Revision 20260408

ID THEFT, FINANCIAL FRAUD & SCAM REMINDER TIP SHEET

"You can ignore reality, but you can't ignore the consequences of ignoring reality." Ayn Rand

It's human nature to believe that nothing bad will ever happen to us. But, we live in very unpredictable times – we see catastrophic events reported on the news every night, whether here in the U.S. or other locations around the world.

First, a brief history lesson: Once upon a time, there were people who thought the telegraph was going to be a passing fad, and then it became an absolute communications necessity during the early years of our country. Then radio came along and became a vital way people got their news and entertainment, but in its early days, it was considered a fad until almost everyone had one in their homes and many cars and it is still used today for all kinds of communications – emergency services, satellites, etc. Then came the telephone and many people thought that it was a passing fad until almost everyone had one in their homes and offices. Then came the television - the efforts of Jenkins and Baird to develop the television were generally greeted with ridicule or apathy. As far back as 1880, an article in the British journal *Nature* speculated that television was possible but not worthwhile: The cost of building a system would not be repaid, because there was no way to make money out of it. Subsequently, an article in *Scientific American* thought there might be some uses for television, but entertainment was not one of them. Most people thought the whole concept was insane. Oh, how unbelievably wrong they were! It was a luxury for many people in its early days, but eventually became a primary way people got their news and entertainment and like the radio, today most people have multiple TV's and radios in their homes and even in their cars and on their smart devices!! Then came the computer (and later the Internet). Who would need one of those except for scientists and engineers, right?? Clearly a personal computer would be a luxury and a passing fad, so why should the average person even bother learning how to use one, right? Then came the cell phone – who wanted to carry around one of those giant bricks? Clearly this was another one of those passing fads, right? Who

needed a cell phone when we had telephones in our homes and pay phones in every gas station, convenience store, restaurant and on every street corner? Then came the integration of the computer into the cell phone to make smart phones, but who really needed one of those, right? Okay, I think you understand what I'm saying, but here's my point: I work with a lot of seniors, many of whom were in their late 20's and early 30's when computers started gaining popularity. Once again, many thought that they were a passing fad and never learned how to use them or didn't learn how to use them much beyond a very basic level. Now, the technology has far surpassed their ability to catch up, so, they either barely use them or don't use them at all. I've had people tell me, "Oh, I'm safe (from cyber fraud) because I'm not online at all; I don't even own a computer." Let me break it to you like a reality sledgehammer shot right between the eyes: You may not be online, but all your personal information is, the criminals know this and that information is easily accessible to them and it is only a matter of time, if it hasn't happened already (but you don't/won't know that because you aren't online), that you and or your information will be exploited by them if you do not take the steps outlined in the guide to secure that information in both your digital and non-digital lives, most of which requires the use of a computer. Sorry, there is no escape from "the machine" now. And I sincerely apologize for being so shockingly and rudely blunt, but you need to hear the truth about this and get with the program because I don't want you to be another victim of this type of crime!! Find a knowledgeable and trustworthy relative or friend to help you secure your personal information by using the steps I have outlined below. In these matters, an ounce of prevention is truly worth a ton of cure!!! And if you don't believe me, ask anyone in law enforcement, banking or finance and they will tell you.

