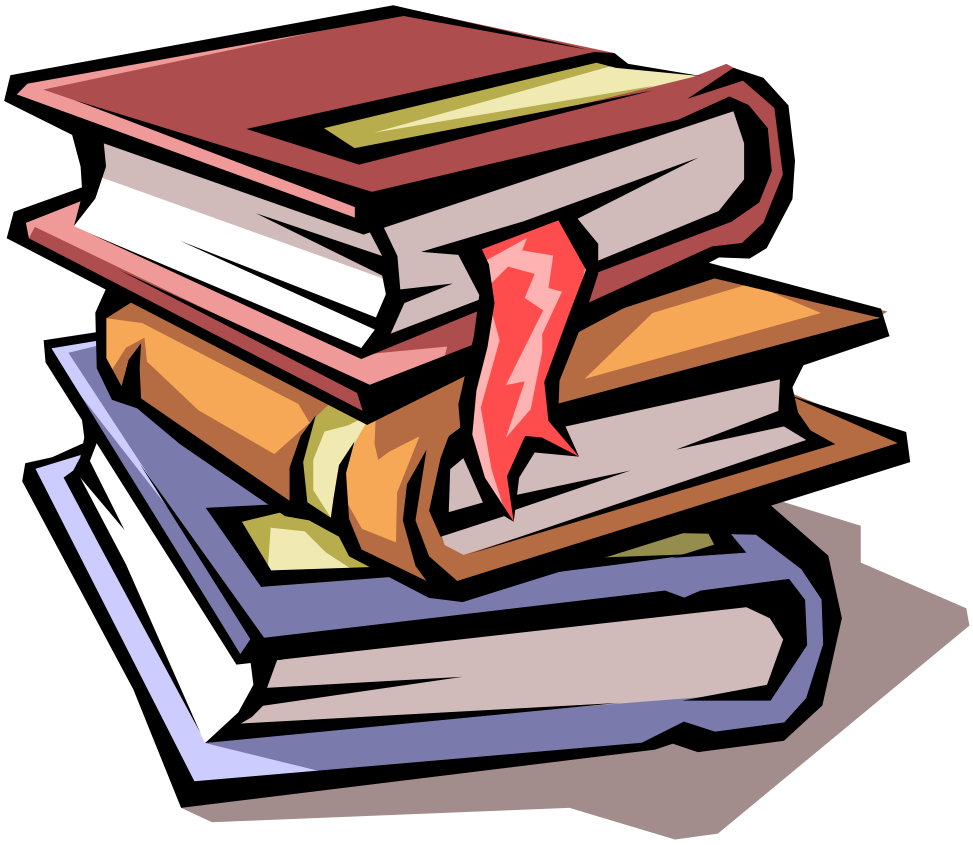
LITTLE BLACK BOOK OF SCAMS



2020 OKLAHOMA EDITION

LEGAL AID SERVICES OF OKLAHOMA, INC.

Making Equal Justice for All a Reality

LSC

United Way

Contents

SUSCEPTIBILTY TO SCAMS

Scams can happen to anyone, anytime and anywhere. Doctors, lawyers, bankers, business people, scientists, and generals have reported being swindled. This makes it difficult to build a profile of a “typical scam victim.” We can, however, point out some behaviors which make it easier for a scam to occur.

• Victim makes the initial contact with the offender, like mailing in a free coupon or a chance to win a trip.

• Victim provides information about him or herself.

• Victim allows the offender to convert what should be a business relationship into a personal relationship to create trust.

• Victim allows the offender to create a scenario or version of events that when believed sets the stage for fraud.

• Victim provides access to funds by writing checks, sending “voided blank checks”, or giving out credit card number.

You may be at increased risk of victimization if you:

• Had ever responded to unsolicited mailings by purchasing an item to become eligible to win a free prize.

• Had given their PIN or ATM code to others.

• Neglected to perform background checks on contractors.

• Neglected to destroy credit card solicitations, or shred important documents prior to disposing.

• Gave your credit card numbers, particularly over a cordless phone.

• Had difficulty in resisting sales pitches and is easily manipulated by flattery.

A study by the American Association of Retired Persons (AARP) reveals the following personality types as more susceptible to scams:

1. **Open to anything:** This group was very open to anything anyone suggested to them over the phone. People in this group are also prone to making investment or lottery decisions on the basis of the amount of the promised return or prize, rather than considering the odds and risks.

2. **You can't fool me:** These individuals self-identified as individuals who were impossible to fool because they had the experience and intelligence to avoid fraud (yet they were among the victims).

3. **Polite and vulnerable**: These individuals were reluctant to hang up the phone or be impolite to anyone, which of course made them vulnerable to crooks calling them on the phone.

4. **Likes to buy**: These individuals are just people who like to shop and spend money. Consequently they are a relatively easy group to swindle.

5. Naive: These individuals seemed to be very trusting of anyone who called and were therefore vulnerable based on their relative naivety.

Loneliness or isolation within the elderly population provides a fertile breeding ground for scams. They find it a pleasant break in their solitary routine when they get a visit or letter from the con man. To keep this "new friend, they will often agree to do business on his or her terms.

Scams really do not occur more in one gender than another. However, elderly women living alone present an inviting target. This is particularly true of widows in a "traditional" type of relationship where her husband handled the finances and the home repair and the wife mainly took care of the housework, cooking and kids. They are particularly susceptible to do "nice" people who purport to act in their interest and may even do little things for free to "polish" their haloes.

Remember that "nice" actions do not mean that the person is honest, informed about the product or service they are selling, or have the required knowledge or experience to do the job correctly and at a fair rate.

Characteristics of a Con Person

As with the victims of swindlers, it is difficult to provide an all-inclusive picture of the scam artist as well. Part of the problem is they have acquired to take on whatever personality they may need to carry out their con and remain on the loose. Still, we can provide some general information.

The con artist's greatest strength is his or her ability to appear ordinary, just like everyone else.

Swindlers are usually charming, charismatic, and adaptable to changing situations. Often, they use this sunny exterior to help gloss over the flaws in their story. They are master manipulators.

Often, part of their pitch will be to dissuade you from doing any checking or thinking about their proposals. Sometimes, they'll urge you to secrecy ("I have this information straight from my cousin in the banking business. It's not illegal, but people might lose their jobs if the word got out"; "Don't ask your doctor. This is the cure the medical and pharmaceutical companies don't want you to know about"; "If it was up to me I'd let you take your time and think about it, but I need your money by 3:00 before the offer expires.")

Most con men don't set out to physically hurt anyone. However, behind their pleasant exterior are often anger, greed, hostility, and aggression. This makes them more dangerous. Admitting the con man to your home puts at risk more than just money and things.

THE DARK TRIAD

The Dark Triad describes many – and perhaps most- of the fraudsters. The traits which define the Triad are as follows:

A. **Narcissism -** Narcissists are extremely self-absorbed and even self-obsessed. They associate with, or seek out, vulnerable people, or those with low self-esteem, because they are easy to bully and intimidate. Because of their ego, narcissists have certain superficial expectations, so they tend to find an attractive or successful partner. But a true narcissist will then delight in gradually eroding their partner's self-esteem until only a shell remains. Narcissists tend to believe they are entitled to what they went. They see themselves as smarter than others. Thus, for example, a narcissist may see nothing wrong with fleecing an elder because the former deserves it more than a common old person. Narcissists occasionally justify themselves by rationalizing what they do as teaching their victim a lesson about greed, gullibility, or the dangers of trying to get a "free lunch" in a transaction. Narcissists also do well in scams which require them to pretend they're someone they're not (Think Leonardo DeCaprio in the movie *Catch Me If You Can*).

