’ stock through false statements in press releases, electronic bulletin board postings, online newsletters, and the like.

“Often using their retirement funds, unsuspecting investors purchased the highly-touted stock - or their unscrupulous financial advisors did so without their knowledge - driving or “pumping” up the price. Then, the fraudsters “dumped,” or sold, their stock for thousands or millions of dollars, causing the stock to plummet and innocent investors to lose their shirts.”

The victims of “Operation Shore Shells” included:

- A doctor from a prestigious hospital who began suffering from severe depression and couldn’t work after learning of the scam.
- A husband and wife who had both developed dementia during the investigation.
A man suffering from multiple sclerosis whose stockbroker had liquidated his pension and IRA and left him nearly penniless.

A victim who not only invested her savings and her pension, but also took out a second mortgage to invest more. She lost everything.

As you can see, Pump-and-Dump Stock Scams can have devastating consequences.

The Do’s and Don’ts to Avoid Pump-and-Dump Stock Scams:

- Don’t believe the hype about any one stock.
- Find out where the stock trades.
- Independently verify claims about the stock.
- Thoroughly research the opportunity of any one stock.
- Beware of high-pressure pitches.
- Take your time.
- Always be skeptical of claims about any one stock.
- Be suspicious of any investment opportunity that makes exaggerated earnings claims.
- Exercise due diligence in selecting investments and the people with whom you invest.
- Consult an unbiased third party - like a licensed financial advisor - before investing.
Pyramid Scams

Very similar to the Ponzi Scams discussed in an earlier chapter, Pyramid Scams rely on the money collected from newer victims of the scam to pay earlier victims to provide an air of legitimacy.

The big difference between a Pyramid Scam and a Ponzi Scam is that in a Pyramid Scam the victims themselves are incentivized to recruit further victims through the payment of commissions.

That’s how the “Pyramid” is constructed.

More specifically, according to scam experts, Pyramid Scams - also referred to as franchise fraud or chain referral schemes - are marketing and investment frauds in which an individual is offered a distributorship or franchise to market a particular product.

The real profit is earned, not by the sale of the product, but by the sale of new distributorships.

Emphasis on selling franchises rather than the product eventually leads to a point where the supply of potential investors is exhausted and the pyramid collapses.

At the heart of each Pyramid Scam is a representation that new participants can recoup their original investments by inducing two or more prospects to make the same investment.

Promoters of Pyramid Scams fail to tell prospective participants that this is mathematically impossible for everyone to do, since some participants drop out, while others recoup their original investments and then drop out.

According to the experts who investigate and prosecute Pyramid Scams, the scam almost always promises high financial returns or dividends not available through traditional investments.

Pyramid Scams collapse when the scammer takes off with the bulk of the money after enough new investor victims can’t be enrolled in the scam so that the scammer can continue to pay the fraudulent “commissions.”

The Do’s and Don’ts to Avoid Pyramid Scams:
- Be suspicious of “opportunities” to invest your money in franchises or investments that require you to bring in subsequent investors to increase your profit or recoup your initial investment.
- Be suspicious of any investment opportunity that makes exaggerated earnings claims.
- Independently verify the legitimacy of any franchise or investment before you invest.
- Exercise due diligence in selecting investments and the people with whom you invest. Do your own research.
- Consult an unbiased third party - like a licensed financial advisor - before investing.
Ransomware Scams

Just like Scareware Scams discussed later in this guide, Ransomware Scams are quickly becoming one of the most widespread and damaging types of cyberscams being perpetrated against computer users.

What is a Ransomware Scam?

Ransomware Scams are conducted by means of an especially vicious form of malware (malicious software) that locks up the victim’s computer and cannot be unlocked until a fee – the ransom – is paid.

Unlike many viruses which activate when users open a file or attachment, some variants of ransomware can install itself when victims simply go to a compromised website.

Once infected, the victim’s computer immediately locks, and the monitor displays a screen message stating that the computer is locked (for any of a variety of fraudulent reasons, including impersonating law enforcement authorities) and that a “fee” or “fine” will have to be paid before the computer can be used again.

Payment arrangements for the ransom often involve using prepaid money card services, money wiring services and other difficult to trace payment methods that make the odds of every recovering the ransom almost nonexistent.

Additionally, many Ransomware Scams are conducted from overseas which further complicates investigation and prosecution by law enforcement.

Some variants of ransomware are almost impossible to uninstall, even by the best computer professionals.

Here’s how one victim of a Ransomware Scam that impersonates the FBI reported what happened:

“While browsing the Internet, a window popped up with no way to close it,” one Reveton (ransomware) victim recently wrote to the IC3. “The window was labeled ‘FBI’ and said I was in violation of one of the following: illegal use of downloaded media, under-age porn viewing, or computer-use negligence. It listed fines and penalties for each and directed me to pay $200 via a MoneyPak order. Instructions were given on how to load the card and make the payment. The page said if the demands were not met, criminal charges would be filed and my computer would remain locked on that screen.”

Of course, this was a Ransomware Scam and the FBI had no role in locking up the computer.
Once the victim pay the “fine,” the money is lost forever and the computer may still be inoperable.

In other Ransomware Scams, the computer is unlocked after payment of the ransom. But, malware that steals the victim’s personal and financial information may still be hidden on the computer.

The Do’s and Don’ts to Avoid Ransomware Scams:

- Ransomware pop-ups are usually impossible to close and rebooting the computer will have no effect.
- As a rule of thumb, never click on any link in a pop-up window. By clicking on the link, you may install the ransomware or other forms of malware.
- Make sure your computer is using legitimate, up-to-date antivirus software, which can help detect and remove fraudulent Scareware scams.
- Do not pay any money or provide any personal information if you become a victim of ransomware.
- Contact a computer professional to remove the ransomware from your computer.
- Be aware that even if you are able to unfreeze your computer on your own, the malware involved with the ransomware may still operate in the background.
- Certain types of malware associated with ransomware have been known to capture personal information such as user names, passwords, and credit card numbers through embedded keystroke logging programs.
Redemption/Strawman/Bond Scams

While not common, the Redemption/Strawman/Bond Scams are designed to attract individuals who mistrust the federal government and these scams can inflict serious financial damage to victims.

According to the experts who investigate and track Redemption/Strawman/Bond Scams:

“Proponents of this scheme claim that the U.S. government or the Treasury Department control bank accounts - often referred to as “U.S. Treasury Direct Accounts” - for all U.S. citizens that can be accessed by submitting paperwork with state and federal authorities.