REMEMBER: These criminals are very sophisticated, both technologically and psychologically. Worldwide, there are tens of thousands of entire groups of people with extensive education and backgrounds in sales, marketing, finance, banking, computers, psychology, sociology, neuro-linguistic programming (NLP), etc. – everything needed to understand how our minds work, what "trips our triggers," and how best to convince us to give them money or for them to scam us in some manner or form. And now they are using AI (Artificial Intelligence) to make the scams even more convincing and effective and it is making matters much worse. Personal loss estimates range from $20-$50 BILLION from 50+ million people annually in the U.S. alone and globally it's hundreds of millions of people affected and over $5 TRILLION, but it could be much worse as much of this crime goes unreported simply because people are ashamed to admit to family, friends, and law enforcement that they got scammed. Posting your personal information on social media only makes you even more of a target by giving them more information and avenues with which to attack you. And stop being so pretentious – I hate to break it to you, but the only ones who care about what is going on in your family's life are those people AND criminals. STOP POSTING EVERYTHING ABOUT YOUR LIFE FOR THE ENTIRE PUBLIC TO SEE – CRIMINALS *WILL* USE ALL THAT INFORMATION AGAINST YOU!!! So, no matter who you are, your age, educational level or socio-economic status, these kinds of crimes affect everyone – 1 person or business every 3 seconds – that's 10,512,000 victims per year, minimum!!! If you suspect you have been scammed or are being abused or exploited, financially or otherwise, please, do not be afraid or ashamed to ask for help – it is not your fault this has happened to you! All the experts admit that unfortunately, we cannot legislate or prosecute our way out of this particular kind of crime. Our financial institutions and law enforcement recognize that these are serious crimes affecting more and more people and businesses each day and they sincerely want to help stop them, but YOU MUST take steps to educate yourself, your family and your friends in order to protect yourselves from this type of crime and immediately report it when it happens. In fact, I encourage you to be brave and share your experience(s) with everyone you can so hopefully they will learn from your experience(s) and take steps to protect themselves before they become victims, too and statistically speaking, there's a very good chance they will at some point and even possibly

multiple times. In today's world, YOU must be your own first responder in ALL aspects of your life!!!

In addition to reporting any crimes to the police and your financial institutions, go to the websites below immediately if you have been a victim – these websites outline everything you need to do to recover and protect yourself and your assets. Time (usually within 72 hours max.) is truly of the essence to the recovery of losses (unless cash and then usually there is no recovery)!:

U.S. Federal Trade Commission: **https://www.identitytheft.gov**
U.S. Dept. of Justice Elder Fraud Hotline: **https://www.justice.gov/stopelderfraud**
Federal Bureau of Investigation: **https://www.ic3.gov**
National Center for Victims of Crime, Financial Fraud Victim Recovery Checklist:
https://victimsofcrime.org/victim-recovery-checklist/
AARP Fraud Watch Network Hotline[1] (Questions? Report, get help/guidance. Free to all!): 877-908-3360

GENERAL WARNING SIGNS OF A SCAM

These usually involve some kind of verbal ruse (usually requiring urgent action on your part) over the phone (or even show up at your home now) from someone you do not know, however, it may be someone you do know or think you know, such as in cases of a romance-related or tie-in scams like the "Granny Scam." Note that legitimate persons from the agencies and organizations referenced below will never call you for official business reasons – they will contact you via official USPS correspondence (letter) or a uniformed law enforcement official will personally serve you with a warrant,….but will not warn you in advance of service!

A. Person contacting you, usually someone you do not know or may have known a long time ago (or pretends to be), demands that you maintain the utmost secrecy and not tell anyone about your actions the caller directs you to take and or the caller requires you to stay on the phone with them so they can "coach" you through the steps they want you to take and help you overcome any objections or questions at a bank, car dealer, or other institution or person you are contacting to assist you with the transaction the caller is requiring of you. They may require you to lie to the banker, etc.

B. You received a deposit to your account from an unknown person/entity and they contact you to re-direct the funds to someone or somewhere else.

1) Person threatens to take some sort of immediate financial or legal action against you unless you provide payment immediately.

2) Person urges or demands that you take some kind of action immediately that will benefit them or an organization in some way, usually financially.

3) Person urges or demands that you provide a credit card number or checking account number to pay a late bill or fine.

4) Person claims they are with a local, federal or state agency (IRS, FBI, Social Security, Medicare, other law enforcement), process server, or utility company, bank, financial institution, etc., and demands that you take some kind of action (usually make a payment with a credit card, gift card or checking account

[1] https://www.aarp.org/money/scams-fraud/helpline.html?intcmp=AE-SCM-FRD-HLPLN

number and/or provide some other kind of personal or financial information) under threat of immediate punitive action against you, including warrants for your arrest.

