SPECIAL REPORT: IDENTITY THEFT, FINANCIAL FRAUD and CYBER-CRIME – PROBLEMS, SOLUTIONS and MITIGATION STRATEGIES

Revised and Updated Frequently

October 9, 2018

This report is available for free in PDF format on the *Publications* page of Magnus Omnicorps' website.[1]

[1] http://www.magnusomnicorps.com/home.html

Disclaimer Summary: *The information in this publication was obtained from various sources. While it is believed to be reliable and accurate, Magnus Omnicorps, LLC does not warrant the accuracy or reliability of the information. This publication is for informational purposes only and is far from all-inclusive or a complete review of the topics discussed. These suggestions are not a complete list of every loss control measure. Use this information at your own risk and discretion. Magnus Omnicorps, LLC makes no guarantees of results from use of this information and assumes no liability in connection with the information nor the suggestions made.* ***The author is not an attorney and does not give legal advice.*** *If you need legal advice, contact a competent, licensed attorney who specializes in the area of law in which you need assistance.*

See full Disclaimer at the end of this report.

Original Publication Date: July 26, 2016

Revision/Update Dates:

September 2, 2018
August 4, 22, 23, 26, 2018
July 26, 2018
June 4, 2018
May 13, 17, 2018
March 24, 2018
February 01, 2018
January 10, 26, 2018
October 12, 2017
September 9, 22, 30, 2017
August 29, 2017
July 2, 18, 2017
April 25, 29, 2017
March 3, 7, 2017
February 7, 2917
January 25, 2017
December 1, 2, 8, 20, 2016
November 8, 11, 19, 27, 30, 2016
August 1, 3, 8, 2016

TABLE OF CONTENTS

If your identity has been stolen and or your financial accounts tampered with, report it to the police and go to the Federal Trade Commission's Identity Theft Resource Center website[2] immediately for step-by-step instructions on what to do next Also see Financial Crimes Victim Recovery Checklists[3].

BREAKING NEWS (Updated October 2018)

****** Credit Freezes are Now Free! Krebs On Security, 9-18-2018[4] ********

Data breach bigger than Equifax - 340 million personal records exposed – Kim Komando, 6-28-2018[5]

Everyone should read the following articles regarding the recent Equifax data breach:

Axios: A Year After Massive Equifax Breach, 'Nothing Changed' | Breitbart 9-7-2018[6]
New Chart Shows All Equifax Breach Stolen Info – Kim Komando[7]
Equifax Reveals Passport Details, Driver's Licenses Stolen in 2017 Data Breach[8]
Clark Howard | Turns Out, The Equifax data breach was even worse than we thought[9]
Kim Komando | Massive Equifax data breach is worse than originally thought[10]
Insurance Journal | Equifax Breach Exposed More Consumer Data Than First Disclosed[11]
Kim Komando | Equifax Security Breach: What You Must Do with Your Social Security Number NOW![12]
Krebs on Security | Equifax Breach: Setting the Record Straight[13]
Krebs on Security | Experian Site Can Give Anyone Your Credit Freeze PIN[14]
Clark Howard | Equifax data breach: What we know and how to protect yourself from what's coming next[15]
Krebs on Security | Ayuda! (Help!) Equifax Has My Data![16]

---

2 https://www.identitytheft.gov/
3 http://victimsofcrime.org/docs/default-source/financial-fraud/victimrecoverychecklists.pdf?sfvrsn=4
4 https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
5 https://www.komando.com/happening-now/467953/data-breach-bigger-than-equifax-340-million-personal-records-exposed-in-another-data-breach?utm_medium=nl&utm_source=alerts&utm_content=2018-06-28-article-title
6 https://www.breitbart.com/tech/2018/09/07/axios-a-year-after-massive-equifax-breach-nothing-changed/
7 https://www.komando.com/happening-now/459994/new-chart-shows-all-equifax-breach-stolen-info
8 http://www.breitbart.com/tech/2018/05/09/equifax-reveals-passport-details-drivers-licenses-stolen-in-2017-data-breach/
9 https://clark.com/consumer-issues-id-theft/identity-theft/equifax-data-breach-new-revelations-worse/
10 https://www.komando.com/happening-now/441134/massive-equifax-data-breach-is-worse-than-originally-thought?utm_medium=nl&utm_source=alerts&utm_content=2018-02-12-article-title
11 https://www.insurancejournal.com/news/national/2018/02/13/480357.htm
12 https://www.komando.com/happening-now/420431/equifax-breach-one-thing-you-must-do-with-your-social-security-number-now?utm_medium=nl&utm_source=alerts&utm_content=2017-09-21-article-title
13 https://krebsonsecurity.com/2017/09/equifax-breach-setting-the-record-straight/
14 https://krebsonsecurity.com/2017/09/experian-site-can-give-anyone-your-credit-freeze-pin/
15 http://clark.com/personal-finance-credit/equifax-breach-how-to-protect-yourself-from-whats-coming-next/?utm_source=Clark+Newsletter+List&utm_campaign=e7f97a5b0c-Clark_Daily_Newsletter&utm_medium=email&utm_term=0_afa92deb83-e7f97a5b0c-71403297
16 https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/

Krebs on Security | The Equifax Breach: What You Should Know[17]
Krebs on Security | Equifax Breach Response Turns Dumpster Fire[18]
Equifax | Equifax Announces Cybersecurity Incident Involving Consumer Information[19]
Kim Komando VIDEO | MASSIVE data breach affects 143 million Americans[20]
Kim Komando | What to do about the Equifax breach[21]
Krebs on Security | Breach at Equifax May Impact 143M Americans[22]
Bloomberg | Equifax Says Cyberattack May Have Hit 143 Million Customers[23]
Clark Howard | Equifax data breach may have exposed personal info of 143M consumers[24]
NBC News | Massive Equifax Data Breach Could Impact Half of the U.S. Population[25]

1. INTRODUCTION

Everyone's heard that there are only 2 things certain in life, death and taxes. However, I would now argue that there are now 3: Death, taxes and your identity or other financial information will be stolen or somehow compromised. **Bottom line:** Almost all our personal and financial information is "out there" (and for sale on the Dark Web[26]) and it's not a matter of if identity theft will happen to you, it's just a matter of when (see **"Biggest Data Breaches of All Time"** list in the **Appendices section** of this report). To make matters worse, victims aren't being notified that their information has been compromised by these companies who lost it for weeks, months or even years after the fact and by that time, it is way too late! So, it is critically important to understand how our information is compromised and take **proactive** and **precautionary** steps to **prevent** it and **protect** ourselves. This report will help you do that.

The quickest and easiest way to see if some of your information has **possibly** been compromised is to enter your email in this website: https://haveibeenpwned.com/ They will tell you if your email address has been compromised, during which breach that loss occurred and what other related information **may** have been disclosed. Keep in mind, this is not 100%; no database is.

We see and hear the stories in the news on almost a daily basis about the latest computer hacking breach of thousands, millions and even a billion individuals' personal information records and online account login credentials. In late 2016 during the general election, government officials at the highest levels were found to be using insecure communications systems, compromising classified material and one high-ranking official fell for an e-mail phishing scam, allowing hackers to steal highly sensitive data. Unscrupulous employees at one of the oldest and largest financial firms in the world were creating thousands of bogus accounts, to generate commissions. In late 2017, Equifax, one of the big 3 credit reporting agencies

[17] https://krebsonsecurity.com/2017/09/the-equifax-breach-what-you-should-know/
[18] https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/
[19] https://www.equifaxsecurity2017.com/
[20] http://videos.komando.com/watch/12858/daily-tech-news-update-massive-data-breach-affects-143-million-americans-supercomputers-and-hurricanes-and-an-app-that-can-help-you-in-an-emergency
[21] https://www.komando.com/happening-now/418420/equifax-breach-impacts-143-million-americans-was-your-info-stolen
[22] https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/
[23] https://www.bloomberg.com/news/articles/2017-09-07/equifax-says-cyber-intrusion-affected-143-million-customers
[24] http://clark.com/personal-finance-credit/credit-agency-equifax-says-cyber-attack-may-have-exposed-personal-info-of-143-million-americans/
[25] https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686
[26] https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/

suffered a breach exposing 143 million individuals' credit files, etc., etc., and more bad news resulting from that breach continues to trickle out as recently as May, 2018. See a longer, but by no means all-inclusive, list of breaches on the Breaking News page of my website[27]. Inasmuch, you'd be hard pressed to today to find someone who hasn't heard about identity theft or someone who's been a victim of it or some other, similar financial crime or scam.

And just because you may have no web presence, i.e., no online accounts, this does not mean that your information is safe – far from it. See this article[28] from cyber-security expert Brian Krebs at Krebs on Security.

Identity theft is still one of the fastest growing crimes in the U.S. with almost 18 million people (1 million are children, each year[29]) having their identities stolen last year alone according to the U.S. Department of Justice. Of those, 15 million credentials have been used fraudulently, totaling approximately $50 billion in losses annually. I even recently heard on the radio that 1 in 4 people suffered some kind of identity theft in 2015. And more people are being affected every year and no one is immune, not even the newly-born or even the deceased!

The Washington Examiner released a story on 9/27/2015 summarizing a recent U.S. Department of Justice report from their statistics branch on identity theft in 2014 (Summary here[30] and full report here[31]). Please take a few minutes to read the brief article here.[32] Here are just a couple of the staggering statistics from the article: About 7% of all persons over 16 years of age in the U.S. were victims of identity theft. While 87% contacted their financial institutions to report problems, less than 10% reported it to police. It is **very important** to report such incidents to law enforcement – they use this information not only to identify and prosecute the specific criminals, but also in many other ways that are critically important to fighting this type of crime.

Again, the fact of the matter is that our personal information is out there and it isn't that hard to obtain by people who don't have our best interests in mind, if you know what I mean. And to make matters worse, we've also all heard the news stories about some negligent employee who lost a laptop or computer disk or thumb drive with anywhere from thousands to millions of customers' unencrypted personal information files on the device(s). Or, there's the proverbial "bad apple in the barrel" - an unscrupulous employee who has access to sensitive personal information and simply steals people's identities that way – known as ***employee access identity theft***. I address that briefly in **section 10., FINAL THOUGHTS.**

We lock our homes when we leave and we lock our cars when we get out of them – we generally understand physical security. But, public awareness to the threats of white collar crime, including identity theft, financial fraud, and other related cyber-crimes, is growing but not to the degree it should and knowledge of strategies to avoid it is even less common, hence, this special report – there are many simple and free steps you can take to protect yourself and mitigate any losses.

Thanks to my company, the generosity and incredible efforts of our law enforcement community and several financial institutions, I am fortunate enough to be able to attend meetings and

---

27 http://www.magnusomnicorps.com/breaking-news.html
28 https://krebsonsecurity.com/2018/06/plant-your-flag-mark-your-territory/
29 https://clark.com/consumer-issues-id-theft/identity-theft/kids-identity-theft-what-to-do/
30 http://www.bjs.gov/content/pub/pdf/vit14_sum.pdf
31 http://www.bjs.gov/content/pub/pdf/vit14.pdf
32 http://www.washingtonexaminer.com/17.4-million-americans-hit-by-identity-theft-in-2014/article/2572908

seminars with a variety of the local, state and federal law enforcement agencies involved in fighting white collar crime, which, for a variety of reasons, continues to grow.

One of the main reasons for this, I believe, is that criminals are always looking for quicker and easier ways to make money (they always take the path of least resistance) and are turning to the Internet and identity theft as opposed to previous "traditional" methods such as property crimes (burglary) and robbery.[33] *(Note: Just in June, 2015, there have been articles published indicating that we are seeing a surge in violent crime, as reported in this Wall Street Journal article.[34] However, other articles, such as this one in the Washington Post,[35] contradict that assertion. And now this latest one from Reuters[36] seems to confirm the increase as does this CNN story[37] which cites this report from the Major Cities Chiefs Association[38]. Since empirical evidence is slow to be compiled, I'll leave it up to you to read the articles and make your own decisions and crime trends can vary greatly from jurisdiction to jurisdiction for a variety of reasons. Even though there may be an upswing in violent crime over the past couple of years, the trend over the past 30 years has been significantly downward.)* ***Feb. 2017 Update:*** *The violent crime spike is now confirmed: Washington Post article[39], Breitbart article.[40]*

Among the other reasons for this apparent shift, I believe, are that many states, but not all, have **finally** adjusted their laws to allow citizens to carry a variety of weapons to defend themselves. Also, technology and competition in the marketplace has made property monitoring/alarm systems much more flexible, user-friendly and definitely more affordable – such as Nest[41], SimpliSafe[42], Arlo[43], Ring[44], Security by You[45], Blink[46], Lighthouse[47] and many others. Prices and features vary widely, so do your homework, read this review article[48] and then do a search for "DIY home security" for more information before making an investment in a system. One feature I would definitely want is cellular backup in the event your Wi-Fi/Internet connection goes down.

The media rarely reports this and statistics vary widely here, but firearms are used to successfully defend persons and property at rates between 10 to 70 times greater than they are used to take lives, either purposefully or accidentally. Recently (early 2018) uncovered evidence from suppressed CDC (Centers for Disease Control) survey data[49] show that guns

---

[33] *For more information on crime statistics, see the* ***U.S. Dept. of Justice's Bureau of Justice Statistics website:*** *http://www.bjs.gov/*

[34] http://www.wsj.com/articles/explaining-away-the-new-crime-wave-1434319888

[35] https://www.washingtonpost.com/news/the-watch/wp/2015/06/08/theres-no-evidence-of-a-new-nationwide-crime-wave/

[36] http://www.reuters.com/article/2015/08/03/us-usa-police-summit-idUSKCN0Q81RB20150803

[37] http://www.cnn.com/2016/07/25/politics/violent-crime-report-us-cities-homicides-rapes/

[38] https://assets.documentcloud.org/documents/2832727/MCCA-Violent-Crime-Data-1st-Quarter-2016-2015.pdf

[39] https://www.washingtonpost.com/news/post-nation/wp/2016/09/26/violent-crime-and-murders-both-went-up-in-2015-fbi-says/

[40] http://www.breitbart.com/big-government/2017/01/13/fbi-largest-cities-saw-21-6-percent-spike-in-murders-in-first-half-of-2016/

[41] https://nest.com/alarm-system/overview/

[42] http://simplisafe.com/

[43] http://arlo.com/en-us/

[44] https://ring.com/

[45] https://www.securitybyyou.com/

[46] https://blinkforhome.com/

[47] https://www.light.house/

[48] http://www.reviews.com/home-security-systems/diy/

[49] http://www.breitbart.com/big-government/2018/04/21/unpublished-cdc-study-confirms-2-million-annual-defensive-gun-uses/

were used **defensively** by victims 3.6 times as often as they were offensively by criminals, which translated into approximately 2.6 million defensive uses. Inasmuch, criminals know these facts and are taking steps to avoid direct confrontations with armed citizens or being caught on camera and apprehended by the police as a result. Also, despite the significant and record increase in per capita firearms ownership and issuance of concealed carry permits over the past 8 years, firearms-related injuries, crimes and deaths have continued decline significantly.[50] Also see this 2015 report on conceal carry permit holders from the Crime Prevention Resource Center.[51]

If carrying a firearm, or **any** defensive weapon for that matter, is something you have been considering, I urge you to check your state laws (usually start with the attorney general's office), get legal, get insured (yes, insured) and get as much training and education as you can! There is **much, much more** to being a safe, responsible and effective gun owner than just buying a gun and getting your carry permit. See the paper "Questions You Need to Ask Yourself Before Getting Your Carry Permit and Cost Considerations" on the Firearms page of my website[52] for more information. Remember, **any** use of force against another person may expose you to criminal and or civil charges. Consult an attorney if you have questions!!!

And on a side note, if you think the Founding Fathers didn't mean for the 2nd Amendment to apply to the average citizen, I challenge you to watch this 4-minute excellent explanation of it by UCLA Law Professor, Eugene Volokh[53] and these videos: Is Gun Ownership a Right?[54] and What Should We Do About Guns?[55] Also read Federalist Papers #29[56] and #46[57]. And see the Firearms page of my website[58] for much more info and resources.

This age of rapidly changing technology in which we live and access to information of all kinds has been both a blessing and a curse – this new interconnectivity has made us vulnerable and information we used to keep locked up in a safe or locked desk drawer, we now put up on social media or store in "the cloud." Compounding the problem is the ever-increasing rate at which technology is becoming integrated into our daily lives. In some cases, we have no choice but to use it to access goods and services and if we don't understand it and how to protect ourselves against technology-related crimes, our risk of being victimized greatly increases.

At any given time, there are hundreds, if not thousands of all kinds of scams and fraud going on out there. The sources of this kind of crime crosses the spectrum from small, one-person operations to sophisticated international crime syndicates and their targets are just about anyone, any business or any governmental organization.

Unfortunately, more and more seniors are being targeted today because of their relative unfamiliarity with technology, general trusting nature, cordiality of their generation and, for the most part, because they have more disposable income than most other groups – they hold approximately 70% of the country's wealth and usually have some kind of monthly income source. The losses annually to seniors nation-wide is estimated to be somewhere between $3 -

---

[50] *For more information on firearms statistics, see the **U.S. Dept. of Justice Special Report on Firearms Violence from 1993-2011, #NCJ 241730, issued May, 2013**.*
(http://www.bjs.gov/index.cfm?ty=tp&tid=43)

[51] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2629704

[52] http://www.magnusomnicorps.com/firearms.html

[53] https://www.youtube.com/watch?v=rEqGBOt32NM

[54] https://www.prageru.com/videos/gun-ownership-right

[55] https://www.prageru.com/videos/what-should-we-do-about-guns

[56] https://www.congress.gov/resources/display/content/The+Federalist+Papers#TheFederalistPapers-29

[57] https://www.congress.gov/resources/display/content/The+Federalist+Papers#TheFederalistPapers-46

[58] http://www.magnusomnicorps.com/firearms.html

$30 billion annually! Seniors grew up when they never locked the doors to their houses or cars and always answered the phone. For the most part, people could be trusted back then, but no longer. To make matters worse for seniors, they often suffer from alienation or isolation and the scammers capitalize on **"the power of loneliness,"** as an FBI agent described it in a recent meeting I attended. Also, they don't report these crimes because the feel ashamed, embarrassed or guilty that they were duped by a scammers slick manipulation skills and fear that their family members will they that they can no longer manage their finances correctly, ultimately leading to a loss of independence when a family member steps in to essentially take over their lives.[59]

But make no mistake, **it matters not** your age, level of education, sophistication, technical expertise, socio-political status, etc., **anyone can become a victim** to this type of crime, even the newly-born or recently-deceased. Yes, it's true.

If you become a victim of identity theft, depending upon the degree of it, it can, and usually does, throw your whole life into a complete tailspin. Trust me when I say that our law enforcement agencies at all levels and financial institutions are working as quickly and diligently as they can to address it. If it happens to you, it will seem as if the authorities are not doing anything to help, but please understand the methods used by criminals are so diverse and this type of crime and fraud are so pervasive in our society today that law enforcement agencies are overwhelmed by it and simply don't have the staff necessary to address it as quickly as they would like. To make matters worse, many of these crimes originate from overseas and with the help of technology and the non-cooperation of foreign governments, resolving these crimes can sometimes be nearly impossible. Therefore, it is imperative that the public at large take steps to protect themselves from this kind of crime. **You are your own first responder.**[60]

Again, it is **crucial** that we be **ever-vigilant** and take **proactive** steps to safeguard our personal and financial information, both physically and in cyberspace. I've been receiving an unusually high number of calls from friends and clients who have either had their identities and or financial information compromised and they want to know what to do to fix it and how to prevent further incidents. Look folks, **no one** else is going to protect your personal information as well as you are, so **just do it!**

So, let's begin:

In the course of our daily activities, we may write a check at the grocery store, charge a meal, rent a car or hotel room, apply for a store credit card to get an instant discount, get cash from an ATM, etc., and most of the time we don't give a thought to these types of routine transactions, but, there are others who might.

The identity theft crime can be simple or complex in nature:

Simple: A thief just physically steals your credit card or checkbook and uses those items to pay for goods and services until you get the account(s) closed.

Complex: Bit by bit and piece by piece, the thief goes about building a profile of you, gathering certain portions of your personal information, from various sources which I will discuss in detail below. Once a single account is created, it helps them build the credibility of their false identity. As they continue to build their false identity, it enables them to commit even more crimes and

[59] http://newsok.com/article/5544433

[60] *Credit to my friends at Conceal & Carry, Inc. Kansas City's conceal and carry specialists. (*http://ccw-kc.com/*)*

fraud in your name. And, with a fake driver's license, he/she may actually pose as you in order to apply for credit, loans, open bank accounts in your name, rent apartments, file bankruptcy, file false tax returns (to get refunds), take money from your accounts, or even get a job. They claim they have moved and provide an alternate address to receive the goods and or services. Significant amounts of money can be stolen from the victim for months or even years before the victim becomes aware of a problem. And there is also something called **affinity crime** (aka **cultivating the halo effect**) – it is another complex strategy criminals use and I address it in detail below in section 2.F.

There are countless other methods criminals use to obtain your personal information and there are numerous, excellent websites that go into much greater detail about all of them than in this report. Please go to the Helpful Info & Links[61] section of my website for a list of sites that I've found to be very helpful. The purpose of this report is not to try to touch on every one of the methods criminals use, but rather to explain, in general, some of the more prominent ones right now and provide you with a few easy steps you can take to help protect your critical information and limit your exposure to fraud.

Please keep in mind that none of these methods are iron-clad guarantees to preventing criminal activity, but they may help in deterring it. Remember, criminals are always looking for an easy mark, so if they run into resistance, they may move on to another target or person. By taking a few simple steps which I describe below, you may just provide the resistance that makes the criminal move on to the next person and leave you alone.

If you find discrepancies on your credit report or have any other credit problems, you have specific rights under these federal laws to protect you, among other federal and state laws:

Fair Credit Reporting Act (FCRA)[62]
Fair and Accurate Credit Transactions Act (FACTA)[63]
Fair Debt Collections Practices Act[64]
Fair Credit Billing Act (FCBA)[65]
Equal Credit Opportunity Act[66]

Go to the Federal Trade Commission's website[67] and the Consumer Financial Protection Bureau[68] to find out more about these laws and go to the respective credit agency's website and follow their instructions to file a dispute.

If you are a victim of identity theft, or any theft for that matter, time is of the essence and you will want to file a report with your local police, federal law enforcement, U.S. Postal Service, the state attorney general's office and the Federal Trade Commission (more on that below). Again, all of the aforementioned organizations are inundated and overwhelmed with such claims and you may have to enlist the assistance of a private investigator and or attorney to assist you.

