

Staying Safe in an Unsafe World

By Robert Thetford
ICJE, Inc.
P.O. Box 293
Montgomery, AL 36111
training@icje.org

Unless you were born after 2015, it is unlikely that you have experienced the level of crime we see in the United States today. We tend to forget unpleasant occurrences, so most of us have no recollection of just how bad crime was in the 1970s. As bad as it was then, it looks like things are getting worse today with the apparent breakdown of our culture and the inability of governments and institutions to deal with the aftermath.

This e-book is designed to provide the reader with a quick summary of the most likely danger areas encountered today and suggestions about what actions will most likely prevent injury, loss of life, or loss of property. The scenarios and suggestions come from a variety of sources, and while they are not guaranteed to be successful in every instance, they are certainly better than doing nothing and should provide a measure of safety if applied correctly.

Table of Contents

1. Overview: The Triple-A Plan.....	P 2
2. Avoidance and Counter-Surveillance.....	P 4
3. Hardening the Target.....	P 6
4. Lights, Cameras, Alarms, and Locks.....	P 9
5. Safer Home Interiors, Travel, and Vehicle Safety.....	P 12
6. Protection from Internet Fraud and Cyberattacks.....	P 17

Overview: The Triple-A Plan

Most Americans understand that violent crime has drastically increased over the last decade, and the increase does not seem to be slowing down this year. The increase in attacks against churches and other worship centers is not as well known. For the past few years, ICJE has offered free seminars to law enforcement and worship center personnel about protecting their organizations from targeted criminal activity.

At the worship center seminars, we were often asked about protecting individuals rather than institutions. In response, we developed an introductory workshop to exchange ideas about how people can better protect themselves, their families, and their property using common sense ideas and practices.

Because the reach of a workshop is necessarily limited, we hope to provide a series of articles to our *ICJE News* subscribers, distilling the major ideas to a few pages and presenting them each month in the newsletter. This e-book is a compilation of those articles.

Of course, there are no guarantees in life, and what we advocate may not be appropriate in your situation, so all of these suggestions must be tailored to your particular circumstances. The basis for our suggestions revolves around what we call the **Triple-A Plan: Awareness, Avoidance, and Action.**

Awareness (Situational)

Awareness is the foundation upon which avoidance and action are built. Situational awareness is simply understanding what is happening around you as it relates to you.

An illustration of this assumption is found in a corollary to the Pareto principle or 80/20 rule, which holds that at any given time, 10% of the people make things happen, 10% of the people understand what is happening, and 80% of the people stand around and say, “what’s happening?”

While this is given somewhat tongue-in-cheek, it does illustrate the fact that most of us are not really aware of the people or things that may adversely affect our safety at any given time. Like most behavioral traits, situational awareness can be learned and applied to provide a higher measure of protection to anyone making an effort to use it.

One of the best books about situational awareness and a book that has been around for some time is ***The Gift of Fear*** by Gavin De Becker. This book is inexpensive, widely available, and well worth reading to give you a sense of what situational awareness is and how it can be applied in your life.

The author stresses that because your safety is ultimately your responsibility, you can't rely on the police, a security agency, or others for your physical protection. His main point is that the solution to personal violence is intuition, that intuition can be learned and sharpened, and that those who follow their intuition are much less likely to become victims.

Law enforcement officers frequently refer to this condition as noticing that something Just Doesn't Look Right (JDLR). You may not be able to articulate what it is, but by training yourself to be more aware of your surroundings, you will instinctively know that something is out of place or that the situation simply feels wrong. Examples are an individual expressing noticeable anger, staring at you, following you, wearing inappropriate clothing, making unexpected noises, or other actions that seem out of place. Of course, to sense these actions, you have to be looking for them. That is the essence of situational awareness.

A great illustration of this is found in the short video accessed through our Screencast link:

<https://www.screencast.com/t/MTuNZRel2Rc>

As you view this video, notice that the customers wearing masks remain standing in line as one unmasked customer becomes increasingly distraught. Not one walked out of the store or intervened. For civilians, the most appropriate response to this or any potentially dangerous confrontation would be to leave and call 911 immediately. The failure to quickly leave the area by the other customers shows a demonstrated lack of situational awareness that could have resulted in injury or death.

Summary: Read *The Gift of Fear* and begin to apply your intuition to the world around you. Using all of your senses, train yourself to look for JDLR events and circumstances. When appropriate, act on your instinct to protect yourself and others.