“Individuals promoting this scam frequently cite various discredited legal theories and may refer to the scheme as “Redemption,” “Strawman,” or “Acceptance for Value.”

“Trainers and websites will often charge large fees for “kits” that teach individuals how to perpetrate this scheme.

“They will often imply that others have had great success in discharging debt and purchasing merchandise such as cars and homes.

“Failures to implement the scheme successfully are attributed to individuals not following instructions in a specific order or not filing paperwork at correct times.

“This scheme predominately uses fraudulent financial documents that appear to be legitimate.

“These documents are frequently referred to as “bills of exchange,” “promissory bonds,” “indemnity bonds,” “offset bonds,” “sight drafts,” or “comptrollers warrants.”

“In addition, other official documents are used outside of their intended purpose, like IRS forms 1099, 1099-OID, and 8300.

“This scheme frequently intermingles legal and pseudo legal terminology in order to appear lawful.

“Notaries may be used in an attempt to make the fraud appear legitimate.

“Often, victims of the scheme are instructed to address their paperwork to the U.S. Secretary of the Treasury.”
The Do’s and Don’ts to Avoid Redemption/Strawman/Bond Scams:

- Do not believe that the U.S. Treasury controls bank accounts for all citizens.
- Be suspicious of individuals or groups selling kits that they claim will inform you about how to access secret bank accounts.
- Be suspicious of individuals or groups proclaiming that paying federal and/or state income tax is not necessary.
- Be suspicious of individuals advocating that speeding tickets, summons, bills, tax notifications, or similar documents can be resolved by writing “acceptance for value” on them.
- If what you’re told seems too good to be true, it probably is.
Scareware Scams

According to scam experts and law enforcement sources, one of the most widespread types of cyber scam being perpetrated against consumers these days involves “scareware” - those pop-up messages you see on your computer saying you’ve got a virus and all you have to do to get rid of it is buy the antivirus software being advertised.

But, what is a Scareware Scam?

Scareware Scams involve malicious software that poses as legitimate computer security software and claims to detect a variety of threats on your computer that do not actually exist.

Victims are informed in popup messages that they must purchase the security software being offered as part of the Scareware Scam in order to repair their computers. Often, when the victims try to close the Scareware Scam popup, they are barraged with aggressive and disruptive notifications of computer viruses until they give in and supply their credit card number to pay a fee that can be in the hundreds of dollars for the worthless Scareware Scam product.

In reality, the victim’s credit card number has just been stolen and will be sold to or used by other scammers and criminals.

Here are a few examples of actual Scareware Scams as provided by law enforcement sources.

The FBI’s Seattle office began looking into a Scareware Scam, later attributed to a group based in Kyiv, Ukraine, that ultimately claimed an estimated 960,000 victims who lost a total of $72 million.

Investigators discovered a variety of ruses used to infect computers with scareware, including consumers being directed to webpages featuring fake computer scans that instead downloaded malicious software.

In another operation, The FBI’s Minneapolis office initiated an investigation into an international criminal group using online advertising to spread its scareware product, a tactic known as “malvertising.”

According to a U.S. federal indictment, two individuals in Latvia were charged with creating a phony advertising agency and claiming to represent a hotel chain that wanted to purchase online advertising space on a Minneapolis newspaper’s website.
After the ad was verified by the paper and posted, the defendants changed the ad's computer code so that visitors to the site became infected with a malicious software program that launched scareware on their computers.

That scheme resulted in losses of about $2 million to its victims.

The Do’s and Don’ts to Avoid Scareware Scams:

- Scareware pop-ups may look like actual warnings from your system, but upon closer inspection, some elements aren’t fully functional. For instance, to appear authentic, you may see a list of reputable icons—like software companies or security publications—but you can’t click through to go to those actual sites.
- Scareware pop-ups are hard to close, even after clicking on the “Close” or “X” button.
- Fake antivirus products are designed to appear legitimate, with names such as Virus Shield, Antivirus, or VirusRemover.
- As a rule of thumb, never click on any link in a pop-up. If you believe it is legitimate, close the pop-up and go to the antivirus product website directly via a bookmark you already have or by obtaining the web address from a reputable search engine like Google.
- Make sure your computer is using legitimate, up-to-date antivirus software, which can help detect and remove fraudulent Scareware scams.
Senior Citizen Scams

Talk to your friends and family and you’ll find that almost everyone knows someone over the age of 65 who got scammed.

Talk to sources in law enforcement and you’ll find that senior citizens are the most targeted group when it comes to scams.

In fact, if scams against senior citizens were a medical condition, it would be declared an epidemic.

After all, the population of senior citizens in the United States is growing by the day.

Baby boomers (born between 1946 and 1964) are now the largest segment of our population. That means the number of senior citizens is rising. Many younger boomers also have considerable computer skills, so criminals are modifying their targeting techniques—using not only traditional telephone calls and mass mailings but also online scams like phishing and email spamming.

According to scam experts and law enforcement authorities, scammers target senior citizens because:

- Many senior citizens have a “nest egg.”
- Senior citizens are less likely to report a fraud because they don’t know where to go or they’re too embarrassed to talk about it.
- If they do report the crime, it’s sometimes hard for them to remember exact details.
- Many of the products/services being hawked by scammers appeal to individuals of a certain age—i.e., anti-aging and other health care products, health care services, and investments related to retirement savings.

Some of the scams targeting senior citizens most frequently include (all covered as individual topics in this guide):

- Identity theft accomplished through “dumpster diving,” phishing, address changes, and old-fashioned theft.
- Health insurance frauds (medical equipment, “rolling lab” scams, Medicare scams, counterfeit prescription drugs).
- Home repair scams.
- Foreign lottery/sweepstakes scams.
- Advance fee/credit card scams.
- Investment scams.
- Charity scams.
And even more horrific are “Recovery Scams” that target senior citizens who have already been victimized by convincing them that their money has been recovered by law enforcement or government officials and they must pay a fee to get it back.

The Do’s and Don’ts to Avoid Senior Citizen Scams:

- Shred credit card receipts and old bank statements.
- Close unused credit card or bank accounts.
- Don’t give out personal information via the phone, mail, or Internet unless you initiated the contact.
- Never respond to an offer you don’t understand.
- Talk over investments with a trusted friend, family member, or financial advisor.
- Require all plans and purchases to be in writing.
- Don’t pay in advance for services.
Shared Community Scams

While the name is a bit awkward and the scam is fairly new, Shared Community Scams are very real.