[61] http://www.magnusomnicorps.com/helpful-info---links.html
[62] http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf
[63] https://www.privacyrights.org/facts-facta-fair-and-accurate-credit-transactions-act
[64] https://www.ftc.gov/system/files/documents/plain-language/fair-debt-collection-practices-act.pdf
[65] https://www.ftc.gov/sites/default/files/fcb.pdf
[66] https://www.consumer.ftc.gov/articles/0347-your-equal-credit-opportunity-rights
[67] http://www.ftc.gov
[68] http://www.consumerfinance.gov

2. HOW YOUR INFORMATION IS COMPROMISED & DEFENSIVE STRATEGIES

First, see the **Appendices** section below for this fantastic list from the Acuant Corporation: **101 Ways Your Identity Can be Stolen and Exploited**.

Also, see this great guide from AARP defining all the terms you hear in the news: Fraud Speak: Learn the Lingo to Beat Scammers[69].

A. DIRECT THEFT: Your wallet, purse, non-password protected computer, cellular phone, etc., are stolen from your house, your person, your car, etc., and they contain your credit cards, ID, etc., which the criminal can use to access your data and or accounts.

Defense:
Obviously, keep your wallets and purses secure. **NEVER** leave them in your car at any time for any reason. Period. And, for that matter, do not leave anything of value in plain sight inside your car. Also, and I see this quite a bit – people leaving their work credentials hanging on a lanyard from their rear-view mirror. Do not do this!! No matter how insignificant (from a security aspect) you think your job or your company is, those ID credentials are valuable to a thief, especially if your ID contains a magnetic strip that allows you to access locked areas with valuable and or high-pilferage items. I also see this – people hanging stethoscopes and handcuffs from the rear-view mirrors. What harm could there be in that, you ask? Other than being somewhat pretentious and a flying-object hazard in a crash, a thief might look at that stethoscope and rationalize that the driver is some kind of medical professional, therefore there may be medical supplies or even prescription drugs in the vehicle. As for the handcuffs, the thief may rationalize that the driver is connected to law enforcement and therefore, there may be weapons, ammunition, police radios or other things of value inside the vehicle. In both cases, just the visible presence of those seemingly innocuous items put your vehicle at a higher break-in risk than others.

And while I've got your attention, if you have a handicapped placard, **TAKE IT DOWN BEFORE OPERATING THE VEHICLE!!** Driving with it hanging on the rear-view mirror creates a huge, dangerous blind spot which is why the police will probably give you an expensive ticket for obstructed driving if they pull you over for some other reason. In some states, they may just pull you over for that reason alone.

When leaving your car, even if just for a minute to run into the convenience store to pick up a newspaper, roll up all the windows, close the sunroof, turn it off and lock the doors.

Ladies, when shopping, keep your purse snapped or zipped closed and be sure to use the baby seat straps in the cart to wrap around the purse handle and **never** walk away or turn your back on your cart.

When you leave home, be sure **ALL** your doors and windows are locked, including the door that goes from the living area to the garage. If you have a pet door or any other small door to the house, seal it up – criminals have been known to use small children to break into houses through these openings.

Never leave your garage door open unless you are in the garage or in direct line-of-site of it all the time!

[69] https://www.aarp.org/money/scams-fraud/info-2017/fraud-scam-speak-terminology-guide.html

In your homes, keep any important items and valuables well-hidden, locked up in a safe, or in a locking fire file cabinet.

Keep a list of all the items you carry in your wallet or purse that are of a financial or personal information nature, i.e., credit card numbers, checking account numbers, etc. and the respective customer service numbers, so, if they are stolen, you can contact the issuers immediately and get the accounts closed and cards re-issued. And **NEVER, EVER** carry your Social Security card in your wallet! You should have that number memorized by now, anyway. I've seen websites that suggest that you photocopy the contents of your wallet – you have to be extremely careful about this because most copiers these days, especially the large, commercial variety at copy stores, store the images they scan on an internal hard drive. The problem is, these hard drives are seldom wiped before the copier is sold or scrapped, so all your information may still be there for the taking by whomever purchases the copier. CBS' 60 Minutes did a report on this in April, 2010 entitled ***"Copy Machines, A Security Risk?"*** You can watch it at *CBS' website*[70] or on *YouTube*.[71] I also have those videos linked up on my website on the Audio and Video page.[72]

From a personal safety standpoint, we must be ever-aware of our surroundings. Stay away from areas known to have high crime. Most local TV stations have "crime tracker" sections on their websites. Also see the Helpful Info and Links page on my website.[73] Don't go out late at night to any store unless it's an absolute necessity and if you must, take someone with you or, if you must go alone, notify a relative, neighbor or friend and set up a time for you to check in.

B. SKIMMING/SHIMMING: This comes in a variety of forms and is one of the most prevalent way thieves steal your information: A small device, about the size of a deck of cards, criminals use to copy (aka cloning) the information from the magnetic strip off the back of your credit card, or in the case of shimming, the new chip embedded in the card. They then use the information to manufacture a duplicate card with a magnetic strip with your information that can then be used/swiped in any terminal to charge goods and services. Skimming/shimming can happen at any time when you hand your credit card to an individual who may have a skimming/shimming device on their person or nearby, say, for example, an unscrupulous server at a restaurant. Also, skimming/shimming devices can be hooked up to gas pumps, ATM's or other similar type terminals where credit cards are swiped, including on terminals inside stores, such as in self-checkout lines. The device is left in place and captures the information from every credit card's magnetic strip or chip that is swiped in the terminal. Depending upon how long the device is left in place, it can capture hundreds or thousands of account numbers. Skimming devices are usually placed **inside** the gas pump or ATM, so usually there is no easy way for you to see if there is one there. Shimming devices are usually inserted from the outside and no access to the internal workings of the machine are necessary. I've been told by security people who service ATM's that sometimes these devices are so sophisticated that even they don't know that they are there. **UPDATE:** New shimmers are becoming very sophisticated, so much so that they can now capture info of the new chips, including PIN numbers and they are so thin,small and easy to install that they are not only being found in gas pumps and ATM's, but also point-of-sale terminals in grocery stores, self-checkouts, etc. See this article from Kim Komando[74].

[70] http://www.cbsnews.com/video/watch/?id=6412572n
[71] http://www.youtube.com/watch?v=z147s6eNZp8
[72] http://www.magnusomnicorps.com/audio---video.html
[73] http://www.magnusomnicorps.com/helpful-info---links.html
[74] https://www.komando.com/happening-now/459420/scam-alert-new-way-crooks-are-stealing-credit-card-info

Another form of skimming involves a chip that is imbedded in some credit cards. This chip allows the cardholder to just tap the card on the terminal or just wave it over the terminal in order to make the purchase. This works because of a small 'RFID" (Radio Frequency Identification) chip imbedded in the card. This chip gives off a weak radio signal that contains the card's account information which is transmitted to the terminal when the card is in proximity of the terminal. It's a pretty neat idea on the surface, but a boon to criminals who, once again, can skim the information from the card, but the twist here is that they only have to be close to you to get the information off the card. They walk by you with a skimming device in their pocket and the device intercepts the signal being broadcast by your card(s) and then they have your information. Not all credit cards have these chips and many institutions are rapidly phasing them out in favor of the new "EMV"-chipped cards – it just depends on the bank or issuer, but you can tell if your card has an RFID chip by looking for a symbol similar to the one below. The letters "RFID" my not be present, but usually the "wave" symbol is.

We did have high hopes that the new chip & pin cards (picture below) would significantly decrease these particular vulnerabilities and in some aspects they do, however, they are not a panacea according to this August 15, 2015, article from Krebs on Security.[75] So, you must continue to be vigilant in the locations you swipe your cards and protect your pin when entering it, when required. Here is a good article[76] that explains the new EMV-chipped cards, but unfortunately, U.S. retailers have been very slow to upgrade their technology to take advantage of all the security features that this chip allows.

Defense:
Use cash only at restaurants or any other place where you may have to hand your credit card to an employee where they will leave your line of sight.

Some types of skimming (or shimming in the case of the new chip & pin cards) are almost impossible to defend against, so if you use your card in gas pumps and ATM's, get one or two cards that you **only** use for those purposes that way if it is compromised, you will still have other cards to operate with.

Before swiping or inserting your card in any device, check put your fingers in the slot to see if anything is loose on the terminal or in the slot – that is usually an indication of some kind of tampering, but it is not an absolute test of terminal security. If there are any stickers on the pump or device around the card slot, press on them to see if they are possibly covering up a

[75] http://krebsonsecurity.com/2015/08/chip-card-atm-shimmer-found-in-mexico/
[76] http://www.nerdwallet.com/blog/top-credit-cards/nerdwallets-best-emv-chip-credit-cards/

hole where scammers may have cut to install a skimming device. Also, you can use this trick with your smartphone[77] to detect the presence some skimming devices.

When swiping your card, if you have to enter a PIN, cover up the keypad with your other hand so that any clandestinely-placed cameras will not be able to record your numbers. Also, AFTER entering your pin, place your fingers/hand over the entire keypad for a few seconds to mask any residual infra-red/thermal patterns that could give away your PIN to someone using new smartphone thermal image scanning technology.

If you have an RFID-chipped credit card, purchase a signal-blocking protective sleeve and place your card(s) in it and **NEVER** hand it to anyone – skimming devices can be hidden anywhere and all they need to do is get the card near it. Or, there are purses and wallets that have the shielding built in. See the **WEBSITE RESOURCES** section below and check online for these items. Better yet, just ask the issuer if they can give you a card without the RFID chip.

Also, many gas stations and convenience stores offer their own pre-pay approval cards that you can swipe and which will allow you to fill first and then go inside to pay with cash. And, many stations are now starting to use safety seals on their pumps as an added layer of security, so be sure to look for some kind of tape or seal across the seam of the front of the machine and ensure that it is intact and hasn't been tampered. If not, go to another pump and report the compromised pump to the station attendant. Note that this is not a panacea for this particular issue as it doesn't protect against unscrupulous employees who have access to new seals and the inside of the pumps.

Keep in mind that almost no amount of physical security/checking will help if the software in the PoS (point of sale) terminal in which you swiped your card has been hacked or infected with malware. Recall that is what happened with the Target breach in 2013. Article 1[78]. Article 2[79]. Again, this is why you should have multiple, dedicated-use credit cards.

Finally, the newest and probably best way to avoid this type of crime is to use the latest payment services on your smart device such as Android (now Google) Pay[80], Apple Pay or Apple Cash[81], and Walmart Pay[82], at retail locations that accept them.

C. PHONE SCAMS:

Here are just a few:

Arrest Warrant
Computer
Credit Card Debt Consolidation
Extended Car Warranties
Fake Charities
Free Prizes
Free Trial Offers
Free Vacations

[77] https://www.komando.com/happening-now/414515/detect-hidden-credit-card-skimmers-with-this-smartphone-trick/all
[78] http://www.pcworld.com/article/2087240/target-pointofsale-terminals-were-infected-with-malware.html
[79] https://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/
[80] https://pay.google.com/about/
[81] https://www.apple.com/apple-pay/
[82] https://www.walmart.com/cp/walmart-pay/3205993

Granny Scam
Home Repairs
IRS Calls
Law Enforcement Calls
Love/Romance Scam (aka "Catfishing" – but usually starts through online dating services)
Lottery Winnings/Sweepstakes Giveaways (It is illegal to play foreign lotteries in the U.S.)[83]
Loans
Medical Alert Scams Targeting Seniors
Phony Debt Collectors

Obviously, these are simply too numerous to go in to, but usually involve someone calling you and using some kind of elaborate ruse to get you to divulge a portion or all of your personal information that may be needed to access one or more of your accounts. They may sound **VERY** convincing because they have scoured the Internet (social media) and built a profile of you and your family and may even pose as a family member to lure you into the scam. You'll hear me repeat this, but stop sharing **everything** about your life with the public through social media websites!! If you must use them, enable strict privacy/security/sharing protocols!!

Rule 1: Most cell phones and home phones have caller ID now – if you don't recognize a number, **DON'T ANSWER THE PHONE!** I can't emphasize this enough! If it is a legitimate call, they will leave a message and you can call them back at your convenience after you have verified the number. If it is a computer-generated and or robo-call, solicitation, or scammer, picking up the phone will only indicate that you **will** pick up the phone and the calls will increase as your number gets passed around on the "suckers list." Read this article about "One Ring" scams[84].

I've heard stories of people who like to "play" with these callers and engage them – **do not do this** – remember you are dealing with criminals and you do not want to aggravate them and risk inviting more annoyance calls to you at the least or even worse kinds of harm to you, your family or your property.

Another note on caller ID: Unfortunately, advances in technology allow scammers to "spoof" just about any phone number from any area code, including legitimate numbers, and attach names of legitimate companies, so you must be extra vigilant to ensure the whomever is calling you is in fact who they say they are. According to this June 17, 2017 article[85] from Krebs on Security, the FCC is working to implement new rules to stop this.

To quickly check a number, simply enter it (without any dashes) into your favorite Internet search engine such as Google, Yahoo, etc. and if it is bogus, you will see numerous links pop up stating that fact.

Rule 2 is just do **not** give out confidential information over the phone unless you initiated the call and know you are calling a legitimate number of a bank, service provider, etc., and you got that phone number from an official source that you trust such as the number on the back of your credit card and or your bank or credit card statement, utility bill, etc.

One of the popular scams right now is some person calls claiming to represent some official federal, or state governmental agency (and even law enforcement) or service provider such as a utility company and demands you provide payment or law enforcement will issue a warrant for

[83] https://archives.fbi.gov/archives/news/stories/2006/august/lotto_scams080906
[84] http://www.wsbradio.com/news/news/local/one-ring-scam-spreads-nationwide/nrLb3/
[85] https://krebsonsecurity.com/2017/06/got-robocalled-dont-get-mad-get-busy/

your arrest and they will be arresting you immediately if you don't pay right now. The electric company is not going to send the police to arrest you for failing to pay your bill. And if there is a warrant out for your arrest, trust me, the police probably already know where you are and they are not going to tell you that they are coming to arrest you. However, if there is a warrant or warrants for you for something such as parking tickets, failure to appear for jury duty, etc., the police may call you and ask you to come in to see the judge. Also, I have been hearing reports of these scammers actually coming to people's homes and knocking on your door. Do not answer the door; legitimate agencies (with the exception of uniformed law enforcement in an officially-marked vehicle) will not come to your home.

Rule 3 is the first sign of a scam is an absolute sense of emergency/urgency with the caller demanding that you provide some kind of personal information or take some kind of action to make a payment to them immediately.

Defense:
It is very rare that any of your service providers – banks, city-state-federal government, utilities, etc., will call you about your account; they will send you a letter. If they do, they will already have your information and will just ask you an absolute bare minimum of information to verify your identity and in almost no instance should they ever ask for your full Social Security Number or even the last 4 digits of your SSN. I have had my bank's fraud department call me when there were some suspicious charges made to my card. Instead of asking me for personal information, they recounted the recent charges I had made and their approximate amounts and asked me to confirm them and then they asked me about the charges in question. If your account is password protected, you can ask **them** to provide you with the password – more on that below.

If you are ever in doubt of the caller's identity or authenticity, politely say that you appreciate them contacting you, but for security purposes, you are going to call them back on the number you have from your credit card, monthly statement, etc., which you know is valid. If it is a legitimate call, they will understand and hang up, but if they persist in trying to get any personal information and or are rude or threatening, that is a good indication something may be amiss – hang up immediately and contact the authorities and entity they are impersonating.

Smishing (aka SMS Phishing) – If you use text messaging on your cellular phone, be aware that scammers are now using this method to get money from you. Most cellular carriers offer a "parental control" or similar type function where a password is required to be entered before any purchases/charges to your account can be made via the text messaging functions. Contact your respective cellular carrier for more information.

See section **4. CUTTING DOWN ON TELEMARKETER CALLS** below for more info.

Romance/Love Scam (aka Catfishing) note: I singled out this because even though it usually starts online, it quickly moves to the phone and this particular scam has a high potential to compromise significant amounts of your personal information, your physical safety and possibly get you unwittingly involved in illegal activities.

There are a lot of lonely hearts out there and also a lot of smooth talkers waiting to befriend them for nefarious purposes, so be very careful!! Consider that the potential love interest probably already knows a lot about you from your profile, so they can easily say everything you like/want to hear. The can build elaborate online profiles, mask their identities using pictures of other people, use untraceable, online phone numbers, and come up with elaborate stories of family and business histories to tug at your heart strings and convince you that they are genuine and quickly and deeply imbed themselves into your life. Believe me, some of them are so good

that if they weren't criminals, they'd have "PhD" after their names and operating legitimate counselling practices. Really, they are that good at social engineering. There are many red flags for this, but again, they usually want to get off the dating website and go "direct contact" as quickly as possible. Eventually, they may want you to do something, such as send or forward some money (under your name) to a sick relative or other distressed family member via Western Union or other service or pick up packages at a local retailer and then have you mail them somewhere else and again, under your name…and they will make these requests with a level of urgency and that is because they have probably obtained the money or goods with a stolen credit card and they are trying to stay ahead of the system. If you do any of these things and suspect you may have done something illegal, you should contact law enforcement immediately and make a report – you do not want to innocently get caught up in a money laundering or stolen goods operation. Romancescams.org[86] is a great website for more information. GetSafeOnline.org has an excellent section for online dating safety as does Lifewire[87].

D. E-MAIL SCAMS (aka PHISHING, SPEAR PHISHING, etc.):
If you are on the Internet and use e-mail, you probably have these things in common with most people:

- You have purchased something online through a major seller such as e-Bay, Walmart, Amazon, etc.
- You have a PayPal account or accounts.
- You subscribe to multiple newsletters – political, financial, hobbies, cooking, etc.
- You receive updates, coupons, special promotion sales, etc., from entities with whom you have done business.
- You receive dozens of non-personal e-mails daily

This scam is similar to phone scams, but they come through the e-mail. In some cases, you may receive an e-mail from what appears to be a legitimate friend or entity with whom you do business when in fact it is an elaborate hoax.

If the e-mail has "hooked" you and you click on a link within the message, it either directs you to a very official-looking, but bogus website where you enter the personal information they need, or the link in the e-mail or the website itself installs some kind of Trojan virus or other malware on your computer that gives the criminals access to your system and therefore, your sensitive financial information.

A new trend I've been seeing recently (mid-2018) are e-mails that say, "Confirm Subscribe," Confirm Unsubscribe," "Update Your Contact Info," etc.

Because of the common factors mentioned above and since we receive so much message traffic as a result, it's hard to keep track of everything, so it is highly likely we would get a legitimate e-mail from any of those entities asking us to confirm a subscription – almost all follow the same protocol, ostensibly out of safety precautions. Unfortunately, the scammers have now latched on to that methodology to get us to once again, click on something in that message that may install some kind of malware or re-direct our browser to a bogus website meant to capture your personal information.

More on computer security in **section 6.** below.

[86] http://www.romancescams.org/
[87] https://www.lifewire.com/online-dating-security-tips-2487806

Defense:
This follows the phone scam methodology, however, it is even rarer that the institutions with which you do business will e-mail you something requesting your account info – they already have it. If you suspect foul play, call the numbers you have on file and **do not click on any links inside the suspect e-mail or respond to it in any way**. You can delete it, however, I would suggest that you hold onto it in case law enforcement and or your financial institution need to examine the file. If you are concerned about even having it on your computer, at least print off a copy of it and save it in case it is needed by law enforcement.

If you suspect the message may be authentic, open another tab in your browser and carefully type in the address (URL) of the company/entity in question and log in to your account to see if there are any messages from the company about a need to update your information. By going directly to the source (company homepage), you avoid the potential for scam websites.

Another way to check is in the e-mail, put the mouse pointer over (hover) the link they want you to click, but **do not** click on it. Somewhere on the browser page, usually in the lower left-hand corner, the actual URL of the link will appear. If it is a strange sequence of characters that makes no sense and doesn't have the company's primary address in it, it may be bogus.

Also, many of us have received e-mails from friends whose addresses we recognize and, as is most common, they say they're stuck somewhere outside of the U.S., have lost their wallet and passport and need you to send money. Or, the message has no text, just a single, strange-looking link that makes no sense, such as http://www.1aseRtz.com/XDTPdsoet/asdiuf.htm . If you click on the link, it can allow any variety of viruses and malware into your computer which can allow access to your data or even destroy your computer. **Do not click on the links and delete these kinds of messages and then empty them from your Trash folder/Recycle Bin.**

See section **"8. OTHER COMPUTER INTERNET SECURITY"** below.

E. REGULAR "SNAIL MAIL" SCAMS
Even in this high-tech age, this is still a criminal favorite and involves the curbside mailbox at your residence (aka the Red Flag Gang or Porch Pirates – the ones who follow delivery trucks around and steal packages off your doorstep). Again, this can be an elaborate hoax similar to what is described in **D.** above, but usually criminals are looking to get their hands on any pre-approved credit offers you may receive, bank or credit card statements and slips, utility bills, etc., or, if you place outgoing mail in that box, checks that they can "wash" or use the account and routing numbers to make counterfeit checks, etc. Since many people still conduct their personal financial business through the regular mail, this can obviously be a treasure trove of information for identity thieves. Thieves can also profile you from a variety of angles just by looking at your mail. For example, if receive mailings from your church, they can find out the regular service times, stake out your house, find out when you go to services and then burglarize it. Just think about all the different pieces of mail you receive and what it might indicate to a criminal.

Also in this category is trash, yes, trash. Thieves have been known to pick up your bags of trash in order to glean any of the aforementioned items that you may have thrown out. Remember, in most jurisdictions and instances, it is legal to go through someone else's trash.[88] The legality comes into question when the trash may be set out in a gated community where it is on private property. Contact a lawyer if you have questions about this. Also, thieves rifle

[88] *United States Supreme Court Case, California v. Greenwood, 486 US 35, May 15, 1988*

through dumpsters (a.k.a. dumpster diving) in apartment complexes, industrial areas, medical and office buildings in search of your items with your personal information on it.

Defense:
Go to the closest, **official, United States Postal Service (USPS) post office** and rent a box. Re-route any critical mail - statements of any kind - to it. I even recommend this to people who live in apartment complexes and have locking mail boxes that are in central kiosks – the potential for your mail to get lost or placed in the incorrect box is just too great. If you need to send mail out, deposit it in either the official USPS blue mail boxes (preferably only those located immediately outside the Post Office or better yet, inside the postal facility. There have been instances of criminals fishing mail out of the blue boxes or stealing the blue boxes, so it is preferable that you deposit the mail inside the post office, if at all possible.

If necessary, you can get a lockable curbside mailbox at your residence, however, most of the ones I've seen aren't that secure; they only serve to "keep the honest people honest," for the most part.

Alternately, if you are comfortable and proficient with the computer, you can go "paperless" and get all your statements online and pay your bills online.

Also, the USPS rolled out (in early 2018) a new service called Informed Delivery[89], but it is not available in all areas just yet. This service sends you an e-mail with pictures of mail and packages that are scheduled to be delivered to you. This is a great service and should help cut down on this kind of crime because you will now know what is coming in your mail and when to expect it.

I will address more about cutting down on the junk mail below.