Avoidance and Counter-Surveillance

As I was beginning to write this series, I went to my local barbershop for a haircut. I was talking with another customer, a retired deputy, when a person who looked unkempt and homeless entered the barbershop, slammed the door, and began muttering to himself. I instinctively looked for a weapon bulge on the individual but didn't see one, so I wasn't too concerned, thinking that this was just another soul who "had issues."

When our barber took the next customer, the unkempt individual became irate, claiming that he was next and cursing all those present. He then stormed out of the shop. I watched him leave and walk across the parking lot. The retired deputy moved so that he could see the person if he returned.

After the incident, and as we were talking, the barber said he wasn't worried because he knew we would protect him. Both of us laughed at that, saying that our concern was whether we could get out the back entrance fast enough if the guy returned.

Lessons Learned:

As we understand the necessity for practicing situational awareness in our daily lives, we also need to avoid the trap of Cognitive Dissonance; that is, believing something but acting in opposition to our beliefs. Examples are not taking threats seriously, understanding that there is a threat but thinking that it wouldn't happen to us (not in our backyard), or thinking that because an incident hasn't happened, it simply won't happen.

A typical example is found in the short video of a shooting event. This video may be viewed in our Screencast streaming account, link below. Watch closely the man in the light blue sportscoat and tan pants:

<https://www.screencast.com/t/Uj3VRfHlOB>

When you hear gunshots and your instincts tell you that there is imminent danger, you should know to remove yourself from the danger; however, this person obviously follows his curiosity rather than his better instincts.

Avoidance Tactics:

1. When in public places, walk with your head up, and never walk while looking at a cell phone.
2. Always stay alert in public. Most public attacks could have been avoided if the victims simply were aware of their surroundings.

3. Always remain in well-traveled public areas. At night, stick to well-lighted areas. Just like the lions shown on the nature videos, most predators pick those on the outside of the herd. You want to remain in the middle of the pack where there is greater safety.
4. When walking in public, pause and occasionally turn, noting the persons around you. Often, predators will stop or turn away when observed.
5. If someone is following you, consider confronting them. This is contrary to our normal instincts, and not everyone can use this tactic, but it can be very effective in startling a would-be attacker and thereby preventing an attack.
6. Change your behavior: Don't walk or run the same route, and don't drive the same route, especially to and from work or school.
7. When driving, check the vehicles following you. If they follow you through more turns than normal, consider driving toward the nearest police precinct.
8. In a restaurant or business, always sit where you can observe the entrance and those who are entering. Also, observe and choose alternate exits.

Summary: Often are aware of danger signals but suppress the signals through curiosity, inertia, or disbelief. Act on your instincts. Also, review the eight avoidance tactics outlined above and incorporate them into your daily life experience.

Hardening the Target

Security experts tell us that crooks hit targets of opportunity much more frequently than preplanned crimes. Another way to put it is that they concentrate on soft targets rather than hard targets. Unless they are under the influence of drugs or alcohol, most crooks are not mentally challenged: they will most likely pick the easy rather than the problematic victim and the easy rather than the challenging target. So how do we harden your home against intrusion and make it a challenging target?

First, let's look at some statistics. From 2003 to 2007, there were 3.7 million burglaries per year in the U.S. Twenty-eight percent of these were home invasions (burglaries where a household member was home). The most likely victim was a single female with children.¹ Obviously, a burglary is bad enough, but a home invasion often involves injury and even death, so the key here is to keep the bad folks out. How do you do this?

An old radio commercial advertising the Barbizon School of Modeling said, "You too can be a model... or just look like one." The idea here is to make your home into a castle or just make it look like a castle. Either way, most common burglars looking for an easy score will likely leave you alone. The first thing a homeowner should do is simply walk around the outside of the home and look for ways a burglar can get in. Are your doors and windows always locked? Are shrubs and other obstacles trimmed so that your house is visible from the street? Burglars normally prefer dark, secluded areas with limited street visibility, so you may need to do a little yard work.



In a "Staying Safe" seminar, I suggested that having a visible dog food bowl on your front porch may dissuade a person from breaking in. I didn't really think it was a great idea, just a suggestion, but the seminar participants really liked the idea, so it may work for you as well.