B. **Psychopaths -** Psychopaths lack empathy. They cannot sympathize with the feelings of others, even when they themselves are the cause of the injured person's pain. When they deprive a victim of their life savings, they feel the same as if they just turned a page in a book. Almost everyone knows a little about psychopaths from watching movies or the news; not every psychopath is a serial killer, but almost all serial killers are psychopaths. Adolph Hitler and the top-commanding Nazis of the Third Reich were almost certainly psychopaths**.** The same might be said for unrepentant swindlers such as Bernie Madoff.

C. **Machiavellianism** - Named after Named after Niccolo Machiavelli, whose book, *The Prince,* details how to manipulate others to get what you want. Machiavellians generally lack a moral compass. They are gifted at manipulation and frequently exploit others for their own personal gain. In fact gain – rather than right or wrong – provide the driving basis for their actions.

TEXAS ATTORNEY-GENERAL'S FIVE HOOKS OF A SCAMMER

1. THEY contacted YOU. Think about it. If you look up a business and call to make an order, you know who is on the other end of the deal. With a con artist, all you know is who that person says he or she is. You are already at a huge disadvantage.

2. They dangle BAIT in front of you. It is almost always a large sum of money, like a prize or an easy loan, or a large income. It sounds so easy! But we all know that people don't give away large sums of money so easily, or pay large incomes for nothing. Only in daydreams.

3. They want your PERSONAL INFORMATION. Anytime someone tries to get your bank account number, Social Security Number, or other sensitive information, you should automatically be on red alert. Don't do it.
4. First, YOU have to pay THEM. Don't be blinded by the promise of a large sum of money in the future. If they are asking you to give them money first, back off. It is illegal

for someone to require up-front payment before funding a loan or paying out a sweepstakes prize. And real employers don't generally ask new hires to shell out money.

5. You have to WIRE or AIRBORNE money instead of MAILING it. This is your last warning: if you are on the brink of wiring somebody money in order to get a prize or a loan, an inheritance or any other large sum of money, STOP! It's a scam, and they are trying to avoid the stiff penalties for mail fraud. You are about to be robbed.

By mail, by phone or face to face, con artists dangle baited hooks in front of honest people every day of the week. It usually begins with an unsolicited contact from a company, individual or organization you never heard of. You do not know who the caller really is. Real lotteries don't call you to say you've won. You don't get grants without applying for them. You don't get easy loans if you have bad credit. Real money is hard to get. It doesn't just come to you. But there are people who would like to take whatever money you have to lose. Don't get hooked!

Myth Busters

Busting these common myths will minimize your chances of being scammed.

• All companies, businesses and organizations are legitimate because they are licensed and monitored by the government: This is not always true. While there are rules about setting up and running a business or a company, scammers can easily pretend they have approval when they don’t. Even businesses that are licensed could still try to scam you by acting dishonestly.

• All Internet websites are legitimate: This is not always true. Websites are quite easy and cheap to set up. The scammers can easily copy an actual website and trick you into believing theirs is legitimate.

• There are short cuts to wealth that only a few people know: This is not always true. Ask yourself the question: if someone knew a secret to instant wealth, why would they be telling their secret to others?

• Scams involve large amounts of money: This is not always true. Sometimes scammers target a large number of people and try to get a small amount of money from each person.

• Scams are always about money: This is not always true. Some scams are aimed at stealing personal information from you.

GOLDEN RULES

Remember these golden rules to help you beat scammers

• Always get advice from a third party if an offer involves money, personal information, time or commitment.

• There are no guaranteed get-rich-quick schemes—sometimes the only people who make money are the scammers.

• Do not agree to offers or deals right away. If you think you have spotted a great opportunity, insist on time to get independent advice from a third party source before making a decision.

• Do not hand over money or personal information, or sign anything until you have done your homework and checked the credentials of the company that you are dealing with.
• Do not rely on glowing testimonials: find solid evidence of a company's success.

• Log directly on to a website that you are interested in rather than clicking on links provided in an email.

• Never send money, or give credit card or online account details to anyone you do not know and trust.

• If you spot a scam or have been scammed, get help. Contact your local police for assistance. See page 34 for contact information.

• Scammers are imaginative and manipulative. They know how to push your buttons to produce the response they want.

INTRODUCTION

Every year, Americans lose millions of dollars to the activities of scammers who bombard us with online, mail, door-to-door and telephone scams.

We are pleased to bring you the first American edition of *The Little Black Book of Scams*. We hope this book will increase your awareness of the vast array of scams that target Americans and share with you some easy steps you can take to protect yourself.

SCAMMERS DO NOT DISCRIMINATE

Scammers target people of all backgrounds, ages, and income levels. Fake lotteries, Internet frauds, get-rich-quick schemes and miracle health cures are some of the favored means of separating the unwary from their hard-earned money. New varieties of these scams appear all the time.

The Internal Revenue Service has seen the devastating effects scams can have on people and their families. One of the best ways to combat this kind of fraud is to take measures to prevent yourself from being caught in the first place.

PROTECT YOURSELF

If you want to stay on top of scams, inform yourself on how to recognize the various types of scams and protect your personal information by visiting law enforcement organizations' websites, the stopfraud.gov or other reputable organizations.

LOTTERIES, SWEEPSTAKES AND CONTESTS

Many Americans are lured by the excitement of a surprise win and find themselves sending huge amounts of money to claim fake prizes.

What to look for

You cannot win money or a **prize in a lottery** unless you have entered it yourself, or someone else has entered it on your behalf. You cannot be chosen as a random winner if you don't have an entry.

Many lottery scams try to trick you into providing your banking and personal details to claim your prize. You should not have to pay any fee or tax to claim a legitimate prize.

Don't be fooled by claims that the offer is legal or has government approval—many scammers will tell you this. Instead of receiving a grand prize or fortune, you will lose every cent that you send to a scammer. And if you have provided other personal details, your identity could be misused too.

A fake prize scam will tell you that you have won a prize or a contest. You may receive a phone call, an email, a text message or see a pop-up screen on your computer. There are often costs involved with claiming your prize, and even if you do receive a prize, it may not be what was promised to you.

The scammers make their money by making you pay fees or taxes, call their phone numbers, or by sending you text messages to claim your prize. These phone calls can be very expensive, and the scammers will try to keep you on the line for a long time or ask you to call a different number.

!	**Protect Yourself**

Remember	Legitimate lotteries do not require you to pay a fee or tax to collect winnings.
Caution	Never send money to anybody you don't know and trust.
Think	Don't provide personal banking details to anyone that you do not know and trust.
Investigate	Examine all of the terms and conditions of any offer very carefully—claims of free or very cheap offers often have hidden costs. Calls to 1-800 phone numbers or text messages that charge you can be very expensive.
Ask Yourself	Did I enter this contest? You cannot win money or a prize in a contest unless you have entered it yourself, or someone else has entered it on your behalf.

