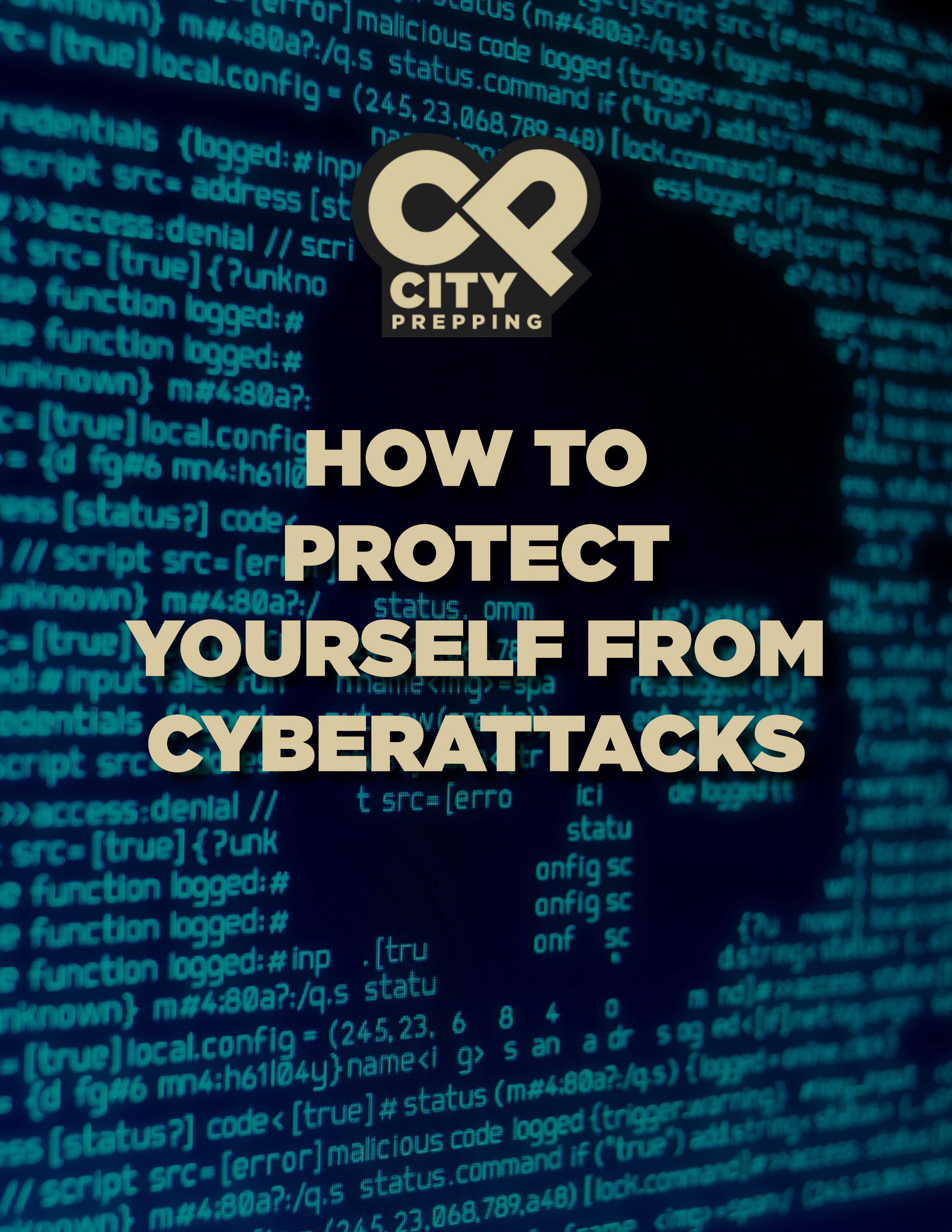


CITY PREPPING

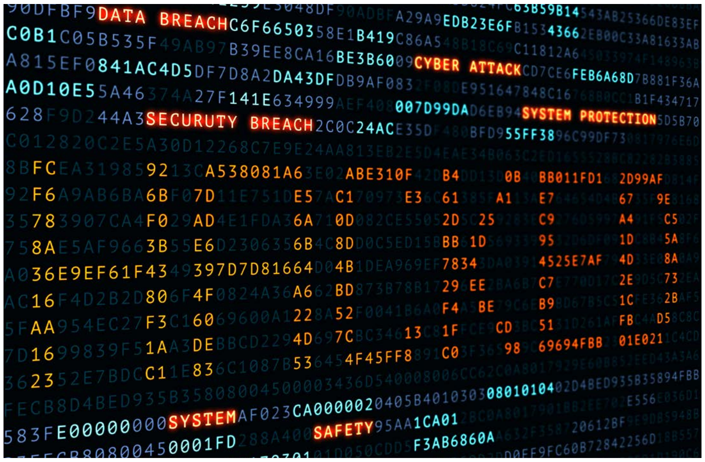
HOW TO PROTECT YOURSELF FROM CYBERATTACKS

INTRODUCTION

Hi, my name is Kris (aka City Prepping) and I have been involved with emergency preparedness for several decades now. Between achieving Eagle Scout in my youth, doing humanitarian work in impoverished areas of Mexico and in 3rd world nations such as Afghanistan, and receiving C.E.R.T. training, I've come to learn the foundations of preparedness that I'll outline in this document.

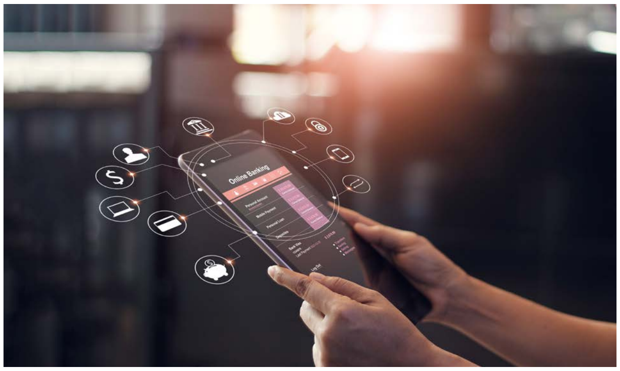
Over the last several years I've developed over 700,000 subscribers on my YouTube channel and during that time, I've both gained a new level of appreciation for being prepared during these times of uncertainty and have learned from the community's insight.

I've created this quick guide to get you started on preparing for cyberattacks. We know that the new wars being waged are far from battle zones. Cyberattacks on financial institutions, municipal utility services, ransomware, and just hacks meant to disrupt scheduled processes can plunge you into darkness, shutdown services you rely upon, or bring the supply chain to a grinding halt. As much as technology makes so many facets of our lives so much easier, it also makes us vulnerable to suffering from the damaging effects of cyberattacks. This document will examine a few of the glaring vulnerabilities and how those could escalate into a major crisis very rapidly. While working on this document, I received several emails asking how folks could protect themselves from the cyberattacks that are clearly going to come out of the current Russo-Ukrainian conflict. That is why I wanted to make this document available to you. As much as it serves as a guide for you, let it also be a conversation starter to help others get prepared.



