Indiana Consumer Protection Guide

Distributed by State Representative

Earl L. Harris Jr.

1-800-382-9842 | www.in.gov/H2

www.facebook.com/inhousedems

@inhsedems @inhousedemocrats

Protecting Yourself from SCAMS

Every day we read of a new scam in which innocent individuals are preyed upon and taken advantage of. If you have ever been a victim of a scam, you are not alone.

Nobody would fall for a fraud if it looks like a fraud. Right? So, most of the time it looks like something else. A good deal, a gift, a business opportunity, or a chance to make a good buck. That's why honest citizens lose millions of dollars to con artists every year.

Most think they couldn't be tricked into handing over hard-earned money for a phony deal. But con artists are experts in human psychology. They know how to gain confidence with smooth talk in a very professional manner.

Con artists and hustlers often prey on people who are not used to making decisions about home repairs or are not knowledgeable about business investments or banking practices. But they will try their tactics on anyone.

This booklet provides valuable information on the latest scams and what you can do to help protect yourself from being a victim.

Information for this book has come from the FBI, National Fraud Information Center, Office of the Indiana Attorney General and the AARP.

This publication was produced by the Publications Office of the Indiana House of Representatives Democrat Caucus.

For additional copies, please contact your State Representative at 1-800-382-9842.

Updated May 2022

Protecting Yourself from SCAMS

Contents

Identity Theft Prevention

Impersonation fraud occurs when someone assumes your identity to perform a fraud or other criminal act. Criminals can get the information they need to assume your identity from a variety of sources, such as the theft of your wallet, your trash, or from credit or bank information. They may approach you in person, by telephone or on the Internet and ask you for the information.

Protecting Your Credit:

Protecting your identity begins by reducing the number of places where your personal information can be found. Reducing the number of credit cards you have and only carrying the cards that you intend to use may help reduce your risk of becoming an identity theft victim. Follow these additional steps to reduce your risk:

1. **The single most important thing you can do to reduce your risk of identity theft is to place a "credit freeze" on your credit reports.** A credit freeze keeps new creditors from accessing your credit report without your permission. If you activate a credit freeze, an identity thief cannot take out new credit in your name, even if the thief has your SSN or other personal information, because creditors cannot access your credit report.

   Any Indiana resident can request a credit freeze free of charge. There is no fee for Indiana residents to place, temporarily lift or remove a credit freeze, or request a new password or PIN. More information about placing a security freeze on your credit reports is available online at www.IndianaConsumer.com/IDTheft or by calling the Indiana Attorney General's office at 1-800-382-5516.

2. **Review your credit report on a regular basis to help deter future ID theft.** Federal law give you the right to one free credit report per year from each of the three major credit bureaus. In order to receive your annual credit reports for free, you must request them online at www.annualcreditreport.com or by phone at 1-877-322-8228.

   The Indiana Attorney General offers a credit report tracker in its online toolkit available at www.IndianaConsumer.com/IDTheft. Since you are not required to request all three credit reports at once, it is recommended that you request one report every four months in order to keep a more continuous watch on your credit. The Indiana Attorney General's tracker tool will record when you requested your free report from each agency and automatically send you an annual email reminder notifying you of when you're eligible to obtain your next free credit report from that agency.

Tips to Avoid Identity Theft:

- Never throw away ATM receipts, credit statements, credit cards, or bank statements in a usable form. Review financial documents and billing statements regularly and shred before discarding them.
- Never give your personal information over the telephone unless you initiated the call and know who you are dealing with.
- Beware of missing bills or unexpected mail such as credit cards or account statements.
- Don't carry your Social Security Card in your wallet or write your SSN on a check.
- Shop with cash when visiting fairs, festivals, luncheons or sporting events.
- Prescription bottles contain vital information and should be disposed of without labels.

If you believe your identity has been stolen:

Download the ID Theft Victim Kit provided by the Indiana Attorney General at **www.IndianaConsumer.com/IDTheft** and click 'Resources' for information about how to restore your identity. You are also encouraged to file an identity theft complaint with the Attorney General's ID Theft Unit by calling 1-800-382-5516.

Health-Related Fraud

Medical Equipment Fraud:

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" Schemes:

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:

Customers or providers bill insurers for services never rendered by changing bills or submitting fake ones.