PYRAMID SCHEMES

Pyramid schemes promise a large financial return for a relatively small cost. Pyramid schemes are illegal and very risky—and can cost you a lot of money.

What to look for

In a typical **pyramid scheme**, unsuspecting investors are encouraged to pay large membership fees to participate in moneymaking ventures. The only way for you to ever recover any money is to convince other people to join and to part

with their money as well. People are often persuaded to join by family members or friends. But there is no guarantee that you will get back your initial investment.

Although pyramid schemes are often cleverly disguised, they make money by recruiting people rather than by selling a legitimate product or providing a service. Pyramid schemes inevitably collapse and you will lose your money. In the United States, it is a crime to promote a pyramid scheme or even to participate in one.

Ponzi schemes are fraudulent investment operations that work in a similar way to pyramid schemes. The Ponzi scheme usually lures in new and well-to-do investors by offering higher returns than other investments in the form of short-term returns that are either abnormally high or unusually consistent.
The schemer usually interacts with all the investors directly, often persuading most of the existing participants to reinvest their money, thereby minimizing the need to bring in new participants as a pyramid scheme will do.

Be cautious, but do not be discouraged from carefully researching business opportunities based on commissions. There are many legitimate multi-level marketing opportunities where you can legally earn an income from selling genuine products or services.

!	**Protect Yourself**

Remember	Pyramid and Ponzi schemes may be sent to you from family members and people you trust—they might not know that they could be illegal or that they are involved in a scam.
Caution	Never commit to anything at high-pressure meetings or seminars.

Think	Don't make any decisions without doing your homework—research the offer being made and seek unbiased advice from a third party before making a decision.
Investigate	Do some research on all business opportunities that interest you.
Ask Yourself	If I am not selling an actual product or service, is participation in this activity legal?

MONEY TRANSFER REQUESTS

Money transfer scams are on the rise. Be very careful when someone offers you money to help transfer their funds. Once you send money to someone, it can be very difficult, if not impossible, to get it back.

What to look for

The **Nigerian** scam (also called the 419 fraud) has been on the rise since the early-to-mid 1990 in the United States. Although many of these sorts of scams originated in Nigeria, similar scams have been started all over the world (particularly in other parts of West Africa and in Asia). These scams are increasingly referred to as "**advance fee fraud.**"

In the classic Nigerian scam, you receive an email or letter from a scammer asking your help to transfer a large amount of money overseas. You are then offered a share of the money if you agree to give them your bank account details to help with the transfer. They will then ask you to pay all kinds of taxes and fees before you can receive your "reward". You will never be sent any of the money, and will lose the fees you paid.

Then there is the scam email that claims to be from a lawyer or bank representative advising that a long-lost relative of yours has died and left you a huge **inheritance**. Scammers can tell such genuine sounding stories that you could be tricked into providing personal documents and bank account details so that you can confirm their identity and claim your inheritance. The "inheritance" is likely to be non-existent and, as well as losing any money you might have paid to the scammer in fees

and taxes, you could also risk having your identity stolen.

If you or your business is selling products or services online or through newspaper classifieds, you may be targeted by an **overpayment** scam. In response to your advertisement, you might receive a generous offer from a potential buyer and accept it. You receive payment by check or money order, but the amount you receive is more than the agreed price. The buyer may tell you that the overpayment was simply a mistake or they may invent an excuse, such as extra money to cover delivery charges. If you are asked to refund the excess amount by money transfer, be suspicious. The scammer is hoping that you will transfer the refund before you discover that their check or money order was counterfeit. You will lose the transferred money as well as the item if you have already sent it.

!	**Protect Yourself**

Remember	If you have been approached by someone asking you to transfer money for them, it is probably a scam.
Caution	Never send money, or give credit card or online account details to anyone you do not know and trust.
Think	Don't accept a check or money order for payment for goods that is more than what you agreed upon. Send it back and ask the buyer to send you payment for the agreed amount before you deliver the goods or services.
Investigate	Examine the information on the FBI website http://www.fbi.gov/scams-safety/fraud for information on how to protect yourself against money transfer scams.
Ask Yourself	Is it really safe to transfer money for someone I do not know?

INTERNET SCAMS

A lot of Internet scams take place without the victim even noticing. You can greatly reduce the chances of being scammed on the Internet if you follow some simple precautions.

What to look for

Scammers can use the Internet to promote fraud through unsolicited or junk emails, known as spam. Even if they only get a handful of replies from the millions of emails they send out, it is still worth their while. Be wary of replying, even just to “unsubscribe”, because that will give a scammer confirmation that they have reached a real email address.

Any email you receive that comes from a sender you do not know, is not specifically addressed to you, and promises you some benefit is likely to be spam.

Malicious software—also referred to as malware, spyware, key loggers, Trojan horses, or Trojans—poses online security threats.

Scammers try to install this software on your computer so that they can gain access to files stored on your computer and other personal details and passwords.

Scammers use a wide range of tricks to get their software onto your computer. They may trick you into clicking on a link or pop-up message in a spam email, or by getting you to visit a fake website set up solely to infect people’s computers.

Phishing scams are all about tricking you into handing over your personal and banking details to scammers. The emails you receive might look and sound legitimate but in reality real organizations like a bank or a government authority will never expect you to send your personal information by an email or online.

Scammers can easily copy the logo or even the entire website of a real organization. So don’t just assume an email you receive is

legitimate. If the email is asking you to visit a website to “update”, “validate” or “confirm” your account information, be skeptical.

Delete phishing emails. They can carry viruses that can infect your computer. Do not open any attachments or follow any links in phishing emails.

Today, phishing attacks look more like they came from a specific company. Called “spearfishing,” hackers pose as your bank, credit card or a site like Dropbox or PayPal., Targets receive an email that looks as if it came from a legitimate business. You might be prompted to click on a link to “verify account details” and from there, fileless malware is installed on your device.

Where you once had to download a file or an app, it’s now a matter of clicking a link. Fileless attacks are harder to detect, as most antivirus programs only scan your hard drive

Smishing scams are like phishing scams but involve a text message. Sometimes it takes the form of a notice that you will be charged for a certain service. If you didn’t sign up for that service, you know it’s a fraud. Never respond to text messages from an unknown source. Even if you get a text message with a link from a friend, consider verifying they meant to send the link before clicking. Always err on the side of caution.

Online auctions and **Internet shopping** can be a lot of fun and can also help you find good deals. Unfortunately, they also attract scammers.

Scammers will often try to get you to deal outside of online auction sites. They may claim the winner of an auction that you were bidding on has pulled out and offer the item to you. Once you have paid, you will never hear from them again and the auction site will not be able to help you.