Regarding the trash issue, invest in a good, cross-cut (not strip) shredder and shred anything that has your name, address and any other type of personal information on it. Be sure to open anything that looks like junk mail before just throwing it in the trash since many times these can be pre-approved credit or insurance offers. Expect to spend about $100 for a really good, heavy duty shredder. It is worth the extra money to buy a good one. Sam's and Costco have good ones for reasonable prices.

In the following sections, I will address ways you can reduce your digital and paper trail, effectively denying criminals even the most basic informational starting points needed to steal your identity.

F. AFFINITY CRIME (aka Cultivating the Halo Effect) & CONTRACTORS:
This is a terrible crime and frequently perpetrated against seniors. It's unfortunate that in this day and age we have to be suspicious of someone offering to do something nice for us for free, but here's a scenario: Your friend down the street told you about her exterminator and what a nice man he was, so, when you discovered an ant problem, you didn't hesitate to call him. He arrived and sprayed for ants, but while he was spraying, he noticed that you had a dripping faucet and offered to fix it for you for free. Then, on his way out, he offers to do any other handyman work you may have in the future. Sounds harmless enough, right? Then, a while later, you work up a list of things that need work and call the very nice exterminator/handyman to come fix them. While he is in your house and you are not watching, he sees your wallet out on the table and quickly takes a peek at your credit card and gets the number and security code and then uses it to make purchases online.

[89] https://informeddelivery.usps.com/

In general, if you have any kind of work done by a contractor, be sure to verify his or her credentials. Any legitimate contractor should be more than happy to provide you with the following items along with the respective websites and or phone numbers that you can call to verify the information:

- State business license or registration number
- Proof of business liability & Worker's Comp insurance (carrier, phone number, policy number, coverage amount, copy of policy)
- Business address and phone number
- Official ID card and or driver's license

It is very important that the contractor have insurance in the event he or she damages your property or if he or she is injured while working on your property and sues you for medical expenses. (And be sure you are adequately insured, as well, just in case the contractor isn't. Contact your homeowner/renter insurance policy company/agent for more information and I suggest that everyone have a **"personal excess liability policy"** aka **"umbrella policy"** for the autos and homes. This is additional liability insurance over and above what is provided in your basic policy and usually offers coverage in increments of $1 million at very reasonable rates.)

And just because the contractor pulls up in some fancy-painted vehicle with numbers plastered all over it, don't assume that they are legitimate, especially if they are not based in your state. In states that have frequent weather damage, it is not uncommon to see out-of-state contractors/vehicles after a weather event. However, most states require out-of-state contractors to at least register with the respective regulatory agency prior to conducting business in the state. Again, ask for all documentation – legitimate contractors know this is an issue and should be well-prepared to provide you with the information you request. Additional tips:

- Beware of contractors going door-to-door soliciting business after a storm or offering to repair your driveway/seal cracks
- Get multiple estimates, but first make sure they are free!
- Never give them any money up front!
- Ask for references from work completed recently and preferably within your immediate area
- Get a written contract that clearly spells out start and finish dates, specific work to be done, complete costs within a certain +/- percentage, satisfaction guarantee, conflict resolution options, etc.
- Most jurisdictions require building permits, so ensure the contractor has one before they start work and verify it with the issuing agency
- Report fraud to your state's Attorney General's office, law enforcement, and the respective licensing authority
- Don't be afraid to ask a knowledgeable friend for help with this process!
- Get the license plate number and vehicle description of the contractor's vehicle

Also, I'm sure most of you have seen and heard the ads on TV and radio for websites that list verified service contractors. Even though they say the contractors are verified, I would still confirm their credentials to ensure they are still valid and up-to-date. Also check the Better Business Bureau's Scam Tracker website[90].

[90] https://www.bbb.org/scamtracker/us

Finally, a very important point: If contractors, real estate agents, etc., are going to be in your home and even if you are going to be present, lock up all valuables, jewelry, firearms, prescription medications, banking/financial statements with account numbers, etc. Also, if you have children in your home or who visit your home or have individuals with mental health issues (including dementia) in your home or who visit your home, it is imperative that you secure your firearms and medications so that they cannot be accessed by unauthorized persons. Check the laws in your respective jurisdiction – some have specific requirements for securing firearms and penalties can be very high for negligence. See the Firearms page of my website[91] for more resources.

3. CUTTING DOWN ON JUNK (SNAIL) MAIL and JUNK E-MAIL

The sale of mailing lists in this country is not just big business, it's **HUGE** business!!! Your name and address lands on these lists no matter how hard you try to keep it off. Anytime you subscribe to a magazine, enter a contest or sweepstakes, fill out a slip for a drawing at the mall, etc., you land on a list. Another huge source for generating lists is when you fill out a product warranty card or register your product online. If you fill these cards out, only include the bare minimum data so they can contact you in case of a recall. Do not fill out any of the additional, optional demographic information which will be used to really target you for all kinds of advertising and look for any boxes on such forms to check off that allow you to **opt-out** of any advertising. Also, if you include your e-mail on any of these items, I strongly suggest you set up a separate e-mail account at Yahoo, Gmail, Hotmail, etc., that you only use for this type of activity because it will limit your personal e-mail account from being inundated with spam. Gmail seems to be one of the best at filtering out spam at the server level.

Approximately once a year, you will probably receive a privacy notice (usually included with your bill or statement) from your bank, insurance company, credit card providers, etc., that explains how and what they do with your personal information. Read these carefully and follow the instructions to minimize how they share your information.

People are surprised to find out that the big three credit reporting agencies, the ones that maintain our credit files, sell our information which is where many pre-approved credit and insurance offers come from, as well as other junk mail. The good news is, you can put a stop to this by calling one central number set up the credit reporting agencies to do this: Call **1-888-5OPT-OUT (1-888-567-8688)** and follow the prompts or go here.[92] More info on this including other steps you can take are at the Federal Trade Commission's website.[93]

Also, on the Digital Advertising Alliance's website[94], go to the **DAA Resources for Consumers** section and follow instructions to limit you advertising exposure.

Also see Clark Howard's "4 Ways to Opt Out of Junk Mail" article[95] here.

However, there are more insidious forces at work when it comes to collecting, compiling and sharing information on our daily habits. Many websites, social media websites, brick-and-mortar businesses, etc., make money by selling their customer information to data collection/sales and

[91] http://www.magnusomnicorps.com/firearms.html
[92] http://www.optoutprescreen.com
[93] http://www.ftc.gov/privacy/protect.shtm
[94] http://digitaladvertisingalliance.org/
[95] https://clark.com/consumer-issues-id-theft/mailings-solicitations/unwanted-mail-marketing/opting-out-of-assorted-junk-mailings/

marketing firms that re-sell your information to other businesses for the purpose of pitching their products and or services to you. For example, have you ever wondered how your auto insurance company knows how much you drive your car? Well if you have your oil changed at a dealership or other participating lube shop, they report all the information regarding that service purchase (including your mileage) into a database that sells it to other companies, including your insurance company. This is just the tip of the iceberg. On the majority of consumers, these databases can contain millions of data points on each individual…yes millions! Again, when you do business with someone and especially when you sign a service contract, for example, with a cell phone company, in the fine print, in most cases, you are automatically **opted in** to information sharing and you will not be allowed to do business with that entity unless you sign that contract. This is why you cannot fully eliminate all junk mail and telemarketer calls. And this is why you also should not be sharing everything about your life on social media – how many of you have security questions on websites that reference your dog's name, where you went to school, etc.? And have you ever mentioned those things on social media? If so, I strongly suggest you go to those websites and change your security question(s) to something you know you haven't ever shared on social media. I'm sure you're starting to get the picture now.

4. CUTTING DOWN ON TELEMARKETER & FRAUDULENT CALLS

Latest: According to this article from AARP[96], scam calls are bad, but getting much worse! In 2017, only 3.7% of calls were fraudulent, but this year (2018) it's reached 29.2% and expected to rise to 44.6% in 2019!

According to this article from CBS News[97] on August 3, 2016, in the past 4 months, American households received approximately 10 **b**illion robocalls and as such, complaints to the Federal Trade Commission (FTC) are up 50% this year. According to this June 17, 2017 article from Krebs on Security[98], the FCC is working to change the rules to put a serious dent in robocalls.

The Federal Government has created the National Do Not Call Registry - a free and easy way to reduce (but won't fully eliminate) the telemarketing calls you get at home. To register your land line, go here[99] or call **1-888-382-1222** from the phone you want to register. You should receive fewer telemarketing calls within three months of registering your number. It will stay in the registry for five years or until it is disconnected or you take it off the registry. After five years, you will be able to renew your registration.

Remember that **legitimate** businesses honor the Do Not Call Registry list; the scammers **do not** and with the help of technology, in many cases, they can remain one step ahead of the authorities which means eliminating calls from scammers is nearly impossible.

It's also pretty much impossible to eliminate all sales calls since so many groups (political, charitable, official government) are exempt, including any business with which you have conducted business within the previous 18 months. Also, with the advent of VoIP (Voice over Internet Protocol) and other phone number-spoofing computer software and computer servers

[96] https://www.aarp.org/money/scams-fraud/info-2018/scammer-calls-increasing.html?cmp=EMC-DSO-NLC-MONY--FWN-MCTRL-100918-F1-3282178&ET_CID=3282178&ET_RID=23171899&mi_u=23171899&mi_ecmp=20181009_MONEY_member_Control_Winner_340000_466203&encparam=L9t%2fZAs4XXRW6mFExjDaF3QLZHcLHF%2f5PE4vpbln04I%3d

[97] http://www.cbsnews.com/news/new-technology-provides-a-solution-for-annoying-robocalls/

[98] https://krebsonsecurity.com/2017/06/got-robocalled-dont-get-mad-get-busy/

[99] http://www.donotcall.gov

based outside of the U.S., it is pretty easy for telemarketers to get around U.S. regulations, but there are still a few steps you can take to decrease, but not eliminate these calls.

Even though several federal and state laws and regulations prohibit marketing companies from calling cell phone numbers, I believe it is a good idea to be proactive and register your cell number anyway. With people dropping their land lines in record numbers and everyone going wireless, I have no doubt that marketing firms will exert extreme pressure on our legislators to change the law and allow access to this information eventually. You can read more about this at Snopes.com.[100] I recently heard rumors that carriers are going to give cell phone numbers to telemarkets – this is **STILL NOT TRUE** – see Snopes article on May 1, 2018 here[101].

Any numbers you register should flow down to your respective state's do-not-call list. If you continue to receive calls from the same non-exempt entity after 3 months and you have asked them to stop calling you, you should file a complaint with your respective state's attorney general's office, consumer affairs department and the Do Not Call Registry's Complaint line[102].

Also, you can have your landline phone number unlisted/unpublished. Believe it or not, they actually charge an extra monthly fee of $5 or more for this service.

And consider the NoMoRobo[103] services for landlines and cell phones mentioned above in the CBS News article or Hiya[104] app for smartphones mentioned in this video[105] by consumer expert Clark Howard. Also, there is the TrueCaller app[106] and the free app for mobile phones from AT&T called Call Protect[107]. AT&T customers with digital landline phones can now use the *61 feature[108] to block up to 100 calls and call blocking can also be managed online by logging in to your account. Check with your respective carriers for similar features – most offer them.

Most smartphones allow you to block callers/numbers quickly and easily right on your phone – no other 3rd party apps or fees required, but the apps help pre-screen out known spam numbers so the calls never come through to begin with and they offer other features to help you report spam calls, helping out other consumers. Every carrier has some way for you to block numbers.

Get more info at the FCC's robocall resource page here[109]. Here's a great article from Kim Komando that gives specific instructions: 7 ways to finally end robocalls, May 20, 2018[110]

5. PROTECTING YOUR BANK ACCOUNTS AND CREDIT

Call or go to your bank or other financial institution where you have your checking, savings, etc., accounts and have them place passwords and or security questions on your accounts. Anytime anyone goes to do anything with your account, including you, they will be required to provide the password before the teller or other representative will proceed with any transactions. Then, call

100 http://www.snopes.com/politics/business/cell411.asp
101 https://www.snopes.com/fact-check/cell-phone-numbers-given-telemarketers/
102 https://complaints.donotcall.gov/complaint/complaintcheck.aspx
103 https://www.nomorobo.com/
104 https://hiya.com/
105 http://www.clark.com/new-app-alerts-you-when-a-scammer-is-calling
106 https://www.truecaller.com/
107 https://www.att.com/offers/call-protect.html
108 https://www.att.com/esupport/article.html#!/u-verse-voice/KM1041912
109 https://www.fcc.gov/consumers/guides/stop-unwanted-calls-texts-and-faxes
110 https://www.komando.com/columns/458656/7-ways-to-finally-end-robocalls

your credit card issuers and do the same thing. This a free and simple step that adds an additional layer of security to your accounts and prevents anyone, no matter how much of your personal information they have, from gaining access to **certain aspects** of your account. However, if someone steals you credit card or clones it, it will not prevent them from making charges to your account until you direct the bank to close the account it.

If you bank online, some banks allow you to set up alerts for specific transaction events. For example, you can set an alert on your account whereby you will be notified via e-mail and or text message if a cash withdrawal is made from your account for over $100.00 (or whatever amount you designate). Another example is setting an alert on your credit card for any transactions that are made overseas or online or from an ATM, etc. This is a great, usually **free** service that you should use.

If you want to be sure that no one, including you, can apply for credit or loans in your name, you can freeze your credit with each the big 3 credit reporting agencies. *(Note that a "freeze" should not be confused with a newly-offered service from credit reporting agencies called a "credit lock." They are not the same and a "lock" does not provide the same level of security that a "freeze" does.)* You go to their websites and follow the links to freeze your file - it usually costs $10 per agency. Once you have set up your account, you can unfreeze your account at any time for a $10 charge and then refreeze it when you are ready for another $10 charge and sometimes the re-freeze is free. **Freezing your credit** file **may** prevent some businesses, employers, utilities, etc., from performing "soft hit or pull" inquiries on your credit file – it depends upon state laws and whether you have an existing account/relationship with the inquiring entity. Here's a good article[111] that explains soft and hard pulls. **A word of caution:** Keep in mind that in some instances, while your credit is frozen, the card issuer may decline to provide you with a replacement card if you call in to report it lost, damaged or stolen. This happened to me with a card I rarely used. The card was damaged and they wouldn't replace it for me until I unfroze my credit, so, I just waited until the card expired and they automatically sent me a new one. That is fine, as long as you don't need to use the card and have others on which to fall back (which you should. Be sure to get clarification from the card issuer regarding their policy under similar circumstances. Also, having your credit file(s) frozen may impact your ability to establish online accounts with Social Security and Medicare and DoD/VA eBenefits, requiring you to unfreeze it/them first. In this case and in light of the 2017 Equifax breach, I advise against unfreezing your credit unless absolutely necessary which means you will have to go to your local Social Security office and they can provide you with a special, one-time account activation code so that you will not have to unfreeze your credit to establish a "mySocialSecurity" online account. Some tips before going to the Social Security office: Be sure you take all your necessary documents AND a valid (not expired) state or federal ID. Go online and set up an appointment time, if possible. If you cannot do that, get there early (because they close at noon for lunch), sign in at the kiosk and get your number ticket. You will have to go through the equivalent of an airport-style security check, so leave any weapons (even if you are a state concealed carry permit holder), pepper spray, knives, metal items, etc., at home (not in your car; you're on federal property and that's not allowed).

Alternately, you can have a **fraud alert** placed on your file. This will alert anyone wishing to grant you credit to take additional identity verification steps before approving you. Again, the limiting factor here is just how vigilant the respective retailer/lender is when it comes to verifying your identity when they see a fraud alert on you file – some are and some aren't. Note that this is not as strong a protection as freezing your credit. A new service being offered by the credit reporting agencies is a **"credit lock."** This is **NOT** the same or as secure as a **"credit freeze."**

[111] https://www.nerdwallet.com/blog/finance/credit-report-soft-hard-pull-difference/

Go to the respective credit reporting agencies' websites for more information on the differences between these services. Here's a brief article from Nerdwallet[112] explaining the differences.

A strong word of caution: Be sure you keep those passwords and PINs in a very safe place – you don't want them falling into the wrong hands or, if you simply lose them and haven't committed them to memory, accessing your account will be very difficult if not impossible. **BE VERY CAREFUL!!**

And when traveling, be sure to call your credit card issuer(s) ahead of time and notify them of your itinerary. With some issuers, you can do this online. If you do not, you could run into difficulty making purchases because due to rampant credit card fraud and identity theft, banks and other issuers will suspend an account if purchases are made that are outside your home area or don't correspond to your usual purchasing habits. And, they may or may not contact your immediately when suspending your account, leaving you in the lurch and very confused about what has gone wrong.

More information at the respective agencies' websites:

http://www.experian.com/
http://www.equifax.com/home/en_us
http://www.transunion.com/
https://www.nctue.com/consumers

IMPORTANT UPDATE! 5-13-2018 – Apparently there is another, more obscure credit reporting agency called the **National Consumer Telecommunications and Utilities Exchange** (NCTUE) that is used to process credit applications for cell phone service and increasingly utilities and cable services. Its database is managed by Equifax, BUT, if you have your credit frozen with Equifax, it does NOT translate over to the NCTUE database, so you have to call them and freeze your credit there, as well. It gets more complicated, so it is very important that you read this article from Krebs on Security[113] about this and take additional steps to protect yourself.

It is highly advisable that everyone review their credit reports from each agency at least annually. A change in federal law (**FACTA** – see below) a few years ago requires each agency to provide the consumer with one free credit report every 12 months. If you have been a victim of fraud, then you can get it free if you are still within the 12-month window. The **ONLY** official website to this is http://www.annualcreditreport.com. There are many other websites with similar sounding names, but they **require** you to sign up for credit monitoring, etc. The official website is 100% free and no obligation whatsoever – it will take you to the websites of the major credit reporting agencies where you can request your report. However, when going through the process of requesting your reports, be sure you don't inadvertently click, check or opt-in for any credit monitoring services that might be **offered** (but not required). If you find discrepancies on the report or have any other credit problems, you have specific rights under these federal laws to protect you, among other federal and state laws:

Fair Credit Reporting Act (FCRA)[114]
Fair and Accurate Credit Transactions Act (FACTA)[115]
Fair Debt Collections Practices Act[116]

[112] https://www.nerdwallet.com/blog/finance/credit-lock-and-credit-freeze/
[113] https://krebsonsecurity.com/2018/05/another-credit-freeze-target-nctue-com/#more-43713
[114] http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf
[115] https://www.privacyrights.org/facts-facta-fair-and-accurate-credit-transactions-act

Fair Credit Billing Act (FCBA)[117]
Equal Credit Opportunity Act[118]

Go to the Federal Trade Commission's website[119] and the Consumer Financial Protection Bureau[120] to find these laws and go to the respective credit agency's website and follow their instructions to file a dispute.

Here's another strategic tip: Credit reporting agencies are supposed to share information, so, theoretically, your report should reflect the same information with each agency. Therefore, if you want to check your credit 3 times a year for free, simply order your report from a different agency every 4 months.

Also, there is a new, free credit service called Credit Karma.[121] This site gives you access to information about your credit report and TransUnion credit score as well as tons of great information to help consumers better manage, repair and improve their credit. They also offer a smart phone application. Another similar service is Credit Sesame.[122] Note that you cannot access these services if your credit is frozen.

FYI, all three credit reporting agencies score your credit with a number from 0 to approximately 850 (I've also heard 930, but couldn't verify that number with a credible source.). They do so by using different models and calculations, which is why your score will probably vary slightly among agencies. The gold standard by which your credit used to be judged was known as your "FIC**O"** score – not to be confused with FIC**A** taxes. However, that is no longer the case and you just have to ask the lending institution, credit card issuer, etc., which agency's score they use as it varies widely. If you are interested in knowing your FICO score, you can purchase it here.[123] I have heard of some outfits that offer it for free now. Also be aware that there can be approximately 50-60 different scores depending upon what kind of loan you are applying for. For example, you have a different score for an auto loan than what you may have for a home mortgage or credit card advance. See **Section 9.** below for more information on credit.

If you are concerned about using your credit card online, some banks and credit card issuers allow you to go to their websites, login to your account and create a single-use, unique credit card number for that specific transaction only, so you are not entering the number that is actually on your card. Also, if you are concerned that your computer may be infected with a virus, some security software suites, such as Bitdefender Total Security[124] or Kaspersky Total Security[125], have a **"virtual keyboard"** that pops up on the screen and allows you to type in information into online forms such that the specific information cannot read or tracked by malware such as Trojans or keyloggers.

---

116 https://www.ftc.gov/system/files/documents/plain-language/fair-debt-collection-practices-act.pdf
117 https://www.ftc.gov/sites/default/files/fcb.pdf
118 https://www.consumer.ftc.gov/articles/0347-your-equal-credit-opportunity-rights
119 http://www.ftc.gov
120 http://www.consumerfinance.gov
121 http://www.creditkarma.com
122 http://www.creditsesame.com
123 http://www.myfico.com
124 https://www.bitdefender.com/solutions/total-security.html
125 https://usa.kaspersky.com/total-security

6. PROTECTING CHILDREN FROM IDENTITY THEFT

Shockingly, children are over 50 times more likely to have their identities stolen than adults (over 1 million children per year fall victim)[126] and the main reason is because their credit history is usually a clean slate and more than likely, any fraudulent activity with their credit files won't be noticed until they reach their latter teenage years when they are applying for college, jobs, loans, financial assistance, etc., and by that time, their credit histories can be severely damaged.

Theft of their identities originates with a family member in approximately 30% of the cases.

Children are particularly easy targets because usually no one thinks to watch their credit.

Children's identities can be easily compromised because so many people have access to their personal information, usually at educational facilities. Almost all the information necessary to steal an identity is in the child's school records – date of birth, address, SSN, etc., so the criminal can use that information to begin submitting false tax returns and building a completely bogus identity and credit history which they can use…..and abuse.

FERPA, the federal Family Educational Rights and Privacy Act[127] protects the privacy of student records and gives parents the right to opt-out of sharing contact or other directory information with 3rd parties including other families.

Also, 22 states have laws that allow parents to freeze a child's credit.

The U.S. Government's Federal Trade Commission has an excellent website that covers child identity theft.[128] And here's a good article from Kreb's on Security[129] about this and another from Kim Komando[130].

Also, if you are going to sell your house, you should remove pictures of the children or anything else that may have identifying information about them. Remember, most real estate companies will post pictures of your home on the Internet for marketing purposes and there will be strangers in your house during open houses and showings.