Medicare Fraud:

Medicare fraud can take the form of any of the health insurance frauds described above. Senior citizens are frequent targets of Medicare schemes, 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 forms. Once a signature is in place, the manufacturers bill Medicare for merchandise or service that was not needed or was not ordered.

Counterfeit Prescription Drugs:

Be mindful of appearance. Closely examine the packaging and lot numbers of prescription drugs and be alert of any changes from one prescription to the next. Consult your pharmacist or physician if your prescription drug looks suspicious. Alert your pharmacist and physician immediately if your medication causes adverse side effects or if your condition does not improve.

Use caution when purchasing drugs on the Internet. Do not purchase medications from unlicensed online distributors or those who sell medications without a prescription. Reputable online pharmacies will have a seal of approval called the Verified Internet Pharmacy Practice Site (VIPPS), provided by the Association of Boards of Pharmacy in the United States. Product promotions or cost reductions and other "special deals" may be associated with counterfeit product promotion.

Tips to Avoid Health Insurance Fraud:

- 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 of 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.

Tips to Avoid Funeral and Cemetery Fraud:

- Be an informed consumer. Take time to call and shop around before making a purchase. Take a friend with you that may offer some perspective to help make decisions. Funeral homes are required to provide detailed price lists over the phone or in writing. Ask if their lower priced items are included on their price list.
- Be informed about caskets before you buy one. It is a myth that funeral providers can determine how long a casket will preserve a body.
- Research funeral home service fees when shopping for products elsewhere. Some of these charges are prohibited by the Federal Trade Commission.
- You should know that embalming is not legally required and that a casket is not needed for direct cremations.
- Do not be pressured by high-priced pitches from funeral industry vendors.
- Require all proposed plans and purchases to be put in writing.
- Remember to carefully read contracts and purchasing agreements before signing. Find out if agreements you sign can be voided, taken back or transferred to other funeral homes.
- Before you consider pre-paying, make sure you are well-informed.
- When you do make a plan for yourself, share your specific wishes with those close to you.

Telemarketing Fraud

When you send money to people you do not know personally or give personal or financial information to unknown callers, you increase your chances of becoming a victim of telemarketing fraud.

Warning signs – what a caller may tell you:

- You must act 'now' or the offer won't be good.
- You've won a 'free' gift, vacation or prize. But you have to pay for postage and handling or other charges.
- You must send money, give a credit card or bank account number, or have a check picked up by courier. You may hear this before you have had a chance to consider the offer carefully.
- You don't need to check out the company with anyone. The callers say you do not need to speak to anyone including your family, lawyer, accountant, local Better Business Bureau or consumer protection agency.
- You don't need any written information about their company or their references.
- You can't afford to miss this 'high-profit, no-risk' offer.

If you hear these – or similar – lines from a telephone salesperson, just say "no, thank you," and hang up the phone.

Top Ten Telemarketing Scams

1) Prizes/Sweepstakes
2) Scholarships/Grants
3) Magazine Sales
4) Credit Card Offers
5) Fake Check Scams
6) Advance Fee Loans
7) Lotteries/Lottery Clubs
8) Work-at-Home Plans
9) Phishing
10) Travel/Vacation

Tips to Avoid Telemarketing Fraud:

It's very difficult to get your money back if you've been cheated over the phone. Before you buy anything by telephone, remember:

- Don't buy from an unfamiliar company. Legitimate businesses understand your request for more information and are happy to comply.
- Always ask for and wait until you receive written material about any offer or charity. If you get brochures about costly investments, ask someone whose financial advice you trust to review them. But, unfortunately, beware – not everything written down is true.
- Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state Attorney General, the National Fraud Information Center or other watchdog groups. Unfortunately, not all bad businesses can be identified through these organizations.
- Obtain a salesperson's name, business identity, telephone number, street address, mailing address and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses and business license numbers. Verify the accuracy of the information you receive.
- Before you give money to a charity or make an investment, find out what percentage of the money is paid in commissions and what percentage actually goes to the charity or investment.
- Before you send money, ask yourself a simple question: "What guarantee do I really have that this solicitor will use my money in the manner we agreed upon?"