!	**Protect Yourself**

Remember	If you choose to shop online or participate in online auctions, make sure you know about refund policies and dispute-handling processes, and be careful that you are not overcharged. Also, you may want to use an escrow service, such as PayPal. This service will hold your payment and only release it to the seller once you have confirmed that you received what you paid for. There is usually a small fee for this service. A legitimate bank or financial institution will never ask you to click on a link in an email or send your account details through an email or website.
Caution	Never buy from bidders with poor ratings on auction sites, and do your best to ensure that you are only making purchases from genuine shopping sites. Never provide your personal, credit card or account information unless you are certain the site is genuine.
Think	Don’t reply to spam emails, even to unsubscribe, and do not click on any links or call any telephone number listed in a spam email. Make sure you have current protective software or get advice from a computer specialist.
Investigate	If an email or pop-up offers you a product or service that genuinely interests you and it seems reasonable, be sure that you understand all the terms and conditions and costs involved before making a purchase or providing your details.

sk Yourself	By opening this suspect email, will I risk the security of my computer? Are the contact details provided in the email correct? Telephone your bank or financial institution to ask whether the email you received is genuine.

CELL PHONE SCAMS

Cell phone scams can be difficult to recognize.
Be wary of somebody who talks as if they know you or of redialing a missed call from an unknown number—there may be hidden charges.

What to look for

Ringtone scams might attract you with an offer of a free or low-cost ringtone. What you may not realize is that by accepting the offer, you may actually be subscribing to a service that will keep sending you ringtones—and charging you a large amount for them. There are many legitimate companies selling ringtones, but there are also scammers who will try to hide the true cost of taking up the offer.

Scammers either don't tell you that your request for the first ringtone is actually a subscription to a ringtone service, or it may be obscured in fine print related to the offer. They also make it difficult for you to stop the service. You have to actively "opt out" of the service to stop the ringtones and the associated charges.

Missed call scams start by scammers calling your phone and hanging up so quickly that you can't answer the call in time. Your phone registers a missed call and you probably won't recognize the number. You may be tempted to call the number to find out who called you. If it is a scam, you could be paying for the call without knowing.

Text message scams work in a similar way, but through a Short Message Service (SMS). Scammers send you a text message from a number you may not recognize, but it sounds like it is from a friend—for instance: "Hi, it's John. I'm back! When are you free to
catch up?" If you reply out of curiosity, you might be charged for SMS text messages.

An SMS contest or SMS trivia scam usually arrives as a text message or in an advertisement and encourages you to take part in a trivia contest for a grand prize. All you need to do is answer a certain number of questions correctly. The scammers make money by charging extremely high rates for the messages you send and any further messages they send to you. With trivia scams, the first set of questions will be very easy. This is meant to encourage you to keep playing. However, the last one or two questions that you need to answer to claim your "prize" could be very difficult or impossible to answer correctly.

!	**Protect Yourself**

Remember	Text "STOP" to end unwanted text messages or to end unwanted subscriptions.
Caution	Never reply to text messages offering you free ringtones or missed calls from numbers that you do not recognize.
Think	Don't call or text phone numbers beginning with 1-800 unless you are aware of the cost involved, and carefully read any terms and conditions when texting short codes like "TEXT WIN" to 5555.
Investigate	Read all the terms and conditions of an offer very carefully. Services offering free or very cheap products often have hidden costs.
Ask Yourself	Do I know how to stop any subscription service I want to sign up to?

HEALTH AND MEDICAL SCAMS

Medical scams prey on human suffering. They offer solutions where none exist or promise to simplify complex health treatments.

What to look for

Miracle cure scams offer a range of products and services that can appear to be legitimate alternative medicines, usually promising quick and effective remedies for serious medical conditions or dieting. The treatments claim to be effective against a very wide range of ailments and are often promoted using testimonials from people who have used the product or service and have been “cured”.

Weight loss scams promise dramatic weight loss with little or no effort. This type of scam may involve an unusual or restrictive diet, revolutionary exercise or “fat-busting” devices, or breakthrough products such as pills, patches or creams. The products are promoted with the use of false claims such as “lose 10 pounds in 10 days” or “lose weight while you sleep”, and often require large advance payments or that you enter into a long-term contract to participate in the program.

Fake online pharmacies use the Internet and spam emails to offer drugs and medicine at very cheap prices and/or without the need for a prescription from a doctor. If you use such a service and you actually do receive the products in response to your order, there is no guarantee that they are the real thing.

There are legitimate online pharmacies. These businesses will have their full contact details listed on their website and will also require a valid prescription before they send out any medicine that requires one.

!	**Protect Yourself**

Remember	There are no magic pills, miracle cures or safe options for serious medical conditions or rapid weight loss.
Caution	Never commit to anything under pressure.
Think	Don't trust an unsubstantiated claim about medicines, supplements or other treatments. Consult your healthcare professional.
Investigate	Check for published, independent medical and research papers to verify the accuracy of the claims made by the promoters.
Ask Yourself	If this really is a miracle cure, wouldn't my healthcare professional have told me about it?

GENETIC TESTING

Genetic testing scams are one of the new kids on the block, a block located at the intersection of Quackery and Theft. The scam, while sounding modern, involves some good, old-fashioned sleight-of-hand to lure the mark, starting out with a deceptive offer to pay in cash, coupons, or gift certificates for participation in this "study". "They're paying me," the victim thinks, "how could *that* be a scam?"

Very easily.

The scammers offer Medicare recipients free genetic tests, sometimes masquerading as promotions from legitimate companies or, perhaps, a government agency. All you have to do is give them your Social Security and Medicare numbers. Once you do that, they have access to your Medicare account. They can commit identity theft and fraud using your information. With this identification information, their potential gain far exceeds the little they've paid you. Your potential loss is also quite high.

Genetics tests analyze human DNA, RNA, chromosomes and proteins to detect alterations related to a inheritable disorder. Genetic tests can also help diagnose inherited diseases caused by problems with a single gene and lead to earlier treatment. At present, however, only a few such strategies are known, and none justify the procedures these companies use as selling points. Neither the American Medical Association, the FDA, nor any other any authority, and they are not FDA-approved for the purposes sold. In addition, most victims never receive test results anyway.

The scammers will try and bill Medicare or your health insurance for the costs of the non-existent tests. When, for example, Medicare, receives such a bill for a test neither medically necessary nor ordered by your doctor, the claim could be denied or, if already paid, require you to repay them. Not only that. Both you and, perhaps, your doctor may be viewed as conspirators rather than as victims.

The Better Business Bureau suggests the following steps to protect yourself:

- **Do not give out your personal information to someone who has solicitated you**. Be suspicious of anyone who requests your Medicare number. If anyone other than your physician's office requests your Medicare information, do not provide it. If your personal information is compromised, it may be used in other fraud schemes.

- **Never Consent to any lab tests at senior centers, health fairs, or in your home**. Be suspicious of anyone claiming that genetic tests and cancer screening are “free” or “covered by Medicare.” If a product or test is truly “free,” you will not have to provide your Medicare number.

- **If you need genetic testing, always work with your doctor**. Medicare only covers DNA or genetic tests that are medically necessary and ordered by your primary physician.

- **Monitor your Medicare Summary Notice to see if there are any services you did not receive (or if you were billed for services that you can’t identify**). People have been stuck with big bills when their insurance plan reviewed the claim and decided the test was not medically necessary.

- **Research any business and its owners carefully**. Check the company’s BBB Business Profile at bbb.org.

- **Do not trust a name or phone number**. Con artist often use official-sounding names or mask their area codes to make you trust them. Medicare will never call you to confirm your personal information, your Medicare number, or ask questions about your personal health.