According to scam experts at the FTC, they are getting reports from diverse communities across the country “about ways scammers are using language, shared customs, relationships and community practices to steal people’s money.”

The FTC reports:

“Scammers might speak your language, share your culture or beliefs, and even attend your place of worship. They might understand the hard personal situations you’re facing – like job loss, immigration status, money woes, or family emergencies. They might come from the same country, neighborhood, or community as you. They might even be a community leader – or have convinced a community leader to help them get the word out about their product or service... which may turn out to be a scam.”

In other words, as with many situations involving fraud, the scammers try to find what they may have in common with a victim and use that commonality or shared community aspect to establish trust with a potential victim.

It’s a shameless tactic but, unfortunately, it often works because it preys on people’s natural affinity to work and do business with those who are most like they are and who share common traits or struggles.

Here are a few scenarios the FTC has observed:

- You get a call from someone who speaks the same language you do, selling you a work-at-home program. You feel comfortable with them, so you share personal information and stories. Before you know it, this feels like someone you can trust. But this could be a set-up. Scammers often use personal connections to make you feel comfortable – and get close enough to get your money.

- You identify with an ad on TV or radio featuring someone who looks or sounds like you. Because you identify with the person in the ad, you might believe what they’re saying. But not every ad is true. It could have been made, and paid for, by a scammer. Ads aren’t reviewed by an outside organization to make sure they’re legitimate before they run. You have to do your own research.

- Someone claiming to be a lawyer or government official tells you about a debt you need to pay, or asks you to buy something. In your community, highly-educated people, officials, and experts might command a lot of respect. But are
they really the experts they claim to be? Check out their claims before you give them information or money.

The Do’s and Don’ts to Avoid Shared Community Scams:

- Be suspicious of anyone who attempts to convince you to purchase a product or service simply because you have a shared personal trait or community aspect.
- Be suspicious of anyone who says you must pay for something immediately based on the authority they claim to have.
- Take your time and research any claims of payments that must be made immediately.
- Ask questions and do your own research on any company that approaches you and insists that you take immediate action or make an immediate payment.
- Don’t provide your personal or financial information to anyone online or over the phone.
Smishing Scams

There are so many scams, at times new words are needed to accurately describe unique types of scams. That is true of Smishing Scams.

Smishing Scams are scams that are conducted, in part, by using SMS text messaging technology.

And if you already understand how Phishing Scams work, you may be correctly guessing - based on the similarity of the words - that Smishing and Phishing are related. Later in this guide you'll learn about yet another related scam called vishing.

Smishing is just another twist on the older scam of phishing. As you may recall, phishing usually involves an e-mail that claims to be from your bank or credit card company (or a range of other financial institutions or businesses) asking you to update your account information and passwords by clicking on a link to what appears to be a legitimate website. In fact, that link will either be used to steal your personal and/or financial information or to plant malware on your computer.

Smishing is very similar to phishing. According to experts, here’s an example of how a typical Smishing Scam might happen:

You receive a text message on your cell phone saying there’s a problem with your bank account. You’re given a phone number to call or a website to log into and asked to provide personal identifiable information—like a bank account number, PIN, or credit card number—to fix the problem.

But, in reality, it could be a Smishing Scam and crooks could be attempting to collect your personal information in order to help themselves to your money. While most cyber scams target your computer, Smishing Scams target your mobile phone, and they’re becoming a growing threat as a growing number of Americans own mobile phones and use SMS text messaging technology on a regular basis.

Here’s how Smishing works:

Scammers set up an automated dialing system to text people in a particular region or area code (or sometimes they use stolen customer phone numbers from banks or credit unions). The victims receive messages like: “There’s a problem with your account,” or “Your ATM card needs to be reactivated,” and are directed to a phone number or go to a website asking for personal information. Armed with that information, the crooks can steal from the victims’ bank accounts, charge purchases on their charge cards, create a phony ATM card or conduct other crimes.
Sometimes, if a victim logs onto one of the phony websites with a smartphone, they could also end up downloading malicious software that could give the scammers access to anything on the phone. With the growth of mobile banking and the ability to conduct financial transactions online, Smishing Scams are becoming even more attractive and lucrative for crooks.

Law enforcement authorities report that actual Smishing Scams have included:

- Account holders at a specific credit union, after receiving a text about an account problem, called the phone number in the text, gave out their personal information, and had money withdrawn from their bank accounts within 10 minutes of their calls.
- Customers at a bank received a text saying they needed to reactivate their ATM card. Some called the phone number in the text and were prompted to provide their ATM card number, PIN, and expiration date. Thousands of fraudulent withdrawals followed.

As you can see, Smishing can have serious financial implications very quickly and on a large scale.

Remember, there can be many variations of Smishing Scams – so you need to be alert!

The Do’s and Don’ts to Avoid Smishing Scams:

- Be suspicious of any SMS text message or email seeking personal or financial information.
- Don’t respond to text messages or automated voice messages from unknown or blocked numbers on your mobile phone.
- Never give out personal or financial information over the phone or by email.
- No reputable business or financial institution will ever ask you to provide personal or financial information or account numbers over the phone or by email.
- If you do believe a SMS text message that you believe is legitimate, call the bank or business back using the customer service number provided when you opened the account or that you have on existing account related documents.
- Treat your mobile phone like you would your computer. Don’t download anything unless you trust the source.
- Never click on links or attachments contained within unsolicited SMS text messages. If you want to go to a merchant’s website, type the URL directly into your browser’s address bar.
Social Security Card Scams

No matter what your position is on the subject, law enforcement officials and scam experts agree that illegal immigration has resulted in an increase in identity theft and other related identity crimes and scams.

One major category of identity-related scams involves Social Security Card Scams.

According to law enforcement officials, Social Security Card Scams are “used by illegal aliens to get jobs as well as to apply for citizenship and residency-related benefits.” Additionally, the scams support “other crimes—and criminals—like credit and bank fraud, tax fraud, identity theft, and pharmaceutical diversion.”

For a better understanding of how Social Security Card Scams operate and how damaging they can be, here’s a recent case as outlined by federal law enforcement right after the arrests. Notice the other types of documents, in addition to Social Security cards, that are involved in these scams.