- You must not be asked to pay in advance for services. Pay for services only after they are delivered.
- Some con artists will send a messenger to your home to pick up money, claiming it is part of their service to you. In reality, they are taking your money without leaving any trace of who they are or where they can be reached.
- Always take your time making a decision. Legitimate companies won't pressure you to make a snap decision.
- Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.
- Before you receive your next sales pitch, decide what your limits are – the kinds of financial information you will and won't give out on the telephone.
- It's never rude to wait and think about an offer. Be sure to talk over big investments offered by telephone salespeople with a trusted friend, family member or financial advisor.
- Never respond to an offer you don't understand thoroughly.
- Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.
- Your personal information is often brokered to telemarketers through third parties.
- If you have information about a fraud, report it to state, local or federal law enforcement agencies.

Indiana's Do Not Call List

All Indiana residents can register their home, wireless or VOIP telephone numbers on the state's Do Not Call list at any time. Once your phone number has been added to the list there is no need to re-register. However, you will need to update your registration if your phone number or address changes.

To register, go online to www.IndianaConsumer.com or call 1-888-834-9969.

National Do Not Call List

Indiana citizens may also register with the National Do Not Call list. For more information, visit www.donotcall.gov or call 1-888-382-1222.

Telemarketing Fraud Checklist

The AARP (www.aarp.org) has developed the following checklist to aid individuals in avoiding fraud. Keep this list handy when telemarketers call. The questions will help you to determine whether a telemarketing call is legitimate or not. You also should save your notes from each call in case you develop concerns about a donation or purchase after the call.

1—Note the date and time of the call

- Is the call before 8 a.m. or after 9 p.m.?

What to watch out for: Hang up if the answer is yes. All organizations that follow federal telemarketing guidelines must limit their calls to this 13-hour period.

2—Has the caller fully identified the organization that he/she represents immediately after you answer?

- Does the caller work for the organization itself or for a fund-raising firm?
- Ask for and jot down the full name, address and phone number of the person making the call and the organization(s) that the caller represents.

What to watch out for: Hang up if the caller hesitates or refuses to provide any of this information. Organizations that heed federal telemarketing guidelines should immediately identify themselves.

3—Does the caller represent a charitable organization?

- What is the charitable purpose of the organization?
- Is it registered with the state (Secretary of State, Department of Justice or Attorney General)?
- What percentage of its total income does the charity spend on its program?

What to watch out for: Don't settle for vague descriptions of the organization's activities that emphasize the problem without explaining what the charity is actually doing about it. Also, make sure that at least 50 to 60 percent of your donation will go toward actual charitable work, not fund-raising expenses.

4—Is the caller offering a product, service or contract of some sort?

- How much does the product or service cost?
- Is the sale final or nonrefundable?
- Does the caller seek payment prior to delivering the product or service?

What to watch out for: Hang up if the caller seeks payment prior to delivery of the product or service or if the offer does not come with a money-back guarantee.

5—Does the caller seek cash?

What to watch out for: Hang up immediately if the answer is yes. Legitimate organizations do not seek cash payments via the phone.

6—Will the caller send details of the charity or product/service in writing and therefore give you time to carefully review the offer?

What to watch out for: Hang up immediately if the answer is no or if you must act "right away." Legitimate organizations will respect your interest in taking time to review offers prior to making a decision.

Investment-Related Scams

Letter of Credit Fraud:

Legitimate letters of credit are never sold or offered as investments.

Legitimate letters of credit 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.

Letter 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. (See Prime Bank Notes below for additional information.)

Tips to Avoid Letter of Credit Fraud:

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

Prime Bank Note Scheme:

International fraud artists have invented an investment scheme that offers extremely high yields in a relatively short period of time. In this scheme, they purport 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 2% profit on 10 separate occasions, or "traunches," the seller would receive a 20% 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 nondisclosure and noncircumvention 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 that is 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.

Tips to Avoid Prime Bank Note Fraud:

- 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 wary of business deals that require nondisclosure or noncircumvention agreements that are designed to prevent you from independently verifying information about the investment.

"Ponzi" Scheme:

A Ponzi scheme is essentially an investment fraud wherein the operator promises high financial returns or dividends that are not available through traditional investments. Instead of investing victims' funds, the operator pays "dividends" to initial investors using the principle amounts "invested" by subsequent investors. The scheme generally falls apart when the operator flees with all of the proceeds, or when a sufficient number of new investors cannot be found to allow the continued payment of "dividends."