5) Person calls or says they are coming to your house to deliver some kind of prize/lottery/sweepstakes winnings or other gift(s). The other sign here is that they say they will need a small (initially) fee, paid in the form of a **gift card** (Green Dot, iTunes, etc.) to pay taxes, register your winnings with the FDIC, IRS, etc. If you legitimately win, the **only** paperwork you should be asked to fill out is a form the prize presenters are required to file with the IRS and state tax commission (and you should never do this online). You **never** have to pay a **fee** for winning a prize, only taxes (which are sometimes taken out **before** you receive your prize money) and **only** to the respective governmental agency **directly**. This ruse is common with Publishers Clearing House (PCH) prize scams and can become a very dangerous scam that can morph into a complete life takeover and drain you of all your assets and even worse, physical harm!

6) **Any type of activity** that involves you paying any kind of fee, most often with a **gift card**, Green Dot card, iTunes card, Vanilla Visa, etc. Remember, gift cards are for **gifts only, not for paying bills!!** Or any transaction requiring payment in gold, silver, cryptocurrency, or any other type of "non-standard" form of payment or that requires you to go to an ATM or Western Union office to make the transaction.

7) Person you've met online (especially if they are overseas) and or may have a romantic interest in asks you to pick up and re-ship (transship) any type of package, goods, etc., to a third party or forward money to a third party via Western Union, MoneyGram, ACH or wire transfers, Zelle, Venmo, CashApp, etc., or asks you to send them money for a plane ticket to come see you, help pay for medical costs for a sick relative, or anything else that involves you moving money or goods for them or sending them money for any reason – this is common in romance scams and may make you a ***"money mule,"*** which is a highly illegal activity. Also, anyone (including close friends and relatives) asking you to perform banking activities on their behalf, e.g., cashing a check or money order, transferring funds, etc.- in almost all cases, there is fraud involved and **YOU** will be responsible for paying the bank back! See the FBI's Money Mule Awareness page here[2].

8) Person calls you out of nowhere with a strange, but seemingly harmless question, then calls you back days or weeks later, for whatever reason, and starts to develop a friendship with you – chances are they are using a technique called "social engineering" to "cultivate the halo effect" and "groom" you for victimization of some kind. This can be a process that goes on for weeks, months or even years before the crime occurs. If you are a prolific user of social media, you are much more susceptible to this type of crime because you have given the criminals a significant amount of your personal information to work with. This is also known as an "affinity" crime and sometimes "pig butchering."

9) Person calls you claiming to be a relative or close friend, and they are in some kind of legal, financial, or other trouble and need you to wire money to them to pay a jail bond, etc., or a carrier may be dispatched to your location to pick up the cash (extremely dangerous!). Person calling may also claim to be an attorney calling on behalf of your relative or friend and may let them talk to you briefly so you can confirm their identity. **However,** with the advent of AI (artificial intelligence) and deep fakes (audios & videos), criminals can very easily spoof actual phone numbers and caller ID's and make voice and faces appear that you are actually talking to someone you know. **Be extremely cautious.** See **#12** below regarding family code words. This ruse is common in "Granny Scams" and "Drug Cartel Scams."

Watch/listen to these YouTube news and investigative video documentaries and podcasts:

[2] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/money-mules

- TAP and You're Broke: The Wireless Skimming Scam Spreading Everywhere – 850 Club Credit 202051031[3] More videos on Ghost Tapping[4]
- Seeing Isn't Believing: The Rise of AI-Generated Fraud – IAFCI 20250312[5]
- How to Spot a Credit Card Skimmer Before You Swipe – NBC 10 Boston 20240724[6]
- Romance Scams – Trafficked with Mariana van Zeller & National Geographic 20240210[7]
- Scams – Trafficked with Mariana van Zeller & National Geographic 20220422[8]
- CBS News Chicago - New technology including AI is being used in romance scams 20240422[9]
- CBS Reports - Anything for Love: Inside the Romance Scam Epidemic 20240731[10]
- CBS Daily Report - Inside look at Ghana's "hustle kingdom" and romance scam operations, 20240926[11]
- CBS Eye on America - Inside an elaborate romance scam that cost a US man $700,000 20240926[12]
- CBS Eye on America - Scammers hire models to fool Americans, 20240927[13]
- CBS Daily Report – 92-Year Old Woman Loses Her Life Savings in Online Scam, 20240924[14]
- Romance scam victim speaks out on "psychological manipulation" that cost her $2.5 million, 20240422[15]
- See other documentaries and exposes on similar types of crime from National Geographic's series "Trafficked" for free on YouTube here.[16]
- For more stories about romance and related scams, search YouTube here.[17]
- Link to all the federal government's various agencies' materials on romance scams[18]

CRITICAL STEPS TO AVOIDING SCAMS

1) **DO NOT** conduct any kind of complicated business when you are physically and or emotionally tired, stressed, distressed, or under the influence of any drugs (Rx or illegal) or alcohol that may cloud an otherwise clear thought process. Ask a trusted, knowledgeable friend or relative for help, if necessary.

2) **DO NOT** answer the phone unless you recognize the number or name. **Even then**, remember, Caller ID's [and now voices and people's images using Artificial Intelligence (AI)] can be spoofed to appear (even on video chat) or sound like anyone from the President to your parents, spouse, child, financial institutions, law enforcement, etc., so be very careful. If in doubt, hang up, get the number yourself off a billing statement, official online website or account, local bank branch, back of credit card, or other trusted source and call them back.

[3] https://www.youtube.com/watch?v=NgIZWZ10nZs
[4] https://www.youtube.com/results?search_query=ghost+tapping
[5] https://www.protectorspodcast.com/episode/seeing-isnt-believing-the-rise-of-ai-generated-fraud
[6] https://www.youtube.com/watch?v=5l_KlO5AkFo
[7] https://www.youtube.com/watch?v=5XfCVk2gZCY
[8] https://www.youtube.com/watch?v=ivWUZf2-M_U
[9] https://www.youtube.com/watch?v=_9eHCzW4eMI
[10] https://www.youtube.com/watch?v=w-75nDH-bbc
[11] https://www.youtube.com/watch?v=Lbc9rRn-PgA
[12] https://www.youtube.com/watch?v=7hFTFlo4d1c
[13] https://www.youtube.com/watch?v=5iXLHm4oT0w
[14] https://www.youtube.com/watch?v=pGWXrjaNg-g
[15] https://www.youtube.com/watch?v=PtjL555xWqg
[16] https://www.youtube.com/playlist?list=PLivjPDlt6ApT3hUwHaxPxoio9Uf3mPcoq
[17] https://www.youtube.com/results?search_query=romance+scams
[18] https://connect.usa.gov/dating-or-defrauding

2).a. **DO NOT (NEVER, EVER)** give out your home address and allow an unknown individual (caller) to come to your house for any reason.

3) **DO NOT** answer the door unless you know who it is. Get an easy-to-set up Blink[19] or other brand wi-fi enabled doorbell camera – $50 or less. Official credentials and uniforms can easily be mimicked by criminals. If someone shows up and claims to be with law enforcement and demands you open the door, call 911 to confirm that they have been dispatched to your location, even if they claim to have a warrant and flash an "official-looking" paper in front of you. Be wary of any ruses to lure you out of the house, e.g., looking for a lost dog, child, etc., damage to your vehicle or house.

4) **DO NOT** let anyone, especially someone you don't know personally, for any reason, intimidate, scare or shame you into providing personal or financial information or payments or coerce you into engaging in questionable activities. (moving money, trans-shipping goods, etc. – See #7 in the previous section.)

5) **DO NOT** open text messages, e-mails, pop-up ads from unknown senders and if you do, **DO NOT** click on any links inside or call any phone numbers contained in them - doing so can install all kinds of malware on your computer or cell phone or put you in personal contact with the scammers. **Think before you click or call!**

5).a. **DO NOT** give out your account login credentials to anyone, especially an unknown individual (caller).