- **Make sure to verify their credentials before you allow them to assist you**. Just because someone is dressed like a healthcare professional, it doesn’t mean they are qualified to practice medicine

EMERGENCY (“Granny”) SCAMS

Emergency scams target grandparents, playing upon their emotions to rob them of their money.

What to look for

In the typical scenario of an emergency scam, a grandparent receives a phone call from a scammer claiming to be one of his or her grandchildren. Callers go on to say that they are in some kind of trouble and need money immediately. They claim to have been in a car accident, are having trouble returning from a foreign country, or they need bail money.

You may get a call from two people, one pretending to be your grandchild and the other pretending to be either a police officer or a lawyer. Your “grandchild” asks you questions during the call, getting you to volunteer personal information.

Callers say that they don’t want other family members to find out what has happened. You will be asked to wire some money through a money transfer company. Often, victims don’t verify the story until after the money has been sent.

In some cases, scammers pretend to be your old neighbor or a friend of the family, but for the most part, the emergency scam is directed at **grandparents**.

!	**Protect Yourself**

Remember	Scammers are counting on the fact that you will want to act quickly to help your loved ones in an emergency.
Caution	Never send money to anyone you don't know and trust. Verify the person's identity before you take any steps to help.
Think	Don't give out any personal information to the caller.
Investigate	Ask the person questions that only your loved one would be able to answer. Call the child's parents or friends to verify the story.
Ask Yourself	Does the caller's story make sense?

DATING AND ROMANCE SCAMS

Despite the many legitimate dating websites, there are many dating and romance scams as well. Dating and romance scams try to lower your defenses by appealing to your romantic and compassionate side.

What to look for

Some **dating and romance** scams work by setting up a dating website where you pay for each email or message you send and receive. The scammer will try to hook you in by continuing to send you vague-sounding emails filled with talk of love or desire. The scammer might also send emails filled with details of their home country or town that do not refer to you much at all. These are attempts to keep you writing back and paying money for use of the scammer's dating website.

Even on a legitimate dating site, you might be approached by a scammer—perhaps someone who claims to have a very sick family member or who is in the depths of despair (often these scammers claim to be from Russia or Eastern Europe). After they have sent you a few messages, and maybe even a glamorous photo, you will be asked (directly or more subtly) to send them money to help their situation. Some scammers even arrange to meet with you, in the hope that you give them presents or money—and then they disappear.

In other cases, scammers will try to build a friendship with you, perhaps even sending you flowers or other small gifts. After building a relationship, the scammer will tell you about a large amount of money they need to transfer out of their country, or that they want to share with you. They will then ask for your banking details or money for an administrative fee or tax that they claim needs to be paid to free up the money.

!	**Protect Yourself**

Remember	Check website addresses carefully. Scammers often set up fake websites with very similar addresses to legitimate dating websites.
Caution	Never send money, or give credit card or online account details to anyone you do not know and trust.
Think	Don't give out any personal information in an email or when you are chatting online.
Investigate	Make sure you only use legitimate and reputable dating websites.
Ask Yourself	Would someone I have never met really declare their love for me after only a few letters or emails?

CHARITY SCAMS

Charity scams take advantage of people's generosity and kindness by asking for donations to a fake charity or by impersonating a real charity.

What to look for

Charity scams involve scammers collecting money by pretending to be a real charity. The scammers can approach you in many different ways—on the street, at your home, over the phone, or on the Internet. Emails

and collection boxes may even be marked with the logos of genuine charities.

Often, the scammer will exploit a recent natural disaster or famine that has been in the news. Other scammers play on your emotions by pretending to be from charities that help children who are ill.

Scammers can try to pressure you to give a donation and refuse to provide details about the charity, such as their address or their contact details. In other cases, they may simply provide false information.
Not only do these scams cost people money; they also deter much needed donations away from legitimate charities and causes. You can also contact your local Better Business Bureau to see if they have any information about the organizations that interest you. If the charity is genuine and you want to make a donation, get the charity's contact details from the phone book or a trusted website.

If you do not want to donate any money, or you are happy with how much you may have donated to charities already, simply ignore the email or letter, hang up the phone, or say no to the person at your door. You do not have to give any money at all.

!	**Protect Yourself** 

Remember	If you have any doubts at all about the person asking for money, do not give them any cash, credit card or bank account details.
Caution	Never give out your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.
Think	If in doubt, approach an aid organization directly to make a donation or offer support.
Investigate	Search the Internal Revenue Agency database to check that the charity that has approached you is genuine.
Ask Yourself	How and to whom would I like to make a contribution?

JOB AND EMPLOYMENT SCAMS

Job and employment scams target people looking for a job. They often promise a lot of income—sometimes they even guarantee it—for little or no effort.

What to look for

Work-from-home scams are often promoted through spam emails or advertisements online or in newspaper ads. Most of these advertisements are not real job offers. Many of them are fronts for illegal money-laundering activity or pyramid schemes.

You might get an email offering a job where you use your bank account to receive and pass on payments for a foreign company. Or you might be offered a job as a “secret shopper” hired to test the services of a check-cashing or a money transfer company. Some “job offers” promise that you will receive a percentage commission for each payment you pass on. Sometimes, scammers are just after your bank account details so they can access your account. They might also send you a counterfeit check along with instructions for you to cash the check and transfer a portion of the sum over a money transfer service.

A guaranteed employment or income scam claims to guarantee you either a job or a certain level of income. The scammers usually contact you by spam email and the offers often involve the payment of an up-front fee for a “business plan”, certain start-up materials or software.

There is a range of scams promoted as business opportunities. You may be required to make an upfront payment (for something that does not work or is not what you expected) or to recruit other people to the scheme (refer to pyramid schemes on page 7).

!	**Protect Yourself**

Remember	There are no shortcuts to wealth—the only people that make money are the scammers.
Caution	Never send your bank account or credit card details to anybody you do not know and trust. If you cash the check and it turns out to be counterfeit, you could be held accountable for the entire monetary loss by your bank.
Think	Don't make any decisions without carefully researching the offer. Seek independent advice before making a decision.
Investigate	Beware of products or schemes claiming to guarantee income and job offers requiring payment of an upfront fee or sending money through a money transfer service. Make sure any franchise business opportunity is legitimate.
Ask Yourself	Did I get all the details in writing before paying or signing anything?

SMALL BUSINESS SCAMS

Scams that target small businesses can come in a variety of forms—from bills for advertising or directory listings that were never ordered to dubious office supply offers.

What to look for

Small business operators and individuals with their own Internet sites continue to be confused and caught by unsolicited letters warning them that their Internet domain

name is due to expire and must be renewed, or offering them a new domain name similar to their current one.

If you have registered a domain name, be sure to carefully check any domain name renewal notices or invoices that you receive. While the notice could be genuine, it could also be from another company trying to sign you up, or it could be from a scammer.

• Check that the renewal notice matches your current domain name exactly. Look out for small differences—for example, ".com" instead of ".org" or missing letters in the URL address.
• Check that the renewal notice comes from the company with which you originally registered your domain name.

• Check your records for the actual expiration date for your existing domain name.

A **directory listing** or **unauthorized advertising** scam tries to bill a business for a listing or advertisement in a magazine, journal or business directory, or for an online directory listing.