¹ <https://www.bjs.gov/content/pub/ascii/vdhub.txt>

If your home has a burglar alarm-protected sign out front and the identical home next door has no sign, most burglars will hit the home with no sign. Of course, it is better to have a burglar alarm and video cameras protecting your home, but if you can't afford those, just having signs may provide some protection. Signs are cheap and may be bought at Amazon and other online retailers.

Here is an example of an alarm sign with window stickers from Amazon:



Although most alarms are supplied with yard signs and window stickers, the security experts frequently advise using a different company's signs. This is because the majority of alarms sold today are wireless and if a person knows the manufacturer of the alarm, it might be possible for that person to override the alarm frequency, thereby defeating the alarm.

Other Outdoor Signs

Besides alarm and video signs, people often place signs in their yards to deter unwanted guests, like "Trespassers will be Shot" and "Protected by Smith & Wesson." It's probably not a good idea to have these signs as it advertises that you have guns and possibly other expensive items that a burglar may want.

I used to think that having an American flag outside your home was a deterrent to an attack, but lately, that doesn't seem to be the case, with a growing percentage of U.S. residents expressing disdain for the flag.

The same thing can be said about vehicles as well. Having a sticker, plate, or sign on your car showing you are a Christian, a gun carrier, or a political supporter may result in an unpleasant encounter in today's environment. Low profile definitely is the best approach to avoid being a victim.

What about driveway alarms? They are usually passive infrared-based (sensing both heat and movement) and will provide an alert up to a half-mile away. The drawback is cost, with the better alarms costing \$100 or more, depending on the number of detectors you add.

The one I use is a Dakota Alert DCMA-4000, purchased at Amazon. One advantage is that it is set to alert by movement from both vehicles and people, so it alerts when the mail or packages are delivered.



Finally, if you plan to be out of town, make sure your garbage can is rolled in, your newspapers are picked up, your mail is halted, and your lawn is cut. These are “red flag” items that telegraph an easy score to the bad guys.

Summary: Protecting your home begins with reviewing the outside from a burglar’s perspective. Next, you should add an alarm and video sign whether or not you have an alarm system. Consider a passive infrared alarm to notify you of approaching vehicles and people, and finally, make sure there are no “red flag” items left outside.

Lights, Cameras, Alarms, and Locks

Lights

If the bad guys enter your yard, particularly if they do so at night, many will be deterred by lights alone. Motion detected lights are best as they often provide a “shock effect” of having the area suddenly illuminated when heat and movement are sensed. These lights come in two flavors: hard-wired and solar-powered.

The advantage of hard-wired lights is their brightness. They are much brighter, on average, than solar-powered and cheaper (\$25 and up at Home Depot), but the trade-off is that you will need a competent electrician to install one.

On the other hand, solar-powered lights are dimmer, have a higher cost (about \$40 at Costco), and need the sun to recharge the batteries but can be installed by any reasonably handy person having access to a ladder. The batteries last about a year and can be replaced with easily obtained rechargeable batteries, usually A.A. size. To give you some idea of the brightness the solar lights produce, see the photo below.



Cameras

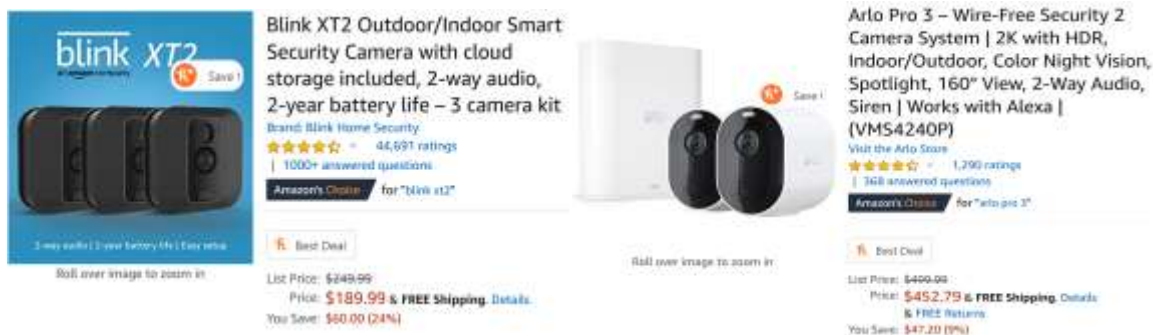
In addition to lights, outdoor cameras are a great asset to a home security package. Like the lights, cameras come in two basic flavors: wired and wireless.