7. PROTECTING AT-RISK SENIORS FROM IDENTITY THEFT

As I've mentioned at numerous places in this report, for a variety of reasons, seniors, as a group, are sadly the victims of this type of crime and other scams and fraud at a rapidly growing rate. Elder financial (& other forms of) abuse is such a concern that the United Nations designated June 15th as World Elder Abuse Awareness Day. 47% of seniors are abused by a caregiver or caregivers, often times they are family members, and the abuse can take countless forms from simple to complex and the annual financial impact approaches $3 billion dollars. It is difficult for the untrained to recognize some of this abuse, so if you suspect it, contact the police or adult protective services. The National Adult Protective Services Association (NAPSA) has

126 https://clark.com/consumer-issues-id-theft/identity-theft/kids-identity-theft-what-to-do/
127 http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
128 http://www.consumer.ftc.gov/articles/0040-child-identity-theft
129 http://krebsonsecurity.com/2016/01/the-lowdown-on-freezing-your-kids-credit/
130 http://www.komando.com/happening-now/467928/babies-personal-information-sold-on-the-dark-web

some excellent resources[131] and the National Center for Victims of Crime-Financial Crime Resource Center[132].

All the tips I've mentioned thus far and below apply to seniors, as well, but I'd like to address those who are in long term care communities – independent living, residential care, assisted living, skilled nursing, long term skilled nursing, etc.

People in these settings are particularly vulnerable because so much of their personal and financial information is exposed to so many sets of eyes, not to mention their personal effects – more on that in a minute. If you are a caregiver, custodian, guardian, spouse, trustee, etc., it is very important that you monitor the person's financial accounts and credit reports for suspicious activity. In fact, I would suggest that anyone in a long-term care community have their credit reports frozen as well as taking the other precautionary steps outlined in this report.

I was recently at an assisted living community and a staff member, who knows what I do, related an incident to me regarding a group who was invited in by another community to speak to the residents about their potential eligibility to receive government assistance through the Veteran's Aid and Attendance Program, a legitimate government program that provides a generous monthly stipend to veterans or their spouses for the purpose of helping defray the skyrocketing costs of long term care. Applying for this benefit is complicated, time-consuming and tedious. This group, a "financial planning firm" offered "free assistance" to the residents with determining their eligibility, but of course, the residents had to provide a lot of sensitive personal information to help the firm's staff process their applications. If you've read this report from the beginning, you know where I'm going with this. The long term care community's staff had not vetted this "financial planning firm" and their staff was vacuuming up the residents' personal data to be used for other than legitimate and altruistic purposes. In cases such as this, a resident's personal information could be used for identity theft or just to pitch additional financial planning services and investment products to them, which they may or may not need, but, in many cases, there are no real "gatekeepers" for these residents to ensure that their best interests and personal information were protected and used properly.

To be fair, I have heard of other such financial planning firms who do offer this much-needed service to seniors and do so with the utmost professional care and due diligence when handling sensitive personal information. Note: If this is the first time you've heard of the VA Aid & Attendance program and are interested in more information, go to the VA's official website for the program here[133] or contact your local VA office for assistance (VA Facility Locator)[134].

Now, to avoid such situations, it is important that you communicate to the resident and the long term care community's staff that they are not to provide any third party vendors with any of the resident's personal information without prior approval of whomever is the resident's designated fiduciary.

Regarding security of personal effects, every long term care community requires new residents sign a waiver limiting the community's liability for lost or stolen valuables. Again, sadly, theft of valuables (rings, ear rings, watches, necklaces, etc.) is a stark reality in these communities where many have a rapidly-revolving employee door. Inasmuch, I recommend that any valuables be photographed and inventoried and appraised, where appropriate. Also, check with your insurance agent as you may want to take out a rider for very expensive items such as

131 http://www.napsa-now.org/policy-advocacy/exploitation/
132 http://victimsofcrime.org/our-programs/financial-crime-resource-center
133 http://benefits.va.gov/pension/
134 http://www.va.gov/directory/guide/division.asp?dnum=3

diamond rings, furs, etc. To help secure such items, I suggest a small security safe/cash box such as those offered by First Alert[135] and various other manufacturers – Walmart and office supply stores usually have good selections. When choosing one, be sure the person who will be using it has the manual dexterity and strength to open the safe – some have heavy doors and complicated locks. Some offer keys, combinations or both. The First Alert 2060F[136] is a good model.

8. OTHER COMPUTER, SMART PHONE/DEVICE & INTERNET SECURITY

What I am about to say next is going to sound harsh and I apologize for it being so, but I am only looking out for your best interest: If, after reading this section, you are saying to yourself, I have no idea what all this technical computer mumbo-jumbo is that he is talking about, then you probably shouldn't be using a computer or smart device for any kind of shopping, banking, medical account management, or any other activity that involves the potential for some hacker to access and steal your critical personal/financial information. Get someone to help you implement the tips I have here and if necessary, take some classes at local vo-techs to help you get up-to-speed with technology. Many offer them at very reasonable prices and at convenient times. Also, some offer classes specifically designed for complete novices and seniors. Class schedules can usually be found at the entrances/exits of most grocery stores. Many cities have private computer clubs that offer such classes at very low cost, too – check at your local library or community center for more information.

Most people's computer, tablet and or cell phone is a treasure trove of sensitive personal information, therefore, it is imperative that you password protect those devices and physically secure them. **It is also imperative that you keep your system clean. In other words, you need start with a system that you are relatively sure has not been compromised, have installed a very good software security suite (anti-virus, firewall, anti-malware), have all the computer's operating system's latest and greatest patches and security updates installed and your Wi-Fi network is secured.**

It is crucial that anyone who uses a computer use and keep their security software up-to-date. I recently stopped in Best Buy and asked their Geek Squad what they recommended and they said any of the Kaspersky-brand products are still the best and preferably one that is a "suite" of products which includes the anti-virus, firewall, and anti-malware functions. Bitdefender Total Security[137] is also an excellent product and an alternative to Kaspersky Total Security[138]. Keep in mind that you must buy the latest version of the software package whenever it is released – just updating the virus definitions and renewing your account annually isn't enough – you need the latest software "engine" to keep ahead of the criminals. Yes, I know there are several good, free programs out there, but the adage, "You get what you pay for" applies here, or, as I like to also say, "You don't get what you don't pay for." Think about it. Here's the latest security software reviews (July 2018)[139].

Another **critical** step is that you ensure you have installed the latest security patches and updates to your computers' and smart devices' operating systems (Windows or Apple iOS), Wi-Fi routers' firmware and software, and whatever Internet browser(s) you are using. With the computers' operating systems, you can usually set the systems to automatically download and

[135] http://www.firstalert.com/products/safes-cash-boxes
[136] http://www.firstalertstore.com/store/products/2060f-first-alert-78-cu-ft-theft-digital-safe.htm
[137] https://www.bitdefender.com/solutions/total-security.html
[138] https://usa.kaspersky.com/total-security
[139] https://www.av-comparatives.org/tests/real-world-protection-test-july-2018-factsheet/

install these updates. *(**Note:** In Windows 10, I have found that these updates do not download automatically, even when clearly set to do so, so be sure you go in and manually check for updates at least weekly, usually on a Wednesdays as Windows sends out updates on Tuesdays. If you don't know how to manually check for updates, just search the Internet for, "how to check for Windows updates.")* Here's why you **must** do this: When a software company releases a patch, it indicates to would-be hackers that there was a problem/vulnerability in the system's software and by examining the patch, hackers can find the vulnerability and begin to exploit it on systems that haven't been updated/don't have the new patch installed.

As you know, to access most of your online accounts, you have to provide your e-mail address (usually) and a password. For starters, use strong passwords, i.e., things that no one could guess or reverse engineer (say with information from your social media postings) – combinations of random letters, numbers and symbols and not something like "password." Hopefully everyone knows about this by now, but if you don't here's a great article[140] about how important it is to have strong passwords. See this article from Kim Komando[141] about the new (2017) password creation protocols. Also, never use the same password for more than one account, especially if for popular websites like Gmail, Amazon.com, iTunes, Yahoo, etc. If thieves can crack one, then they know that chances are good you may have an account with another popular website and probably use the same password with it. Many websites, especially e-mail and banking websites, have secondary levels of security you can enable, i.e., two-factor authentication (aka two-step login). For example, with most popular online e-mail providers like Gmail and Yahoo, after you enter your password to access your e-mail account, you can require it to prompt you to ask you a security question to which only you know the answer, or, you can have it send you a random 6-digit number via text message to your cell phone (or automated call to your land line with a number) which you have to enter to gain access to your account. It is very important to do this in light of all the different cloud-based e-mail addresses that have been compromised over the past couple of years. And be sure to read this article: Plug the Security Holes in Your Two-Factor Authentication[142]. And regarding security questions, again, don't use anything for an answer that could be reverse engineered from your social media postings such as your pet's name, etc.

If you are the ONLY person who uses your computer, you can operate it as the administrator, but, if anyone else uses your computer, like the children or grandchildren, you should set up separate profiles for each person – by doing so, you can limit their access to system resources and their ability to make changes to your system, i.e., install or remove software, change passwords, etc.

If you have Wi-Fi in your home, most of them have the network password on the device. It is very important that you remove that password and then go into the router's management software and change the password. This will prevent any unauthorized users from gaining access to your Wi-Fi signal and using your bandwidth or worse, hack into your computer. Again, like your computer, you can set up a "guest user" password for friends and family who come over and want to connect to the Internet via your Wi-Fi signal. Also, for security purposes, don't forget to frequently open the router's software program and check for firmware and

[140] http://www.dailymail.co.uk/sciencetech/article-2331984/Think-strong-password-Hackers-crack-16-character-passwords-hour.html

[141] https://www.komando.com/tips/417563/youve-been-doing-your-passwords-all-wrong-fix-them-with-these-new-tricks/all

[142] http://lifehacker.com/plug-the-security-holes-in-your-two-factor-authenticati-1798403323?rev=1503606340330&utm_campaign=socialflow_lifehacker_facebook&utm_source=lifehacker_facebook&utm_medium=socialflow

software updates. Even with this, your router is subject to what is called DNS hijacking and if that happens, criminals can watch everything you do on the computer and capture all your keystrokes. Read this article from Kim Komando[143] and use the free tool at F-Secure's website[144] to check for vulnerabilities. And while you're at it, go to Gibson Research Corporation Security's website and use their free tool to test your firewall for vulnerabilities. Here's another article from Kim Komando explaining that.

Also, for convenience purposes, I know many people who store user ID's and passwords in their Internet browsers (on smart phones & tablets, too) so they don't have to repeatedly enter them. This is poses a **huge** security risk in the event your computer gets infected with a Trojan virus or some other type of spyware or malware that allows a hacker into your system or if the computer physically gets stolen. All browsers are different, so go the Help section of your respective browser to find out how to delete saved information in your browser and prevent it from doing so in the future. If this is an issue for you, there are many slick (and some free) password managers out there which can solve this problem for you – here are a couple of excellent articles to help you decide which one would be best for you:

Lifehacker – Faceoff: The Best Password Managers Compared[145]
Lifehacker – The Five Best Password Managers[146]

Following above, don't write your passwords down and keep the list in a location someone could easily find. Just writing them down is a bad idea anyway. Ditto for saving them in a file that you stash in your e-mail account or file in a cloud-based file sharing service you might use for back-up, etc. Get a good password manager program that encrypts your data.

Physical security: Many laptops and desktops have a slot where you can attach a steel cable locking device to it – Kensington is a popular manufacturer or just search for "laptop security cable."

For cell phones, tablets and other smart devices, there are numerous applications that can help protect your information on them and help you remotely locate and or wipe them clean if they are stolen. Go to the respective device's application store and search for "security." Also, most of us have heard of LoJack[147] to help police locate stolen vehicles, well, they now have it for computers, as well. And be sure to read this important article from Kim Komando[148] about "drawing pattern" screen locks.

Do not charge your device by plugging in to any USB port in a public place – the port could be compromised and hackers could access your data. This is known as **"juice jacking."** Instead, get an portable battery pack (juice pack) that are available just about everywhere and in various shapes, sizes, prices and mAH (milliamp hour) capacities) to give your device a boost when it is running low on power. Here's a good article about this from CNN Money[149]. Personally, I don't even take my A/C - USB adapter and plug it in to any public electrical outlets to charge my phone.

[143] https://www.komando.com/cool-sites/312613/test-your-router-to-see-if-its-been-hacked-heres-how
[144] https://campaigns.f-secure.com/router-checker/
[145] http://lifehacker.com/lifehacker-faceoff-the-best-password-managers-compare-1682443320
[146] http://lifehacker.com/5529133/five-best-password-managers
[147] https://lojack.absolute.com/en
[148] http://www.komando.com/tips/322577/one-big-pass-code-mistake-phone-and-tablet-owners-make/all
[149] http://money.cnn.com/2017/02/15/technology/public-ports-charging-bad-stop/

You can get applications (apps) for your smartphones, tablets and other smart devices from a variety of sources, but be sure you only get them directly from official, reliable sources such as the Google Play website or Apple App store so you don't introduce any malware into your device.

Also, for your computer, there are tens of thousands of freeware and shareware programs, utilities, games, etc. You must be extremely careful when installing such software onto your system. Go to reliable, independent review source such as CNET's Download website[150] and look up the software and read the official and user reviews to see if the software you are considering installing has caused problems for other users.

Keeping up with all this technology and the threats to your device and personal information is daunting, however, there are some great websites that focus directly on consumer technology and safety and I suggest your subscribe to their e-mails to get the latest alerts and fixes.

Kim Komando[151]
Krebs on Security[152]
Kurt the Cyberguy[153]
TWiT[154]

Here's another twist on the phone scam from **section 2.C.** above: Scammers/hackers call and tell you they have detected a problem with your computer and need you to go to a certain website, click on a link and install some software so they can access your computer and repair it. This happened to a client of mine (twice) – she was lured in because the name of the "technical service" calling sounded very similar to that popular, nationwide electronics store that has the well-known computer repair department….and she had purchased the computer from that store and had their computer department set it up. Another angle on this is where you click on something in an e-mail and it installs malware on your computer and either immediately or delayed, a very official-looking pop-up appears informing you that your system has been infected with a (named) virus and you need to call the number (of an official-sounding company) in the pop-up to get assistance. When you call the number, they will get you to give them remote access to your computer, spend several hours "fixing" your computer and then sock you with a hefty charge. If you don't have a credit card, they may even ask you to write a check, put it on your scanner and then they can get an image of it and then they really go to town on your account!

GetSafeOnline.org[155] is an incredible website on this subject.

A. REMOVING YOUR NAME FROM INTERNET DIRECTORY WEBSITES:

Most of us have tried to find friends and relative via such popular websites such as those listed below, among many, many others. If you wish to shrink your online exposure, aka your "digital footprint," you can have your contact information removed from these sites. The procedure varies for each one and finding the instructions to do so at each site can sometimes be difficult. Therefore, if you want to remove the information, I suggest you start by using Google or Bing and search for phrases such as, "How do I delete myself from Spokeo?" or "How do I remove

150 http://download.cnet.com
151 http://www.komando.com/
152 http://www.krebsonsecurity.com/
153 http://www.cyberguy.com/
154 https://twit.tv/shows?shows_active=1
155 https://www.getsafeonline.org/

my name from the Whitepages?" etc. If that doesn't work, just go to the respective website and search through the Help section.

www.411.com
www.beenverified.com
www.familytreenow.com
www.intelius.com
www.lookup.com
www.lookupanyone.com
www.mylife.com
www.peekyou.com
www.peoplefinder.com
www.peoplefinders.com
www.peoplelookup.com
www.peoplesmart.com
www.phonebook.com
www.pipl.com
www.privateeye.com
www.public-records-now.com
www.publicrecords.com
www.radaris.com
www.spoke.com
www.spokeo.com
www.usa-people-search.com
www.usidentify.com
www.ussearch.com
www.veromi.com
www.wink.com
www.whitepages.com
www.zabasearch.com

Yes, there are some services such as Deseat[156], Reputation Defender[157], RemoveYourName[158], Delete Me[159], ManageYOURiD[160] among others that claim to be able to do this for you for a fee, but I do not have any experience with them. Read this article from CNET: 6 Ways to Delete Yourself from the Internet-Oct. 20, 2016.[161]

Here's a great article from Kim Komando on this topic: Remove yourself from people search sites, August 11, 2018[162]

Also, keep in mind that if you haven't taken the steps I have outlined to limit your exposure **(see sections 4. and 11.)** and prevent your data from being sold to marketing firms, chances are that your information will re-appear on these websites at some point, so go through the list and check periodically.

156 https://www.deseat.me/
157 https://www.reputationdefender.com/
158 http://www.removeyourname.com/
159 https://www.abine.com/deleteme/landing.php?utm_medium=blur-offer
160 https://www.manageyourid.com/
161 https://www.cnet.com/how-to/remove-delete-yourself-from-the-internet/
162 https://www.komando.com/cool-sites/7766/remove-yourself-from-people-search-sites

9. WHAT TO DO IF YOU BECOME A VICTIM

If your identity has been stolen and or your financial accounts tampered with, report it to the police and go to the Federal Trade Commission's Identity Theft Resource Center website[163] immediately for step-by-step instructions on what to do next. Also see Financial Crimes Victim Recovery Checklists[164]

First let me repeat this from the **INTRODUCTION** section. If you become a victim of identity theft, depending upon the degree of it, it can and usually does throw your whole life into a complete tailspin. Again, trust me when I say that our law enforcement agencies at all levels and financial institutions are working as quickly and diligently as they can to address it. If it happens to you, it will seem as if no one is doing anything to help, but please understand this type of crime and fraud are so pervasive in our society today that law enforcement agencies are overwhelmed by it and simply don't have the staff necessary to address it as quickly as they would like. Therefore, it is imperative that the public at large take steps to protect themselves from this kind of crime. You must be your own first responder!

Recovering from ID theft/fraud starts with filing the correct reports with the respective federal, state and local law enforcement agencies – you will have to decide whom to contact depending upon the nature of the crime, but you almost always must at least contact the 3 main credit reporting agencies, your respective financial institutions and your local law enforcement authorities. Inasmuch, please understand that recovering any stolen funds may or may not be possible and if you've sent money overseas, chances of recovery are practically nil. However, by reporting the crime, you are helping to "get the word out" and may help law enforcement arrest the perpetrators and save others from falling victim in the future. A number of government agencies track scams and investigate scam-based crimes.

As you go through the process of addressing your identity theft, document everything you do – everyone you speak with, times, dates, specific conversation details, etc. And be sure to let whomever you are speaking with know which other agencies you have already notified. After you speak with someone, ask for a name and address to send a follow-up letter to document the conversation.

One of the best places to start with a good system to walk you through the process is the U.S. Government's Federal Trade Commission's Identity Theft Center**.**[165]

To file fraud reports with the big 3 credit reporting agencies or place account freezes:

Experian Fraud Division
1-888-397-3742

Equifax Fraud Division
1-800-525-6285

TransUnion Fraud Division
1-800-680-7289

NCTUE (National Consumers Telecom and Utilities Exchange) Fraud Division
1-866-349-3233

---

[163] https://www.identitytheft.gov/
[164] http://victimsofcrime.org/docs/default-source/financial-fraud/victimrecoverychecklists.pdf?sfvrsn=4
[165] http://www.consumer.ftc.gov/features/feature-0014-identity-theft

Driver's License Number Fraud
Notify your state's Department of Motor Vehicles. Find your DMV here.[166]

Social Security Number Fraud
Notify the Federal Trade Commission at 1-877-ID-THEFT (1-877-438-4338)
and 800-269-0271
http://oig.ssa.gov/report

Passport Stolen/Fraud
Contact the U.S. State Department, Passport Services Department
http://travel.state.gov/content/passports/english/passports/lost-stolen.html
http://travel.state.gov/content/passports/english/passports/information/where-to-apply/agencies.html

Mail Fraud
Visit the U.S. Postal Service® Website, Government Services:
https://postalinspectors.uspis.gov/
https://postalinspectors.uspis.gov/forms/MailFraudComplaint.aspx

If financial loss was involved via an Internet scam, report to:

Internet Fraud
Internet Crime Complaint Center (IC3): http://www.ic3.gov/
Federal Trade Commission: https://www.ftccomplaintassistant.gov 1-877-FTC-HELP (1-877-382-4357)

For significant financial losses report to the U.S. Secret Service:
http://www.secretservice.gov/field_offices.shtml

Resources for victims of international fraud:
http://travel.state.gov/content/passports/english/emergencies/scams/resources.html

IF YOU HAVE CREDIT PROBLEMS OR ARE DENIED CREDIT:

A quick word on credit: I have run across several young people lately who have been taught in their "financial literacy" class in high school that they should pay cash for everything and do not get a credit or debit card. While I agree that you should avoid going into debt at all costs, (and do not have a debit card) having a credit history is almost imperative in today's economy. You cannot rent a car or get a hotel room without a credit card and I think you would have a very difficult time booking passage on any common carrier, especially aircraft, with just cash. Furthermore, having a good credit score gets you better interest rates on loans, insurance, etc. And what if you have an emergency, such as a car breakdown, and don't have enough cash to cover repairs, but need that car to get back and forth to a job or take the kids to school, etc.?? See what I mean? You can have credit, just understand how it works, the penalties for non or late payments and use it judiciously.

If you are denied credit (have a loan application denied) for any reason or if a lender took adverse actions against you such as increasing your interest rate based on your credit report,

[166] http://www.dmv.org/

you have rights under the federal law's Equal Credit Opportunity Act (ECOA)[167] to know exactly why the lender took such actions.

The **ECOA** also spells out your rights against discrimination when it comes to applying for credit. It is very important that everyone know and understand these rights. You can read about your rights against credit discrimination here.[168]

So, if you are denied credit or have other adverse actions resulting from your credit report, the lender is required to:

- Tell you it denied your application (or took other adverse actions)
- Provide you the numerical credit score it used in taking the adverse action and the key factors that affected your score
- Give you the name, address, and telephone number of the credit reporting company/agency that provided the report
- Tell you about your right to get a free copy of your credit report from the credit reporting company that provided it within 60 days of your adverse action notice
- Explain the process for fixing mistakes or adding missing items to your report

Under the ECOA, you may not be discriminated against by creditors/lenders because of these factors:

- Race
- Color
- Religion
- National origin
- Sex (gender)
- Marital status
- Age, unless the applicant is not legally able to enter into a contract
- Receipt of income from any public assistance program
- Exercising in good faith a right under the Consumer Credit Protection Act (such as disputing information in your credit report)

This also means that a creditor/lender may not use any of the above reasons to:

- Refuse you credit if you qualify for it
- Discourage you from applying for credit
- Provide you credit on terms that are different from the terms given to someone else who is similarly situated to you, such as having similar creditworthiness
- Close your existing account

Don't ignore mistakes on your credit report. If there are mistakes (inaccurate information) on it that caused a denial or change in your credit status that resulted in you not receiving the best interest rates/terms available, be sure to dispute the inaccurate information and get it corrected. Info on how to do that is here.[169]

If you find any other discrepancies on your credit report or have any other credit problems, you have specific rights under these federal laws to protect you, among other federal and state laws:

[167] http://www.consumer.ftc.gov/articles/0347-your-equal-credit-opportunity-rights
[168] http://www.consumerfinance.gov/fair-lending/
[169] http://www.consumerfinance.gov/askcfpb/314/how-do-i-dispute-an-error-on-my-credit-report.html

Fair Credit Reporting Act (FCRA)[170]
Fair and Accurate Credit Transactions Act (FACTA)[171]
Fair Debt Collections Practices Act[172]
Fair Credit Billing Act (FCBA)[173]
Equal Credit Opportunity Act[174]

Go to the Federal Trade Commission's website[175] and the Consumer Financial Protection Bureau[176] to find out more about these laws and go to the respective credit agency's website and follow their instructions to file a dispute.