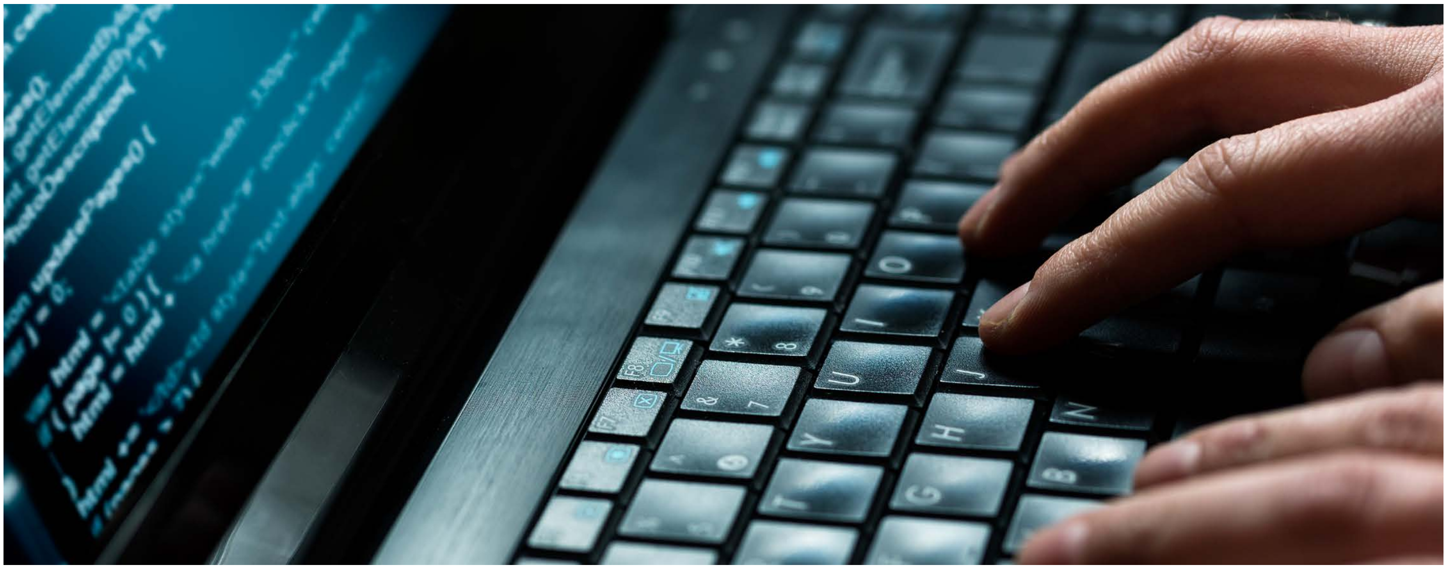
UNDERSTAND THE REAL THREAT

If you only ever have a few dollars in your checking account, it's not likely anyone will specifically target you. Your account may be swept up en masse with other accounts like a school of fish trapped in the cyberattacker's net. Your ability to access your account pages on the internet or conduct any transactions on the internet may be halted. You cannot just dismiss this with a "Well, I don't interact on the internet, so no big deal." It is a big deal. You might not access your accounts online, but your banks and stores often access the same systems over the same networks. Have you ever been in a store and had to wait on your transaction because systems were down? It's like that. Even if you are only paying in cash, that point of sale is tied to a more extensive network. We don't live in a time where things can just be written down in a ledger and transacted in cash. When was the last time you had a clerk who could count back change appropriately without seeing the calculated total of your change on their computer terminal?



Beyond the point of sale and temporarily losing access to your accounts, though, you will more likely feel the effects of bigger network targets trickling down to you. In a world of consolidation to maximize profits, there are a total of four big beef companies in the United States. There are nine cardboard manufacturing companies based in the United States, and much of that cardboard is manufactured in Mexico or at overseas plants. There are fourteen major U.S.-based polystyrene companies that are capable of making those trays the meat is placed on at your store. Not all of them do. All along the way, the consolidation and lack of competition is a vulnerability that cyberattackers can exploit. If a major meat processing or packaging plant is knocked offline like what happened to JBS earlier this year, it doesn't matter what the herd looks like; it won't be making it to your store. If one or more major cardboard manufacturing plants or polystyrene companies get knocked offline, it won't matter how much meat is processed; it won't be delivered to your store or to you as the consumer. And that's just one of the systems with just 3 points of vulnerability. There's also the feed supply system feeding this system, the retail store's point of sale selling the final product, and many USDA guidelines and restrictions, also regulated via computer systems and inspectors, that are in place to deliver meat to you in precise and regulated ways to make it certifiably safe for you to consume. It's a house of cards with multiple vulnerabilities.

The real threat to you is the larger targets that impact your life directly and indirectly. We have seen in recent years water treatment plants knocked offline because the computer systems they were operating were made in the late 80s. That's over 40 years of missed updates and OS releases meant to harden systems against attack. Trains, planes, automobiles, traffic systems, tracking systems, transaction systems, logistics and shipping systems, utilities, medical records, and databases at major corporations that provide you anything and everything from physical products to services are all vulnerable. We would be mistaken to think that they have invested heavily in securing their systems against outside attacks. In reality, recent hacks and ransomware attacks have soberly proven otherwise. Anyone system can stop a multitude of other systems, and the house of cards could quickly come crashing down around you, bring down your grid, your networks you rely upon, or plunge the world into chaos and dark ages. It's not a pretty picture when you spell it all out, but there are still things you can do.



#1 HACKING STARTS WITH YOU

While you cannot get your region's electrical provider to upgrade their systems, you can still do your part to protect yourself from those that would exploit you and to recover your assets after systems are restored. You have to start by securing your corner of the system, and here is a quick list of ways you can do that.

First, let me say that I have worked in the IT industry for years, even as the owner of my own successful company web development agency. Some of the people who have worked for me started programming, web design, and web security back when building webpages could only be done in Microsoft notepad. If you don't know what I mean by that, just know that there's a long history and understanding of network security and the internet here. These more prominent hacks you hear about on the news, the millions of other breaches you don't hear about, and the hacks already made, laying dormant and ready to be initiated, all started with a single user or a single port accessed. The CIA's exploit of the Iranian nuclear processing system resulted from one user plugging his infected thumbdrive into one of the centrifuges networked computers. Often the larger financial institution exploits come from one user on a secure system clicking a link they weren't supposed to or unknowingly providing access to their username and password. Malicious actors gain higher-level permissions on a system or network by piggybacking off that one unknowing user. From emails allegedly sent from your company's CEO with exploitive links and files to stolen federal laptops that lack good user security to disgruntled employees selling information and databases, larger exploits come from individual users. Don't be that guy, and also harden yourself off from being exploited with these basic steps:

UPDATE YOUR SYSTEMS AND APPS

If you are like me, you hate updating your systems. It's a big time suck, and it can sometimes change the way you navigate or the look and feel of your operating system. Every time I update my system or an application, it's always with a deep breath and with my fingers crossed. Still, updates often result from the providing company realizing an actual or potential vulnerability. They are trying to get ahead of it with the fix. That being said, one of the largest hacks in recent history, the SolarWinds hack, was through an update on systems. That hack impacted numerous companies, even the Departmental Offices division of Treasury, home to the department's highest-ranking officials. If your update notification comes through your computer or on your phone, wait a few days before allowing the installation and switch off automatic updates on your systems until the threat of cyberattacks lessens a bit. That pop-up on your computer warning you about the critical updates you need to make may be bogus. Most software companies don't communicate like that with their consumers, and most provide you the option not to update. If it's an exploitive update, you will probably hear about it on the news within a few days. The best way to update your systems is to go to the sites that provide you the software and actively seek out their "Check for Updates" pages. Do update your systems in this way if you are running old operating systems or frequently use the same Apps. One recent study found that the latest version of Microsoft Windows had a total of 907 vulnerabilities. One hundred thirty-two of those vulnerabilities were classified as critical. You can bet that the company is shutting them down as they find them, but you leave your door unlocked if you don't update your system regularly.