“According to indictments filed in U.S. District Court in Los Angeles and unsealed today, investigators have identified several false document manufacturing networks in the MacArthur Park section of Los Angeles and elsewhere. One of the main targets of the investigation is Alejandro Morales Serrano, who allegedly manufactures raw materials that are then used to manufacture false documents on a large scale from California and other states, including Nevada, Oregon, Texas, Illinois, and Michigan. The false documents generated by the rings included United States Permanent Resident cards, Social Security cards, Mexican Consular Identification cards, and driver’s licenses. The indictment alleges the Serrano and other co-conspirators support the manufacture of false driver’s licenses for approximately 40 of the 50 states and within Mexico. …

“Serrano and his co-conspirators allegedly supply other manufacturers of false documents with hundreds of document-making implements, including sheets of plastic laminates bearing false authentication features. These features replicate legitimate ones used by the United States and Mexican governments to limit fraud. The investigation revealed that the plastic laminates, and other document-making implements supplied by Serrano and others over several years have been used to manufacture thousands of false documents. The indictment alleges that Serrano has been intercepted on a wiretap discussing the fact that he has been engaged in the false document business for more than a decade. …

“Evidence developed during the investigation revealed that the fraudulent documents were utilized by illegal aliens to gain employment, as well as other citizenship and residency related benefits. In addition, the operation supported a variety of criminal
activity, in that the false documents were instrumental in the commission of credit and bank fraud, tax fraud, identity theft, and pharmaceutical diversion schemes.

“The indictments allege that the Serrano false document manufacturing ring produced raw materials for the manufacture of thousands of documents per month that were distributed in California and across the United States.”

Remember. That is just one indictment involving one group conducting this scam and many other related crimes.

These scams take place every day across the country.

The Do’s and Don’ts to Avoid Social Security Card Scams:

- If you have any question about the validity or legitimacy of a Social Security card or number presented to you as an employer, contact local, state or federal authorities who can direct you on how to verify the document or information.
- Similarly, if you have any question about the validity or legitimacy of any other “official” documentation (passport, driver’s license, military or student identification card, etc.) presented to you as an employer, contact local, state or federal authorities who can direct you on how to verify the document or information.
Soldier Love Scams

It’s often hard to decide which types of scams are the worst. But the Soldier Love Scam would certainly be near the top of the list. After all, it takes a heartless or sick scammer to impersonate someone valiantly serving overseas in the military.

But according to law enforcement experts that is exactly what is happening.

For example, an Oregon newspaper recently reported:

“Oregon Attorney General Ellen Rosenblum has a warning for people looking for love online: That soldier who’s been professing devotion via email may actually be a con artist looking for cash.

“Local police departments are reporting more complaints about what is being called “The Soldier Scam” in which Internet scammers posing as romantically minded members of the U.S. military are conning people out of millions of dollars, including a Hillsboro woman who recently lost more than $750,000, said Jeff Manning, spokesman for the Oregon Department of Justice.

“Attorney General Rosenblum advises Oregonians to always maintain a healthy skepticism. The anonymity of the Internet means that you cannot be sure of the real name, age, marital status, nationality or even gender of your new “heartthrob.”

“The con artists are often from foreign countries using untraceable email addresses. Once these “soldiers” make a connection, they begin asking for money for transportation, medical bills, cell phone and Internet charges — even the cost of a wedding.

“They route accounts through numerous locations and use pay-per-hour Internet cyber cafes, which makes finding the scammer and recovering the money extremely difficult.”

So be careful. Soldier Love Scams take place every day across the country – not just in Oregon.

The Do’s and Don’ts to Avoid Soldier Love Scams:

- Do not wire money to someone you have not met in person. Be wary of warp-speed proclamations of love, particularly if they are accompanied by requests for cash.
- Be suspicious if you never get to actually speak with the person on the phone or are told he or she will not receive letters in the mail. Legitimate servicemen and women serving overseas will often have an APO or FPO in their mailing address.
- Do not send money or packages to a third party or company, especially to parties or companies in an African country.
Spear Phishing Scams

You already know about Phishing Scams from an earlier chapter. But there are more refined Phishing Scams that target specific individuals, groups or customers.

These are called Spear Phishing Scams.

Here’s a common example from the files of law enforcement:

Customers of a telecommunications firm received an email explaining a problem with their latest order. They were asked to go to the company website, via a link in the email, to provide personal information—like their birthdates and Social Security numbers. But both the email and the website were bogus.

Those who clicked on the link and provided their personal information became victims of Spear Phishing.

As experts warn, Spear Phishing scammers don’t waste time sending out random fraudulent emails like a regular phishing email scam. Instead, spear phishers target select groups of people with something in common—they work at the same company, bank at the same financial institution, attend the same college, order merchandise from the same website, etc. The emails are ostensibly sent from organizations or individuals the potential victims would normally get emails from, making them even more deceptive and more likely to succeed.

According to experts, here’s how the typical Spear Phishing Scam works.

First, the scammers need inside information on their targets to convince them the emails are legitimate. They obtain this information by hacking into an organization’s computer network (which is what happened in the above case) or sometimes by combing through other websites, blogs, and social networking sites.

Second, they send emails that look like the real thing to targeted victims, offering all sorts of urgent and legitimate-sounding explanations as to why they need your personal data.

Finally, the victims are asked to click on a link inside the email that takes them to a phony but realistic-looking website, where they are asked to provide passwords, account numbers, user IDs, access codes, PINs, etc.

Once criminals have your personal data, they can access your bank account, use your credit cards, and create a whole new identity using your information.
Spear phishing can also trick you into downloading malicious codes or malware after you click on a link embedded in the email...an especially useful tool in crimes like economic espionage where sensitive internal communications can be accessed and trade secrets stolen. Malware can also hijack your computer, and hijacked computers can be organized into enormous networks called botnets that can be used for denial of service attacks.

As you can see, Spear Phishing Scams can create a lot of damage and, unfortunately, people fall for these scams every day as the scams and emails become more and more sophisticated.

The Do’s and Don’ts to Avoid Spear Phishing Scams:

- Keep in mind that reputable companies, banks, agencies, and other firms don’t request personal information via email.
- If in doubt about a specific email, call the sending institution but don’t use the phone number contained in the email as that may be fraudulent and direct you to the scammers. Obtain the phone number from a source, directory or document you’ve used before.
- Use a phishing filter that most web browsers and email programs have installed or available as plug-ins.
- Never follow a link to a secure site from an email. Always enter the URL for the website manually or from a previously used and trusted bookmark.
- Stay abreast of the latest scams so you won’t be fooled when you receive a spear phishing email.
Sports Memorabilia Scams

The United States is a country that loves sports and, for that reason, many Americans trade, sell and collect sports memorabilia.