If you need assistance repairing your credit, first, beware of places that claim to be able to "magically" eliminate all your debts – if it sounds too good to be true, it probably is. Repairing your credit will take **time** and **effort** on your part. You will want to contact an NFCC (National Foundation for Credit Counseling)[177] – affiliated non-profit credit counseling office. Here is a link to their affiliate office locator page[178]. In many cases, they go by the name "Consumer Credit Counseling Services of (name of your city, state or region) office. Also, see the U.S. Department of Justice's webpage[179] on this including a list of approved credit counseling services. And here[180] is some good information from the Federal Trade Commission on choosing a credit counselor.

10. FINAL THOUGHTS

I'm sure you're wondering why I didn't address credit and bank monitoring services – there are many out there and it's almost impossible to miss their ads on TV and popular radio talk shows. I have no personal experience with such services (since I use my bank's free services) nor do I know anyone who has, so I'll leave it up to you to make a decision on them, but do perform the appropriate due diligence before deciding to sign up. And if you do sign up, be sure to test the system. For example, if you have set a $200 per day ATM withdrawal limit on your bank account, try withdrawing more than that amount to see if you get an alert from your service. As I understand it, these systems are dependent upon the bank and the service's computers "talking" with each other and if any changes are made in the bank's system and they don't notify the service provider of the changes, then you may not get an alert. And remember, credit monitoring is just that, monitoring; it won't necessarily **prevent** the malicious activity from occurring. And you can take many preventative steps on your own and at no cost, such as fraud alerts, credit locks, credit freezes, and banking and credit e-alerts that you can place on your account(s) for free with your financial institutions, all of which I've outlined in this report.

Dave Ramsey, noted national financial educator and nationally syndicated radio talk show host endorses a plan from Zander Insurance Company.[181] I have no personal experience with this plan, but it might be worthwhile looking in to.

---

170 http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf
171 https://www.privacyrights.org/facts-facta-fair-and-accurate-credit-transactions-act
172 https://www.ftc.gov/system/files/documents/plain-language/fair-debt-collection-practices-act.pdf
173 https://www.ftc.gov/sites/default/files/fcb.pdf
174 https://www.consumer.ftc.gov/articles/0347-your-equal-credit-opportunity-rights
175 http://www.ftc.gov
176 http://www.consumerfinance.gov
177 https://www.nfcc.org/
178 https://www.nfcc.org/locator/
179 https://www.justice.gov/ust/credit-counseling-debtor-education-information
180 https://www.consumer.ftc.gov/articles/0153-choosing-credit-counselor
181 http://www.zanderins.com/idtheft/idtheft.aspx

In the **INTRODUCTION** section, I briefly touched on the information age and ***employee access identity theft***. Being in security and private investigations, I know a little bit about background checks and enough to know that not all companies are as thorough as they should be, ***in my opinion,*** when it comes to checking employees' backgrounds. And, believe it or not, legislation and regulations have been proposed to restrict employers' abilities to conduct background checks for individuals applying for "low-risk" positions, a.k.a. **"Ban the Box"** laws. And, for the purposes of some job positions and housing evaluations, there are legal restrictions as to how far back you may look into an individual's background or what information you may use for certain evaluation purposes. Even if companies use background checking services, do they really know how thorough that service is? Keep in mind that no database is 100% complete or accurate because not all jurisdictions report into the central databases and if they do, sometimes they aren't able to do so in a timely fashion, or sometimes errors occur when keying in the information, or sometimes people and records simply fall through the cracks for other reasons. Sadly, due to budgetary constraints, our law enforcement departments and court systems just don't have all the manpower and resources they absolutely need. In order to thoroughly check a person's background, you need to know every address where they've lived for as far back as possible in their history and then go to each respective jurisdiction and check with the local authorities and other sources, as well. Of course, that usually requires the resources of a licensed private investigator with access to several different, proprietary databases and $200 or more from the inquiring party and even they are limited by law as to what information they can access and provide to the client. Obviously, in our revolving-door employment society, that is not a very financially feasible option for most businesses and probably not absolutely necessary except with certain security-sensitive jobs/fields. Employment law and background checks are very tedious things and are always changing, so be sure to check with your company's human resource department and/or lawyer to ensure you stay within the limits of the law and your company's policies, even if accessing any publicly-available court records online.

With that in mind, back to the credit and bank monitoring services: Of course, what information you share with these services is completely up to you. I think most of them are probably just fine, however, ***I am of the opinion*** that no one entity should have that much unfettered access to your personal information except you and probably your spouse. Personally, I do not want that much information housed at any one central location where a hacker could possibly get to it or an employee could inadvertently lose or otherwise compromise it or just outright steal it. I don't care how rigorous their security protocols are; I've seen too many lapses and again, we've all seen and heard the stories in the news about companies that "lose" customers'/clients' account data and then fail to make the compromise known to the general public for weeks, months or even years! And in the latter part of 2016 we saw that no one, not even our highest government officials and systems are invulnerable to hacking. If that doesn't convince you that your sensitive personal information is **not** safe out there in cyberspace, I don't know what will.

Also, with regards to your sensitive documents – marriage license, real estate deeds/titles, original birth certificates, passports, etc. – these items should not be kept in one place in your home. If you haven't figured it out by now, identity theft is a HUGE and growing crime, so burglars are sometimes just stealing file cabinets because they know that they usually contain treasure troves of information that they can sell and or exploit. For these documents and other valuables, the best thing to do is put them in a safety deposit box at the bank. Seal them in Ziplock-style plastic bags in case there happens to be a water leak in the bank's vault. Also, shop around – rental fees for boxes vary greatly and most only require that you open a very basic checking account with a very small minimum deposit in order to rent a box. If you are placing expensive jewelry in the box, check with your insurance agent as you may need to adjust your coverage.

Below in **section 12., INTERNET RESOURCES**, is a list of websites that I have found to be helpful. While the list is by no means all-inclusive, they are some of the most comprehensive sources I've found on the subject matter, but new ones are always popping up. Be sure to frequently check the Helpful Info & Links page of my website[182] for additional resources and updates to this report.

When it comes to cutting down on the junk mail and telemarketer calls, be patient - sometimes it can take several months for you to see a reduction, but it will work and I speak from experience.

A couple of the time-tested adages that can be applied to this subject are:

"If it sounds too good to be true, it probably is."

"There is no free lunch."

"When in doubt, check it out."

[182] http://www.magnusomnicorps.com/helpful-info---links.html

11. IDENTITY THEFT PREVENTION CHECKLIST:

Yes, this list appears long, but most of the items are easy to take care of and in many cases, you only have to do them once. The rest are just daily habits you to which you will have become accustomed.

Because of the massive (1 billion) Russian gang password breach in 2014, the U.S. Government's OPM (Office of Personnel Management) breach in 2015, Yahoo breach in 2016, the Equifax breach in 2017, and many, many other breaches, we must all remain vigilant with our online accounts and activities. I am advising my clients to:

IN GENERAL:

- ☐ Our lives and society in general have become so complicated with all the rules and regulations, etc., that mistakes and omissions are rampant, causing ripple effects of strife in your daily lives. Inasmuch, **you** must be your own personal auditor. In other words, **you** must follow-up on everything to ensure the actions you expected to be performed by another party or parties has/have actually occurred. I'm talking about things as simple as going online to see if checks for your bills have cleared to logging in to your service provider accounts to ensure that your accounts have been properly credited. This is true even if you pay your bills electronically or by auto-draft – sometimes the bank or the service provider has a hiccup in their system. Or, if you still get paper bills through the mail, pay attention to when they usually arrive and call your service provider if they do not – someone may have gone to the Post Office and submitted a change of address form so they can get your mail at their address. And if you do any corresponding that involves the use of a fax machine, you **MUST** follow-up immediately to ensure the intended recipient received the information. I recommend against faxing any documents with personally sensitive information on them.

- ☐ Minimize the identification information and the number of cards you carry. Take only what you'll actually need. Don't carry your Social Security card, birth certificate, or passport, unless absolutely necessary; your state-issued driver's license usually suffices for most identification needs.

- ☐ Get a state-issued ID card (not driver's license) and keep it in a safe place, not in your wallet or purse with your driver's license. In case you lose your driver's license or let it expire, this is one of the most widely, and sometimes only, other accepted form of ID, with the exception of a U.S. Passport, which I also recommend everyone have. See the **Safety & Security** section, **Traveling** subsection of the **Helpful Info & Links page** on my website[183] for info about how to get a Passport and or Passport Card.

- ☐ Sign up for e-mail alerts from Krebs on Security[184] and Kim Komando.[185] These two are the best at giving everyone the earliest possible "heads-up" to data breaches and other elements of financial fraud and give you tips to secure your electronic life.

[183] http://www.magnusomnicorps.com/helpful-info---links.html
[184] http://www.krebsonsecurity.com
[185] http://www.komando.com

- ☐ Do not use your mother's maiden name, your birth date, the last four digits of your Social Security Number, or a similar series or sequence of numbers as passwords for anything.

- ☐ Do not give out personal information over the phone, through the mail, or over the Internet unless YOU have initiated the contact and are absolutely certain you know with whom you're dealing. Identity thieves will pose as bank representatives, Internet service providers (ISP's), and even government and law enforcement officials and have elaborate ruses to get you to reveal identifying information.

- ☐ Do not put specific birth and death dates in any obituaries or online in social media. Yes, even the dead can be victims of posthumous identity theft and it can wreak havoc on the decedent's estate when it comes to closing it out and cause countless problems for survivors who may be depending upon proceeds from the estate. http://www.fightidentitytheft.com/posthumous-idtheft

- ☐ Establish online accounts with the IRS[186], Social Security Administration[187], Medicare[188] and eBenefits (for DoD/Veterans)[189] and USPS[190] before someone else does it for you!

- ☐ There are many websites out there that appear to be official, U.S. government-operated websites, but unless they have the **.gov** extension in the URL, they are not! There is one exception, the United States Postal Service's website is: https://www.USPS.**com**

- ☐ Under no circumstances send or receive critical correspondences (bills, bills with checks, account statements, etc.) at your residential curb-side mailbox – get a box at the nearest, official United States Postal Service substation and, if available in your area, sign up for USPS's Informed Delivery service[191].

- ☐ Your tax returns pose a huge risk. If a criminal gets them, they have all the information they need to wreak havoc on your life. If you mail your taxes, be sure to send them via certified, return-receipt mail. I do this for all my correspondence to the IRS and state tax commissions.

- ☐ Spend the money to buy a good, large, cross-cut shredder (Sam's and Costco have them for reasonable prices.) Shred any and all documents with financially or personally-sensitive information. This includes pre-approved credit or insurance offers – very important to shred those.

- ☐ Do not print your phone number, Social Security Number, or driver's license numbers on checks or receipts. It should be extremely rare that any non-governmental entity would need your SSN. Exceptions would probably be your employer, bank and medical provider. If a business requests your SSN, give them an alternate number or ask them to assign you an alternate number and explain why. If a government agency requests your SSN, there must be a privacy notice accompanying the request.

---

186 http://www.IRS.gov
187 https://www.ssa.gov/myaccount/
188 https://www.mymedicare.gov/
189 https://www.ebenefits.va.gov/ebenefits/homepage
190 https://www.usps.com
191 https://informeddelivery.usps.com/

- ☐ Exercise caution when using ATMs, phone cards or any other activity with a credit-type card where you need to enter a PIN. Someone may look over your shoulder (known as "shoulder surfing") to get your PIN numbers, possibly giving them access to your accounts. Cover the keypad with your other hand when entering your PIN in case of hidden cameras. Also, AFTER entering your pin, place your fingers/hand over the entire keypad for a few seconds to mask any residual infra-red/thermal patterns that could give away your PIN to someone using new smartphone thermal image scanning technology. And always save your ATM receipts so you can reconcile them with bank statement – don't throw them away.

- ☐ Do not use your mother's maiden name as a security confirmation question – with the Internet and genealogy websites, maiden names are too easy for criminals to discover now. Use a unique password or PIN, etc.

- ☐ Keep confidential information in a secure location such as a bank safe deposit box or a locking fire file cabinet and don't share the information with anyone – things such as PINs, passwords, SSN's, driver's license numbers, account numbers, answers to security challenge questions, etc.

- ☐ Do not leave your purse or wallet unattended in your car for any amount of time. And do not leave any valuables in plain sight in your car. And don't forget to close your sunroof when you park your car.

- ☐ Do not leave ID credentials, stethoscopes or handcuffs hanging from your car's rear-view mirror

- ☐ Do not answer the phone if you don't recognize the number on the caller ID. If you do and it is a scammer, do not engage or otherwise taunt them; just hang up.

- ☐ Do not answer/open your door unless you are expecting someone and always ask who it is before you open it or look through the peep-hole.

- ☐ If you have contractors come in to your house or do any work for you, be sure to verify their credentials.

- ☐ When placing an obituary, do not include the decedent's exact birth date or death date.

- ☐ Secure all firearms, jewelry, medications in your home such that they are not accessible by unauthorized persons, children, contractors, individuals with dementia or other mental health issues.

- ☐ Do not give your keys (car, home, office, etc.) to anyone you don't absolutely trust. There are new apps for smart phones that take a picture of your key and then a new key can be made at a variety of self-kiosks in retail stores, just by uploading that picture from the smart phone.

FOR CREDIT CARDS AND OTHER FINANCIAL:

- ☐ Physically secure and protect your credit cards, checks and any other financial instruments with critical personal information.

- ☐ Make a list of all your credit card numbers and customer service contact numbers and keep them in a safe place such as a safe deposit box at the bank. (Do not photocopy them or any other sensitive information on a public copying machine! Watch this video[192] about the risks.

- ☐ When writing out checks, to prevent "check washing" fraud, use only pens with special "check fraud prevention" ink. These pens are sold just about everywhere and you can always find them at office supply stores. **Uni-Ball® 207™ Retractable Fraud Prevention Gel Pens**.

- ☐ Contact your bank(s) and have them set passwords and or security questions on your checking and savings (and any other) financial and or investments accounts.

- ☐ Password protect credit card accounts.

- ☐ If you bank online, set up security (e-mail and or text message) alerts for certain types of transactions.

- ☐ Monitor your bank accounts and credit card accounts very closely. Save your receipts and reconcile your credit card statements at the end of every month just like you do your checking accounts. Watch out for charges (aka "soft hits") for $1 or $10 – an indication that someone may have your credit card number and is testing to see if they can use it effectively and without you noticing.

- ☐ If you use a debit card, think again - read Kim Komando's articles, Worst Places to Swipe Your Debit Card[193] and the One Essential Thing You Need to Know to Protect Your Debit Card[194] and Clark Howard's 9 Places You Should Never Use A Debit Card.[195] Cancel it and go back to using a regular credit card, or in some instances, you may be able to have the bank disable the debit feature of the card so it will only function as a true credit card and not be able to access your bank account directly.

- ☐ In certain cases, you may want to place fraud alerts, lock or freeze your files with the big 3 credit reporting agencies. Clark Howard, noted consumer advocate, has a great page on his website with instructions on how to do this.[196] Children are one of the highest risks for identity theft, so consider freezing their credit files. Here's a good article from Kreb's on Security[197] about this and another from Kim Komando[198].

---

192 http://www.youtube.com/watch?feature=player_embedded&v=z147s6eNZp8
193 http://www.komando.com/tips/245380/3-worst-places-to-swipe-your-debit-card
194 http://www.komando.com/tips/247376/the-one-essential-thing-you-need-to-do-now-to-protect-your-debit-card/all?auth=checked
195 http://www.clarkhoward.com/5-more-places-you-should-never-use-debit-card
196 http://clark.com/personal-finance-credit/credit-freeze-and-thaw-guide/
197 http://krebsonsecurity.com/2016/01/the-lowdown-on-freezing-your-kids-credit/
198 http://www.komando.com/happening-now/467928/babies-personal-information-sold-on-the-dark-web

- ☐ Get **(100% free, no obligation, no credit card required)** copies of your credit reports at: AnnualCreditReport.com.[199] This is the **ONLY** government-approved site established in conjunction with the big 3 credit reporting agencies – there are many others with similar names, but this is the **ONLY** one. If there are discrepancies, address them immediately. You have specific rights under the law. Every credit agency should have instructions on how to dispute questionable items on your report(s). If you are offered credit monitoring products/services during the process, you are **NOT** required to sign up for or purchase them to get your reports. Remember, if you have frozen your accounts, you will have to unfreeze them temporarily to get your reports – there is usually a nominal charge to unfreeze your account.

- ☐ When swiping your card, if you have to enter a PIN, cover up the keypad with your other hand so that any clandestinely-placed cameras will not be able to record your numbers. Also, AFTER entering your pin, place your fingers/hand over the entire keypad for a few seconds to mask any residual infra-red/thermal patterns that could give away your PIN to someone using new smartphone thermal image scanning technology.

- ☐ Have dedicated-use credit cards – for example, one that you **only** use to swipe in machines (gas pumps, retail purchases, etc.), another **only** for restaurant purchases, another for **only** online purchases, another for **only** recurring payments (cable, utilities, phone bill, etc.) This way, if any one gets compromised, it won't wreak total havoc on your purchasing abilities.

- ☐ Use cash at high-fraud risk locations such as restaurants, gas pumps, 3rd party ATM's. Even better, use services such as Android Pay (now Google Pay, Apple Pay/AppleCash, Walmart Pay whenever possible.

- ☐ When traveling, be sure to call (or go online) your credit card issuer(s) ahead of time and notify them of your itinerary. If you do not, you could run into difficulty making purchases because due to rampant credit card fraud and identity theft, banks and other issuers will suspend an account if purchases are made that are outside your home area or don't correspond to your usual purchasing habits. And, they may or may not contact your immediately when suspending your account, leaving you in the lurch and very confused about what has gone wrong.

- ☐ Establish a savings account with your bank and have all direct deposits made to that account, not your checking, then you can transfer funds over to your checking account as needed. Why? If your checking account is compromised, you will have to contact all direct deposit institutions and update your information and that usually requires using regular mail, which can take several days and possibly create delays in you receiving money you need to cover bills, loans, insurance policies, etc.

- ☐ Put valuable papers (marriage licenses, property deeds, birth certificates) in a bank safety deposit box.

[199] http://www.annualcreditreport.com

CUTTING DOWN ON JUNK MAIL, TELE-MARKETER CALLS AND LIMITING YOUR EXPOSURE.

- ☐ Have your phone number unpublished/unlisted. There will probably be a fee for this.

- ☐ Place your cellular and land line phone numbers on the National Do-Not-Call Registry.[200] Remember, there are exemptions – charitable and political organizations, companies with whom you currently do business and companies with whom you have done business in the past 18-months are still allowed to contact you.

- ☐ Contact your cellular provider and enable Parental Controls and or set a password to limit the ability to make charges/purchases/donations via text messaging.

- ☐ Call 1-888-5-OPT-OUT (1-888-567-8688)[201] and follow the prompts. This will prevent the credit reporting agencies from selling/sharing/distributing your personal information to marketing companies and as such, in time, will greatly reduce (but not completely stop) your junk mail including such identity-theft high risk items such as pre-approved credit and insurance offers and unsolicited telemarketing calls and e-mail, etc. You can confirm the veracity of this number by going to the U.S. Government's Federal Trade Commission's website[202] and searching on the site for the phone number.

- ☐ Stop annoying and sometimes fraudulent robocalls with this service for landlines and cell phones: NoMoRobo[203] or Hiya[204]. Also for mobile phones, TrueCaller[205] or AT&T's free service app, Call Protect[206].

- ☐ Do not disclose your credit card number to an Internet vendor unless their website is encrypted and secure. Look at the first part of the web address in your browser; it should read http**S**://.

- ☐ Do not receive critical mail in your residence's curbside mailbox, rent a post office box at an official United States Postal Service (USPS) facility. If available in your area, sign up for the USPS' Informed Delivery service[207]

- ☐ When you order new credit cards in the mail or previous ones have expired, watch the calendar to make sure you get the card within the appropriate time. If the card is not received within that time, call the credit card issuer immediately to find out if the card has been sent. If you don't receive the card, check with the U.S. Post Office to make sure a change of address was not filed.

---

200 http://www.donotcall.gov
201 https://www.ftc.gov/search/site/1-888-5-opt-out
202 http://www.ftc.gov
203 http://www.nomorobo.com
204 https://hiya.com/
205 https://www.truecaller.com/
206 https://www.att.com/offers/call-protect.html
207 https://informeddelivery.usps.com/

- ☐ Pay attention to your billing cycles. Write on a calendar the dates when respective bills usually arrive. Follow up with creditors if bills don't arrive on time. A missing credit card or other bill could mean an identity thief has taken over your account and changed your billing address.

- ☐ Cancel all credit cards that you have not used in the last six months. Open credit is a prime target.

- ☐ Do not post your real birth date on any unofficial documents such as social media websites, etc.

- ☐ **Stop sharing everything about your life on social media!!** Especially things such as when and where you are going on vacation or any other items that could be used to social engineer a scam against you. If you have no idea what I'm talking about, Google it! Don't "check-in" at restaurants or other places – thieves will then know you're away from home. And be sure to review the privacy settings on your social media accounts and tighten them up – don't make everything available to the general public – that's a recipe for complete disaster!

- ☐ Any official communications you have, especially with the government (taxes, etc.) and or court/legal system, should be sent via certified return-receipt mail.

- ☐ Write to Direct Marketing Association, Mail Preference Service, PO Box 9008, Farmingdale, NY 11735 to get your name off direct mail lists. More info here.[208]

- ☐ On the Digital Advertising Alliance's website[209], go to the **DAA Resources for Consumers** section and follow instructions to limit you advertising exposure.

- ☐ Seniors, if you are fortunate enough to have a TRIAD/SALT program in your area (through your sheriff's office), **get involved!!** See the (unofficial) TRIAD page on my website[210] for more information.

- ☐ If you need resources to assist with all this, please check the Helpful Info and Links page on my website.[211]

[208] http://www.ftc.gov/privacy/protect.shtm
[209] http://digitaladvertisingalliance.org/
[210] http://www.magnusomnicorps.com/oklahoma-county-triad.html
[211] http://www.magnusomnicorps.com/helpful-info---links.html

COMPUTER RELATED:

- ☐ Change passwords on critical accounts regularly and every account should have its own unique password – no duplicates!!! Enable two-factor authentication (aka two-step login) (see **Section 8.** above).

- ☐ Use strong passwords. See these articles from Kim Komando: Article 1[212], Article 2[213], Article 3[214]..