The scam might come as a proposal for a subscription disguised as an update of an existing listing in a business directory. You might also be led to believe that you are responding to an offer for a free listing when in fact it is an order for a listing requiring later payment.
Another common approach used by scammers is to call a firm asking to confirm details of an advertisement that they claim has already been booked. The scammer might quote a genuine entry or advertisement your business has had in a different publication or directory to convince you that you really did use the scammer's product.

Be wary of **order forms** offering advertising opportunities in business directories. These order forms may look like they originate from a well-known supplier of directory advertising, when they don't.
An **office supply** scam involves you receiving and being charged for goods that you did not order. These scams often involve goods or services that you regularly order— for example, paper, printing supplies, maintenance supplies or advertising.

You might receive a phone call from someone falsely claiming to be your "regular supplier", telling you that the offer is a "special" or "available for a limited time", or pretending to only confirm your address or existing order.
If you agree to buy any of the supplies offered to you, they will often be overpriced and of bad quality.

!	**Protect Yourself**

Remember	Make sure that the people processing the invoices or answering telephone calls are aware of these scams. They will most often be the point of contact for the scammers. Always check that goods or services were both ordered and delivered before paying an invoice.
Caution	Never give out or update any information about your business unless you know what the information will be used for.

Think	Don’t agree to a business proposal over the phone—always ask for an offer in writing. Limit the number of people in your business that have access to funds and have the authority to approve purchases.

Investigate	If a caller claims that I have ordered or authorized something and I do not think it sounds right, shouldn’t I ask for proof?
Ask Yourself	Effective management procedures can go a long way towards preventing these scams from succeeding. Having clearly defined procedures for the verification, payment and management of accounts and invoices is an effective defense against these types of scams.

SERVICE SCAMS

Many Americans are being targeted by individuals claiming to offer reduced rates or deals for various services.

What to look for

These scams typically involve individuals that make offers for telecommunications, Internet, finance, medical and energy services. This category of scams may also include offers such as extended warranties, insurance, and door-to-door sales.

The two most reported service scams targeting Americans are the antivirus software scam and credit card interest rate reduction scams.

The scammers involved in the antivirus software scam promise to repair your computer over the Internet. This can involve the installation of software or permission to have remote access to your computer. Payment for the software or repair is typically made by credit card.

wnloading software from an unknown source or allowing someone to remotely access your computer is risky. Scammers could use malicious software to capture your personal information such as user names and passwords, bank account information, identity information, etc.

Everyone likes to get a deal and scammers know this. The people behind credit card interest rate reduction scams often impersonate financial institutions and claim to negotiate with credit card companies to lower your interest rates. They guarantee they can save you thousands of dollars in interest. The caller will tell you that the lower interest rates are for a limited time only and that you need to act now.

You might receive an automated call, prompting you to “press 1” and provide personal information, such as your date of birth and credit card number. You will also be asked to pay a fee up front for the service. The scammers will use this information to make purchases on your credit card or to access cash advances.

!	**Protect Yourself**

Remember	Only your service provider can offer you a better rate or price for their services.
Caution	Be wary of unsolicited calls from people offering a great deal “for a limited time only”.
Think	Don’t give out your credit card number over the phone unless you made the call and the number came from a trusted source.
Investigate	By offering up this information, am I putting myself at risk?
Ask Yourself	If a caller claims to represent your bank, telephone your bank to ask whether the offer you received is genuine.

GOVERNMENT AGENT SCAMS

Many scam artists pose as Government Agents (IRS, FBI, Secret Service, CIA or local police) in an effort to gain access to your information or admission into your home. Here’s what you should know:

Federal and State agencies do not initiate contact with taxpayers or other citizens by email, text messages or social media channels to request personal or financial information.

Often people report getting emails from someone giving a rank (“Captain Smith” or “Sargent Jones”) with a federal agency or law enforcement. **Be aware that only the military and the State Department use ranks.** If the communications name any other agency it is almost certainly a scam.

You can verify the legitimacy of any government representative by calling your local office. **Do not use a number given to you by the person contacting you.** Call the office directly at the number given in your telephone directory or on line. In no event should you admit someone into your home without first verifying they are the genuine article.

In the Oklahoma City area, municipal employees will have an ID card and a picture card on a lanyard.

The IRS never:

- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer. Generally, the IRS will first mail a bill to any taxpayer who owes taxes.
- Demand that you pay taxes without the opportunity to question or appeal the amount they say you owe. You should also be advised of your rights as a taxpayer.
- Threaten to bring in local police, immigration officers or other law-enforcement to have you arrested for not paying. The IRS also cannot revoke your driver’s license, business licenses, or immigration status. Threats like these are common tactics scam artists use to trick victims into buying into their schemes.

Individuals posing as Social Security employees call and ask for personal information like your name, Social Security number and bank account information. The caller alleges that they need this information to issue you additional funds or rebates or they allege that because of a computer glitch your personal information has been lost.

Another scam used an email that was designed to look like it came from Social Security. It provided information about the annual cost-of-living-adjustment and directed readers to a website designed to look like Social Security's site so people could "update their information" — valuable information to identity thieves and criminals.

Scammers pretending to work for Social Security may say they need to update your records. They for all kinds of personal information that identity thieves crave, such as your Social Security number, address, birthdate, bank account number, mother's maiden name, and so on.

In yet another, the scammer tells you that he or she can get you bigger Social Security checks -- for a fee. Never do business with any such person. There are indeed strategies you can use to get bigger benefits, but you should find them online or at the library or by consulting a financial advisor. (It's also possible to appeal the size of your checks with Social Security, but AARP advises:

> If you feel you're due a higher benefit, you can file an appeal yourself, at no cost. It can be a complicated process, so you're allowed to hire someone to help you — but you should find that person yourself. Social Security regulates what these people can charge; representatives may face prosecution if they charge more.

Beginning April 2018, Medicare issued new cards to all Medicare recipients. The new cards will no longer use Social Security numbers. Instead, members will be identified by a unique, eleven-character ID composed of numbers and letters. Only the cards changing, not the benefits. **The new cards cost nothing**. **If you're asked to pay a fee to expedite or process shipment of your new card, it's a scam**. Also, Medicare does not accept payment in the form of gift cards, wired money, or credit card.

Social Security **will not** send you an email asking you to give us your personal information, such as your Social Security number, date of birth, or other private information. If someone saying they are from Social Security does email you requesting information, don't respond to the message. Instead, contact your local Social Security office or call us at 1-800-772-1213 (TTY 1-800-325-0778)

HANDY HINTS TO PROTECT YOURSELF FROM SCAMS

Protect your identity

• Only give out your personal details and information where it is absolutely necessary and when you trust the person you are speaking to or dealing with.

• Destroy personal information: don't just throw it out. You should cut up or shred old bills, statements or cards—for example, credit cards and ATM cards.

• Treat your personal details like you would treat money: don't leave them lying around for others to take.

Money matters

• Never send money to anyone that you don't know and trust.

• Do not send any money or pay any fee to claim a prize or lottery winnings.

• "Jobs" asking you to simply use your own bank account to transfer money for somebody could be a front for money-laundering activity. Money laundering is a serious criminal offence.

• Avoid transferring or wiring any refunds or overpayments back to anyone you do not know.

The face -to -face approach

• If someone comes to your door, ask to see some identification. You do not have to let them in, and they must leave if you ask them to.