In fact, the sports memorabilia market is huge.

Scammers know that and are on the prowl to take advantage of the unwary.

In fact, in just one federal investigation of a Sports Memorabilia Scam – code named Operation Bullpen – the following results were obtained:

- There were 63 criminal charges and convictions.
- There was $15,253,000 in economic loss prevented in the seizure of tens of thousands of pieces of forged memorabilia through 75 search warrants and over 100 undercover evidence purchases.
- There were seizures in excess of exceeding $4.9 million, including 5 homes, cash, bank/investment accounts, jewelry, a Ferrari, a boat, and a Harley Davidson motorcycle.
- There were 18 forgery rings dismantled.
- There was over $300,000.00 in restitution paid to over 1,000 victims.

According to law enforcement sources:

In Operation Bullpen, the San Diego Division of the FBI conducted well over 1,000 consensually recorded audio and video tapes. During the consensually recorded conversations, numerous co-conspirators made incriminating statements which illuminated the nature and common practices involved with sports memorabilia fraud.

For example, one of the conspirators liked to joke to the undercover agent how Mickey Mantle still has one arm out of the grave signing autographs. Other conspirators were noting how Wilt Chamberlin was still available for signing long after his death.

In a second phase of Operation Bullpen, the FBI expanded the investigation from predominantly Southern California to a nationwide investigation.

During this phase, a multitude of undercover scenarios were instituted to focus on celebrity forgeries in addition to sports forgeries. In this phase, over 2000 consensual recordings were made. Conspirators bragged how their forgeries were better than those of other forgers that they knew. One conspirator claimed if he went to trial, he would testify he actually becomes Babe Ruth. He then joked he could also say he becomes Jackie Robinson and then said he would turn Black (he was Caucasian) for the jury.
Additionally, the second phase was also an investigation in ‘cyber space’. The industry, as a whole, has moved in this direction where individual collectors can now easily sell pieces. The forgers unfortunately led the way, realizing the anonymity that the Internet provided for dealing their forgeries.

The second phase also convicted numerous Internet auction site sellers, who generated millions of dollars in sales.

The subjects convicted of selling celebrity memorabilia in this phase of the investigation had all used the story line that their celebrity signed pictures and posters were obtained by ‘runners’.

Runners are people who happen to catch a celebrity at an event and obtain a signed picture there. Most of the convicted subjects obtained one or two signatures in this manner and then simply forged many more, claiming they were from the meeting.

All of the convicted subjects noted that it was impossible to make a living as a runner. The amount of time needed to get the couple of signatures a person needs, does not generate an adequate income.

The overwhelming number of celebrity signed photographs and posters being sold throughout the world are sold under this pretense; investigations suggest they are almost all forged by scammers.

The Do’s and Don’ts to Avoid Sports Memorabilia Scams:

- Try to get the signatures in-person either at an event where they’re performing or at an event where they’re signing.
- Buy from companies that get witnessed-based signings and that document the authenticity. Major League Baseball, for example, has a program that uses certified accountants as the witnessing agent with tamper-proof holograms affixed to items that are uniquely numbered and tracked in a database. Many companies offer this program, be sure to ask.
- If the above options are not possible, aggressively question the seller about the exact history of the item you want to buy. Be sure you are completely comfortable that you are dealing with an honest broker.
- Always obtain a money back guarantee in writing and a receipt.
- Get your items evaluated by professional authenticators – not the bogus authenticators that forgers set up to hide behind. Even independent, legitimate authenticators can be fooled from time to time, but they are your best bet to keep from being cheated.
- If the price is too good to be true, it is probably a forgery.
- All of the above applies to celebrity memorabilia as well.
Staged Auto Accident Scams

It’s a safe bet that as long as there have been automobiles and automobile insurance, there have been crooks looking to conduct scams to get their hands on insurance payouts.

One of those ways is the Staged Auto Accident Scam. Unfortunately, it’s a fairly common scam and one you may have heard about or read about in the newspaper.

According to experts, here’s a typical scenario.

You’re stuck in heavy traffic on a busy highway. Another vehicle cuts off the driver of the car in front of you, forcing him to slam on the brakes. You try to stop, but there’s no time and you rear-end the car in front of you.

Unbeknownst to you, you may have just been made the victim of a Staged Auto Accident Scam. It may have even been conducted an organized criminal gang.

Staged Auto Accident Scams have a huge financial impact on everyone who has car insurance. Staged accidents cost the insurance industry about $20 billion a year. Those losses get passed on to all of us in the form of higher insurance rates—an average of $100-$300 extra per car per year.

According to experts, in the above example of a staged accident, everyone in the car you rear-ended – often four or more people – will file fraudulent injury claims with your automobile insurance company. Each of the “victims” will complain of whiplash or other injuries that are difficult for doctors to confirm.

In fact, if operating as part of an organized ring, they will go to dishonest physical therapists, lawyers, and auto repair shops to further enhance their insurance claims.

Insurance scam experts have learned of other variations of Staged Auto Accident Scams, including:

- **The drive down.** You’re attempting to merge when another driver waves you forward. Instead of letting you in, he slams into your car. When the police arrive, he denies ever motioning to you.
- **The sideswipe.** As you round a corner at a busy intersection with multiple turn lanes, you drift slightly into the lane next to you. The car in that lane steps on the gas and sideswipes you.
- **The t-bone.** You’re crossing an intersection when a car coming from a side street accelerates and hits your car. When the police arrive, the driver and several planted “witnesses” claim that you ran a red light or stop sign.
As you can see, the possibilities when it comes to Staged Auto Accident Scams are almost endless.

The Do’s and Don’ts to Avoid Staged Auto Accident Scams:

- If you’re in an accident, call the police immediately.
- Report accident claims to your insurance company.
- Never settle at the scene of the accident for cash.
- Be careful with your personal information, it may be used for identity theft.
- If you can, photograph the car and passengers and write down names, addresses, and phone numbers.
- Only use medical, car repair, and legal professionals you know and trust.
Surrogacy Scams

To understand what a Surrogacy Scam is, consider this recent case straight from the files of law enforcement.

Three women recently pled guilty in San Diego, admitting to taking part in a scheme to illegally create an inventory of babies to sell to unwitting would-be parents for fees of between $100,000 and $150,000 each.