PASSWORD1234

Update every one of your passwords right now, especially if you use the same password wherever you can. If your password is already compromised from a previous hack, it won't be usable anymore in that earlier version when the hackers flip the switches on their exploit. Second, stop using the same passwords. Many critical systems have two-layer authentication, PINs, biometric, password vaults, or authenticator Apps like Google Authenticator. It's a hassle, for sure, but you need to take advantage of these protections. Not using them is like buying locks for your house but never installing them. When you make a password, take advantage of all the numbers and special characters available to you. Make it complex and avoid any familiarities.

Many years ago, I had a simple password that used my pet's name and some other memorable numbers and words. I mainly used it for simple apps for health and diet, but sometimes for other sites too. These simple apps often lack security and protection and get hacked. That password associated with my email and additional public record information might be enough to access more significant accounts. Use as complex of a password as you can. If you have to write it down, write it down in two places, one secure at home and one for your wallet if it's something you need to access when away from home. It's much safer in the back of your desk drawer at home or in your wallet than it is in an electronic file or floating around the internet. If you have it in an electronic file on your computer or a thumbdrive, make that file password protected too.

Run something like Google Account Password Checkup. This will inform you as to which passwords may have been compromised. A password checker will also tell you where you are re-using passwords and where your passwords are weak. You may find some old accounts that you don't use anymore. Shut them down and delete your profile. At the very least, make sure they don't share email addresses and passwords with your critical accounts. Finally, get in the habit of changing your way-too-complex-too remember password on a regular schedule, like every 3 to 6 months. It's a hassle, and I stagger mine, so I am not doing them all at once and sometimes still neglect them, but as I will point out in my next point, sometimes your password is already known, and the bad guys are just waiting to pull the trigger on your account. I also recommend a paid tool like lastpass.com or 1password.com. I have used these services over the years to secure passwords and they have tools to alert you if there's been a compromise.

UPDATE ACCOUNT PROFILES

Have you moved or changed cellphone numbers or email accounts? If you have, you want to update all your account profiles online. Even if you haven't, you will still want to do this. About two years ago, I was doing this at my primary banking site, and I noticed the email address they had was some weird address I had never heard of or used. I thought, "That's weird." So, I changed it to what it should be and made a mental note to circle back and recheck it in a few days. A few days later, I went back into the account, to my profile page, and it was changed back to that weird address. I called the bank, and we discussed it. I told them I didn't know that address, and I had corrected it and changed it back to what it should have been. Long story short, after a lengthy call with my bank and them reaching out to their IT folks, they had to shut my account down entirely and open a new account for me. That was likely an exploit in their system, unmonitored but awaiting activation. It was changing my email to that other email, even overwriting my corrections, so when their system implemented a password update, the email would go to that weird address, and voila--they were in my account. I hope my bank was able to audit their systems for other customers that may have been affected, but the whole event underscores the need for you to conduct your own audit of all of your profile pages and settings at every major site that you use. This keeps you one step ahead of any hackers who may have already acquired your information but don't know how to use it or any who are lying in wait for official orders like a sleeper cell.

STOP CLICKING WEIRD THINGS ON THE INTERNET

No African princes, Iraq warlords, or recently deceased super-wealthy family members want to circumvent the banking system to get you your new inheritance. You probably aren't a guaranteed winner, and no company in their right mind is going to give the first 1,000 people who forward an email anything. Those are obvious do not clicks. There's also a good chance your CEO doesn't have an urgent message or a file attachment she urgently needs your feedback on before the end of the day. If you still have pop-ups enabled on your computer, get rid of those as soon as possible. As a rule, don't click messages that pop up, open files you aren't absolutely sure are from people you know or even go to sites with known exploits in them. If it's too good to be true or requires your immediate attention, it is likely some type of fraud or phishing attempt. Make sure your SPAM filter is on for your emails. If a significant institution asks something of you, know that they don't usually do it that way because that's a known means of exploiting people. They will call if it is crucial. Their website will inform you if it is urgent. If I suspect the email at all, I will open a new browser, go to the site, and verify that they need me to make a change. Watch your emails for misspelled words or incorrect sentence structures, as many of these hackers don't have a stellar grasp of your native tongue. Hover your mouse over links or right-click the link to view the address and make sure it comes from the actual domain of the institution. Don't forward things on, and never respond or click in any way any email that has more than you as the recipient. Official emails from institutions will never go out with many people CC'd on them. Also, is it the correct email address associated with that account? I don't even have an account at SAM's Club, but I get emails saying my account needs to be updated. I also get emails about my Amazon account at an email address I don't use for that account. If you have a shred of doubt about the email or webpage you are on, just don't click anything there or submit any information or click on any pop-up or alert—x out of it.

ANTIVIRUS SOFTWARE & SECURITY COMPANIES

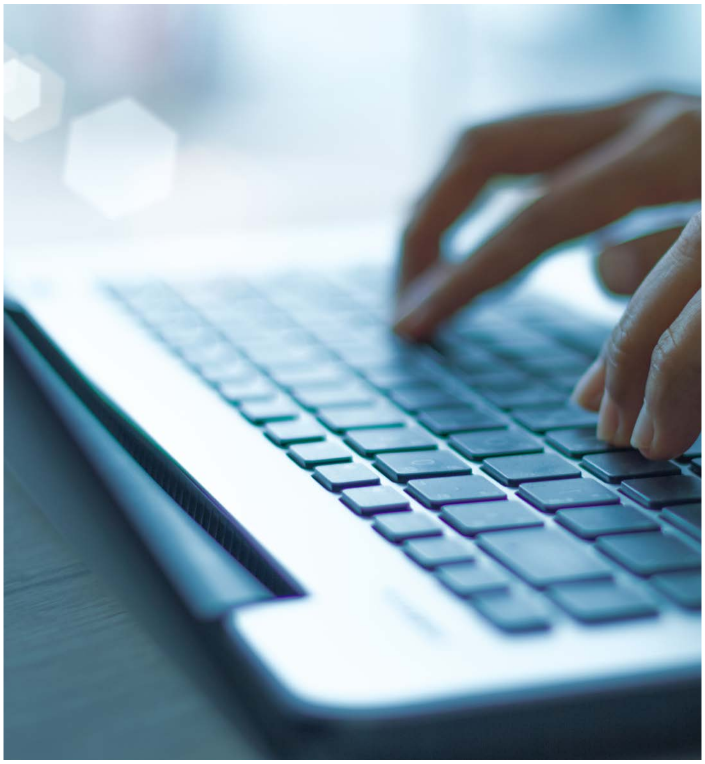
Consider antivirus software or a company like LifeLock. I think of this as installing lights around your house. Bad guys looking for an easy score are less likely to see my house as a target because the light lets me see them first, and they know that. A far easier target is the person who bites on the phishing email sent because they didn't have virus software that alerted them that the email was suspect. Antivirus software and companies like LifeLock, which force specific rules on your accounts before information can be changed, are like throwing roadblocks between you and the attacker. Eventually, the attacker will move to more accessible or higher-profile targets. Plus, these companies have the sole purpose of rooting out bad guys and nefarious hackers and figuring out how to protect you from them. It's like hiring your own security guard. At the very least, use your operating systems software protection. Avoid installing more than one antivirus software on your system, though, as this will significantly degrade your capabilities as they compete to scan the same files. Finally, if you haven't run a scan of your system in a while, now is the time to do so. Protecting your firewall and concealing your vital information is something you should get in the habit of doing monthly. Then, if your data is compromised somewhere else, your updates will hopefully prevent further exploits.