6) **DO NOT** give anyone remote access to your computer unless **you initiate** contact and you are **absolutely certain** they are a legitimate computer repair service and not a scam. Pop-up warnings for virus infection/tech support on your computer are generally scams. Do an Internet search of their name and or toll-free number for scam reports. If you do get an intrusion into your system, physically disconnect from the Internet, turn your computer off and take it to a computer professional to have it cleaned and disinfected. *(The last time I had this done by the Best Buy Geek Squad in 2020, it cost a little less than $200, but that may vary depending on a variety of circumstances.)*

7) **DO NOT** use (insert or swipe) a **debit** card in **any** point-of-sale terminal, gas pump, etc., where skimmers/shimmers may be present. *(In fact, consider getting rid of any **debit** cards – they can give criminals **direct access** to all the money in your bank account and replacing those funds can take time and is a tedious process -see articles below.)* Commercially, publicly available devices claiming to be able to detect the presence of skimmers/shimmers may not always detect all of them. Pay with cash, dedicated gas station credit card, other credit **(not debit)** card, limited amount gift card.
   - Why You Should Never Use A Debit Card to Pay for Anything – Clark Howard[20]
   - 5 Reasons You Probably Shouldn't Use a Debit Card – Reader's Digest[21]
   - 5 Reasons Always Using A Debit Card is a Major Mistake – Yahoo Finance[22]

8) **DO NOT** store payment information (credit card numbers, bank account numbers, etc.), on websites that offer this as a convenience for making future purchases. **See #1 below.**

9) **DO NOT** send money, funds, anything of value, etc., in any form or via any method or give out personal information to someone you don't know.

[19] https://blinkforhome.com/
[20] https://clark.com/personal-finance-credit/never-use-debit-card-pay/
[21] https://www.rd.com/list/times-shouldnt-use-debit-card/
[22] https://finance.yahoo.com/news/5-reasons-why-almost-never-220012233.html

10) **DO** exercise **extreme caution** when making purchases of any goods or services, especially real estate rentals, automobile purchases, work-at-home jobs, etc., through social media, message boards, etc. – these are rife with scammers and other bad actors. **DO NOT** arrange to meet people you don't know. But if you must, say for a legitimate transaction (purchase or sale) for goods, meet in a very public place, like the public parking area at a police station, and take a friend with you and let a 3rd party who will not be present know the full details of those activities and set a time for you to check in with them and establish an emergency code word/phrase.

11) **DO** add a "trusted contact" (not necessarily a joint owner) to your financial accounts in the event you become incapacitated or a victim of fraud. Make sure you know and trust this person very well!

12) **CRITICAL: DO** have a special family "code word or phrase" for emergencies so you know you are really speaking with an actual family member and not a scammer or AI impersonating someone. Do not e-mail, text or post anywhere online this code word/phrase. Make the code very unique.

13) **DO** use a Medicare Healthcare Journal and compare it to your EOB's (Explanation of Benefits) or MSN (Medicare Summary Notice) paper or online statements for fraudulent activity or billing errors. Be very wary of significantly delayed billing dates from what you have in your journal. **Note:** People on Medicare Advantage Plans and Medicare Part D receive EOB's and people on regular Medicare receive MSN's. In Oklahoma, order journals by calling the Medicare Assistance Program office at 800-763-2828. If you are in another state, just do an online search for "(your state's name) Medicare Assistance Program)"." You can also view your Medicare statements/charges with your online account at: https://www.medicare.gov

CRITICAL STEPS TO SECURING YOUR PERSONAL INFORMATION

First let me ask you a question: Would you leave your house unlocked when you leave and then wait until it is burglarized to start locking it up? Of course not. You lock it when you leave as a preventative measure against crime because you know that picking up the pieces in the aftermath of a burglary is much more difficult, time-consuming and expensive than locking it when you leave and setting the alarm, right? Then why do you leave your financial and cyber-life wide open to the criminals? Here is how you lock them up! I can't tell you how many people I have furnished this guide to, only to have them call me later and need help because they are victims of some kind of fraud. When I asked them if they followed the steps I have outlined in this guide, invariably the answer is, "no" and at that point, I just refer them back to this guide.