Wired camera systems are generally better quality but are more expensive and have high installation costs if you aren't technically handy or your home doesn't have adequate space to run the wiring. The major advantage is that the cameras can be continuously monitored as they are always active and recording. Most have an Internet connection which allows for cellphone monitoring as well. Wired systems cost between \$700 - \$1,200, not including installation. Below is a typical wired package from Revo America:



On the other hand, wireless systems are relatively cheap when compared with wired systems and are somewhat simple to install but are usually battery (or battery/solar) charged, so they don't offer the continuous monitoring option. Most wireless cameras activate and record for a short time when sensing heat and movement. Unlike wired systems that record to an on-premises hard drive, most wireless systems save the recording to an online source, requiring a monthly fee.

The most popular wireless systems include the modestly priced Blink system and the more expensive but higher resolution Arlo system:



In addition to standard camera systems, homeowners are increasingly adding doorbell cameras to their home security systems. The most popular of these is the Ring camera (below); however, if you add a burglar alarm, you might consider installing a doorbell camera that integrates with your alarm system. The doorbell cameras are either battery operated (easy to install, but batteries must be changed periodically) or hard-wired into existing doorbell wiring (more difficult but no batteries to change). Either system links to your Internet router to view the doorbell area or receive doorbell alerts via a smartphone.



Alarms

Residential Burglar alarms have improved dramatically over the last decade, moving from older wired systems that were difficult to install, very expensive, and subject to false alarms. Today, most alarms employ wireless installation, are relatively inexpensive, and are much more reliable due to advances in alarm technology. Perhaps the most popular system designed to be installed by the homeowner is that produced by Simplisafe. This alarm is easy to install as it relies on wireless technology, meaning that the detectors are pressed into place with double-stick tape so the entire system can be set up in about an hour. Although not totally necessary, securing the detectors with the included screws is advisable.

The base price for a Simplisafe system is around \$250 and up, depending on the number and type of detectors; however, the company offers frequent online sales and discounts, so it pays to sign up on their website (www.simplisafe.com).

The system may be monitored for \$27/month, which includes a smartphone app. With fewer options (no app), the monitoring runs \$15/month. Of course, without any monitoring, the system still functions as an alarm but does not call the owner or police if a detector is triggered.

One nice feature of the Simplisafe system is a built-in cellphone for the monitoring alert. Because burglars often disable any visible telephone line and Internet cable, a monitoring system that relies on the Internet or telephone would also be disabled. Having an internal cellphone with battery backup means that your monitored alarm signal will be sent even if the Internet (and power) are out.

Locks

High-quality deadbolt locks on all exterior doors are absolutely essential for your home's protection. Please understand that most deadbolt locks will slow an illegal entry but won't necessarily prevent entry. Also, as a general rule, the more expensive locks (like Medeco or Schlage) will offer more protection than cheaper locks.

An inexpensive addition to exterior locks which will provide an extra layer of protection is the Door Guardian. This device is easy to install and should slow or prevent forced entry for any exterior door.



Finally, every home should have the ability to view persons seeking entry without first opening the door. Even if you have a camera system, a peephole provides a quick way of observing anyone at your door. Peepholes are inexpensive and easy to install, so every home should have one in solid exterior doors.



Summary: Lights, cameras, locks, alarm systems, and peepholes work together to offer a level of protection that is affordable to most people today. The technology improves yearly, and the costs are no longer prohibitive. Many of these may be installed by the homeowner, making them even cheaper to employ.

Safer Home Interiors, Travel, and Vehicle Safety

Home Interiors – Safe Rooms



In the last section, we discussed making your home safer with exterior locks, burglar alarms, and outside lights. As a practical matter, all of these are meant to alert the homeowner to a potential threat and to slow entry if there is an attempt at a hostile intrusion, but for the average home, none of these protective measures will guarantee that all attempted entries will be unsuccessful. So what can you do if someone is determined to gain entry to your home illegally?

There are a couple of things that should be happening at the outset. Assuming you have an operating alarm system, don't wait for the system detectors to alert the alarm company. If possible, you should have panic buttons that can be activated whether your alarm system is on or off. Panic buttons are inexpensive and can be located throughout your home, on your keychain, or on a smartphone if you have one. Another excellent location for a panic button is in your safe room.