ANTI VIRUS
MAINTENANCE
ACCOUNT
SETTING
QUICK SCAN
SCANNING...
C:\RawPixel\Pixel.NET\Framework\v6.03.072\webenginw.dll
2855 files
14 minutes, 22 seconds left...
STOP
PAUSE
RESUME
please wait...
your computer is scanning
UPDATE

CHANGE THE WAY YOU BROWSE

If you get pop-ups or loads of advertisements, understand that your computer is probably loaded with cookies, and they aren't the kind you eat. They're little snippets of data collected about you. They are often text files with small pieces of data like your username and password. They identify you and sometimes the network you are on when you are on the internet. Marketers use info like this to feed certain advertisements to areas where searches are highest. For instance, if you and your neighbors are all searching for how to grow a patio garden, don't be surprised if the Yahoos and Googles of the world start feeding you gardening ads. Why do I mention this here in a conversation about hackers? It's because hackers can use data files like these to play into your interests and feed you specific things. That's essential to know in the next point I will tell you about regarding misinformation, but here you should probably just change the way you surf or browse the internet.

Consider the newer Brave browser or maximize your existing browser's Private or Incognito modes and clear its history and cache. Brave Browser is built to help make your browsing secure, free of ads, and free of cookies and scripts. Plus, it's the only browser I know of that has the advertisers paying you directly if you're into cryptocurrencies. They provide you Basic Attention Tokens in exchange for your attention to specific marketing. It's not a lot, but it's better than nothing, and it's a good deal when you consider that you aren't just leaving your data and info out there like you do with other, less-secure browsers. If you are unwilling to switch to a different browser, make sure your current browser has Java disabled, an ad-blocker, uninstall extensions you don't use, and maybe install something like Noscript– an add-on that disables things like JavaScript from running on websites you visit. Javascript and other scripts are antiquated but often are used to carry malicious commands for your system. Think of changing your browser or the way you browse as your nighttime check that the outside lights are on and the windows and doors are locked. You don't expect anyone to crawl through the window while you're sleeping, but you lock it just to be sure.



INFORMATION & MISINFORMATION

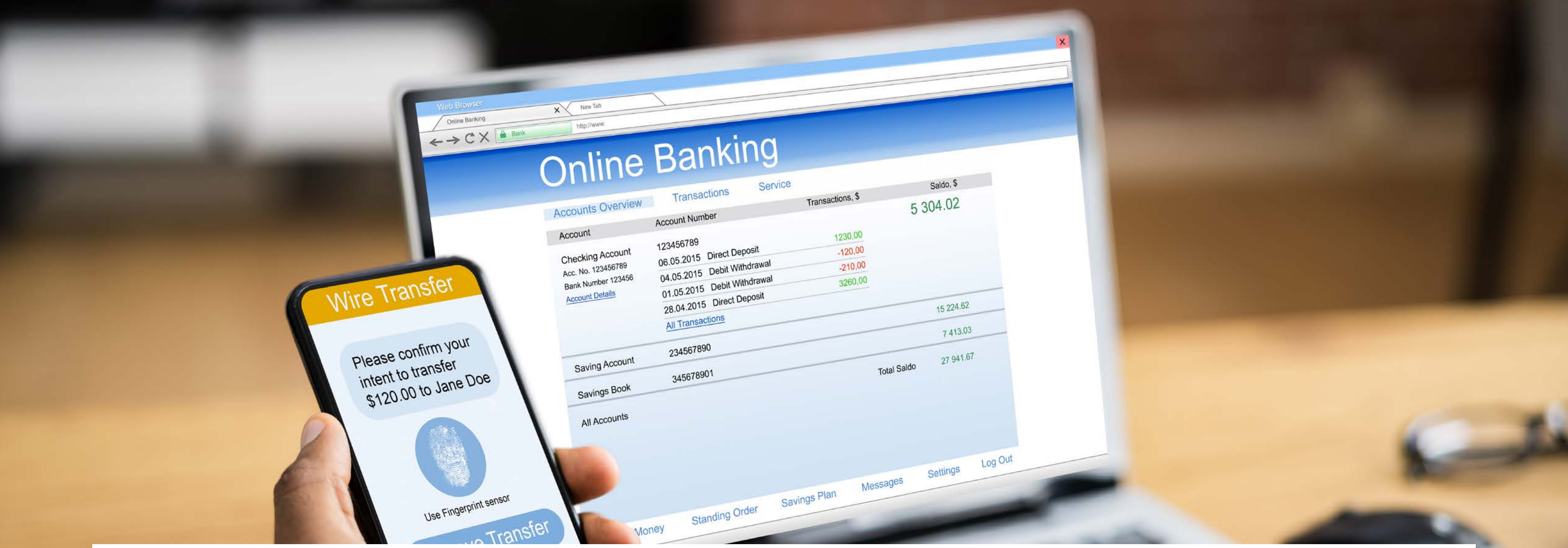
One of the most potent and most effective weapons cyber attackers use is the misinformation campaign. Troll farms are intentional groups meant to buddy up to some, provoke arguments with others, and sow division. Even information you might think is real is often faked. I mean, we want to know what is going on in Ukraine, for example, but many of the live feeds aren't live. Some of the videos coming out on TikTok or other short media services are sometimes faked or made to look like they are really happening right now when it's old footage that has been adjusted. It's enough for many to give up on all of it once they realize they have been duped. Don't give up on it all, though. Just don't accept it all as truth at your first glance. There are groups out there intentionally trying to befriend you, outrage you, rile you up, and encourage your donation or support for their cause. Some are real, and some are fake. All of them would love whatever personal data about yourself they can get. A name, picture, phone number, email address, and the like can all be fed into the same dark web.

When there is enough info about you, someone with an even more nefarious plan can leverage it to their advantage. Marketers have long known that just using a person's name in a marketing piece dramatically increases the response rate. If you would like to test this theory of information and misinformation, build an alias profile online with an email you don't often use. Watch how that email starts filling up after a while with emails specifically using that alternate name. Treat the information you put out there and the information you believe is accurate with conservative skepticism. Withhold judgment on information coming in, and be cautious about releasing even your dog's name to anyone online. By the way, if one of your passwords is also your pet's name, you really need this information now.

GET CONTROL OF YOUR SUBSCRIPTIONS & TRANSACTIONS

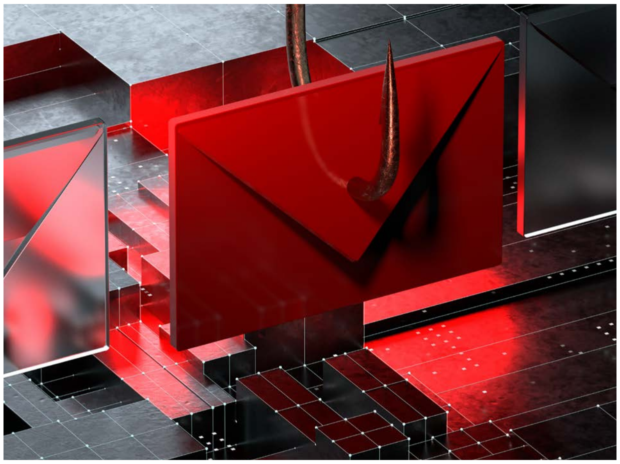
Your major bank might not get exploited, but that little database at your gym might get stolen. One of the most overlooked and undetected scams out there still hasn't made it to the mainstream media, and you might not even notice when it happens to you. It's happened to me twice. Say you have a magazine subscription or a streaming media subscription. You get charged once in January when you set it up for the year's service. Then, sometime in March, you get another charge, or maybe you get another charge next year, even though you aren't on auto-subscription. After all, you may have thought you were signing up for two years, but maybe you just did for one year. The service provider says they didn't make the charge, and perhaps they didn't. You see it on your statement, but it is slightly differently titled than the first charge. Unfortunately, it has become an all too common practice for low-paid and often disgruntled online and sales workers to sell your information to skilled hackers. A similar-looking account can be set up and all those charges sent out through your credit card. The criminals don't need to get them all to go through. Suppose the amount is 19 dollars or 99 dollars. In that case, they only need a few thousand of the hundred thousand or more to go through before a savvy enough customer recognizes the faulty charge, navigates the legitimate company's phone tree and online customer service, contests the charge on their bill, and, well, you see it's a lot of work to explain how this scam goes. That's if you even see the charge and recognize it. Even when that big company discovers the fraud took place, they don't want to say anything because that would result in people not trusting their services.