The three took advantage of couples who desperately wanted children, offering them seemingly legitimate surrogacy situations. They also took advantage of women recruited as “gestational carriers” to carry pregnancies to term after having embryos transferred to their uteruses.

The defendants in this case included two lawyers who specialized in reproductive law: Theresa Erickson, a well-known California attorney, and Hilary Neiman, who operated an adoption/surrogacy agency in Maryland. The third conspirator was Carla Chambers of Nevada, who served as the “surrogacy facilitator.” Together, they circumvented surrogacy regulations that say contracts between surrogates and intended parents must be executed before a pregnancy occurs, and lied to surrogates, intended parents, and the California family court.

Surrogacy Scams are as despicable as they sound because Surrogacy Scams are so emotionally gut wrenching for victims because of their desperate desire to have children. They can also victimize the “gestational carrier” who may be misled about her role in the scam.

According to law enforcement experts, the actual Surrogacy Scam referenced above was conducted in a manner that is illustrative of how many surrogacy exams work.

According to those experts, here’s what happened.

Chambers admitted visiting adoption/surrogacy-themed online chat rooms and forums in search of surrogates and parents. Erickson and Neiman also used their own sterling reputations to legitimize the scheme.

Surrogates were made to travel to Ukraine in Eastern Europe to become implanted with embryos derived from anonymous donors—Chambers usually made all the arrangements—with the promise that they would be compensated by the intended parents. The women were led to believe that they were participating in legal surrogacy arrangements and that there was a waiting list of potential parents for the babies. They also had to agree to give birth in California.
They were promised quick matches with intended parents, but the co-conspirators usually waited until the second or even third trimester of the pregnancies before seeking parents. Neiman and Erickson then drafted contracts between the surrogates and intended parents, well after the time frame required by law.

The hopeful couples were told the unborn babies were the result of legitimate surrogacy arrangements, but the original intended parents had backed out. They were offered the opportunity to “assume” the non-existent surrogacy agreement. The parents would hand over between $100,000 and $150,000 to the defendants, but less than half of that went to the surrogate—Erickson, Neiman, and Chambers pocketed the rest.

The scammers typically used the Internet to recruit, solicit, and communicate with surrogates and intended parents. Most of the surrogates and parents lived outside of California.

One of the most critical aspects of the scheme involved Erickson filing fraudulent documents in California court stating that a surrogacy agreement had been in place from the start and asking for what’s called a “pre-birth judgment” that would establish parental rights. That way, under California law, the names of the intended parents could be placed on the birth certificate when the baby was born.

The scam was uncovered when one of the surrogates, nearly seven months pregnant, was worried that parents hadn’t been found for the baby she was carrying. She contacted a lawyer, who then contacted the FBI’s San Diego office.

Again, this scam takes advantage of good people who are seeking to adopt a child and may not be aware of surrogacy laws and the scams that seek to circumvent the law.

The Do’s and Don’ts to Avoid Surrogacy Scams:

- Do your due diligence to find out the average costs of surrogacy services (there should be no “facilitator” fees).
- Make sure you have a signed agreement in place before the start of any medical tests or procedures.
- Be leery if you’re offered a last-minute surrogacy arrangement and are told the original intended parents changed their minds (that rarely happens).
- If at all possible, work with a local attorney or agency that you can meet with in person.
- Ask lots of questions about the process, about financial arrangements, about the surrogates or biological parents. Keep asking questions until you’re completely satisfied.
- If you still don’t feel quite right about it, find another attorney or agency that you are comfortable with.
Tech Support Scams

Perhaps the best way to learn how the Tech Support Scam works is to read the following interview of an actual scammer. This particular crook from India hides behind the name “Alan Smith” and he specializes in credit card fraud using the Tech Support Scam.

Asked to describe the scam and how he gets the personal information of victims, “Alan” walked us through a typical scam telephone call.

“We call normal citizen who have computers at their home and say: ‘My name is Alan and I am calling you from the technical department of CEF org that provides technical support to the windows operating system. The reason of my call is to make you aware of some corrupted application files and online threats that has been created online in order to damage computers, corrupt computers and many people in your locality have been complaining us about this kind of issue......so we are calling you to check if you have the same infections running onto your computer or not....so are you there in front of your computer right now?’

If the victim answers, “Yes,” Alan says:

“When you see all the icons of your desktop please let me know...now look at the left bottom corner you have start...give a single left click on start and you will get an option called computer...give a single right click on computer...you will get some drop down options...open explore, search, manage...give a single click on manage and you will get a pop up called computer management...just below computer management you will see an option called EVENT VIEWER give a double left click on event viewer and you will get some drop down options like application, security, system, Internet explorer...now you need to give a click on application and something will come on the right hand side like information...you need to scroll that page very slowly and in case you come across any errors or warnings let me know.”

Because almost all computers will have a list of errors and/or warnings, “Alan” then “explains” (falsely) what that means, stating:

“The errors and warnings are the infections that has been created by the hackers and that has been crashing down computers...many people in U.S. and U.K. have lost their vital information and banking details because of this particular reason only...Now this infections are very powerful and harmful and they can damage your computer at any moment...what they do is, they slowly and gradually get into the security of the computer...once the security gets corrupted then the computer can crash in no time...
So you need to get rid of these problems ASAP…and you do not have to worry because we will be helping you out.”

Once “Alan” has convinced the victim that the computer has been hacked, he offers to fix it, stating:

“Now I will get you connected to the technical department wherein the certified techs will be taking care of your computer.”

At this point, “Alan” described how he takes control of the victim’s computer:

“So we take control of the computer by using Aammy (software) or any remote desktop support tool. Then we open up the task manager and show them that their window is expired and they have malware and virus installed in the computer…Then we give options to the customer to choose different kind of plans we offer like $99 one time clean-up, $199 one year service, $299 lifetime service plan.”

As soon as the victim agrees to buy the Technical Support plan to fix their computer, “Alan” moves in to steal the victim’s personal and financial information.

“We open a payment page for the customer and ask them to pay to us, so we move further…while the customer is filling the payment page we are taking screenshot of all the information they fill up… We are done once the “payment” is made. We ask the customer to leave their computer ON for an hour so our technician can work on it…After this we charge the [victim’s credit] card as many place we can and take the money out.”

At this point “Alan” and other Tech Support Scam crooks have all they need to use the victim’s information and credit cards to steal.