1. **DO** use passwords/passphrases at least 15 characters long (combination of upper and lower case letters, numbers, symbols, spaces). Use a unique password for each account – no duplicates. Change passwords every 6 months. **DO** use a third party password/credential manager like Dashlane[23], BitWarden[24] (or others) on all your electronic devices to secure your information. Alternatively, here is info on constructing a paper password management system[25]. **DO NOT** use any of these 50 most common passwords[26]. If keeping your passwords in a book, etc., **DO ALWAYS** keep that information in a safe, secure place, preferably in a safe or other type of locked container. **ASSUME** anyone entering your home – children, relatives, workmen, etc., could take pictures the information contained therein to commit fraud.

[23] https://www.dashlane.com/
[24] https://bitwarden.com/
[25] https://www.blackhillsinfosec.com/the-paper-password-manager/
[26] https://thriveweb.com.au/blog/50-most-common-passwords-2022

2. **DO** enable 2-step login (aka 2 factor authentication, 2FA) protocols on **ALL** your online accounts where you have to enter your user ID and password to log in. Alternate methods include Authenticator apps, Passkeys, PIN's, biometrics or combination thereof.

2.a. **DO** (in addition to above) set a PIN on your cell phone provider account to prevent porting of your phone number and account takeover.

3. **DO** set up text alerts on all your banking and credit accounts so that you will receive an alert text or e-mail any time **any** transaction has occurred with those accounts. Immediately contact the fraud departments of those accounts if you did not initiate the transaction.

3.a. **DO** ask your financial institution(s) to place a password on your account. This is not your online login password, but rather a password either you or the bank (depending upon who is calling whom) must provide in order to continue to provide information/services.

4. **DO** review your consumer credit reports[27] and ChexSystems[28] reports at least annually. Because of all the Covid-related fraud, the credit bureaus are still allowing you to view them for free on a weekly basis.

5. **DO** consider signing up for free credit monitoring services with Credit Karma[29] and Credit Sesame[30] **BEFORE** taking step 7.).

6. **DO** set up online accounts (before someone else does it for you) with: Social Security (includes Medicare)[31], VA[32] (military & government benefit recipients), USPS[33], USPS Informed Delivery[34] **BEFORE** taking step 7.).

7. **DO STRONGLY** consider a credit **freeze** or credit **lock** (they are different – article here[35]) with the Big 3 credit reporting agencies[36] and the NCTUE[37], even and especially for children. If you do, be sure to keep your login credentials in a very safe place!!! And do this **AFTER** steps 4.) thru 6.), otherwise you will have to go through the process of unlocking or unfreezing your accounts to sign up for some of them or get a special temporary passcode from the government agencies. Here are two good articles on this subject explaining the process: Article 1[38]. Article 2[39]. **You have rights under federal law to dispute and have corrected any improper billing or information with your credit – more info here from the CFPB[40].**

---

[27] https://www.annualcreditreport.com/index.action
[28] https://www.chexsystems.com/request-reports/consumer-disclosure
[29] https://www.creditkarma.com/
[30] https://www.creditsesame.com/
[31] https://www.ssa.gov/
[32] https://www.va.gov/
[33] https://www.usps.com/ *(Yes, it is **.com** in this case since the USPS is not an official government agency)*
[34] https://www.usps.com/manage/informed-delivery.htm
[35] https://www.nerdwallet.com/article/finance/credit-lock-and-credit-freeze
[36] https://www.annualcreditreport.com/index.action
[37] https://www.nctue.com/consumers
[38] https://clark.com/credit/credit-freeze-and-thaw-guide/
[39] https://pirg.org/edfund/resources/identity-theft-is-soaring-reduce-your-risk-dramatically-by-simply-freezing-your-credit-files/
[40] https://www.consumerfinance.gov/consumer-tools/credit-cards/