This type of scheme is named after Charles Ponzi of Boston, Mass., who operated an extremely attractive investment scheme in which he guaranteed investors a 50 percent return on their investment in postal coupons. Although he was able to pay his initial investors, the scheme dissolved when he was unable to pay investors who entered the scheme later.

Tips to Avoid Ponzi Schemes:

- As with all investments, exercise due diligence in selecting investments and the people with whom you invest.
- Make sure you fully understand the investment before you invest your money.

Pyramid Scheme:

Pyramid schemes, 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 scheme there is typically a representation that new participants can recoup their original investments

by inducing two or more prospects to make the same investment. Promoters 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.

Tips to Avoid Pyramid Schemes:

- Be wary 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.
- Independently verify the legitimacy of any franchise or investment before you invest.

Tips to Avoid Investment Fraud:

- Don't invest in anything based on appearances. Just because an individual or company has a flashy website, doesn't mean it is legitimate. Websites can be created in just a few days. After a short period of taking money, a site can vanish without a trace.
- Don't invest in anything you are not absolutely sure about.
- Do your homework on the individual or company to ensure legitimacy.
- Check out other websites regarding this person/company.
- Be cautious when responding to special investment offers (especially through unsolicited e-mail).
- Be cautious when dealing with companies from outside your own country.
- Inquire about all the terms and conditions – too good to be true probably is.

Advance Fee Scheme:

An advance fee scheme occurs when the victim pays money to someone in anticipation of receiving something of greater value, such as a loan, contract, investment, or gift, and then receives little or nothing in return.

The variety of advance fee schemes is limited only by the imagination of the con artists who offer them. They may involve the sale of products or services, the offering of investments, loans, lottery winnings, "found money," or many other "opportunities." Clever con artists will offer to find financing arrangements for their clients who pay a "finder's fee" in advance. They require their clients to sign contracts in which they agree to pay the fee when they are introduced to the financing source. Victims often learn they are ineligible for financing only after they have paid the "finder" according to the contract.

Tips to Avoid the Advanced Fee Schemes:

- Follow common business practice. For example, legitimate business is rarely conducted in cash on a street corner.
- If you have not heard of a person or company you intend to do business with, learn more about them. Depending on the amount of money you intend to spend, you may want to visit the business location, check with the Better Business Bureau, or consult with your bank, an attorney or the police.

Green Dot "MoneyPak" Scams

The Indiana Attorney General's Office has seen a rise in complaints involving schemes that use the Green Dot "MoneyPak" cards sold at convenience stores, pharmacies and major retailers. The cards offer a convenient way to pay bills online and make purchases on the Internet. Scammers have found ways to deceive consumers into handing over the MoneyPak 14-digit security code over the telephone, thereby allowing the scammers to immediately transfer the money out of the account. Once transferred, the consumer's money is lost.

- Make sure you fully understand any business agreement that you enter into. If the terms are complex, have them reviewed by a competent attorney.
- Be wary of business deals that require you to sign nondisclosure or noncircumvention agreements that are designed to prevent you from independently verifying the identity of the people with whom you intend to do business. Con artists often use noncircumvention agreements to threaten their victims with a civil suit if they report their losses to law enforcement.

Mortgage Foreclosure Fraud

If your home is facing foreclosure, you are facing one of the worst financial crises of your life. There are many scam artists promising to help people facing foreclosure save their homes. Mortgage fraud has escalated into one of the fastest-growing white-collar crimes in the nation and can end up costing you the home and equity you're desperately trying to save from foreclosure.

There are many companies and individuals who will promise to help you avoid foreclosure or to modify your loan for a fee. Indiana law regulates the activities of foreclosure consultants and the Office of the Indiana Attorney General enforces those laws.

Tips to Avoid Mortgage Foreclosure Fraud:

- Contact the Indiana Foreclosure Prevention Network (IFPN) for **free** foreclosure consulting services. IFPN is a non-profit, statewide network of certified housing counselors who can be reached toll-free at 1-.877-GET-HOPE (1-877-438-4673).
- Indiana law requires foreclosure consultants to have a $25,000 surety bond on file with the Attorney General's Office. If the foreclosure consultant asks you for money before services are complete, ask the foreclosure consultant for a copy of the surety bond.
- If you enter into a contract for foreclosure consulting services, make sure the contract has a detailed description of the services and the cost of the services; information regarding your right to cancel the contract before midnight of the third business day after the transaction; and that you and the foreclosure consultant sign and date the contract.
- Retain a copy of the contract and any receipts, cancelled checks, or other evidence of payment. Under state law, foreclosure consultants are required to retain all customer records for at least three years.

helpful TIPS

- Ensure every aspect of any real estate transaction is in writing.
- Be wary of undisclosed costs, interest rates or fees.
- Do not sign any document before you read and understand it.