At this point, you may be thinking that you don't have thousands of dollars to invest in a steel or concrete safe room with all of the trappings that are usually associated with them, and that is understandable, but it doesn't mean that you are excused from having a safe room. In fact, having one is vital in protecting you and your family. So, where do you start?

Take a look at the accessible rooms in your home. A safe room is not necessarily designed to keep out an army of invaders, but it is a room designed to at least temporarily keep those bad guys who have gained entry into your home from reaching you and your family until law enforcement arrives.

Safe rooms for normal people are simply interior rooms with solid wood or metal doors (not hollow-core doors) that have substantial locks (preferably deadbolts) on the inside. These are “last-ditch retreat” rooms that your family would use to gather in case of an intrusion into your home. Most designated safe rooms are either closets or bathrooms.

Consideration should be given to installing a panic button if your home has an alarm system, and having a mobile phone with you is a huge plus for protection and communicating with law enforcement.

Once your safe room is designated and equipped, your family should be given a code word that will alert them (and you) to immediately enter the room with the appointed items, such as mobile phones, keys, pepper spray, or other defensive weapons. Most newer cars with key fobs have an included panic button, and it’s a good idea to have this accessible so that the horn alarm in your vehicle car can be activated.

Travel Safety

Have you ever looked at something that seems familiar, but you couldn’t quite remember where you saw it or just couldn’t place it? That happened to me not long ago when reading about the increase in carjackings throughout the U.S.



Carjacking incidents (forceable taking of cars from an owner or legal driver) have exponentially increased in the last few years with a 500% increase in Minneapolis and Washington D.C., while Chicago reported over 1,400 carjackings last year. Although Alabama apparently doesn’t publish detailed statewide carjacking statistics, a quick online search reveals numerous incidents in our state in the last few years.

Carjackings have increased primarily because of the rising value of used cars, but the increase may also be due in part to the appearance of more youthful offenders. It is not unusual to see carjacking offenders today who legally aren’t old enough to drive the cars they are stealing.

So why the feeling of déjà vu? One tip I learned years ago was never to stop your law enforcement vehicle so close to the car in front of you that you would be unable to drive around the car if the situation called for it.



The same principle holds true for anyone stopping behind any vehicle, whether at a stop sign or stoplight. In order to elude a carjacker, you can't be so close to the car in front that you are unable to pull around it quickly and escape. So the tip here, whether you are driving a law enforcement or private vehicle, is to stop far enough behind the car that you can see the rear wheels of the vehicle in front of you. That way, you will always have enough room to move either to the left or right if you need to do so.

It goes without saying that your doors should always be locked and your windows closed as well. Finally, check your surroundings before entering or leaving your car or anytime you stop in traffic.

Hotel Safety

Long ago, I was advised by a fellow employee never to stay in an apartment or hotel room above the sixth floor. The reason given was that fire trucks with ladders can reach the sixth floor but no higher. I have taken that advice seriously since then. Additionally, I learned that most hotel room break-ins occur on the first through the third floor, as the lower floors provide a quick exit for burglars. This translates to staying on the fourth, fifth, or sixth floors if at all possible.

Other hotel security tips include never attempting to enter your room when strangers are nearby, always using a doorstop or doorstop alarm for extra protection, and reviewing the locations of the exit locations on your floor.

If you leave your vehicle in a hotel parking lot, make sure the doors are locked, all personal items are removed from view, and, if possible, leave your car in a high-traffic area.

Hopefully, these tips will help keep you safe from some of the threats in today's world.

Summary: Every home should have a designated Safe Room, and families need to practice entry with mobile phones, keys, and any other desired protective items. Travel safety includes situational awareness, keeping doors locked, and being prepared to quickly exit a dangerous encounter. Hotel safety should include room location, use of doorstops, and awareness of your surroundings when entering or exiting rooms.

Protection from Internet Fraud and Cyberattacks

Internet Fraud and Other Fraud Schemes

As if things weren't bad enough with everyday cyber-criminals, now we know that the same cyberattacks that the Russians are using against Ukraine can just as easily be switched to the U.S. with much greater effect. Our increased vulnerability is due to our dependency on the Internet for everything from the electrical grid to financial, water, and transportation systems, not to mention our personal computer systems.

The suggestions provided below apply to any online attack, and while there are no guarantees that your system will be safe, you will be protected to a much greater extent than those who have little or no safeguards in place.