Know your subscriptions and get rid of any subscriptions you don't use. This lowers your profile and reduces your electronic footsteps. Review your bank statement at least every payday. Understand each and every charge. If you are at all suspicious, call your bank directly at the number you look up on your own and get further information or contest the charge. If you end up accidentally canceling a payment you committed to but forgot, don't worry, I am sure that the company will circle back with you and remind you. Every subscription is info about you that you have put out there. Every transaction you need to verify is legitimate.



SWITCH TO ONLINE BANKING AND CASH

It may seem counterintuitive to protect yourself from cyberattacks by switching to online banking, but you protect yourself a bit from fraud when you do. This is a 360-degree approach to your fiscal survival that also means you should have your assets spread out to survive significant calamities and minor infractions. I'll give you an example here. I was working late one night when my wife was out of town, and I got an alert on my cellphone asking if I had just made a transaction at the Microsoft Store. Well, my son does play games online, but he shouldn't have access to the ability to pay for anything, and he better be asleep at 11:39 PM. My wife was out of town and sometimes expenses pop-up in weird places, but I just texted her to confirm it wasn't her. What I think happened since I watch my card so closely, again watch every transaction, is that when we were coming back from his practice, we stopped at a fast-food restaurant's drive-through. We were talking, so it barely registered when the worker took my card and set it on the counter next to the register. I figured he would run it in a minute, and I was talking to my son. I think, though, maybe he had his phone propped up and filmed the front and the CVV number on the back. That's all he would have needed.



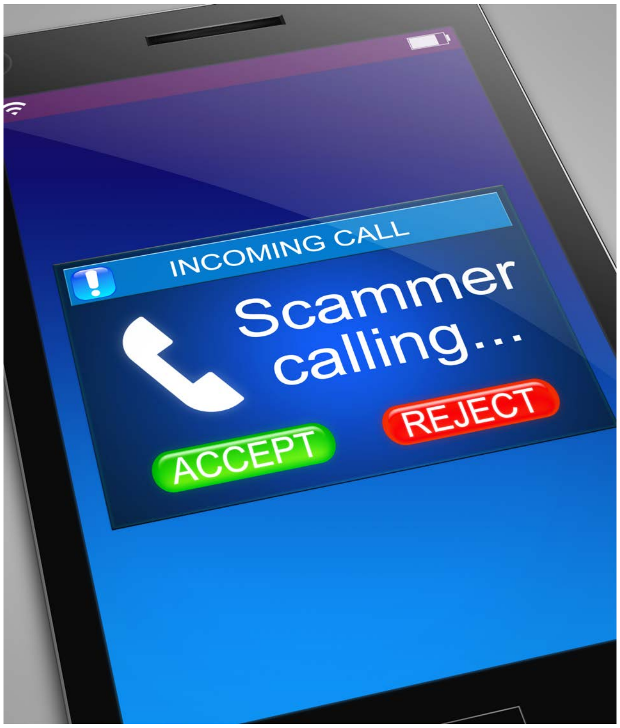
I guess it could have happened anywhere, and it does millions of times per day. I can't prove anything, but the first thing I did was not reply to the alert I got on my phone. That's a known phishing hack too. I logged into my bank from my computer and saw almost 700 dollars of transactions in the last two hours. The bad guys were on a spending spree from the Apple store to Tacos in Las Vegas to groceries in West Covina and a few places I couldn't discern. Though I could easily eat $56 of tacos in Vegas, I was at home. Within minutes of calling the bank, though, the card was knocked out of service, a new card was on its way to me in the mail, and once the transactions cleared or failed, I could file online the fraud claim and was reimbursed 100% of all the lost money.

So, within 2 hours, my account was drained $700, and it took a week to get it back, but there are two takeaways here. First, I was protected because so many of my transactions are electronic, and I bank online with my electronic devices and safeguards in place. If they could take $700 in under two hours, they could have drained my entire account by morning. If I didn't bank online, I might not have known until my balance hit zero or my own transactions failed. Second, the bank reimbursed my losses within a week. They see it all the time. They know the score, so they act fast and hope to minimize their losses while retaining me as a customer. If you still send paper checks, realize you are sending account details, addresses, names, and routing numbers through the mail, handled by many hands and potentially stolen right out of your or someone else's mailbox. At the same time, most banks offer online bill pay that connects right up to the provider's account. Companies that don't have an account can often be issued and mailed a check right from your bank. Shift the liability over to the institution in charge of keeping your money safe. Limit the exposure of your information in the world by focusing it in with your online banking. Let them handle the security.

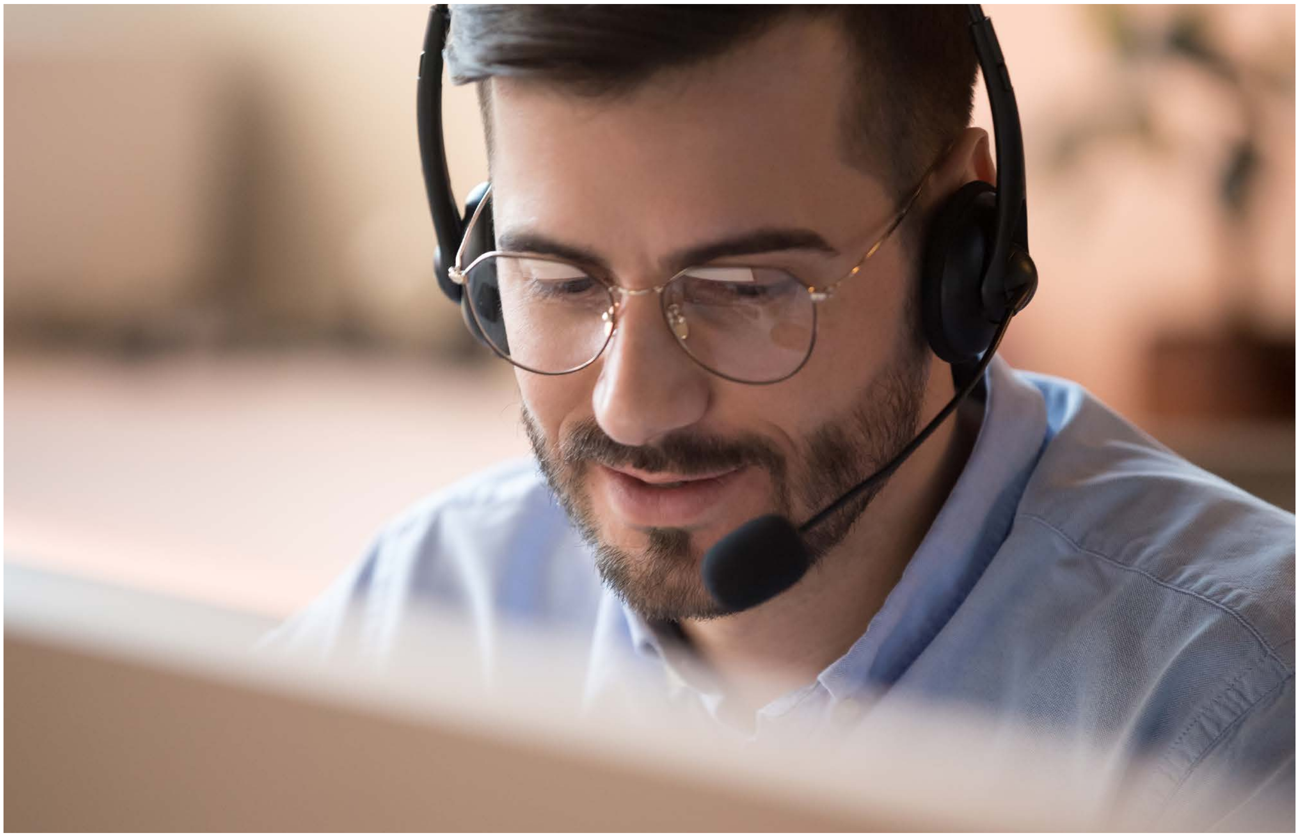
This is not to say that you shouldn't have cash on hand. When it all goes down, and systems fail, you will be glad to have $300-$600 in low denomination bills. When your check or credit isn't accepted, your greenbacks may still hold perceived value.