Internet Fraud

"Nigerian" Scams or "419" Fraud:

"Nigerian" scams combine the threat of identity theft with a variation of an advance fee scheme in which an email from someone claiming to be an official, businessperson or surviving relative of a former government official from another country offers the "opportunity" to share in a percentage of millions of dollars that they are trying to transfer out of their country. The recipient is encouraged to send identifying information to the scammer, such as bank name and account numbers. The scheme relies on convincing a willing victim to send money to help pay transfer costs, attorney's fees or taxes to access the money.

Payment of taxes, bribes to government officials and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are transferred out of their county. In actuality, the millions of dollars do not exist and the victim eventually ends up with nothing but loss. Once the victim stops sending money, the perpetrators have been known to use the personal information and checks that they received to impersonate the victim, draining bank accounts and credit card balances until the victim's assets are taken in their entirety. Millions of dollars in losses are caused by these schemes annually. Some victims have been lured to other countries where they have been imprisoned against their will, in addition to losing large sums of money. The schemes, which seem to have first originated in Nigeria, violate section 419 of the Nigerian criminal code, hence the label "419" fraud.

"Free" Trial Offer Scams

Misleading free trial offers online for diet supplements, penny auctions and money-making schemes blanket the internet, resulting in thousands of complaints every year. The free trial offers seem no-risk, but complainants state they were repeatedly billed every month and found it extremely difficult to cancel.

Phishing Emails:

Phishing – also know as carding or brand-spoofing – is a type of deception designed to steal your identity. In a phishing scam, a thief tries to get information like credit card numbers, passwords, account information or other personal information from you by convincing you to provide it under false pretenses.

In a phishing scam, the messages often look very authentic, featuring corporate logos and formats similar to the ones used for legitimate messages. Typically, they ask for verification of certain information, such as account numbers and passwords, allegedly for auditing purposes.

Overpayment Scams:

In check overpayment scams, the con artist responds to an item you may have for sale online. They send you a check payable for more than the agreed upon price along with a reason why they are writing the check for more. They ask that you deposit the amount in your bank account and wire or transfer the extra amount to a foreign account. The scammer vanishes after the money is deposited. At that point, the check bounces and you are required to pay for the entire amount.

Lottery/Sweepstakes Scams:

In foreign lottery scams, you receive an email claiming that you are the winner of a foreign lottery or sweepstakes. All you need to do to claim your prize is send money to pay the taxes, insurance, or processing or customs fees. Sometimes you will be asked to provide a bank account number so the funds can be deposited. In reality, your bank account is likely to be depleted. You end up shelling out your hard-earned money for "winnings" you will never receive.

Disaster Relief Scams:

Every time there is a disaster such as a tsunami, tornado or earthquake, millions of citizens want to do something to help the victims. Scammers take advantage of this by setting up scam charity institutions that rob the money that you wanted to send to the victims of the disaster. Scammers also attempt phishing by sending you donation requests via email where you can click on a link that leads you to a website designed to steal your passwords and other personal information.

Tips to Avoid Internet Fraud:

- There is no reason to give out your social security or driver's license number to anyone online.

- Be cautious when responding to special offers or emails claiming you have won a lottery or sweepstakes in a foreign county. It is illegal for you to play a lottery or sweepstakes in a foreign country unless you are physically in that country.

- One way to better protect yourself against hackers is to use two-factor authentication on important accounts such as banking, investment, and retirement accounts. This is because often a password is easy to guess for a hacker, but another layer of protection through an authenticator makes your accounts much more secure. Authenticators send you a unique code that you must type in after every time you enter your password. You can set up two-factor identification through mobile apps such as the Google or Microsoft Authenticator.