The Do’s and Don’ts to Avoid Tech Support Scams:

- Never provide your personal or financial information over the phone if you didn’t initiate the call.
- Microsoft, Apple and all other computer companies do not telephone customers and tell them they have a hacked computer or virus.
- Never allow anyone to install remote viewing software on your computer unless you initiated the call and are absolutely certain who you are dealing with.
- Never click on links at websites you are directed to by someone who calls you on the phone.
Telemarketing Scams

Telemarketing Scams typically involve offers of free prizes, low-cost products, or inexpensive vacations in exchange for providing personal information and/or an upfront “processing and delivery” fee. These scams often target individuals over the age of 60. Specifically, older women who live alone are frequent targets for scams selling fraudulent products and services by telephone.

Warning Signs of Telemarketing Scams:

Telemarketing offers that include the following statements are often scams.

- “You must act immediately.”
- “This is a limited offer.”
- “You’ve won a free gift, vacation, or prize.” But you have to pay for “postage and handling,” “processing and delivery” or other fees and charges.
- “You must send money, provide a credit card or bank account number, or provide a check to a courier who will come to your home.”
- “You don’t need to check out the company with anyone.” The callers will try to convince you not to mention the offer to anyone, including your family, lawyer, accountant, or consumer protection agencies.
- “You don’t need anything in writing because we have a track record of success.”
- “You can’t afford to miss out on this offer. It will never be offered again.”

The Do’s and Don’ts to Avoid Telemarketing Scams:

Here are some points to keep in mind before buying a product or service by phone – particularly if the “salesperson” initiates the call.

- Don’t buy from a company you’ve never heard of before.
- If the business is legitimate, they won’t pressure you and will provide any information you request.
- Always request written material about any product, service or charity. Do nothing else until you’ve received the written materials you requested. Even then, remember that just because an offer is in writing doesn’t make it legitimate.
- Perform a background check of any company with a consumer protection agency, Better Business Bureau, state attorney general, or the National Fraud Information Center. Still, remember that not every illegitimate business will be known to consumer protection organizations.
- Obtain identifying information about the “salesperson” including name, phone number, physical location and mailing addresses, and business license numbers. Verify the accuracy of this information before conducting any transaction.
- Don’t pay in advance for services. Payment should only be provided after the service is completed to your satisfaction.
- Don’t agree to pay a courier sent to your home. You will have no record who you paid or where they are located.
- Legitimate businesses won’t pressure you to make an immediate decision. Take your time and discuss the offer with someone you trust.
- Don’t pay fees or taxes for a “free prize.”
- Don’t provide financial information over the phone if you didn’t initiate the call.
- Always discuss any investment offered by a telephone “salesperson” with a financial advisor or family member.
- If you don’t understand every aspect of a sales offer, don’t accept the offer.
- Never send money or provide credit card numbers, bank account numbers, social security numbers or any other personal or financial information to companies you don’t recognize or have a pre-existing relationship with.
- If you do become the victim of a scam, be aware that other scammers may call offering to help. Do not accept any offers of help made by phone.
- If you do become a victim or suspect a call as being a scam, call the police.

Remember: If you have any doubt at all, contact a consumer protection agency, the Better Business Bureau, your state attorney general’s consumer protection division, the National Fraud Information Center, or your local police. Any reputable company will be happy to wait for your business and will not try to convince you not to speak to others about their business.
Telephone Denial of Service Scams

While almost everyone has heard of denial of service computer attacks that hackers use to knock websites offline, very few people have heard of the Telephone Denial of Service Scam.

And unless you’ve seen a Telephone Denial of Service Scam that’s underway, it’s hard to imagine how outrageous the scam can be.

According to law enforcement sources, here’s how a typical Telephone Denial of Service Scam unfolds.

Imagine that you’re getting hundreds or thousands of calls on your home, business, or cell phone, tying up the lines. And when you answer, you hear anything from dead air to recorded messages, advertisements, or even phone sex menus.

While you’re wondering what’s causing what you believe to be an extremely annoying and inconvenient glitch in your phone service, it could actually be a sign that you’re being victimized by a Telephone Denial of Service Scam.

And, most important, the Telephone Denial of Service Scam could be targeting your bank account.

The scammers use automated dialing programs and multiple phone accounts to overwhelm the phone lines of an unsuspecting victim.

In reality, the blizzard of phone calls are just a smokescreen. While the victim’s phone lines are jammed, the scammers impersonate the victim and gain access to the victim’s bank and other financial accounts.

According to the FBI, here’s how it works:

- Weeks or months before the phone calls start, a criminal uses social engineering tactics or malware to elicit personal information from a victim that this person’s bank or financial institution would have—like account numbers and passwords. Perhaps the victim responded to a bogus e-mail phishing for information, inadvertently gave out sensitive information during a phone call, or put too much personal information on social networking sites that are trolled by criminals.
- Using technology, the criminal ties up the victim’s various phone lines.
- Then, the criminal either contacts the financial institution pretending to be the victim or pilfers the victim’s online bank accounts using fraudulent transactions. Normally, the institution calls to verify the transactions, but of course they can’t get through to the victim over the phone.
If the transactions aren’t made, the criminals sometimes re-contact the financial institution as the victim and ask for it to be done. Or they add their own phone number to victims’ accounts and just wait for the bank to call.

By the time the victim or the financial institution realizes what happens, it’s too late.

In an actual case from Florida, a dentist lost $400,000 from his retirement account after a denial-of-service scam on his phones.

The Do’s and Don’ts to Avoid Phone Denial of Service Scams:

- Never give out personal information to an unsolicited phone caller or via email.
- Change online banking and automated telephone system passwords frequently.
- Check your financial account balances often.
- Protect your computers with the latest virus protection and security software.
- If you think you may have been targeted by a telephone denial-of-service scam, contact your financial institution, telephone provider and the police.
Timeshare Scams

A timeshare typically involves joint ownership of a resort property. Depending on how the timeshare is structured, a single property or unit can have up to 52 owners - one for each week of the year. The timeshare is usually managed by the resort where it is located.

According to law enforcement authorities, Timeshare Scams are a growing problem. Because of the Great Recession, a significant number of timeshare owners decided they could no longer afford their timeshare property.

Scammers know this and try to take advantage of the timeshare owner’s desire to sell their timeshare because of the financial stress they may be experiencing.

According to experts, in a typical Timeshare Scam, the scammers telephone or email timeshare owners who, in many instances, advertised their desire to sell in newsletters and on websites.