DON'T CONFIRM YOUR IDENTITY

There's a low-end telephone scam where they ask for you by name. Is this "so and so?" Your instinct is to say yes but don't. Don't ever say yes on the phone. Don't press one, two, or any number to get off the list. If it's a scammer, you could be affirming the charge they are about to make, or they can use the recording to prove you consented to the charge. It's the same with pressing a number, even if the recording says the number is to unsubscribe from their calling list. You may be consenting to a charge by pressing that number. Again, these little scams may seem small in the big picture of cyberattacks, but one $2.00 scam that works on a half-million of the 330 million people in America, raises a million dollars for the enemy. That's a lot of roubles. Even if it isn't some state-sponsored activity and it's just a small-time scam, it gets your information in a database that will move its way through the dark web to more sophisticated operations.



Implement a free or pay call filter if one is available through your phone service provider. You can't always stay free of the hackers with your information. I recently refinanced my house. There are court filings and legal information that are public records. I cannot tell you the number of unsolicited calls I got where the person knew my name and home address. I was getting five or more per day and couldn't get them to remove my number from their circulating lists until I implemented a call filter. I would ask them if I requested the call. I would tell them I am on the do not call list. I would ask them nicely not to call me again. Nothing worked but the call filter. Like a spam blocker, it looks for weird activities like robocalling or number spoofing and rolls the call to voice mail. I haven't had another call trying to sell me solar or an energy audit since I activated a free call filter. I also haven't missed a call I wanted.



The chances are that you can't call into the social security administration, DMV, or the IRS and get a live person, so it is doubtful they are calling you directly now. They aren't going to email you either. I once had a toll fine go for over a year. It turned into a hefty fine, but nobody told me about it until I tried to register my car in person because the systems wouldn't let me do it online and gave me no explanation as to why. No letter was ever sent to me, and no email was ever sent to me. Nobody called me. Just because someone knows your name, address, or phone number doesn't make them legitimate. Giving them information or confirming your information just makes you a higher profile target for more sophisticated rings of hackers and scammers.

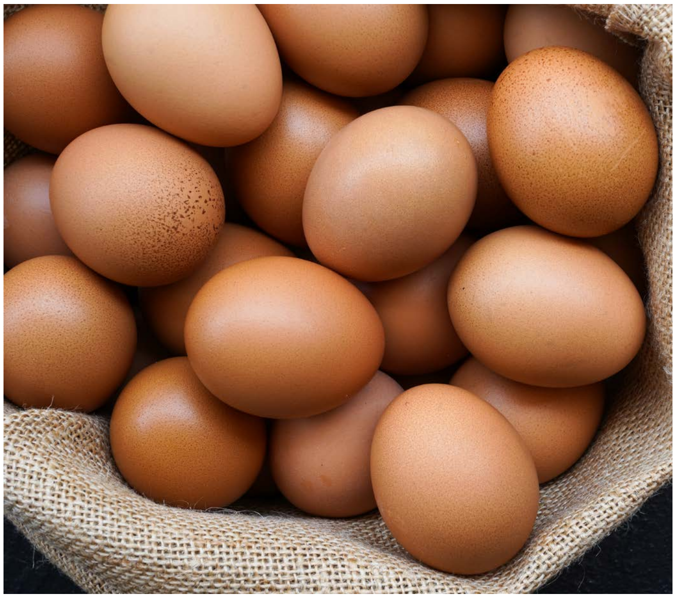
Realize this, though, I know a good deal about cybersecurity, and I keep an ever-constant eye on my assets and transactions. Still, I have told you how I have been hacked in small ways. Imagine how many less knowledgeable people are getting hacked and never realizing it or ever unraveling it. Two dollars here and nineteen dollars there done thousands of times supports terrorists, autocracies, and kleptocracies worldwide. Nobody would be doing it if there weren't profit in your information and feeding you misinformation.

#2 FINANCES

Let's assume for a moment that a more extensive cyberattack has occurred against the financial institutions or the Treasury, or the banking systems as a whole. When it comes to getting your money back, at what point in the line are you compared to the millionaire across town? The bank is probably still going to want whatever payment you owe them monthly, but they aren't exactly getting all Dick Tracy about your measly savings account. In a more significant economic collapse, your currency could become worthless. However, I think debt collectors would still call you even knowing that the currency and economy have tanked.

Even after a significant cyberattack that brings a partial grid-down, finances are still critical. Assuming systems will eventually be restored, you will need records of what you had where. From bank accounts to credit card statements to loan papers, you will need to prove what was yours and what was owed and what was owned. My Survival Binder that comes with my Prepper's Roadmap course has some of this information in it, but for the specific instance of making it through and restoring your life after a significant cyberattack on fiscal systems, have these things in place. First, have recent pay stubs and banking statements to show the regular patterns of your income and expenses, and balances. Also, have printouts of the first page and balance statements of major accounts updated with some regularity. It will be nice to prove you lost everything in your IRA or 401k if you ever have to do that.

If the attack leads to a grid-down, partial grid-down situation, or even just significant supply chain disruptions, you will want to have between $300 and $600 or more in denominations of $20 and under. Even if the dollar is worthless tomorrow, it will retain some value for those who hold on to the hope of a recovery. Even if it doesn't get that bad, cash is still king, as they say. That store is likely to do that small transaction for you in cash even if the point-of-sale system isn't working. You are instantly trustable to them with $40 in hand, whereas that piece of plastic that doesn't work doesn't lend you any credibility in their eyes.



Build your bartering skills and network. Sure, now you can buy a dozen eggs at the grocery store for a few dollars, but what will you do when the egg ranches go offline? Do you think those farmers who are barely making a living wage from their corporate bosses are going to jump through extra hoops to get eggs they don't actually own to you? You would be much better off if you knew someone with a few chickens and you made something, hunted and processed game, or had some skill or knowledge you could trade for a dozen or more eggs. You would be even better off if you had chickens of your own and thereby had a commodity to barter with in fresh eggs. Understand the value of things and skills when the ordinary means of measuring value, your currency, is worthless.