- Another way that hackers could gain access to your information is through weak passwords for important accounts. Your passwords for your important accounts should be different for different accounts, which ensures that even if a hacker guesses the password for one account, they cannot gain access to all of your accounts. Additionally, it is recommended that your passwords are longer than eight characters. This could look like using a string of words such as "bee honey bourbon rain" for your password, instead of a shorter one-word passcode.

- Don't give out your credit card number(s) online unless the site is a secure and reputable site. Look for the indications that your information will be encrypted such as a URL that begins with "https:" instead of "http:" and a padlock icon. If the padlock is closed, the information is encrypted. Some attackers try to trick users by adding a fake padlock icon, so make sure that the icon is in the appropriate location for your browser.

- You should also keep a list of all your credit card issuers' contact information. If anything looks suspicious or you lose your credit card(s), you should contact the card issuers immediately.

- If you are going to participate in online auctions, understand as much as possible about how they work, what your obligations are as a buyer, and what the seller's obligations are before you bid. Learn as much as possible about the seller, especially if the only information you have is an e-mail address. If it is a business, check the Better Business Bureau where the seller/business is located. Determine what method of payment the seller is asking from the buyer and where he/she is asking to send payment. If a problem occurs with the auction transaction, it could be much more difficult if the seller is located outside the U.S. because of the difference in laws.

Romance Fraud

Confidence or romance fraud occurs when someone deceives you into believing that you have a trusted relationship, such as being a friend, family member, or romantic interest, which they then use to convince you to send them money, provide personal information or purchase items of value for them. It is believed that around two-thirds of romance fraud victims are women, with an average age of 50.

Many scammers will use online dating sites to pose as potential romantic interests, and earn the victim's trust. After doing this, they might ask for things like money for airfare to visit or ask for gifts from the victim.

How to protect yourself:

1. Use your best judgement when interacting with others online. Keep note of any inconsistencies in facts they tell you about themselves.
2. Be wary of those who ask for financial assistance, give vague answers to your questions, claim early in communication that your introduction was "fate" or "destiny," or ask to immediately begin chatting on a service outside the dating site.
3. Avoid revealing too much personal information in a dating profile or to someone you've chatted with only online. Scammers can exploit details like your last name or place of work to manipulate you or commit identity theft.
4. **Never** send money to anyone that you meet online, especially by wire transfer. **Never** provide credit card information or bank account information, or personal identifying information, such as your Social Security Number, with someone who does not need to know this information.
5. Don't feel a false sense of safety because you're the one who made first contact. Scammers flood dating apps and websites with fake profiles and wait for victims to come to them.

Why should Senior Citizens be concerned?

According to the FBI, the elderly are targeted for fraud for several reasons:

1) Older American citizens are most likely to have a "nest egg," own their home and/or have excellent credit, all of which the con-man will try to tap into. The fraudster will focus his/her efforts on the segment of the population most likely to be in a financial position to buy something.

2) Individuals who grew up in the 1930s, 1940s and 1950s were generally raised to be polite and trusting. Two very important and positive personality traits, except when it comes to dealing with a con man. The con man will exploit these traits knowing that it is difficult or impossible for these individuals to say "no" or just hang up the phone.

3) Older Americans are less likely to report a fraud because they don't know who to report it to, are too ashamed at having been scammed or do not know they have been scammed. In some cases, an elderly victim may not report the crime because he or she is concerned that relatives may come to the conclusion that the victim no longer has the mental capacity to take care of his or her own financial affairs.

4) When an elderly victim does report the crime, they often make poor witnesses. The con man knows the effects of age on memory and he/she is counting on the fact that the elderly victim will not be able to supply enough detailed information to investigators, such as: How many times did the fraudster call? What time of day did he/she call? Did he provide a call back number or address? Was it always the same person? Did you meet in person? What did the fraudster look like? Did he/she have any recognizable accent? Where did you send the money? What did you receive, if anything, and how was it delivered? What promises were made and when? Did you keep any notes of your conversations?

The victims' realization that they have been victimized may take weeks or, more likely, months after contact with the con man. This extended time frame will test the memory of almost anyone.

5) Lastly, when it comes to products that promise increased cognitive function, virility, physical conditioning, anti-cancer properties and so on, older Americans make up the segment of the population most concerned about these issues. In a country where new cures and vaccinations for old diseases have given every American hope for a long and fruitful life, it is not so unbelievable that the products offered by these con men can do what they say they can do.