• Before you decide to pay any money, if you are interested in what a door-to-

door salesperson has to offer, take the time to find out about their business and their offer.

• Contact the Better Business Burea
are unsure about a seller that come
door. See page 30 for contact infor

Telephone business

• If you receive a phone call from sc
you do not know, always ask for the
of the person you are speaking to a
they represent. Verify this informati
calling the company yourself.

• Do not give out your personal, cre
or online account details over the p
unless you made the call and the pl
number came from a trusted source

• It is best not to respond to text me
or missed calls that come from num
do not recognize.
Be especially wary of phone numbe
beginning with 1-800. These may b
charged at a higher rate than other
and can be very expensive.

Email offers

• Never reply to a spam email, ever
unsubscribe—often, this just serves
"verify" your address to scammers.
course of action is to delete any
suspicious emails without opening t

• Turn off the "viewing pane" as just
the email may send a
verification notice to the sender tha
a valid email address.

• Legitimate banks and financial institutions will never ask you for your account details in an email or ask you to click on a link in an email to access your account.

• Never call a telephone number or trust other contact details that you see in a spam email.

Internet business

• Install software that protects your computer from viruses and unwanted programs and make sure it is kept current. If you are unsure, seek the help of a computer professional.

• If you want to access a website, use a bookmarked link to the website or type the address of the website into the browser yourself. Never follow a link in an email.

• Check website addresses carefully. Scammers often set up fake websites with addresses very similar to legitimate websites.

• Beware of websites offering "free" downloads (such as music, adult content, games and movies). Downloading these products may install harmful programs onto your computer without you knowing.

• Avoid clicking on pop-up ads—this could lead to harmful programs being installed on your computer.

• Never enter your personal, credit card or online account information on a website that you are not sure is genuine.

• Never send your personal, credit card or online banking details through an email.

• Avoid using public computers (at libraries or Internet cafes) to do your Internet banking or online shopping.

• When using public computers, clear the history and cache of the computer when you finish your session.

• Be careful when using software on your computer that auto-completes online forms. This can give Internet scammers easy access to your personal and credit card details.

• Choose passwords that would be difficult for anyone else to guess—for example, passwords that include letters and numbers. You should also regularly change passwords.

• When buying anything online, print out copies of all transactions and only pay via a secure site. If using an Internet auction site, note the ID numbers involved and read all the security advice on the site first.

IN CASE OF DOUBT ASSUME IT'S A SCAM!

Spoofing

It's like a scene from a late-night from a late-night horror flick. You know, the one where the baby sitter receives threatening calls only to be told by the police that the calls came from inside the house.

Imagine your own surprise when you get a call and the caller ID displays your own number. Surely you didn't call yourself, so what gives?

It's called spoofing, and it's a scam. Spoof technology allows the scammer to steal other folks' number so that it shows up on Caller ID as that of a friend, neighbor, or local business. They avoid the suspicion that an (800) (900) or out-of-state number might trigger by posing as an innocent local number. You soon find out that the caller is not the friend or neighbor you thought it was, and the caller tries to peddle a loan, a credit card, or other product, or they ask you to provide information.

Make no mistake: spoofing is a scam. But, given the state of technology and the number of phone companies, it's a difficult scam to combat.

Sometimes the call will come from your own phone number or a number just a digit or two off from your number. The caller will then say that it's from the phone company testing the line and requiring identifying information such as social security numbers of dates of birth.

If you receive a call from yourself, the safest is approach is to simply not answer. The same is true for a call from a number nearly identical to yours, unless you recognize it as that of a friend or neighbor.

The moment you realize that the number on your Caller ID was a decoy, hang up immediately.

Do not disclose any information of any sort.

Sometimes you may be requested to punch a number or series of numbers to test the line, or you may be given a number to punch in to remove yourself from their calling list. Do Not punch those numbers!!

12 SCAMS OF CHRISTMAS

1. **Phony or Misleading Charities** - Many charities come knocking, calling or mailing you for donations. During the holidays, people remember that part of being human is helping out those less fortunate. Unfortunately, many so-called charities are fakes. According to the Federal Trade Commission, many of the calls you get this year will be from scam artists. The FTC has a checklist of warning signs to help you steer clear of charity scams. Your best bet is to not make any quick decisions, ask for information in writing and research the charity before cutting any checks

2. **Grab and Dash** -Not all holiday scams are high-tech. Some of the most bold and heinous crimes committed during the holidays are good old-fashioned purse snatchings, pocket pickings and laptop swipes. People tend to be friendlier and more trusting during the holiday time, and public places are often more packed with holiday shoppers and merry-makers. This makes for a perfect storm of criminal activity. Stealthy thieves can make off with someone's valuables in the blink of an eye and then disappear into the crowd. Even if the victim is aware of the theft immediately, he or

she may not react quickly enough to catch the thief. But perhaps the worst thing about such crimes is that they almost invariably lead to identity theft, which can have far more devastating consequences than the loss of a wallet full of cash. Stay safe and secure during the holiday season.

.

3. Work Scams - A lot of people take part-time jobs during the holidays to make extra cash. But for some, a holiday job can lead to the poor house. Bogus advertisements offers quick cash but very little information about the company. Once a job-seeker responds, he or she may be sent a check along with instructions to send a portion of the money to someone via wire transfer and to keep the rest. They are often told that they will need the money to complete whatever assignment they have applied to do. It seems like a great deal until the "employee" realizes that the check is no good and they've sent money to a stranger who is no longer taking their calls.

4. **Hot Gift Scams** - Every year it seems that there is one book, toy or designer item that all the kids want for Christmas, Hanukkah or Kwanzaa. However, those items are invariably gone from retailers' shelves as soon as the holiday season approaches. So, what are desperate parents to do? Many turn to fly-by-night retailers offering the "it" gift just in time for Christmas. It sounds tempting, but often the gift never arrives and parents are left holding an empty bag. They may also become victims of identity theft by the unscrupulous merchants. To avoid gift scams, only shop at retailers you know and trust, go directly to their Web sites rather than responding to an email or pop-up advertisement, and use a credit card rather than debit card or other form of payment. With a credit card, you're less likely to have to pay for fraudulent charges

5. **Worthless Gift Cards** - Gift cards have become the present of choice for many holiday shoppers. However, not all gift cards are created equal. A favorite trick of scammers is to swipe the information from gift cards on display in stores and then periodically check to see if they've been activated. Once active, the thieves can use the cards to shop online. Bogus gift cards can also be sold over the Internet. When the card arrives in the mail, the purchaser soon realizes it has no value. Such scams are difficult to trace, since thieves can create temporary user accounts. Keep your gift cards safe during this holiday season by purchasing them directly from reputable stores instead of online auctions.