- ☐ Password protect your computer. If you know how, set a boot-up password, too. Use biometric authentication if your device has that technology. Ideally, use both a password and biometric authentication.

- ☐ Set up guest-user profiles to prevent others from accessing your system and making changes, installing/removing software, changing passwords, etc.

- ☐ If you have Wi-Fi set up in your house, be sure you have changed the password on your Wi-Fi router from the password that it came with from the manufacturer and which is printed on the unit itself. Set up a "guest-user" password for friends and family to control bandwidth usage and system access.

- ☐ Read this article from Kim Komando[215] and use the free tool at F-Secure's website[216] to check your Wi-Fi router for vulnerabilities. And while you're at it, go to Gibson Research Corporation Security's website and use their free tool to test your firewall for vulnerabilities. Here's another article from Kim Komando explaining that.

- ☐ Password protect your cellular phones and tablet devices.

- ☐ Physically secure your computer – most computers have built-in slots for attaching safety cables, aka Kensington Lock slots. Also consider LoJack for your computer, especially if it is a laptop.

- ☐ Personally-sensitive information (account numbers, password files, medical and other financial information, etc.) should be stored in an encrypted, secure virtual vault – there are many great software products out there for this.

- ☐ Do not use your mother's maiden name, your birth date, the last four digits of your Social Security Number, or a similar series or sequence of numbers as passwords for anything.

- ☐ For account security questions, do not select questions where the answer could easily be obtained via Internet records, social media, etc.

---

[212] https://www.komando.com/tips/417563/youve-been-doing-your-passwords-all-wrong-fix-them-with-these-new-tricks
[213] https://www.komando.com/tips/9092/dont-make-these-common-mistakes-with-your-passwords/all
[214] https://www.komando.com/tips/370729/3-proven-formulas-for-creating-hack-proof-passwords/all
[215] https://www.komando.com/cool-sites/312613/test-your-router-to-see-if-its-been-hacked-heres-how
[216] https://campaigns.f-secure.com/router-checker/

- ☐ Ensure you are running the **LATEST PAID** version of a software security suite (anti-virus, anti-malware, anti-spyware, firewall) from dependable outfits such as Kaspersky Total Security[217] or BitDefender Total Security[218]. At the very least, purchase the latest software suite annually.

- ☐ Back up your computer files on a cloud service such as Mozy, iDrive, Carbonite, etc. External hard drives and flash drives in your home are okay, but they are vulnerable to the same virus infection, hacking, physical damage, theft and crashes as your computer.

- ☐ Use your computer's operating system's utilities to make back-ups of all your system's critical software, i.e., bootable disks. Your anti-virus software will usually have a similar utility – be sure you make those disks, as well.

- ☐ Remove all documents with personally-sensitive information from your hard drive before discarding your computer or sending it in for repair. When disposing of a computer, remove the hard drive and destroy it. I use a sledge hammer for this.

- ☐ Do NOT store/save user ID's and passwords in your computer's Internet browser and remember to uncheck the "remember this computer" box when logging in to websites that require a user ID and password and that is especially true if you are using a public computer, such as at the library. Use a third-party password manager.

- ☐ DO NOT store/save credit card/payment info on merchants' websites. I know this can be a pain, but instead, use a password manager, like Dashlane, which will auto-fill those fields when you are ready to make a purchase and keep your information encrypted and safe until you need it.

- ☐ LOG OUT/LOG OFF when finished using any accounts to which you had to log in.

- ☐ Clean you Internet browser's cache (and your system) frequently with a program like Piriform's CCleaner,[219] etc. The free version is fine. When going through the installation process (with this or any other freeware program), select the "custom or advanced installation" and un-check/de-select any other freeware, like browsers, toolbars, etc., that may be offered.

- ☐ **CRITICAL:** Ensure you have installed the latest security patches and updates to your computers' and smart devices' operating systems (Windows or Apple iOS), Wi-Fi routers' firmware and software, and whatever Internet browser(s) you are using and **especially:** Java (check version here)[220], Adobe Flash (check version here)[221], Adobe Shockwave (check version here)[222]. In most cases, the latter three aren't needed anymore, anyway, but some website content may not run without it – you can usually allow their usage on a case-by-case basis – look for the icons in your browser's address bar and right-click on them for options. This also goes for your smartphones and tablets.

---

217 https://usa.kaspersky.com/total-security
218 https://www.bitdefender.com/solutions/total-security.html
219 https://www.piriform.com/ccleaner/download
220 https://www.java.com/en/download/installed.jsp
221 http://www.adobe.com/software/flash/about/
222 https://get.adobe.com/shockwave/

- ☐ Only download apps, freeware, shareware and other software from reliable sources. Check it out at review sites such as CNET's Download Center.[223]

- ☐ Do not charge your device by plugging in to any USB port in a public place – the port could be compromised and hackers could access your data.

- ☐ When using public computers, such as at the library or using public Wi-Fi hotspots, such as at your favorite coffee shop or restaurant, unless you know how to secure your connection, **DO NOT** log in to any of your accounts while using these methods to connect to the Internet as your login credentials could easily be compromised. Rather, a safer way is to disconnect/turn off your Wi-Fi and connect to the Internet via the cellular network or consider purchasing your own, portable Wi-Fi hotspot device (and most smartphones have this capability – called "tethering," but that is usually an additional expense to your cell phone bill and uses your data plan). Also, you can also get a VPN (Virtual Private Network) service that will encrypt your communications when using a public Wi-Fi network and even your home network. Here's a good article.[224] Note that there is usually a monthly fee for this service, but it is very reasonable considering the amount of security it provides. It is available for laptops, tablets and smartphones.

- ☐ Enable a 2-step login process, i.e., two-factor authentication (See **section 8.** above), where after you have entered their user ID and password, you receive a text message on their cell phone (or an automated voice call to a landline) with a random 6-digit number that they also have to enter before accessing their accounts or enable any other type of 2-step (or greater) login authentication measures provided by the website, such as security questions.

- ☐ If you get a pop-up box **in your Internet browser** (that's a key point) that says your computer is slow or you need a driver, or you have become infected, etc., and it tells you that you need to call the toll free number for technical support and or should click on the box to remedy the situation, **DO NOT CLICK ON THAT BOX OR CALL THAT NUMBER!!!** Close it and run a FULL system scan with your security software and in the meantime, call someone you trust to assist you with assessing if you have a problem and eradicating any viruses or malware. If your computer gets infected, go to a computer you know to be safe and download (onto an empty flash drive) a copy of Windows Defender Offline. Google it and follow the instructions from Microsoft – this is pretty easy and most basic computer users can use this tool to eradicate malware from a computer.

- ☐ Don't click on links or open attachments in e-mails you weren't expecting to receive, even if the sender's address looks as if it came from a friend.

- ☐ Don't respond to or click on any links in e-mails from your bank or any service provider with which you have an account where they ask you to verify your account information. If you are concerned, close the e-mail, go directly to the website's official URL and log in or call your service provider with a number you know to be accurate and legitimate.

[223] http://download.cnet.com
[224] http://www.greycoder.com/best-vpn-service/

- ☐ If your computer freezes up and you get a screen that, for example, has the FBI logo and says that the FBI has frozen your computer and you must pay to get it unfrozen, that is known as **"ransomware."** Trust me, the FBI is not going to lock up your computer and charge you to unlock it. You will have to take your computer to a professional to have this removed or you may have to have the hard drive formatted to get it cleaned off and that means you will lose all your information – I hope you had it backed up to the cloud with one of the services I mentioned earlier! And have used your operating system's utilities to make a back-up of all your critical software and bootable files? Your anti-virus software will probably have a utility to do this also.

- ☐ Beware of pop-ups on your screen that are in generic grey boxes and tell you that your computer is infected or otherwise compromised in some way and that you need to call "Microsoft" or some other official-sounding computer company name for assistance and states the phone number to call. In most of cases, this is a phishing scam and if there was a real threat AND you are running good security software suite like Kaspersky Total Security[225] or BitDefender Total Security[226], it would be clear that the alert was from either one of those programs. Of course, you can run any number the pop-up tells you to call through any search engine to see if it comes up as a scam. People who fall for this scam are asked to go to a website, install software to allow the "technician" to remotely access your computer so he/she can "repair" it and what happens is they install more malware that will steal more of your data and then charge you for the "repair." And once you give them your credit card number and security code, then they really go to town!

- ☐ Stop sharing everything about your life on social media websites. Remove anything that indicates your address and phone number. Do not take pictures of the outside of your home. Turn off the geo-location function on your cell phone or digital camera – a feature that imbeds the time and location the picture was taken into the picture itself. Do not indicate when posts are made in real-time when you are away from home - it indicates to thieves when you are not at home!

- ☐ Beware of phone calls alerting you that they have detected a problem with your computer and want to either send you an e-mail with a link or go to a website, click on a link and install software that will allow them to access your computer so they can "repair" it.

- ☐ Only download apps (applications/programs) for your cell phone, smart phone, tablet or other smart device directly from official, reliable sources such as the Google Play website or Apple App store so you don't introduce any malware into your device.

- ☐ To keep up-to-date with the latest threats and fixes, subscribe to these websites' e-mails:

  Kim Komando[227]
  Krebs on Security[228]
  Kurt the Cyberguy[229]

[225] https://usa.kaspersky.com/total-security
[226] https://www.bitdefender.com/solutions/total-security.html
[227] http://www.komando.com/
[228] http://www.krebsonsecurity.com/
[229] http://www.cyberguy.com/

- Be sure to review this excellent list of vulnerabilities in the Appendices section below: **101 Ways You Identity Can Be Stolen and Exploited by the Acuant Corporation.**

12. INTERNET RESOURCES

This list is not all-inclusive. Please keep checking for updates to this report and check the **Helpful Info & Links** page of my website[230] for dozens more links.

Federal Trade Commission – Identity Theft Resources (excellent)
https://www.identitytheft.gov **(Your first stop if you've been a victim!)**
http://www.consumer.ftc.gov/features/feature-0014-identity-theft

Federal Trade Commission – Bureau of Consumer Protection
http://www.ftc.gov/bcp/index.shtml/

Consumer Financial Protection Bureau (excellent)
http://www.consumerfinance.gov/

National Center for Victims of Crime
http://victimsofcrime.org/

Government & Private Resource for Online Safety Issues
http://www.onguardonline.gov/

Privacy Right Clearinghouse
https://www.privacyrights.org/
Everything about your personal privacy.

National Crime Prevention Council (McGruff the Crime Dog)
http://www.ncpc.org/

FBI – Fraud & Seniors
http://www.fbi.gov/scams-safety/fraud/seniors/seniors

Consumer Federation of America
http://www.consumerfed.org/

Senior Fraud Protection Kit (Outstanding – download this report)
http://www.caregiverstress.com/senior-safety/con-cheat-seniors/senior-fraud-protection-kit/

Consumer Information/Advocacy
http://consumerist.com/

International Association of Financial Crimes Investigators
http://www.iafci.org

[230] http://www.magnusomnicorps.com/helpful-info---links.html

Fight Identity Theft (EXCELLENT)
http://www.fightidentitytheft.com/

Identity Theft Resource Center
http://www.idtheftcenter.org/

Internet Security at About.com
http://netforbeginners.about.com/od/antivirusantispyware/u/webdefense.htm

Get Safe Online
An outstanding website with tips on just about everything to do with online safety.
http://getsafeonline.org/

RFID Blocking Gear
http://www.idstronghold.com/

U.S. Government Consumer Publications
http://publications.usa.gov/USAPubs.php

National Sex Offender Registry
http://www.familywatchdog.us/

Love Fraud
Sociopaths, psychopaths, anti-socials, con artists – know the signs and don't fall victim to these.
http://www.lovefraud.com/

100% Free, No Obligation, No Credit Card Required Credit Monitoring
http://www.creditkarma.com
http://www.creditsesame.com

Note: *Will not work if you have your credit file frozen.*

TrustedID
Among other services, it scans websites known to traffic in stolen identity information (SSN's, etc.) and notifies you if your information is found on any such sites.
https://www.trustedid.com/

Scam Advisor
Enter a website's URL to see if it is legitimate and can be trusted to buy products from.
http://www.scamadviser.com/

Should I Remove It?
Don't know if that program is supposed to be on your computer? Go here to check:
http://www.shouldiremoveit.com

Scam, Fraud, Myth, & Hoax-Busting Websites

Important Note: *As if we didn't already know, the 2016 general election definitively confirmed that there is a lot of misinformation and disinformation floating around out there, even from websites and other sources that claim to be legitimate fact verification websites and yes, the same ones that are often cited by the mainstream media as holy grails of truth. Unfortunately, I cannot recommend one website from which to get absolutely accurate information, so I suggest that you consult multiple websites and just because they echo each other's claims doesn't necessarily make the claim true. Also, I'm sure everyone's heard the adage, "follow the money." Find out who operates and funds the website or source and you can pretty much tell whether you're dealing with a biased resource and whether you can trust it.*

http://scam-detector.com/
Excellent resource to research scams. Also have an app for smart phones

http://www.aarp.org/money/scams-fraud/fraud-watch-network/?cmp=EMC-EDO-032214-FraudWatchNetwork

http://www.acfe.com

http://www.crimes-of-persuasion.com/

http://www.consumerfraudreporting.org/

http://www.scambusters.org/

http://scam-detector.com/

http://www.scamwarners.com/

http://www.hoax-slayer.com/

http://www.fraud.org/

http://www.hoaxbusters.org/

http://urbanlegends.about.com/

http://www.ripoffreport.com/

http://www.quackwatch.org/

http://www.truthorfiction.com/

http://dontbeamoneymule.org/

http://www.fraud.org/

http://www.consumerfraudreporting.org/

http://www.scam.com/

http://www.justfacts.com/

http://www.quackwatch.org/

http://www.realscam.com/

http://phishtank.com/

http://800notes.com/

Use very cautiously and cross-check any information with several other sources:

http://www.factcheck.org

http://www.politifact.com/ (article: Running the Data on PolitiFact Shows Bias Against Conservatives 12-16-2016)

https://www.washingtonpost.com/news/fact-checker/

NewsGuard (article: Robert Spencer in FrontPage: Steven Brill's NewsGuard and the "Fact-Checking" Scam 07-16-2018)

http://www.snopes.com (article: Why the Left Loves Snopes 07-25-2017) (article: SNOPES busted – sold favors, slanted opinions 08-19-2015) (article: How Facebook & Other Fact-Checking Websites Are Fact-Checking Conservative Sites into Oblivion 07-03-2018)

NewsGuard (article: Robert Spencer in FrontPage: Steven Brill's NewsGuard and the "Fact-Checking" Scam 07-16-2018)

CASE STUDY: CATFISHING (aka Romance Scam)

OCCURRENCE DATE: March 2017
SUBJECT: Romance Scam Involving Internet Dating Website

Subject, "Nancy," contacted me (too late) to inform me that she had been the victim of a romance scam.

BACKGROUND:
Nancy, being a widow of many years and, for the most part, out of the dating scene for almost as many years, was encouraged by her pastor try an online dating website. She had tried several different ones before, but never had much luck and found it to be too much of a hassle. Nevertheless, she was encouraged by her pastor's anecdotes of successful relationships and marriages he'd seen that had grown out of online dating connections.

So, Nancy signed up with one of the most popular online dating websites. She surfed around for a couple of weeks, but didn't find anyone of interest. Then, one day when she was about to sign off, a connection request appeared. She had never seen this man's profile before, but he sounded (and looked) very nice, so she responded to Mike.

They corresponded for just a couple of days through the online dating website's internal messaging system and then Mike wanted to "go direct" since that would be easier. So, Nancy gave him her cell phone number and he gave her his.

They texted and talked for a couple of more days and became better acquainted with each other. He lived in another large city in the same state as she and was a widower of several years (wife and daughter died in a car collision). He was also a successful business owner and devoted church goer. His mother lived in Spain, but was in poor health.

Nancy, being somewhat cautious and weary based on all the stories she'd heard in the news about scams and fraud, searched for Mike's name and company but could find neither and his phone number was through a popular online search engine website (VoIP – Voice Over Internet Protocol). She didn't think much of any of it, chalking it up to her inexperience with the Internet and Mike was just so nice. All this time she had been keeping her pastor apprised of the situation and her pastor even contacted the pastor at Mike's church, but the pastor there had never heard of him. Nancy questioned Mike about this and just thought that she had given the wrong name of his church to her pastor and left it at that.

She really liked everything about Mike and he even sent her some flowers and chocolates for Valentine's Day. She was enamored by his thoughtfulness and accent and she really liked that he was so devoted to his faith, as was she.

About a week after talking back and forth, Mike told Nancy that he needed to get some money to his ill mother in Spain and asked if she could go to a Western Union and take care of it for him. He wasn't asking her for money, only to forward the money to his mother in Spain. Mike couldn't do it because he was very busy preparing for an upcoming business conference. Nancy was just getting over the flu and didn't feel too well and didn't want to get out and do it, but Mike kept stressing the urgency, so she did.

Nancy found a store that had a Western Union terminal. She pulled up the account, but strangely, the name on it was some other woman, not Mike's. She wasn't sure how to operate

the terminal or complete the transaction, so she asked the store clerk for assistance. They were unable to forward the money because the Western Union terminal flashed a message saying that the amount was over the limit allowed. Nancy contacted Mike who assured her that the amount was well below the limit and couldn't understand what went wrong and just told her to forget it. Nancy went home not thinking too much about it.

A couple of days later, Mike asked Nancy to go to a large electronics store way on the other side of town and pick up a couple of computers that he was going to need for his upcoming business conference in another state. Again, she still wasn't feeling well, but he stressed the urgent nature and she agreed. When she went to pick up the computers, which were already paid for, she noticed that a different woman's name was on ticket, not Mike's. She questioned him about this and he said that she worked for his company and made the purchases for the company. She took the computers home.

In the meantime, Mike and Nancy were getting along very well. He'd sent her more pictures of himself and his mother in Spain, including a picture of her in the hospital, but it didn't quite look like her based on the other pictures he'd sent, but the picture wasn't high quality and from an odd angle. She didn't think too much about this.

Mike told Nancy that his mother had suggest that he get her a promise ring, so he told Nancy that the ring would arrive on a Wednesday and gave her the tracking number and the company who was sending the ring. Nancy checked out the jewelry company and it was legitimate. The ring didn't arrive on Wednesday, so she called the company and they said that they'd had some problems with the shipment and it would arrive the next afternoon, which it did, but instead of Mike's name on the shipping document, it had Jeff's name. She wondered why that was and asked Mike about it. Mike said that Jeff was his assistant at the company and had owed him some money, so Mike just had Jeff pay for the ring himself and that's why Jeff's name was on the shipping document. Okay, she thought, that sounded reasonable. It was a lovely gold ring with some small diamonds. Based on what she saw on the seller's website, the ring was worth around $1000.

A couple of days later, Mike asked Nancy to take the computers she'd picked up earlier to the nearest UPS store and have them shipped to the city where his business conference was going to be. He e-mailed her the mailing labels, she printed them off and took the computers and labels to the UPS store and paid $40 to have them packed.

She started to think about all this and realized things didn't add up, so she called the local police and related the above story to an officer who made a report. The officer didn't seem overly concerned and downplayed the whole situation, but made a report, nevertheless.

A couple of days later, she received a call from UPS's fraud division questioning her about the computer shipment. Apparently, the computers had been purchased with a stolen credit card. She told the UPS representative about suspecting fraudulent activity and that she filed a police report, so UPS didn't pursue any charges against her. At that point, Nancy blocked Mike's number and called the police back and wanted to inform them of what happened and amend/update the report. The officer said they couldn't update or amend a report, but everything was okay since she had made a report before all this happened and was "covered." She also mentioned the ring, but the officer didn't seem concerned about that either since, at that point, there was no reason to believe that sale/purchase was anything but legitimate.

Nancy eventually returned the ring to the seller, thinking it also may have been purchased with a stolen credit card, but she never found out either way. Mike continued to try to contact her, but she no longer answers numbers she doesn't recognize.

CASE STUDY: PHISHING (Computer Tech Support Scam)

OCCURRENCE DATE: January 2017
SUBJECT: Scam Involving Landline Telephone & Computer

Client, "Sue," contacted me about a computer problem she'd been having. Even though she was highly-educated and had been using computers for decades and even started by learning how to program them with the Fortran language, she is, by most measures today, a novice computer user, especially when it comes to recognizing scams and fraud.

In the past, I had helped her purchase a computer at a local Best Buy store and had their in-house Geek Squad set it up for her and purchased a one-year service contract with them. After the Geek Squad was finished setting it up, I picked up the computer, took it to her home, installed it and have helped her maintain it and instructed her on certain software program usage from time-to-time.

Recently she told me that she had received a phone call on her landline from **"Geek Support Live Services"** and that they had discovered that she had something wrong with her computer and that she needed to go to a website and download some software so they could remotely access the computer and repair it.

She did as they requested and spent about 2 hours on the phone with technician Adam Lee (who had a strong eastern Indian accent), who was ostensibly walking her through repairs. This was later in the evening and she got tired and they ended the session and she agreed to continue the follow day. The next day she spent 5 hours on the phone with Adam "repairing" her computer.

After he finished he requested a payment of $499 for his services. Fortunately, she was unable to pay as her bank had shut down her only credit card because of an unrelated fraud incident. Her new card was supposed to arrive the next day via Fedex and Adam agreed to call back the next day to obtain payment.

I received an e-mail from her later that day informing me of what happened. I knew that it didn't sound right, so I went over to her house to examine the computer. The computer was functioning properly, however, there were several new software programs icons on the desktop. I wasn't familiar with any of the programs (G-Dock, Anti-Hacking Software, etc.), and had never seen any of them on her computer before. Adam also said he installed Windows Network Security 4.1.1 (there is no such program according to Best Buy's Geek Squad). Also, there was a toll-free "tech support" number at the bottom of her screen in the taskbar. I Googled the number and multiple "who called me" type of websites all listed it as a scam.

She showed me an e-mail they had sent her with an impressive looking Geek Support Live Services logo and a business card icon with her account number, etc. It all looked official, however, absent was the well-known orange and black Best Buy **Geek Squad** logo with which just about everyone is familiar.

I pointed out to Sue the difference between Geek Support Live Services and Geek Squad and the play on the name.

At that point, I was quite convinced she had been scammed, so I disconnected the computer and took it in to a local Best Buy store and dropped it off at the Geek Squad desk. The computer was still covered under her original tech support contract, so there would be no charge for their services.

While Sue's computer was at Best Buy being repaired, Adam Lee continued to call daily asking Sue for payment for services rendered, to the amount of $499. She told him she couldn't understand him because of his strong accent and her hearing impairment, which is true, and hung up. I instructed her to stop answering the phone when numbers she didn't recognize came up on her caller-ID. Eventually she did stop answering the phone.