To give you some idea about the magnitude of fraud schemes today, the FBI's Internet Crime Complaint Center (IC3) provided a report in 2020 showing the following reported complaints in the U.S. where Elders were listed as victims:²



But it is not just elders who are victims of online fraud, as it affects all age groups:

² https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3ElderFraudReport.pdf

2020 VICTIMS BY AGE GROUP

Victims		
Age Range ²	Total Count	Total Loss
Under 20	23,186	\$70,980,763
20 - 29	70,791	\$197,402,240
30 - 39	88,364	\$492,176,845
40 - 49	91,568	\$717,161,726
50 - 59	85,967	\$847,948,101
Over 60	105,301	\$966,062,236

The Federal Trade Commission report for 2021 showed that social media is a current cesspool of fraud attempts. In fact, more than one in four people who lost money to fraud in 2021 said it started on social media with an online ad or a message (email or text). The FTC data indicated that online scamming was more profitable than almost any other fraud scheme, with losses totaling about \$770 million in 2021.³

Email phishing (involving email scammers) is today's most popular online fraud scheme, more than doubling from 2019 to 2020. Some of the most prevalent fraud schemes involve these topics:

- ☐ Romance scam
- ☐ Tech support scam
- ☐ Grandparent scam
- ☐ Government impersonation scam
- ☐ Sweepstakes/charity/lottery scam
- ☐ Home repair scam
- ☐ T.V./radio scam
- ☐ Family/caregiver scam

³ <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021>

So what do you look for to indicate that the solicitation or contact is fraudulent? Here are the FBI's top Red Flags:

- The scammer requests payment via gift cards, wire transfers, or virtual currency.
- The scammer creates a sense of urgency or deadline to pay quickly.
- The scammer demands secrecy from you.
- The contact contains poor grammar or misspellings.
- Payments are offered in amounts higher than a listed or normal price.
- Email addresses are disguised to seem legitimate.
- Unsolicited emails, texts, etc., requesting you confirm usernames and/or passwords.
- Requests to move to a new platform to communicate.
- Requests to access your personal bank or other financial accounts to pay you for a service.
- Unsolicited emails with links or attachments.

Vital Defensive Measures

Because we can't always recognize the contact as fraudulent, a few defensive measures can assist in keeping our identity and information private and safe.

1. Use a Virtual Private Network (VPN). A VPN will hide your identity and location, making it much more difficult for scammers to obtain your personal information, particularly in open access areas like hotels, airports, and restaurants. Without a VPN, it's as if you are inviting the bad guys into your home. Avoid the free VPNs as they don't normally offer the same protection as the paid services provide. Recommended VPNs are Express VPN, Private Internet Access, and Hideaway VPN.
2. Use a Password Manager. The password manager securely stores your passwords, so you don't have to remember them. Password managers provide very strong passwords for all of your secure online sites and should be used by anyone linking to any financial or commercial site. A couple of the most popular are Dashlane and Roboform. These are easy to use and highly recommended.

3. Use Two-Factor Identification (2FA) whenever possible. 2FA adds an extra layer of security to your accounts by adding an additional step between putting in your password and accessing your account. This additional step is added to the log-in process and usually consists of a code sent to your phone or email or a fingerprint scan before accessing your account. It's like providing your PIN number before being allowed to access your ATM account. You may have the card, but without entering the PIN, no cash can be disbursed.
4. Also, make sure you have an anti-virus (A.V.) program. There are many free A.V. programs, but like the old saying, "There's no such thing as a free lunch," many of these programs collect and sell your personal information. For this reason, paid programs like Norton, Webroot, or Bitdefender are generally considered much better. Some programs, like Norton, offer security suites that include VPN and password managers in addition to the A.V. feature.
5. Back up your files frequently through an external hard drive or an online service. Backing up your system offers protection from both equipment failure and ransomware attacks.
6. Finally, for those of you who are paranoid (and you should be), consider using an identity theft service like LifeLock or Identity Guard. They are not cheap, but with the increasing number of cyber-attacks, these programs have moved from the luxury class to the necessary class. The last time I checked, Identity Guard was a little cheaper than LifeLock for the same level of service.
7. Another highly recommended program to protect against email Spam or Phishing attacks is Mailwasher (www.mailwasher.net). Mailwasher is a program that reviews all of your incoming email messages and flags those that it recognizes as spam or malware. You can also review the message and sender, and if they look suspicious, you can mark them as spam, and they will be automatically deleted before they reach your email inbox. Mailwasher has a free version. If you find the program useful, keep the free version, or for more options, use the paid version.