I am not a financial consultant, and I don't give financial advice, but I will tell you this final point on your finances, and that's to lock up any abundance. If you have thousands in savings, it is losing money for you every day, whatever the paltry interest rate you are getting on it. Inflation and deflation will make it worth less in the future than it is right now. Far better would you be to have it tucked away in a retirement account, savings bonds, or use it to refinance your house, pay off debt, or pay off your car. This converts your money now into future money, provides you resources now and in the future, and takes it off the table when cyber hackers rob your institution where you keep it. You could keep it under your mattress or in a wall or buried in a mason jar on your property as your great grandparents did. Heck, the ancient Romans used to bury it outside the castle, city, or estate walls just because invaders and robbers would look within the walls. The problem with this strategy, though, is it's just sitting there losing value until some successive generation stumbles upon it.

No talk of protecting yourself from cyberattacks would be complete without addressing what you need to truly survive these events: water, food, and energy.

#3 WATER

On a planet that's blue from space because of the amount of water, it's important to realize that only .3 percent of it is drinkable. Of that amount, much of that will still make you sick from viral, toxic, or bacterial contaminants. Humans do a great job all on their own polluting that small amount. I cannot stress the need for water more, especially with the type of disaster that comes with cyberattacks. These large-scale operations are on infrastructure targets because they cause the populous the most chaos, pain, immediacy, and anxiety. Still, most people are entirely reliant upon their municipal water sources. When it rains, that rain is swept away from their property, and not a drop is retained.

These big companies that control the flow of water to your tap have made it illegal in some states even to put a rain barrel under your gutter to collect water for your lawn or garden. These are also the same companies that have spent so little on hardening off their systems that they are running Windows 98 to mix the proper chemicals to treat your drinking water. These are the same big companies that don't upgrade their systems, and we hear about their huge profits and high levels of lead or other toxins in the drinking water. The water system is incredibly vulnerable as it is and more so because so many are utterly reliant upon it.

Take steps now to store 3-months of drinking water for each person and pet in your home. Beyond that, have the means to filter and treat the water you collect from the wild. Many will die of dysentery in their very private lakeside communities in a grid-down situation. Others will be so desperate for a drink of water that they will steal it from anywhere they can get it. Don't depend on getting the water you need to survive from the government relief truck that may or may not come into your neighborhood with drinkable water for the masses. It might not come. It might not have enough for you after the thousands of desperate people clamor to get theirs. Survive a largescale cyberattack by having the water you need to survive stored in your home. Cans and bottles of water from the store to replace your flowing tap will be the first thing depleted and looted from those stores.

This is a small thing. When we look at it now, it's a small task, but it will rise to a matter of life and death the moment the grid goes down in even a partial way.

#4 FOOD

Just like water, you need food to survive a large-scale cyberattack that could render the supply chain from farm to table useless. Corporate farmers might have bigger hearts than the corporations they answer to, but they don't own that grain or that harvest. Here is another example of what I mean. In the recent shutdowns from the pandemic, millions of people were no longer eating out. The demand for potatoes for everything from fries to chips plummeted. Did those farmers process those potatoes into dehydrated mash potatoes? They didn't have the means to do so. Even the companies that do that didn't have the means to process that overabundance. Did they give the potatoes away? In some cases, they gave tons of them away to local residents. I don't live near a potato farm, and you probably don't either, so I didn't get any of those free potatoes. You probably didn't either. In many cases, the farmers dug giant pits with costly backhoes and simply buried all those potatoes and wrote off the loss.

Your food supply chain is vulnerable. From production to logistics, there are many exploitable points along the way. So, what can you do? First, start storing enough food to get you by for an incredibly long period, and know how to cook it when the power goes out. Canned goods are great and not as susceptible to inflationary forces in the short term, but they come with an expiration date. Dehydrating food will give you up to a year on that expiration date-- sometimes longer and sometimes shorter. Knowing how to can or pickle food can not only extend shelf life but provide you with a useful skill when your refrigeration no longer works, or you are collecting your own food. Freeze-drying your own food or buying freeze-dried foods comes with a heftier price tag upfront but can give you meals that will taste fresh and last for 25-years or more. I cannot imagine what 20 pounds of beef will cost in the year 2047. It might cost the same as a freeze-dryer purchased today.

It may seem odd to fight a cyberwar by growing your own food, but you need to start a victory garden of your own, either on your land or someone else's. You need to know the edible plants in your area, and you need to know how to preserve, freeze-dry, dehydrate, and pickle every scrap of food you acquire. Get to the point of zero waste. If you only grow patio plants, it's something. It may not sustain you entirely on its own, but it will stretch and supplement your foods. It will give you something to trade and barter with. Build a supply of shelf-stable foods. It may not end up being enough to keep you for months or years after a significant breakdown of systems, but it may be enough to help you survive through to a better day. The ultimate goal is always self-sufficiency, of course, but that isn't always a possibility for most on limited land and with limited resources. Focus on your 3-week, 3-month, then a year or more supply like I outline in my course and work from there.