I even happened to be present at Sue's house when Adam called back on one of those days wanting payment. He started out being very courteous and cordial, but gradually became very demanding. I became impatient and told him that I was a detective working for Sue and asked him if he understood what a detective was. He said he did, but he remained undeterred in demanding payment. He even said we could pay with her bank account and routing number – I declined that option, of course. I told him I had taken the computer to the Best Buy Geek Squad for a second opinion and he would receive payment when I was satisfied the computer was properly repaired and hung up.

Sue, being the honest person she is, thought that she owed Adam and Geek Support Live Services their fee because they did, after all, spend several hours working on her computer. I told her that we would make that determination after we got Best Buy's Geek Squad report.

Two days later, the Geek Squad called for me to pick up the computer. The technician informed me that they had found 17 incidences of viruses and other malware installed on the computer – it was heavily infected.

Sue continued to want to pay Adam for his services, but I told her, "Sue, if Adam had done what he had said and repaired all the problems with your computer, Best Buy's Geek Squad would not have found it so heavily infected, so apparently Adam either did not do his job properly/adequately or this is a scam and I'm quite certain it is the latter and she finally agreed.

A few days after we got the computer back from Best Buy's Geek Squad, the e-mail ***(see below)*** arrived from Adam. Everything about this message is so bad that it would be funny if he wasn't trying to perpetrate a crime. I think the best part of it is where he says, *"So Mam We have fixed all your Computer problem So geeks squad will not get any issue in your Computer."*

I believe this was only a scam to get money and her credit card or bank account number and not necessarily information on her computer. However, we did change all the passwords on critical accounts and had the Geek Squad install some very robust security software (Webroot).

UPDATE (May 2017):

Adam has continued to call Sue and, despite my constant urgings, she continues to answer the phone when she does not recognize the number. This time she said he called from number with our area code and only asked for $199 instead of the original $499. She even insisted, again, that she pay him *something* because he did work on her computer, after all. And I reminded her that if it was a legitimate business, he wouldn't be calling from numbers with constantly changing area codes. Further, I reminded her that when he was "repairing" her computer, he was actually loading it up with all kinds of malware that the Best Buy Geek Squad found and removed – she had forgotten about that. She continued to insist that she looked up the company and that it was a legitimate company based out of London. I told her that I

checked into it and the service I used could not absolutely verify that it was a legitimate company. I reminded her that if she ever did provide payment with a credit card or bank account number, this Adam and his cohorts would be off to the races on her dime and there would be no retrieving of the money since it was coming from overseas. After some continued back and forth, I was satisfied that I had convinced her (again) that this was a scam and she relented.

UPDATE (July 2017)

I received a call from Sue – she was having computer problems again. This time a blue box popped up informing her that her computer was infected with the Zeus virus and that she needed to contact MS InfoTech for assistance and gave her a toll-free number to call. She got scared and thought that since the name of the company had "MS" (short for Microsoft) in it, that it was legitimate.

She called the toll-free number and allowed the "technician" remote access to her computer. They took control and spent 6 hours "fixing" the problems. She eventually paid for the service by writing out a check for $299 and placing it on her scanner so the technician could scan an image of it and use it for payment.

For some reason, she called me and related this incident to me shortly after she hung up with the technician. I immediately knew it was a scam and went over to her house, checked her computer and it had all the same software installed on it that the scammer in the original example had installed.

I had her call her bank and lock up her account immediately. Fortunately, the scammers had not attempted to cash the check.

I then disconnected her computer and took it to Best Buy Geek Squad for analysis/repair. They found it heavily infected with malware and cleaned it off. Fortunately, no data was lost and even if it had been, her information was backed up in the cloud through the Carbonite online backup service.

I eventually determined the source of the problem. At some point, she had decided to play the Publisher's Clearing House sweepstakes, online. Well, she received an e-mail informing her that she could've possibly won $1 million and she clicked on a link in the e-mail and it installed some kind of malware on her computer that cause the blue box Zeus virus warning to appear with the toll-free tech support number to call.

Again, she was somewhat insistent that the whole ruse was in fact legitimate and it only took me a few minutes of Google searching the company name and phone number to prove to her that it was yet another scam. I also showed her articles about the e-mail/tech support scam and PCH scam and that PCH does not notify sweepstakes winners by e-mail.

Hi,

Sue.

Hope Doing Well.

This is **ADAM LEE** your computer Technician. **i Fixed your computer on 15 & 16 Jan 2017.**
And before i fixed your computer there was lots of problem in your computer. We fixed your **Hacking problem,** We fixed your **antivirus problem,** We **Updated your computer,** We **upgraded your computer, Activated firewall** And We have **Removed all Bad File** which was running Behind your computer.
And after fixed your all computer problem i also shown you that **Now your computer is fixed.**

And for That all Services and Fixing all problem, i told you, you have pay the Money. But still **We didn't get any Money from you.**So please Mam i request to you **please Pay the Amount Which i told you.**
And mam you told me You have given your Computer to Geeks Squad. So Mam We have fixed all your Computer problem So geeks squad will not get any issue in your Computer.

And Maim i apologise For 'if you will not pay the amount, So our company will stop all services which i done on your Computer' AND After stopping all services.., Your Computer will get Infected again. and you will lose your Thousands of Doller Any time by Attacker. And might be your computer will not turn on You will lose your HARD DRIVE. So mam we Don't want to stop services of your computer which we put.

So Please Maim, **I REQUEST TO PLEASE PAY THE AMOUNT**

Thank's

Regard's
Adam Lee
(computer Technician)

If you've read this far, congratulations and thank you for your interest!!! The best thing we can all do to help stem this tide of criminal activity is to continually educate ourselves, stay aware of the latest scams and fraud, and take precautionary and protective measures.

At this point, as if you didn't already know, I'm sure you realize that keeping track of and up-to-date on all the latest scams and fraud is nearly an impossible task these days, even for professionals who work in this field. So, below I have tried to develop a brief, general "tip sheet" of scam avoidance strategies, fraud indicators and the best websites to keep up with them.

If you have a loved one or know someone who has been a victim or almost victimized and may be at risk of being victimized again, print off the next 3 pages and give them to that person so they can have them for future reference.

ID THEFT, FINANCIAL FRAUD & SCAM REMINDER TIP SHEET

CRITICAL STEPS TO AVOIDING SCAMS

1) **DO NOT** answer the phone unless you recognize the number or name.

2) **DO NOT** answer the door unless you know who it is.

3) **DO NOT** let anyone, 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.)

4) **DO NOT** open e-mails from unknown senders and if you do, **DO NOT** click on any links inside them; doing so can install all kinds of malware on your computer.

5) **DO NOT** give anyone remote access to your computer unless you are **absolutely certain** they are a legitimate computer repair service and not a scam. Google search their name and or toll-free number for reports of a scam.

GENERAL WARNING SIGNS OF A SCAM

This usually involves some kind of verbal ruse over the phone.

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.

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 threatens immediate warrant/arrest by law enforcement if you don't provide the information/payment immediately.

5) Person says they are coming to your house to deliver some kind of prize winnings or other gift(s).

6) Person claims they are with a local, federal or state agency (IRS, FBI, other law enforcement, utility company, etc.) and demands you take some kind of action (usually make a payment with a credit card or checking account number) under threat of immediate arrest.

REMEMBER THESE WORDS OF WISDOM

1) If it sounds too good 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! (Google search for scam-related reports.)

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)[231]!!! OPEN TO THE PUBLIC, FUN, FREE & NO COMMITMENTS. DO IT NOW!!!

[231] http://www.magnusomnicorps.com/oklahoma-county-triad.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/scams-fraud/fraud-watch-network

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

http://www.fraudoftheday.com/

http://www.krebsonsecurity.com

http://www.getsafeonline.org

https://www.consumer.ftc.gov

http://www.cyberguy.com

http://www.komando.com

http://www.clark.com

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

http://www.magnusomnicorps.com/publications.html

In addition to reporting any crimes to the police, go here immediately if you have been a victim – this website outlines everything you need to do to recover and protect yourself and your assets:

U.S. Federal Trade Commission-sponsored website:
https://www.identitytheft.gov

101 Ways Your Identity Can Be Stolen and Exploited

Source: https://www.acuantcorp.com/101-ways-your-identity-can-be-stolen-and-exploited/

1. Using your social security number to get insurance
Some crooks obtain your social security number or other private information over the phone posing as someone from your insurance company, and then they use it for themselves.

2. Stealing identifying information from your license
If someone has your driver's license information, they don't even need your physical license to cause all kinds of trouble.

3. Identity fraud for property purchase
A theft could use your identity and social security number to apply for a rental property or to purchase a house.

4. Creating a new identity
Some criminals use others' identities to stay off the grid or because they need a new identity.

5. Using a child's identity
Thefts target children's identities because it often takes a lot of time until the crime is discovered, giving the theft plenty of time to use the child's identity for opening up lines of credit as issuers do not authenticate the age of every applicant being processed.

6. Stealing from your mailbox
Often people get credit card and loan offers in the mail. A criminal could steal these, fill them out using your private information, and use a different address then your own so they don't get any notices.

7. Phishing emails
Phishers target the elderly especially with this technique, as they tend to respond with their information.

8. Nigerian letter scheme, or 419 fraud
This common scam combines an advance fee scheme, where thieves get people to send money and checks, and try to gain access to your bank account.

9. Telemarketing calls
Sometimes you may get a call from some organization or department that seem legitimate and for a good cause. If you feel the need to donate, find the organization's number online and call that directly to assure yourself you are dealing with the organization itself, not a scammer that is pretending to work for them.

10. Sharing your vacation pictures while you're away
Everyone loves to show off their vacation pictures on social networks these days. What you may not think of is that criminals can lurk online seeing that you are away and that your house could be left unattended.

11. Sharing sensitive information on social media
As you update your family and friends with your daily whereabouts, criminals could also see this to learn your schedule. They can figure out when you tend to be away from your home to stage a break-in.

12. Stolen cellular phones
If you have private information like online passwords and any financial information on your phone and it gets stolen, the theft could use this to access your accounts and go on a spending spree. Call your phone company right away to see if they can locate it or to wipe the phone's data remotely.

13. Using your debit card for online shopping
Don't ever use your debit card to shop online because, unlike credit cards, you are not backed by a credit card company for any fraudulent charges.

14. Going through your trash
Whenever you throw out personal information, you should always use a shredder.

15. Changing your mailing address
Changing your mail to another address is easy if you have enough of the suspect's information to do so. You can do it pretty simply online, and mail is sent to the current address to verify the change that a thief can easily intercept – so you are unaware of the change for at least a few days.

16. Illegally tapping into your computer
Any expert hacker can easily hack into your computer, especially if they have your IP address. Doing so will get them access to all of your personal documents, and if you use a password manager, they could find out all of your account login information as well.

17. Having weak wireless security
If you use Wi-Fi at home, which about 58% of American households use according to Strategy Analytics, you should use some form of security and password to keep others out.

18. Using public Wi-Fi
Never do any online shopping or anything personal when you are connected to a public Wi-Fi.

19. Weak passwords
Using weak passwords online and on your computers that are short and don't include numbers or special characters can be easily hacked.

20. Keeping your social security card in your wallet
If your wallet is lost or stolen, you don't want just anyone to have access to this. Always keep your social security card stored in a safe place.

21. Credit card skimming
Thieves can use credit card skimming devices at gas stations, ATMs, and restaurants to make a copy of your credit card, so be sure you know how to spot a skimmer device.

22. Responding to or downloading attachments from spam
Spam e-mails are getting better at reaching your inbox and looking legitimate, but if there is anything that seems fishy from an e-mail, then don't open or respond to it. If you don't know the sender then never open the attachment. Spammers can send from any e-mail address, so don't think an email is safe even if it looks like it is from a reputable source.

23. Never checking your credit
You should have alerts set up with a financial institution in case your credit scores changes due to someone else using your identity and financial accounts to make purchases or open new credit cards.

24. Accessing fake credit card sites
It isn't hard these days to create a legitimate-looking credit card website to fool others into filling out their personal information to apply for a credit card.

25. Going on fake financial or utility websites
A lot of phishing emails look like they are coming from your bank or from PayPal, when really they are just a scam to "update your account information" on a site that is cloned just like the real site.

26. ATM watchers
Thieves set up cameras at ATM machines to watch you enter your PIN number and gather any other identifying information.

27. ATM overlays
Overlays are devices placed over the keypad of an ATM, typically designed to look just like the original keypad. These capture your PIN number, and work with other technology such as skimmers and cameras, to catch your data.

28. Grocery store PIN thieves
Just like with ATM machines, people could overlook you entering your PIN number when you use your debit card at checkout lines.

29. Downloading torrents
Torrent files can be full of malware and viruses that can be used to access your computer and files to be used to steal your identity.

30. Falling for "free" offers, like vacations, gifts, and prizes
Anytime you're offered a luxury item or trip for free, but you're being pressured to sign up now because the contest is almost over, be wary. Identity thieves use urgency to get people to make decisions they wouldn't normally make.

31. Soliciting credit card information by phone
Giving your credit card over the phone from a number you did not yourself call, even if it sounds like a legitimate company, is an easy way for it to end up in the wrong hands.

32. Overusing your SSN for medical identification
When you overuse your social security number for medical identification, your Medicare card becomes vulnerable.

33. Sharing of private data on hacker networks
Hacker networks gather password and authentication information, and often share that information with other hackers or sell it.

34. Bulk gathering of IDs via black market
Major data breaches often collect large numbers of IDs. When this happens, the identification information is often traded and sold on the black market.

35. Failing to destroy old hard drives and computers
Don't just throw them out or sell them on Craigslist. If you sell your computer, also take out the hard drive and replace it with a new one.

36. Stealing your electricity
This is also known as electricity theft or energy theft. Utility theft occurs when individuals bypass energy meters, tapping power lines, and more in order to steal electricity.

37. Job thieving
Undocumented workers or individuals with a criminal history will often use another individual's identification information to obtain employment.

38. Social engineering
Typically, when a swindler knows enough legitimate information about an individual to make themselves seem trustworthy and deceive the victim into divulging sensitive information.

39. Vishing, or "voice fishing"
Voice fishing is a type of scam that involves a phone call or robo-call to get you to call back a legitimate organization, like a government agency. They fake an emergency, or claim that you've won a prize, in order to get that coveted SSN or credit card number.

40. Baiting by pretexting
Often, criminals will do an extensive amount of research on an individual beforehand to scam them into believing they are a legitimate business. They call on the phone collecting your name, address, and phone number, and use this to seek even more information.

41. Man-in-the-middle attack
Criminals intercept information between two individuals, record it, and use the information to steal an individual's identity.

42. Pharming
Pharming occurs when hackers reroute individuals from the desired URL to an impostor website, and get them to reveal credit card and other identity information.

43. Malware-based phishing
This uses harmful computer programs that look like helpful ones, such as anti-virus, and use screen loggers to capture sensitive data.

44. Corporate data breaches
When hackers breach bank or shopping data from a large company, thousands of people can be put at risk for identity theft.

45. Keystroke logging
Keystroke loggers capture every key that you type into a computer, allowing data thieves to retrieve your passwords and even sensitive messages.

46. Rootkits
Rootkits are a class of malicious software that allows programs to run in stealth, without the detection on a computer, in order to have privileged access to the information the computer stores.

47. Scam texting—SMiShing
Thieves send extremely urgent-sounding text messages posing as a trusted organization, and get your information when you click on a link in the message.

48. Viruses and worms
The installation of a virus on your computer can allow hackers to gather your information such as names, dates of birth, and of course, social security, and bank account numbers.

49. False claims for refunds from the IRS
Thieves often steal identity information in order to file multiple claims with the IRS.

50. Passport thieves
Take care of your passport when you're on vacation. This important means of identification in America is often stolen and used as a form of identification by thieves.

51. Publicly listing your hobbies, memberships, and employer
The beginning of an identity thief's search usually involves personal information. Why? People are more likely to respond to requests for information from affiliations and groups they might be a part of. Not being aware of how this information can be manipulated is dangerous.

52. Driver's license theft
Your driver's license is unique to you. Using it, an individual can pretend they're you at traffic stops and more. Even just your driver's license number can be leverage enough.

53. Using your mother's maiden name
This question is often asked as verification when, for instance, your password is forgotten. Simply by learning your mother's maiden name, an identity thief now has a key detail about you that can be used to pretend they're you to get into your bank account.

54. Defrauding banks
Identity theft and bank fraud go hand in hand for obvious reasons. Thieves use personal information and even create fake checks and IDs in order to steal millions of dollars from individuals' accounts at financial institutions. These instances are unfortunately on the rise.

55. Impersonating missing children
This frightening scenario has happened more than once. Individuals can use information about missing children in order to con friends and even family members to believe they've returned after years.

56. Fake being a financial adviser for the famous
An identity thief was able to get enough information on famous people like Stephen Spielberg to successfully pose as their financial adviser—and then stole from their bank accounts.

57. Stealing the identity of a missing person
As strange as it sounds, this has happened, as recently as 2008. A high school dropout used the identity of a woman who had disappeared eight years prior to gain admission to two Ivy League schools. In a related turn, many college students who apply for credit cards and loans for the first time find that their identities had been stolen years prior.

58. Faking one's own death
Identity thieves have been known to fake their own death in order to assume the identity of another individual with a clean record.

59. Synthetic identity theft
This form of identity theft is particularly malicious and complicated. Thieves combine stolen information (for instance, a social security number) and combine it with other real and fake information to create a "new," synthetic identity which can be used to obtain new credit cards and take out loans. These crimes can go on undetected for years.

60. Having a publicly listed number
Pay a little extra to get your number privately listed so that telemarketers can't call you, which lowers your chances of getting into a scam.

61. Keeping credit cards, checks, and bank statements in your car
If your car were to get broken into, all of your private financial information would be at thieves' fingertips.

62. Not using a safe at home
Play it safe in case your home is ever broken into by keeping anything confidential in a safe.

63. Not using a security service
Services like Life Lock have a $1 million guarantee to protect your identity.

64. Not freezing your credit card accounts
Credit report agencies can freeze your accounts so that no one else can open up an account or take out a loan in your name until you unfreeze it. If you don't freeze your account after a suspected breach, more of your data is susceptible to theft.

65. Leaving receipts behind
Always take your receipts with you, even if they only display the last few digits of your card.

66. Not writing "check ID or license" on the back of your cards
Do this instead of signing your signature so cashiers always check your photo ID to verify it is you using your card.

67. Failing to consider one-off credit cards
If you aren't a frequent online shopper or you really want to be safe, you can get one-time use credit cards for online shopping.

68. Shopping on un-trusted websites
Look for https in the URL to be sure the site is secure. Also, look for the Trust e-symbol, or PayPal or Better Business Bureau stamps.

69. Not having anti-virus software on your PC
Install anti-virus software as well as anti-spyware to monitor your system for viruses and hacking attempts.

70. Using the same passwords online
Sure, it's easier to remember them, but then it's easier for a hacker to access all of your accounts.

71. Never changing your passwords
You should change all of your passwords every few months or at least once a year.

72. Logging into accounts on public computers
While they are easier for hackers to access public networks, you may also forget to log out.

73. Putting checks in the mail
Put your checks in a piece of paper inside an envelope or a non-see through envelope so they can't be seen through lights.

74. Leaving bills at your mailbox for pick-up
Always deliver your bills personally to the post office.

75. Moving out
Make sure to call all of your credit card companies, utilities, creditors, your bank, the IRS and any other financial institution when you change your address.

76. Not opting out of credit card offers
Go to optoutprescreen.com to opt-out of pre-approved credit card offers and other junk mail.

77. Not using online billing options
If there is an option for online billing, sign up for it. No more chances for lost mail.

78. Using unsafe mailboxes
If you live in an apartment complex where others can possibly access your mail, open up a P.O. box.

79. Forgetting to check links online
Hover over a link before clicking on it. Doing so shows a preview in the lower left corner of your browser so you know the site you will be visiting. Look out for pages that redirect to others.

80. Accepting strange friend requests
It's just not worth getting your Facebook friends up to 1000 if you have some people who you really aren't sure who they are… even if you have mutual friends.

81. Not wiping your phone
Have an app in case your phone gets stolen that you can remotely clean all of your data. Also do this before selling a phone.

82. Using one email account for everything
Use a different email account for your bank, financial accounts, and social networks. If one is hacked then they don't have access to all of your other accounts.

83. Thinking Macs are impenetrable
While it is more difficult for malware, viruses, and hacks on Macs, it is not impossible.

84. Storing credit card information for later use
Even if it is a store you recognize or shop at a lot, take the time to type credit card information in every time instead of storing it. We've seen that even the biggest stores online can have their data breached.

85. Not using two-step verification if available
For sites like Gmail that offer a second step to verify your account, which is a code that is sent to your phone by text message. If a hacker figures out your password, they will be stuck in the second step of verification.

86. Not changing your home locks and using a "do not duplicate" label on your keys
If someone "borrows" your keys they can very easily go make copies if those keys are without a "do not duplicate" label.

87. Not using a lock on your phone or tablet
Always lock your devices with a code, password, or swipe sequence.

88. Using camera phones
When you're in a situation that requires identifying information to be displayed, whether at the bank, the store, or the gas station; be wary of your surroundings. The ubiquity of camera phones means, even if you're quick, vital information about you can be stolen and stored.

89. Pickpocketing
The old school way of stealing your identity by taking your wallet or phone to get your information is alive and well.

90. Ordering unauthorized credit reports by posing as a landlord
Someone could pretend to be a landlord to run your credit report.

91. RFID scanners
Wireless technology used in some credit and debit cards to allow contactless payments, but thieves can use a RFID scanner if they get close enough to you.

92. Using your place of birth as a security question
Thieves can easily find out the hospital or town you were born in to answer your security questions to gain access to your accounts.

93. Obtaining information for use as revenge or blackmail
Some scoundrels collect information gleaned from susceptible computers and other sources to simply blackmail an individual or business by threatening to go public with sensitive information.

94. Stealing information from doctor's office
Health records from a doctor's office contain vital information about your identity. Many identity thieves try to hack a medical facility's EHR (electronic health records) to steal sensitive, identifying information.

95. Filling out car loan applications
Identity thieves can buy cars by taking a loan application out in the name of another person.

96. Clicking on pop-ups
Always avoid pop-ups. When you click them, they could start a download in the background, which possibly contains a virus or malware.

97. Thieves going through pharmacy waste baskets
Unfortunate as it is, pharmacies don't always shred sensitive information about prescription holders. Waste paper baskets are often full if information thieves can use.

98. Mortgage ID theft
In most cases of mortgage fraud identity theft, victims have no clue that criminals obtained financing in their name and ran with the money until they're faced with an eviction notice.

99. Opening cyber greeting cards
A cyber greeting card sent from a "friend" could contain malware that invades your computer undetected and steals your passwords, bank numbers, and credit card information.

100. Installing electronic surveillance
In a day and age of heavy surveillance, installing cameras to steal credit card numbers, debit card PIN numbers, bank statements, and more is a growing threat.

101. Payroll data breach
Your company's payroll system or an outsourced payroll system can be hacked, which can put customers' corporate bank accounts and employees' personal information in the hands of hackers. This is why it's so important for every business to have identity solutions in place to protect themselves and their customers.