8. **DO** only use a Uniball Signo brand #207[41] anti-fraud gel ink pen to fill out checks and **ONLY** place outgoing mail in a drop box **inside** a U.S. Postal Service substation during business hours. Note that **not** all "gel" ink pens use the special anti-fraud ink; it must say so on the packaging. Also, hold the envelope up to a bright light - be sure the envelope has adequate security features to mask what is inside (like a check) and insert additional pieces of paper to mask the contents, if necessary. **Best practice:** Go "paperless," get your monthly bills via e-mail, pay them online and avoid writing **any** checks if at all possible – they are one of the most compromised methods of payments at this time because our entire mail system is compromised now. Go to your local bank branch and sign up for online banking. Pay bills with a credit card (**NOT** debit card – *see articles in #7. in previous section*) or use auto draft to your checking account to pay monthly bills. You should have a **dedicated credit card** for recurring payments that is never used/swiped in a Point-of-Sale terminal like the gas station or grocery store. Also, you should have at least 2 bank accounts – one where the majority of your money is housed (and that you do not give out the account number) and a smaller one where you only move enough money each month to cover your bills. **Ideally,** pay each bill manually (instead of auto-draft), monthly once you receive your e-bill – this avoids you having your account number information stored on someone else's server where it could be subject to data breaches. Some banking apps, security software suites and PayPal allow you create a unique (virtual), one-time-use credit card number (tied to your actual credit card number) to make payments, that way, the vendor, nor anyone else, ever sees your real credit card number. Pay your taxes electronically, as well and if you have to send them through the USPS, send them via **Certified Return Receipt.**

9. **DO** run some sort of **paid**, not free, third-party full software security suite (firewall, anti-virus, anti-spam, anti-malware, anti-ransomware, etc.) to protect against malicious websites, spam, malware, viruses, keyloggers, other system intrusions, etc. (Yes, Windows includes Windows Defender Security Suite and it is good, but it is not good enough, in my opinion.) If you use a computer, this is absolutely a **critical** step you **must** take, **no exceptions!** Bitdefender Ultimate Security[42], Norton 360 Deluxe[43] and McAfee[44] consistently get the highest ratings from industry publications and most also include apps for your smart phone/device. Just do a search for "best software security suite" for other options. Also, be sure to have a knowledgeable person take time with you to select the exact package you need -they have lots of options - and adjust the software's settings to ensure that you have the maximum protection enabled. If you cannot afford this product, at least get the free software and apps from providers like Avast[45], AVG[46] and Malwarebytes[47]. Just remember, as I like to say, *"You get what you pay for and you **don't** get what you **don't** pay for!"* There are many other steps you need to take to be cyber-secure, so for more computer safety tips, be sure to read my free 190+ page ***Identity Theft*** e-Book on the **Publications** page of my website[48].

9.a. **DO ONLY** use payment apps such as Zelle, CashApp, Venmo, etc., to send money to friends and family and not for purchases from unknown third parties. If you must, use PayPal or some banks' websites or the aforementioned software security suites that offer "secure" or "safe pay" features that allow you generate a one-time-use only credit card number to use in that particular instance.

[41] https://uniballco.com/collections/207
[42] https://www.bitdefender.com/
[43] https://us.norton.com/#
[44] https://www.mcafee.com/en-gb/index.html
[45] https://www.avast.com/
[46] https://www.avg.com/
[47] https://www.malwarebytes.com/
[48] https://www.magnusomnicorps.com/publications.html

10. **DO** backup your computer files and smart devices regularly. You can use an external hard drive such as a Western Digital Passport[49] external hard drive, or cloud back-up service like Carbonite[50] or iDrive[51]. Just remember, external hard drives are still susceptible to the same damage, loss, failure, and theft as your computer. **DO** password protect such devices.

11. **DO** check with your local county clerk or assessor to see if they offer some type of "lien alert system" to notify you about unexpected changes to your home's (or other real estate holding's) title(s) and or deed(s) and sign up for it. Yes, home theft is becoming a big problem.