Below is a sample of Mailwasher incoming emails. Note the red email headers (flagged as spam) vs. the green headers (friends). If you get a lot of emails, particularly spam emails, this is a great program to have.


Classify	Dr Status	From	Subject	Received
Friend		Amazon Accounts Payable (noreply@amazon.com)	KDP Royalty Payment Notification - ICJE, INC.(EPHRY) - 166...	6/20/2021, 10:...
Back...		Luis Castillo (luis@chattanooga-webdesigns.com)	What I found on icje.org	6/20/2021, 11:...
Back...		Luis Castillo (luis@chattanooga-webdesigns.com)	What I found on icje.org	6/20/2021, 11:...
Back...		Mr Edward Anodu (test@edaco.co.jp)	[SPAM] COMPENSATION ALERT	Today 12:59 AM
Friend		Amazon Marketplace (marketplace-messages@amazon.com)	Robert T. Thetford, will you rate your transaction at Amazon...	Today 1:05 AM
Spam		Mr Julian Amin (ja62667811@gmail.com)	MY MAIL!!!	Today 3:17 AM
Back...		Stefano (corporate@mirabach.com)		Today 3:18 AM
Spam		Richard Corey (felpo@tintaviva.com)	[SPAM] Greetings to you	Today 3:23 AM
Friend		Amazon.com (delivers@amazon.com)	iRobot Roomba Robotic Vacuums and Braava M6 Mops	Today 3:34 AM
Spam		masteroffice card (mastercard11@outlook.com)	CONGRATULATIONS TO YOU	Today 3:46 AM
Friend		Gastone Institute (list@gastoneinstitute.org)	The US-Backed Palestinian Human Rights Violations	Today 4:16 AM
Friend		dilbert@email.dilbert.com	Dilbert.com - Daily Strip Email	Today 4:34 AM
Back...		Benorte en su Empresa (carolinamarotomes@prodigy.net.mx)	[SPAM] Your Bitcoin Details.>	Today 5:24 AM
Good		Military.com (do_not_reply@e1.email.military.com)	Daily Brief: She Was a Pioneering Navy Submarine Officer...	Today 5:31 AM
Back...		Mrs. Mariam Ali (laurenaldjenaczowski23811@outlook.com)	[SPAM] Mrs. Mariam Ali a s'rieusement aimé cette idée et...	Today 5:39 AM
Friend		xgboys-request@xgboys.com	Xgboys Digest, Vol 2341, Issue 1	Today 6:01 AM
Good		TrainingMagNetwork.com (ccemails@trainingmagnetwork.com)	3 Keys to a Successful Women's Leadership Program	Today 6:03 AM
Spam		"Ox & David Dry Fire Training Cards" (support@surviveinplace.com)	This Fires AR-15 "Overpenetration" For Home Defense	Today 6:02 AM
Spam		Administrator_icje.org (jaless1@stuttsfordmalawi.com)	rthetford@icje.org You Have Pending Unread Message.	Today 6:06 AM

Sample Threat Emails

Below are some sample threat emails that are obvious (and not so obvious) attempts to have the recipient respond or click a link. Either response may ultimately lead to accessing your system, including your financial records. My comments are in the flag box.

From: Andrew Bailey
Sent: Wednesday, April 28, 2021 4:44 AM
To: rthetford@icje.org
Subject: [Norton AntiSpam][SPAM] INHERITANCE CLAIMS!!!! 58.215.166.242

Follow Up Flag: Follow up
Flag Status: Flagged

 Beware of anyone offering to give you something for free.

Hello,

Hope you are having a good day and the Covid-19 is not hitting hard on your side. I would like to know if you got my previous email with regards to the inheritance claims I informed you about earlier. Please let me know your interest. I will send further details if you wish to proceed.

Best regards,
Andrew Bailey

From: Lee Young <powerball@saocarlos.sp.gov.br>
Sent: Tuesday, April 27, 2021 4:09 AM
To: undisclosed-recipients:
Subject: [Norton AntiSpam][SPAM] Ref #: EAAL/851QYH1/15




Follow Up Flag: Follow up
Flag Status: Flagged

Dear Beneficiary,

Your email was selected in Powerball Online Lottery Promo 2021 Draw with the sum of \$350,000.00 USD.