These scammers, posing as timeshare resellers, promise a quick sale, often within 60-90 days. Some victims report that the “sales representatives” pressured them into a quick decision by claiming they had a ready buyer on the other line or in their office who wanted to buy their timeshare immediately.

Timeshare owners who agree to sell are then told they have to pay an upfront fee - anywhere from a few hundred to a few thousand dollars - to cover various costs such as advertising or closing fees. In many cases, victims provide credit card numbers to pay the fees.

While the timeshare owner thinks they’ve sold their timeshare, in reality they’ve been scammed.

When the victim tries to contact the “reseller” to determine why the sale hasn’t been finalized, their phone calls and email go unanswered because the scammers have moved on to new victims and scams.

The Do’s and Don’ts to Avoid Timeshare Scams:

- Don’t agree to anything on the phone or online until you’ve had a chance to check out the reseller.
- Research the reseller by contacting the Better Business Bureau, your state’s attorney general’s office, and/or local consumer protection agencies where the reseller is located.
- Demand that the salesperson provide all information in writing.
- Be sure the reseller’s agents are licensed to sell real estate where your timeshare is located.
- Verify licensing with the state’s real estate commission.
- Get references.
- Ask how the reseller will advertise and promote the timeshare unit. Will you get progress reports? How often?
- Ask about fees and timing. It’s preferable to do business with a reseller that takes its fee after the timeshare is sold. If you must pay a fee in advance, get all refund policies and promises in writing.
- If you want an idea of the current value of the timeshare, consider using a licensed timeshare appraisal service.
- Before you sign any sort of contract, make sure you get the details of its terms and conditions, including the services the reseller will perform; the fees, commissions, and other costs you must pay and when you must pay them; whether you can rent or sell the timeshare on your own at the same time the reseller is trying to sell your unit; the length or term of the contract to sell your timeshare; and who is responsible for documenting and closing the sale.
- If the deal seems too good to be true, it probably is.
Vishing Scams

There are so many scams, at times new words are needed just to accurately describe unique types of scams. This is true of Vishing Scams.

Vishing Scams are scams that are conducted, in part, by using Voice over Internet Protocol (VoIP) technology.

And if you already understand how Phishing Scams work, you may be guessing - based on the similarity of the words - that Vishing and Phishing are related.

In fact, Vishing is just a new twist on the older scam of phishing. As you may recall, phishing usually involves an e-mail that claims to be from your bank or credit card company (or a range of other financial institutions or businesses) asking you to update your account information and passwords by clicking on a link to what appears to be a legitimate website. In fact, that link will either be used to steal your personal and/or financial information or to plant malware on your computer.

Vishing is very similar to phishing. But, for the professional scammer, vishing has advantages over phishing.

VoIP service is inexpensive (often free) which makes it easy and attractive to crooks looking to place scam calls. And, because VoIP uses the Internet, scammers can use software to create an unlimited number of fake “customer service” lines.

Even more nefarious, vishers can mask the number they are calling from, making Caller ID useless. In fact, vishers can make the phone number of your banking institution (or any other phone number) appear on your Caller ID, so that when you look at Caller ID you think it is your bank.

According to scam experts, here are several Vishing Scams.

- You receive an email that claims to be from one of your financial service providers or a company with whom you routinely do business. The email directs you to call a provided “customer service” phone number to update your account information. Once you call the “customer service” number (in actuality a VoIP account, not a real financial institution) you are led through a series of voice-prompts that ask for account numbers, passwords, and other critical information. You’ve just been vished!
- You receive a phone call. The call may from a “live” person or a recorded message stating that you need to take immediate action to protect your financial, consumer or business account information. The “customer service representative” (actually a visher) may already have some personal information
of yours, like your consumer account or credit card numbers. By using that information, the scammer (who is untraceable because of VoIP) may lure you into a false sense of security and you provide the additional information the scammer is looking to steal from you as part of identity theft. You’ve just been vished!

Remember, there can be many variations of Vishing Scams – so you need to be alert.

The Do’s and Don’ts to Avoid Vishing Scams:

- Be suspicious of any phone call or email seeking personal or financial information.
- Never give out personal or financial information over the phone or by email.
- No reputable business or financial institution will ever ask you to provide personal or financial information or account numbers over the phone or by email.
- If you do believe a phone call is legitimate, hang up and call the bank or business back using the customer service number provided when you opened the account or that you have on existing account related documents.
Work at Home Scams

When economic times are difficult, Work at Home Scams pop up like weeds. As with all scams, it’s important to be suspicious of any offer that promises fast and easy money for little work.

The Most Common Work at Home Scams Include:

- **Mystery Shopper Scam** – You receive a large check and are instructed to deposit the check into your bank account. You’re then told to withdraw money from your account and go shop a local store. You’re told to keep a small amount of the money for your “work,” but you must mail or wire the remainder of the money to the individual who “hired” you as a mystery shopper. Of course, the check you deposited was counterfeit or stolen and once your bank determines the check is worthless you are responsible for the money that has been lost by the bank.

- **Pyramid Scams** – You’re hired as a “distributor” and shell out big bucks for promotional materials and product inventories with little value (like get-rich quick pamphlets). You’re promised money for recruiting more distributors, so you talk friends and family into participating. The scheme grows exponentially but then falls apart—the only ones who make a profit are the criminals who started it.

- **Unwitting Criminal Activity Scams** – Criminals - often located overseas - use unwitting victims to advance their operations, steal and launder money, and maintain anonymity. For example, they may “hire” you as a U.S.-based agent to receive and re-ship checks, merchandise, and solicitations to other potential victims…without you realizing it’s all a ruse that leaves no trail back to the crooks.

- **Advance Fee Scams** – In one version, you’re told that starting a home-based business is easy. You’re told that all you need to do is invest a few hundred dollars in inventory, set-up, and training materials. Of course, if and when the materials do come, they are totally worthless…and you’re stuck with the bill (These are so prolific, we discuss them separately under the heading Advance Fee Scams)

The Do’s and Don’ts to Avoid Work at Home Scams:

- Contact the Better Business Bureau to determine the legitimacy of the company.
- Be suspicious if money is required up front for instructions or products.
- Don’t provide personal information when first interacting with your prospective employer.
- Do your own research into legitimate work at home opportunities using resources that are available at most local libraries.
- Ask questions of potential employers. Legitimate companies will have answers for you and will not rush you in providing those answers.