12. **DO** use a VPN (Virtual Private Network) if you connect to the Internet through **any public Wi-Fi** such as in a restaurant, coffee shop, hospital, etc., even if the public Wi-Fi hotspot is provided by your Internet carrier. Many software security suites (see #9 above) offer VPN options, sometimes at additional cost and some also have broadband (data & speed) limits. Use an unlimited, 3rd party VPN like ExpressVPN[52] or NordVPN[53] – they are very easy to install and use on your computer and smart phone/device. If you do not have or cannot afford a VPN, when in public, simply switch off your Wi-Fi and connect to the Internet through a cellular (LTE or 5G) connection – it's not as fast as Wi-Fi, but definitely more secure. However, be careful not to exceed your monthly Internet data usage limits through a cellular connection. Also remember, your cell phone can be "tethered" and act as a **cellular (not Wi-Fi)** hotspot and allow most devices such as an iPad, tablet or laptop, that may not have built-in cellular capabilities, to connect to the Internet. This "tethering" feature for cell phones is sometimes at an additional cost to your monthly cellular plan and again, be aware of data and speed limits.

REMEMBER THESE WORDS OF WISDOM

1) If it sounds too good (or unbelievable) to be true, it probably is.

2) There is no free lunch.

3) If you didn't enter the contest, you can't win. (Foreign lotteries are illegal in U.S.)

4) When in doubt, check it out! (Do an Internet search for scam-related reports, phone numbers, etc.)

5) Think before you click or call!

6) Be wary of unknown people bearing gifts, free money, etc.

7) An ounce of prevention (from taking steps laid out in this report) is truly worth a ton of cure when it comes to this kind of crime.

[49] https://www.westerndigital.com/
[50] https://www.carbonite.com/
[51] https://www.idrive.com/
[52] https://www.expressvpn.com/
[53] https://nordvpn.com/

STAY UP-TO-DATE WITH ALL THE LATEST SCAMS & FRAUD & GET THE BEST SAFETY TIPS BY JOINING YOUR LOCAL COUNTY SHERIFF'S TRIAD GROUP (more info here)[54]!!! OPEN TO THE PUBLIC, FUN, FREE & NO COMMITMENTS. DO IT NOW!!!

For more information, get your free, 190+ page e-book

Special Report: Identity Theft, Financial Fraud & Cyber-Crime – Problems, Solutions and Mitigation Strategies *at:*
https://www.magnusomnicorps.com/publications.html

BEST INTERNET RESOURCES TO KEEP ON TOP OF FRAUD AND SCAMS

I strongly suggest subscribing to the periodic newsletters (e-mails) and podcasts from the websites that offer them. These websites do not sell or otherwise share your contact information.

http://www.aarp.org/money/fraudwatchnetwork (excellent, free!)
AARP Fraud Watch Network Hotline[55] (Questions? Report, get help/guidance. Free to all!): 877-908-3360

https://www.bbb.org/scamtracker/us

https://fraudoftheday.com/

https://www.krebsonsecurity.com

https://www.getsafeonline.org

https://scamspotter.org

https://fightcybercrime.org

https://www.consumer.ftc.gov

https://www.cyberguy.com

[54] http://www.magnusomnicorps.com/oklahoma-county-triad.html
[55] https://www.aarp.org/money/scams-fraud/helpline.html?intcmp=AE-SCM-FRD-HLPLN

https://www.komando.com

https://www.clark.com

https://richontech.tv/

https://twit.tv/shows?shows_active=1

https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

https://www.upguard.com/blog/biggest-data-breaches

https://www.identityforce.com/blog/2023-data-breaches

https://www.identityforce.com/blog

https://www.bitdefender.com/en-us/blog/hotforsecurity/tag/digital-privacy

https://www.consumeraffairs.com/finance/identity-theft-statistics.html

https://www.magnusomnicorps.com/publications.html
(be sure to see the **FRAUD AND SCAMS** section)