Below is a list I compiled from 2 sources and include the latest breaches through 2017.

For 2018 breaches, also see:

Business Insider (8/22/2018): If you shopped at these 16 stores in the last year, your data might have been stolen[232]

Barkly (July 2018): The 10 Biggest Data Breaches of 2018….So Far[233] (Includes Facebook, Under Armour, Ticketfly, Panera Bread, Exactis and others.)

Biggest Data Breaches of All Time

The list below is a partial take from the referenced source and includes breaches through 2017.

Source: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Adult Friend Finder
Date: October 2016
Impact: More than 412.2 million accounts
Details: The FriendFinder Network, which included casual hookup and adult content websites like Adult Friend Finder, Penthouse.com, Cams.com, iCams.com and Stripshow.com, was breached sometime in mid-October 2016. Hackers collected 20 years of data on six databases that included names, email addresses and passwords.

Most of the passwords were protected only by the weak SHA-1 hashing algorithm, which meant that 99 percent of them had been cracked by the time LeakedSource.com published its analysis of the entire data set on November 14.

[232] https://www.businessinsider.com/data-breaches-2018-4
[233] https://blog.barkly.com/biggest-data-breaches-2018-so-far

CSO Online's Steve Ragan reported at the time that, "a researcher who goes by 1x0123 on Twitter and by Revolver in other circles posted screenshots taken on Adult Friend Finder (that) show a Local File Inclusion vulnerability (LFI) being triggered." He said the vulnerability, discovered in a module on the production servers used by Adult Friend Finder, "was being exploited."

AFF Vice President Diana Ballou issued a statement saying, "We did identify and fix a vulnerability that was related to the ability to access source code through an injection vulnerability."

Read more about the Adult Friend Finder data breach...

Equifax

Date: July 29 2017
Impact: Personal information (including Social Security Numbers, birth dates, addresses, and in some cases drivers' license numbers) of 143 million consumers; 209,000 consumers also had their credit card data exposed.

Details: Equifax, one of the largest credit bureaus in the U.S., said on Sept. 7, 2017 that an application vulnerability on one of their websites led to a data breach that exposed about 147.9 million consumers. The breach was discovered on July 29, but the company says that it likely started in mid-May.
Read more about the Equifax breach...

Uber

Date: Late 2016
Impact: Personal information of 57 million Uber users and 600,000 drivers exposed.
Details: The scope of the Uber breach alone warrants its inclusion on this list, and it's not the worst part of the hack. The way Uber handled the breach once discovered is one big hot mess, and it's a lesson for other companies on what not to do.

The company learned in late 2016 that two hackers were able to get names, email addresses, and mobile phone numbers of 57 users of the Uber app. They also got the driver license numbers of 600,000 Uber drivers. As far as we know, no other data such as credit card or Social Security numbers were stolen. The hackers were able to access Uber's GitHub account, where they found username and password credentials to Uber's AWS account. Those credentials should never have been on GitHub.

Here's the really bad part: It wasn't until about a year later that Uber made the breach public. What's worse, they paid the hackers $100,000 to destroy the data with no way to verify that they did, claiming it was a "bug bounty" fee. Uber fired its CSO because of the breach, effectively placing the blame on him.

The breach is believed to have cost Uber dearly in both reputation and money. At the time that the breach was announced, the company was in negotiations to sell a stake to Softbank. Initially, Uber's valuation was $68 billion. By the time the deal closed in December, its valuation dropped to $48 billion. Not all of the drop is attributable to the breach, but analysts see it being a significant factor.

Read more about the Uber breach…

The list below includes breaches through 2016.

40 Biggest Data Breaches of All Time

Source: https://www.acuantcorp.com/40-biggest-data-breaches-time/

The internet has become a pervasive entity in the lives of businesses everywhere, making communication, marketing, and doing business easier than ever. However, the rising number of data breaches has begun to paint a darker picture of the internet and what it has in store for companies in the coming years.

Data breaches explained

A data breach occurs when any sensitive, internal information is exposed, regardless of whether it's for malicious reasons or not. This data includes business, employee, and even customer information—often personally identifiable information (PII), such as names, social security numbers, payment card numbers, and more. Cyber criminals can sell this information they steal from your servers, or use it to make fraudulent purchases and steal identities.

Hacking, ineffective counter-measures to malware and inadequate network security/encryption all have the potential to lead to a data breach.

Price of becoming compromised

It's difficult to put a price on data breaches. Aside from money lost to lawsuits, there's the cost of IT to repair the damage or hardware, loss of reputation, future revenue with the loss of clients and customers. It's difficult to quantify just how much money these data breaches cost companies because of the non-material things, such as reputation, that can also be lost as a result. In 2015, it was estimated that the average, per-record cost of a data breach had reached $154.

The integrity of your internal network and the skill level of your IT team is paramount in protecting your business's data. No one is immune to data breaches, however; but it can help to have a preparedness plan in place should one occur.

The companies with inadequate post-breach plans, or that lack one altogether, are typically the ones who suffer the largest setbacks. They may not become aware of malicious attacks until hours, days, or weeks after they've occurred, in which time the hackers may have already caused irreparable harm with the stolen data.

Between 2005 and 2015, there were over 5.5k data breaches in the United States alone—and these were only the ones publically announced. We've outlined 40 of the largest data breaches of all time to illustrate the lasting damage these malicious cyber-attacks can have on businesses large and small.

1. Epsilon

Year of breach: 2015

Number of records affected: 60-250 million

Handled communications for more than 2,500 clients worldwide—including seven Fortune 10 companies. Hackers stole records of 50 Epsilon clients, exposing at least 60 million customer emails, but potentially as many as 250 million emails may have been obtained. Breach affected companies such as Best Buy, JPMorgan Chase, Capital One Bank, and Verizon.

Monetary cost of breach: The number could reach $4 billion depending on what happens to the data that was stolen.

2. Experian (owner of "Court Ventures")

Year of breach: 2012

Number of records affected: 200 million

Credit bureau Experian purchased Court Ventures, a firm that aggregated, repackaged, and distributed public record data. They continued reselling data to a third party without Experian's notice and awareness. A Vietnamese hacker was found to be responsible for the illicit use of the purchased personal information of 200 million individuals.

Monetary cost of breach: Unknown.

3. U.S. Voter Database

Year of breach: 2015

Number of records affected: 191 million

Breach exposed names, addresses, birth dates, party affiliations, phone numbers, and emails of voters in all 50 U.S. states and Washington.

Monetary cost of breach: None.

4. NASDAQ

Year of breach: Between 2005 and 2012

Number of records affected: More than 160 million

Foreign hackers stole more than 160 million credit and debit card numbers, targeting more than 800,000 bank accounts. NASDAQ servers were also compromised.

Monetary cost of breach: Unknown.

5. eBay

Year of breach: 2014

Number of records affected: 145 million

Hackers gained access to a database holding eBay customers' names, home addresses, dates of birth, and encrypted passwords.

Monetary cost of breach: The company spent about $200 million to settle class-action suits and regulatory fines.

6. Saudi Aramco

Year of breach: 2012

Number of records affected: 145 million

This Petroleum and Gas Company responsible for suppling at least 10% of the world's oil was hit by a virus, causing them to lose almost 35,000 of the company's computers. They

were forced offline completely and had to rely on fax and typewriters to continue business. Aramco lost its ability to process payments and temporarily ceased the sale of oil to gas trucks. After 17 days, they had to give oil away free to fulfill Saudi oil needs.

Monetary cost of breach: Unknown costs of massive IT and security overhaul, more than 50,000 new hard drives, software, and "giving away" oil.

7. Heartland payment Systems

Year of breach: 2008-2009

Number of records affected: 130 million

More than 250,000 businesses across the country were affected after the 130 million credit and debit card records of major credit card companies were stolen by hackers.

Monetary cost of breach: Eventually payed more than $110 million to Visa, MasterCard, American Express, and other card associations to settle claims related to the breach.

8. Target Stores

Year of breach: 2013 & 2014

Number of records affected: 30 million & 70-110 million

The credit and debit card numbers of 30 million customers were stolen during the 2013 post-Thanksgiving shopping surge. In 2014, 70-110 million customers were compromised when full names, addresses, email addresses, and telephone numbers were hacked, many of whom had previously lost their credit and debit card information in the 2013 data breach.

Monetary cost of breach: Incurred total net expenses of $148-162 million for both 2013 and 2014 data breaches.

9. Sony Online Entertainment Services

Year of breach: 2011

Number of records affected: 102 million

Hackers obtained the login credentials, names, addresses, phone numbers, and email addresses for users on the PlayStation Network, Sony Online Entertainment, and Qriocity video- and music-streaming services. 23,400 Sony Online Entertainment users in Europe had their credit-card data stolen.

Monetary cost of breach: Resulted in 65 class-action lawsuits totaling $171 million to $1.5 billion.

10. Anthem

Year of breach: 2015

Number of records affected: 69-80 million

The second-largest health insurer in the U.S., Anthem, lost names, addresses, dates of birth, social security numbers, and employment histories of its customers in a data breach that affected upwards of 80 million individuals.

Monetary cost of breach: Nearly $100 million spent to address the breach, but the final cost may well exceed that number.

11. National Archive and Records Administration

Year of breach: 2008

Number of records affected: 76 million

Malfunctioning hard drive containing the names, contact information, and social security numbers of 76 million U.S. military veterans was sent for repair. When the contractor determined the drive could not be fixed, it was designated as 'scrap' but no confirmation was made as to whether the drive was actually destroyed. NARA launched an investigation and determined that no breach of personally identifying information (PII) had occurred, however they were forced to change their policies for the destruction of malfunctioning storage media containing PII.

Monetary cost of breach: None.

12. Securus Technologies

Year of breach: 2015

Number of records affected: 70 million

As a leading provider of phone services inside the nation's prisons and jails, Securus Technologies lost 70 million records of phone calls and links to downloadable recordings of the calls—many including conversations between attorneys and their clients. This not only exposed individuals to fraud and phishing scams, but brought to light potential breaches of attorney-client privilege on behalf of Securus.

Monetary cost of breach: Unknown.

13. The Home Depot

Year of breach: 2014

Number of records affected: 56 million

Handled communications for more than 2,500 clients worldwide—including seven Fortune 10 companies. Hackers stole records of 50 Epsilon clients, exposing at least 60 million customer emails, but potentially as many as 250 million emails may have been obtained. Breach affected companies such as Best Buy, JPMorgan Chase, Capital One Bank, and Verizon.

Monetary cost of breach: Between $40-80 million was spent between both breaches.

14. Evernote

Year of breach: 2013

Number of records affected: More than 50 million

Note-taking and archiving service lost email addresses, usernames, and encrypted passwords to data breach. Left users vulnerable to spam emails and phishing campaigns, and further attempts at obtaining user passwords through phishing.

Monetary cost of breach: Experts estimate that Evernote spent "many millions of dollars" in expenses following the breach.

15. Living Social

Year of breach: 2013

Number of records affected: More than 50 million

Daily-deals site lost the names, email addresses, birth dates, and encrypted passwords of more than 50 million customers worldwide.

Monetary cost of breach: Unknown.

16. TJX Companies Inc.

Year of breach: 2006-2007

Number of records affected: Around 46 million

Parent company of major retail brands such as Marshalls, T.J. Maxx, and HomeGoods. At least 45.6 million credit and debit card numbers were stolen over an 18-month period, but estimates put number closer to 90 million. About 450,000 TJX customers affected, loss of PII, including driver's license numbers.

Monetary cost of breach: Costs have ballooned to $256 million.

17. RSA Security

Year of breach: 2011

Number of records affected: 40 million

Breach allowed hackers to steal information on the company's SecurID authentication tokens.

Monetary cost of breach: $66 million on remediation.

18. Sony Pictures Entertainment

Year of breach: 2014

Number of records affected: Everything

Movie and television production division of Sony was held ransom when hackers threatened to release everything the company had on file. The cyber criminals exposed the social security numbers and scanned passports of actors and executives, unpublished scripts, marketing plans, internal passwords, legal and financial information, and four entire unreleased Sony films. 6,800 employees and an estimated 40,000 more faced potential identity theft. Rival Hollywood studios received detailed blueprints of Sony Pictures' accounts, future plans, and internal workings.

Monetary cost of breach: Upwards of $35 million.

19. CardSystems Solutions

Year of breach: 2005

Number of records affected: 40 million

An attack on the company's database exposed names, account numbers, and verification codes of more than 40 million card holders for Visa, MasterCard, and American Express. The hackers exploited the weakness of the system's encryption.

Monetary cost of breach: Unknown, but company was forced into acquisition following the breach.

20. Adobe

Year of breach: 2013

Number of records affected: 38 million

In addition to nearly 3 million encrypted customer credit card records, approximately 38 million encrypted passwords and Adobe IDs of active Adobe users were taken by cyber criminals.

Monetary cost of breach: $1.1 million in attorney fees and an undisclosed sum to victims of the breach.

21. Zappos
Year of breach: 2012
Number of records affected: 38 million
Customer names, home and email addresses, phone numbers, the last four digits of credit card numbers, and encrypted passwords were taken by hackers.
Monetary cost of breach: $106,000.

22. AshleyMadison.com
Year of breach: 2015
Number of records affected: 37 million
The company's user databases, financial records, and other proprietary information was compromised by hackers.
Monetary cost of breach: Unknown, but costs incurred in the UK alone could go up to 1.2 billion depending on filed suits.

23. Valve Corporation
Year of breach: 2011
Number of records affected: 35 million
Hackers gained access to user names, hashed and salted passwords, game purchases, email addresses, billing addresses, and encrypted credit card information. Valve was uncertain whether breach affected all active accounts or just a portion.
Monetary cost of breach: Unknown.

24. ESTsoft
Year of breach: 2011
Number of records affected: 35 million
Malware uploaded to company server resulted in the loss of names, user IDs, hashed passwords, birthdates, genders, telephone numbers, and home and email addresses. Considered South Korea's biggest theft of information in history.
Monetary cost of breach: Unknown.

25. Department of Veterans Affairs
Year of breach: 2006
Number of records affected: 26.5 million
Unencrypted national database with names, social security numbers, dates of births, and disability ratings for veterans, active-duty military personnel, and their spouses were obtained through a data breach.
Monetary cost of breach: Cost is anywhere from $100-$500 million for prevention and coverage of possible losses from the theft.

26. Office of Personnel Management
Year of breach: 2015
Number of records affected: Over 25 million
Over the course of two separate breaches, the records of 21.5 million federal works and 4.2 million individuals fell into the hands of hackers. Personal information, background checks, names and addresses, and fingerprints were among the data obtained by Chinese hackers during the breaches.

Monetary cost of breach: Full dollar cost unknown, estimated to be within the range of $900 million.

27. Korea Credit Bureau
Year of breach: 2014
Number of records affected: 20 million
An employee was found responsible for the theft of at least 20 million bank and credit cards from three different credit card firms in South Korea. The stolen data included customer names, social security numbers, phone numbers, credit card numbers, and expiration dates.
Monetary cost of breach: Unknown.

28. Experian / T-Mobile
Year of breach: 2015
Number of records affected: 15 million
Breached data included names, addresses, birth dates, Social Security numbers, driver's license numbers, and passport numbers of T-Mobile applicants.
Monetary cost of breach: Unknown.

29. Premera BlueCross BlueShield
Year of breach: 2015
Number of records affected: 11.2 million
The breach exposed subscriber data, which included names, birth dates, social security numbers, bank account information, addresses, and other information.
Monetary cost of breach: Unknown.

30. Data Processors International
Year of breach: 2003
Number of records affected: Up to 8 million
A hacker obtained access to information on as many as 8 million credit card accounts across Visa, MasterCard, Amex, and Discover.
Monetary cost of breach: Unknown.

31. Vtech
Year of breach: 2015
Number of records affected: 6.4 million
The company's Learning Lodge app store database had been compromised, exposing the names, email and home addresses, and passwords of parents who had used or authorized use of the app store. This information makes it possible to link children to their parents, gaining access to their identities and personal information as well. The hacker responsible claimed they did not intend to do anything with the information.
Monetary cost of breach: Unknown.

32. Facebook
Year of breach: 2013
Number of records affected: 6 million
While using the social media site's 'download your information' tool, users were able to inadvertently download phone numbers and email address of users they were friends with or had some connection to—information that was otherwise intended to remain private.
Monetary cost of breach: Unknown.

33. SnapChat
Year of breach: 2013
Number of records affected: 4.7 million
Hackers discovered an exploit in the smartphone photo and chat app that allowed them to access the user details, including phone numbers, of 4.7 million users.
Monetary cost of breach: Unknown.

34. Ubuntu
Year of breach: 2013
Number of records affected: 2 million
Hackers gained access to email addresses and password data of Ubuntu forum users due to a weak password algorithm encryption.
Monetary cost of breach: Unknown.

35. Staples
Year of breach: 2014
Number of records affected: 1.16 million
A breach that affected more than 100 stores belonging to the office-supply retailer may have had 1.16-million customer payment cards hacked. The incident was traced back to a malware infection of the chain's point-of-sale systems.
Monetary cost of breach: Unknown.

36. Global Payments
Year of breach: 2012
Number of records affected: 1.5 million
The payments processing firm compromised credit and debit card information from major credit card brands Visa and MasterCard when they detected unauthorized access to their servers.
Monetary cost of breach: $84.4 million.

37. Gawker Media
Year of breach: 2010
Number of records affected: 1.3 million
Hacker group exploited weak password storage and compromised email addresses and passwords of commenters on blogs such as Lifehacker, Jezebel, and Gizmodo. The source code for Gawker's custom content management system was also stolen.
Monetary cost of breach: Unknown.

38. CareFirst BlueCross BlueShield
Year of breach: 2015
Number of records affected: 1.1 million
Names, birth dates, email addresses, and subscriber information were stolen by hackers. Member password encryption prevented the perpetrators from gaining access to any other personally identifying information, such as social security numbers, medical claims, or financial data.
Monetary cost of breach: Unknown.

39. Utah Department of Technology Services
Year of breach: 2012
Number of records affected: 780,000
A European hacker exploited a weak password and broke into the Utah Department of Technology Services where the social security numbers for Medicaid claims were stored.
Monetary cost of breach: Potentially upwards of $406 million.

40. New York Taxis
Year of breach: 2014
Number of records affected: 52,000
Data on 173 million individual taxi journeys was released with a freedom of information request, unintentionally revealing Driver IDs, pickup and drop off times, and GPS routes. Poor anonymization was to blame for the info leak.
Monetary cost of breach: Unknown.

Preparation to secure a business and customers
Many companies simply don't utilize the proper measures to maintain the confidentiality of business and client information. Paired with a poor response time, targeted businesses seldom succeed in alleviating the concerns of victims who are most often their customers.

Securing your data, having loss-prevention plans in place, and practicing safer network security practices—such as consulting IT security firms—can turn a devastating data breach into a manageable problem with minimal casualties. If the above 40 data breaches demonstrate anything, it's that the cost of handling cyber-attacks can be incalculable.

From millions of dollars spent on litigation and IT fees, to a steep drop in revenue and resigning CEOs, a data breach has no definitive cost or solution. Only preparedness can mitigate the damage potential of an attack. Without a proactive strategy at your disposal, your company could become the next target for cyber criminals looking to make their payday.

In addition, ensuring that your business information is protected can mean updating visitor management and access with higher standards. In today's environment, a simple visitor or access log isn't enough to prevent the wrong people from getting sensitive information; Acuant solutions provide the opportunity to efficiently register and manage visitors, verify identification, and allow secure access by authorized individuals. Learn more about Acuant's security solutions here.

End of Acuant article.

Full Legal Notice & Disclaimer:

The author is not an attorney and does not give legal advice. If you have questions of a legal nature, contact a licensed attorney who specializes in the area of law in which you have questions.

Limit of Liability and Disclaimer of Warranty: Magnus Omnicorps, LLC has used its best efforts in preparing this publication and the information provided herein is provided "as is." Magnus Omnicorps, LLC shall in no event be liable for any direct, personal, commercial or otherwise, indirect, special, incidental, consequential or other losses or damages arising out of any use of this publication or the performance or implementation of the contents thereof. Magnus Omnicorps, LLC, makes no representation or warranties, expressed or implied, including, but not limited to, accuracy or completeness of the contents of this publication and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose, non-infringement, or title, that the contents of the publication are suitable for any purpose, nor that the implementation of such contents will not infringe any third party patents, copyrights, trademarks, or other rights.

Please note that parts of this publication are based on personal experience and anecdotal evidence. Although Magnus Omnicorps, LLC has made every reasonable attempt to achieve complete accuracy of the content in this publication, it assumes no responsibility for errors or omissions. Also, you should use this information as you see fit, at your own discretion and at your own risk. Your particular situation may not be exactly suited to the examples illustrated here; in fact, it's likely that they won't be the same, and you should adjust your use of the information and recommendations accordingly.

Any trademarks, service marks, product names or named features are assumed to be the property of their respective owners, and are used only for reference. There is no implied endorsement if we use one of these terms.

Trademarks: This publication may identify product names and services known to be trademarks, registered trademarks, or service marks of their respective holders. They may be used throughout this publication in an editorial fashion only. In addition, terms suspected of being trademarks, registered trademarks, or service marks have been appropriately capitalized, although Magnus Omnicorps, LLC cannot attest to the accuracy of this information. Use of a term in this publication should not be regarded as affecting the validity of any trademark, registered trademark, or service mark. Magnus Omnicorps, LLC is not associated with any product or vendor mentioned in this book nor does it necessarily endorse its product(s) or service(s).

Finally, use your head. Nothing in this publication is intended to replace good sense, legal, medical or other professional advice, and is meant to inform and entertain the reader.

The name and trademarks of copyright holders, author and publisher may NOT be used in advertising or publicity pertaining to this document or its contents without specific, written prior permission. Title to copyright in this publication will at all times remain with copyright holders.

SHARING:

Unless this report was offered free-of-charge from my website, the following applies:

Much work that went into putting together this publication. I can't tell you how many hours were spent compiling it. That means that this information has value and your friends, neighbors, and co-workers may want to share it.

The information in this publication is copyrighted. I would ask that you do not share this information with others-you purchased this publication and you have a right to use it on your system. Another person who has not purchased this publication does not have that right. It is the sales of this valuable information that makes the continued operation of Magnus Omnicorps, LLC possible. If enough people disregard that simple economic fact, these types of publications will no longer be viable or available.

If your friends think this information is valuable enough to ask you for it, they should think it is valuable enough to purchase on their own copies. After all, the price is low enough that just about anyone should be able to afford it.

In all cases, it should go without saying that you cannot post this publication or the information it contains on any electronic bulletin board, website, FTP site, newsgroup, etc. You get the idea. The only place from which this publication should be available is Magnus Omnicorps, LLC's website. If you want an original copy, visit Magnus Omnicorps, LLC at the following address: http://www.magnusomnicorps.com/