Kindly the complete details for your claims.

Name:
Address:
Mobile Number:
Home/Alternative Phone Number:
Age:
Occupation:
Nationality:
Country of Residence:

 Beware of any email sent from a foreign country.

Yours Sincerely,
Lee Young
Notification Officer (Sec. Zonal Co-coordinator)


[SPAM] Fw: Invoice - Payment receipt



Account Depth <hsbc@paymentdepth.pro>
To: rthetford@icje.org

 Reply  Reply All  Forward ...


Tue 4/20/2021 2:30 PM

 Follow up: Start by Tuesday, April 20, 2021. Due by Tuesday, April 20, 2021.



rthetford,

PAID
Tuesday, April 20, 2021 9:30 p.m.

 Beware of opening any email attachment from an unknown source.

rthetford@icje.org

The Obvious: Join the Illuminati



Tatiana Postnova - Tele2 <tatiana.postnova@tele2.ru>

To: Undisclosed recipients:

From Russia

Reply

Reply All

Forward

Fri 4/30/2021 9:1

Greetings, from The Illuminati world elite empire. Bringing the poor, the needy and the talented to limelight of fame, riches, powers and security, get recognized in your business, political race, rise to the top in whatever you do, be protected spiritually and physically! All these you will achieve in a twinkle of an eye when you get initiated to the great Illuminati empire. Once you are initiated to the Illuminati empire you will get numerous benefit, knowledge with new ideas.

Note: that this email message was created solely for the purpose of our recruitment scheme which will end next month and this offer is for unique ones only, if you are not serious on joining the Illuminati empire, then you are advise not to contact us at all. This is because **disloyalty is highly not tolerated here in our organization.**

Do you agree to be a member of the Illuminati new world order? If YES!. Then kindly reply us back on our direct recruitment email only at: illuminatiinvitation@outlook.com

Please note, Kindly make sure all your response are send directly to the email stated above only at: illuminatiinvitation@outlook.com

For more instructions on our membership process.

Note: Some email providers incorrectly place official Illuminati messages in their spam / junk folder or promotion folder. This can divert and exclude our responses to your emails.

The Illuminati.



Beware any OBVIOUS or SUSPECTED
THREAT.

If you see a link embedded in your email, always place your cursor over the link, and the origin will pop up. If the source is not the same as your sender, this is probably spam or malware. Notice in the email below that the sender alleges to be from Spectrum, but the link is actually to a site in Brazil.

From: Charter.Spectrum <emurphy2@99charter.net>
Sent: Wednesday, April 28, 2021 8:31 PM
To: [redacted]@charter.net
Subject: [Norton AntiSpam]Action Required !

<http://blog.bazarhorizonte.com.br>

Two Clues when Cursor
Placed over Link:

1. No https in name
2. Not the same name as sender

Update Payment Information

Dear Spectrum Customer,

It has come to our attention that your payment Information records are out of date. That requires you to verify the Payment Information. Failure to verify your records will result in account suspension. you'll need to Update your payment Information using the link below Then follow prompts .

[Update payment information](#)

Thank you,
Charter Communications

←Hover cursor over link to
reveal link address.

Finally, it's not a bad idea to check and see if your email or accounts appear on the "dark web," meaning websites that traffic in stolen email, financial and other private information. Here is the link to the "Have I Been Pwned" website, a legitimate free service that keeps track of stolen identity information and allows you to see if your identity is available to others.

Pwned is gamer talk for "owned," so if you have been pwned, someone "owns" you.

(<https://haveibeenpwned.com>)



Hopefully, these tips will help keep you safe from some of the online threats in today's world.

Summary: There are no guarantees that your computer system will be protected against cyberattacks, but there are specific steps you can take to avoid or mitigate attacks. These steps include using a Virtual Private Network, a Password Manager, Two Factor ID, and an Anti-Virus program. Don't forget to back up your files frequently and closely examine emails before opening them.

This concludes our Staying Safe e-book. I hope you gained some tips to keep you and your family safe during these increasingly troubling times. Please let us know if you have any questions or tips that we can pass on to others.

For comments or suggestions, please get in touch with us at training@icje.org.

Thanks, and stay vigilant.

Bob Thetford

ICJE, Inc.