6. **Evil E- Cards** - People love to send e-cards, especially during the holiday season. But e-greetings can deliver more than just music and merriment. Some contain horribly destructive computer viruses cleverly disguised in holiday cheer. As soon as the recipient opens the e-card or a link contained within it — often appearing to come from a friend or family member — a nasty virus is unleashed into his or her computer. On the plus side, there are usually clues that an e-card may be trouble. Be suspicious of any greeting with spelling errors or without your name on it. Also, check the URL of any link contained in the e-card and only click on sites you trust. You can't beat holiday e-greetings for convenience and versatility, but remember that if something looks odd about an e-card you receive, just don't open it

7. **Dangerous Downloads** - Anyone with a bit of holiday spirit can appreciate a downloadable dancing elf, Hanukkah jingle or Santa Claus screensaver. But what happens when we click on something more sinister in those spirited online offerings? For starters, we can infect our computers with a dangerous virus, worm or Trojan, which can wreak havoc on an operating system. What's worse, some holiday-themed downloads can leave you vulnerable to identity theft and fraudulent activity. Don't let that yuletide ring tone destroy your new year. Always be extremely careful about what you install or download from the Internet.

8. **Scrooge Loans** - Some people are so cash-strapped during the holiday season that they'll turn to desperate measures to come up with a little extra purchasing power. They may be lured in by slick Web sites or phone calls from con artists who promise quick cash and guaranteed credit, even for those with less-than-perfect credit histories. The catch with these scams is that borrowers must pay a fee up-front before to receive their loan. And once they pay up, the "lender" simply disappears. To avoid falling for a bogus loan or credit deal, be suspicious of any offer of credit without a credit check and keep in mind that a legitimate lender's fees will be made clear in writing.

9. **Hidden costs** - The holiday shopping season is in full swing and will peak within the first week of December. If you are planning to buy gifts online or from Infomercials on television, Better Business Bureau has a warning about the way retailers make money on your orders by charging separate shipping and handling fees. Some retailers are finding ways to make extra money with special promotions such as “order now and we’ll double your order,” or “buy now and we’ll include a free gift” – it may sound like a good deal at first, until you realize that you will be charged separate shipping and handling fees on each item, including the “free” gifts and the “bonus” products. All of these shipping and handling fees can actually add up to more than the total cost of the products you’re ordering.

10. **False verifications** - With only a few weeks left to get holiday cards and gifts sent to loved ones, another risk consumer’s face is phishing scams. Scammers are pretending to be customer service personnel from some of the biggest names in business—including FedEx and UPS. Hackers are impersonating well-known companies in order to gain access to your computer drives, files and accounts to steal your personal information including Social Security, bank or credit card numbers.

Hackers send phishing e-mails from “shipping companies” claiming that there is a problem with package delivery. Commonly, the e-mail will include a hyperlink for recipients to click on that will take them to another Website that might install malware or solicit personal information. A message currently making the rounds has a subject line that looks like, “Subject: Tracking Number 13040065504.” The body of the message claims that a package could not be delivered and advises the recipient, “to print the copy of the invoice that is in the added file.” The attachment is actually a virus that will infect the computer.

11. **High pressure sales** - Perhaps the most annoying scam is the legal one: the high-pressure sale. It can happen anywhere -- the mall, the car lot, over the phone and even in the salon. You've been through it before: "No, really, you have to have this mousse so your hair will sit correctly. I'll just add it onto your bill," or "We have only two of these carrot juicers left. After these are gone, I won't have any more," and "This is a special price just for you, so take it or leave it because I am just about to close up shop." Rest assured, there are lots of carrot juicers in the world, and if one person is willing to give you a "good deal" on it, someone else will too. Go home, research the product and prices online, and save yourself from paying too much.

12 **Emperor’s New Clothes** - What better gift could you give someone than the symbol of the first Christmas -- a star? Various companies claim you can name a star for between $20 and $150. These companies will send you a certificate with the name and location of "your star" and promise that your star's name will be in a star registry. Here's the problem: Stars are named by the International Astronomical Union. Names for stars (and most are given numbers) are assigned according to the internationally accepted rules of the IAU. Anyone else who claims to be able to name stars has no more legal standing than your neighbor's Rottweiler.

SCAMS AND YOU: WHAT TO DO IF YOU GET SCAMMED!

Your authorities may not always be able to take action against scams, even if it seems like a scammer might have broken the law.

Reducing the damage

Although it may be hard to recover any money that you have lost to a scam, there are steps you can take to reduce the damage and avoid becoming a target for a follow-up scam. The more quickly you act, the greater your chance of reducing your losses. Report a scam. By reporting the scam to authorities, they may be able to warn other people about the scam and

minimize the chances of the scam spreading further. You should also warn your friends and family of any scams that you come across. Details on how to report a scam are on page 30 of this publication.

If you have been tricked into signing a contract or buying a product or service

Contact your Sheriff of District Attorney's office and consider getting independent advice to examine your options: there may be a cooling-off period or you may be able to negotiate a refund.

If you think someone has gained access to your online account, telephone banking account or credit card details

Call your financial institution immediately so they can suspend your account and limit the amount of money you lose. Credit card companies may also be able to perform a "charge back" (reverse the transaction) if they believe that your credit card was billed fraudulently.

Do not use contact details that appear in emails or on websites that you are suspicious of—they will probably be fake and lead you to a scammer. You can find legitimate contact details in the phone book, an account statement or on the back of your ATM card.

If the scam relates to your health

Stop taking any pills or substances that you are not sure about. See a doctor or other qualified medical professional as soon as you can. Be sure to tell them about the treatment that the scammer sold (take along any substances, including their packaging). Also tell them if you have stopped any treatment that you were taking before the scam.

If you have sent money to someone that you think may be a scammer

If you sent your credit card details, follow the instructions in the section opposite.

If you sent money through an electronic funds transfer (over the Internet), contact your financial institution immediately. If they have not already processed the transfer, they may be able to cancel it.

If you sent a check, contact your financial institution immediately. If the scammer hasn't already cashed your check, they may be able to cancel it.

If you sent money through a wire service (such as Western Union or Money Gram), contact the wire service immediately. If you are very quick, they may be able to stop the transfer.

If you have been tricked by a door-to -door seller

You may be protected by laws that provide you with a "cooling-off" period, during which you can cancel an agreement or contract that you signed. Contact your provincial or territorial consumer affairs office for advice about door-to-door sales laws.

If you have been scammed using your computer

If you were using your computer when you got scammed, it is possible that a virus or other malicious software is still on your computer. Run a full system check using reliable security software.
If you do not have security software (such as virus scanners and a firewall) installed on your computer, a computer professional can help you choose what you need.

Scammers may have also gained access to your online passwords. Change these using a secure computer.

If the scam involve s your mobile phone

Call your telephone provider and let them know what has happened,

Getting help and reporting a scam

The best agency to contact depends on where you live and what type of scam is involved.

If you think you have spotted a scam or have been targeted by a scam, there are a number of government and law enforcement agencies that you can contact for advice or to make a report. This may help you and prevent others from being ripped off by scam operators.

Internal Revenue Service
www.irs.gov
Better Business Bureau
www.bbb.org
(405) 239-6081
US Postal Inspectors
(877) 876-2455

Local scams: Contact your local offices

Oklahoma County Sheriff's Office
(405) 713-1093
Canadian County Sheriff's Office
(405) 422-3187
Oklahoma County DA
(405) 713-1600
Canadian County DA
(405) 262-0177
Oklahoma Attorney General (Public Protection Unit)
(405) 521-3921
Oklahoma Bankers Association
(405) 424-4518 (x101)-Fraud Unit
Gatekeepers (Oklahoma County)
(405) 840-9676
Legal Aid Services of Oklahoma
1-855-488-6814