#5 ENERGY

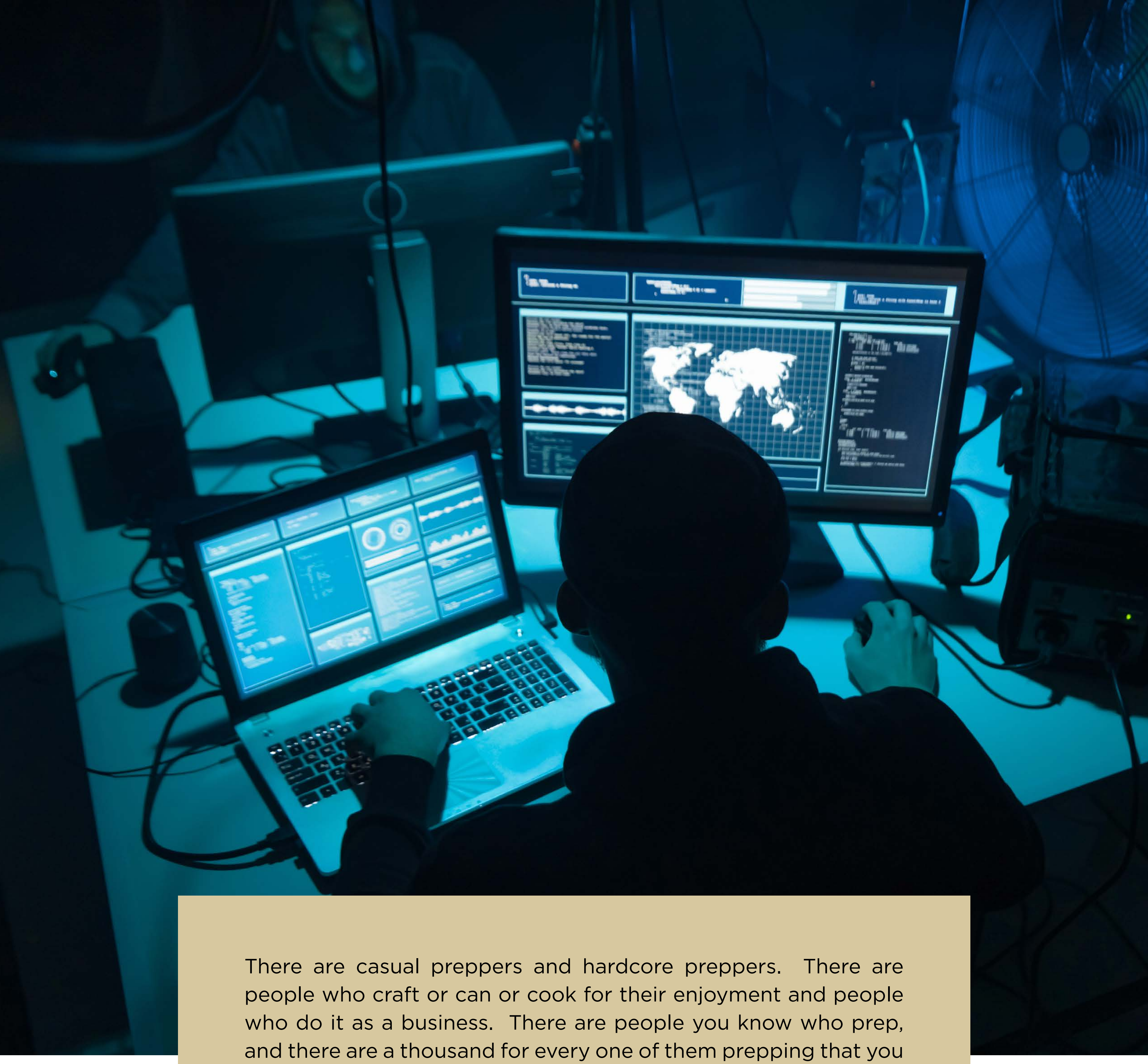
There are other pillars of survival that I could cover, but water, food, and energy are the three biggies when it comes to insulating yourself from cyberattacks. That is because these three pillars of survival are also the most vulnerable systems that we have exposed to cyberattackers. When it comes to energy, I mean all forms of personal energy that you use. If the grid goes down tomorrow and remains ransomed for weeks or systems are simply destroyed by hackers, your problems become much bigger than flipping a switch and realizing the lights are out. Your phones will be down. Security systems will be down. Medical, EMS, fire, and police services will be down. All forms of utilities beyond electricity will eventually be down. Even natural gas isn't a magical delivery system of flowing air. It relies on pumping stations and monitoring equipment. Some of those run generators on the natural gas they produce, but the same isn't necessarily true at the furthest points on the capillaries from the pumping stations. Water is often fed to communities through gravity from those massive hillside water towers. Still, those are replenished and continually filled by electric pumps that push the water up to them.

When the energy stops flowing, just consider that all systems as you currently know them will eventually fail. I don't have a well or a natural gas main. I don't even have a forest nearby to provide me and everyone else with burnable wood. You need energy from refrigeration to charging radios, flashlights, walkie-talkies, or reusable batteries. At the very least, you may need biomass energy to boil wild water. You may not be in a position to install a home power solar system and battery like I just showed in a recent video. Maybe that system or an even smaller system with a few other products could keep you cooking, boiling water, charging phones, and whatever else you absolutely need to survive.

Approach your energy needs first by assessing what you absolutely need. Understand the vulnerability of the current system. Review the video posted on my YouTube channel which goes into great detailing explaining how to determine your power needs, and understand what you will need to get by on your own. Then, start building the same way you approach the other preps. Get your self-sufficiency to 3-weeks at the bare minimum. Maybe batteries are what you need for that. Then get to 3-months or more. Perhaps a solar generotr or other renewable system is what you need. Simply having a gas generator as backup won't be enough after 3-months when gasoline is scarce. You may be surprised with how little you need to get by, but energy provides us light and heat when properly harnessed. Do you have hurricane candles, a means to heat or cool your living space? Do you have the means to cook and purify water for three or more months? Don't overlook your energy needs. Look at it from all angles and make yourself as infrastructure dependent as you can be for the longest amount of time.

GET YOUR EDC BAG TOGETHER

There isn't much warning that the network and infrastructure are going down in a cyberattack. At one moment, you are scrolling your Facebook on your lunch break or trying to make a purchase at the store, and your page won't load, or the sale won't go through. The extent of the attack isn't entirely known in the minutes and hours following the attack. Just as you would prepare for a hurricane you know is coming by setting up some supplies, you should be equipped with an EveryDay Carry (EDC) bag and make a point to keep it handy and with you, until the larger threat passes. If the grid goes down and traffic lights stop working along with metro systems and gas stations, you could find yourself miles from home. Even a few miles could equate to a perilous journey. The EDC bag is designed to allow you to respond to an emergency and to allow you to get out or get home after a disaster. Things to include in your EDC Bag are essential medicines and first aid, a stainless steel non-insulated water bottle, firestarters, flashlight, folding knife, a multi-tool, glasses and/or readers, spare keys, important legal documents, a personal water filter, glow sticks, KN95 mask, SAS survival guide, emergency blanket/poncho, pen, pencil, small memo pad, carabiners, compass, region map, small denomination cash, sewing kit, snack bars, and more. What you put in your bag and the bag you choose will depend on your environment and situation. I know some people who live in a more rural setting who have put foldable saws in their EDC to deal with downed trees that may obstruct their path home. Consult my course or videos on my channel to determine what should be in your EDC bag beyond what I have outlined here, but do build one and start carrying it with you wherever you go, even if that's just in the trunk of your vehicle. The likelihood of a cyberattack striking when you are away from home is high. If you want to get back home, build an EDC bag.



There are casual preppers and hardcore preppers. There are people who craft or can or cook for their enjoyment and people who do it as a business. There are people you know who prep, and there are a thousand for every one of them prepping that you don’t know about. There are rich people looking to escape into space or in their triple insulated bomb shelters far underground, and there are those who, on meager funds, are learning to do for themselves and how to survive, even thrive after life throws the worst at them. I don’t know where you are on any of those scales, but I know it doesn’t matter. If you look at the long arc of history and you look at how recent global upheaval has predictably panned out, you would be foolish not to brace for even more tribulation and chaos.

We are engaged in what can only be characterized as World War III. I can't imagine that when Albert Einstein said, "I know not with what weapons World War III will be fought, but World War IV will be fought with sticks and stones" that he ever thought one of the weapons of World War III would be cyberwarfare; yet, here we are. We have already seen the weapon wielded in many ways over the years. From individuals to state-sponsored operations, many cyber groups openly threaten to attack for one side or another. This isn't a question of if. It is a question of when. Use this guide to harden yourself off from attack and develop resources sufficient to outlast the potential chaos.

I would like to say that things will get better tomorrow. I would also like to say that the price of gasoline will one day go back under two dollars. Both statements would probably be lies or, at least, gross understatements of the realities we are facing. Many cyberattacks have already been launched since the start of the Russo-Ukrainian war, and many more are to be expected. Most people will be blindsided when one of these attacks impacts them directly. Some people will even criticize the advice and explanations I am giving here. That's okay. There's lots of opinions and information on all sorts of matters, but that doesn't change the fact that some, as again my great grandfather used to say, would "Miss the forest for the trees." You don't have to be most people if you start diligently and methodically prepping today. I tell you this because, if it all goes, as my great grandfather also used to say (he was full of aphorisms), to "Hell in a handbasket," I would like to think that I helped a few people make it through to better days. I would like to believe that others will be standing with me on brighter days when we rebuild a better future together.

Take a look at the content on the City Prepping YouTube channel and the CityPrepping.com site for a more in-depth look at some of the things I have covered here, and watch for future releases. You can also sign up for our Prepper's Roadmap course to build your foundation for emergency preparedness.

And, as always, stay safe out there.

CITY
PREPPING