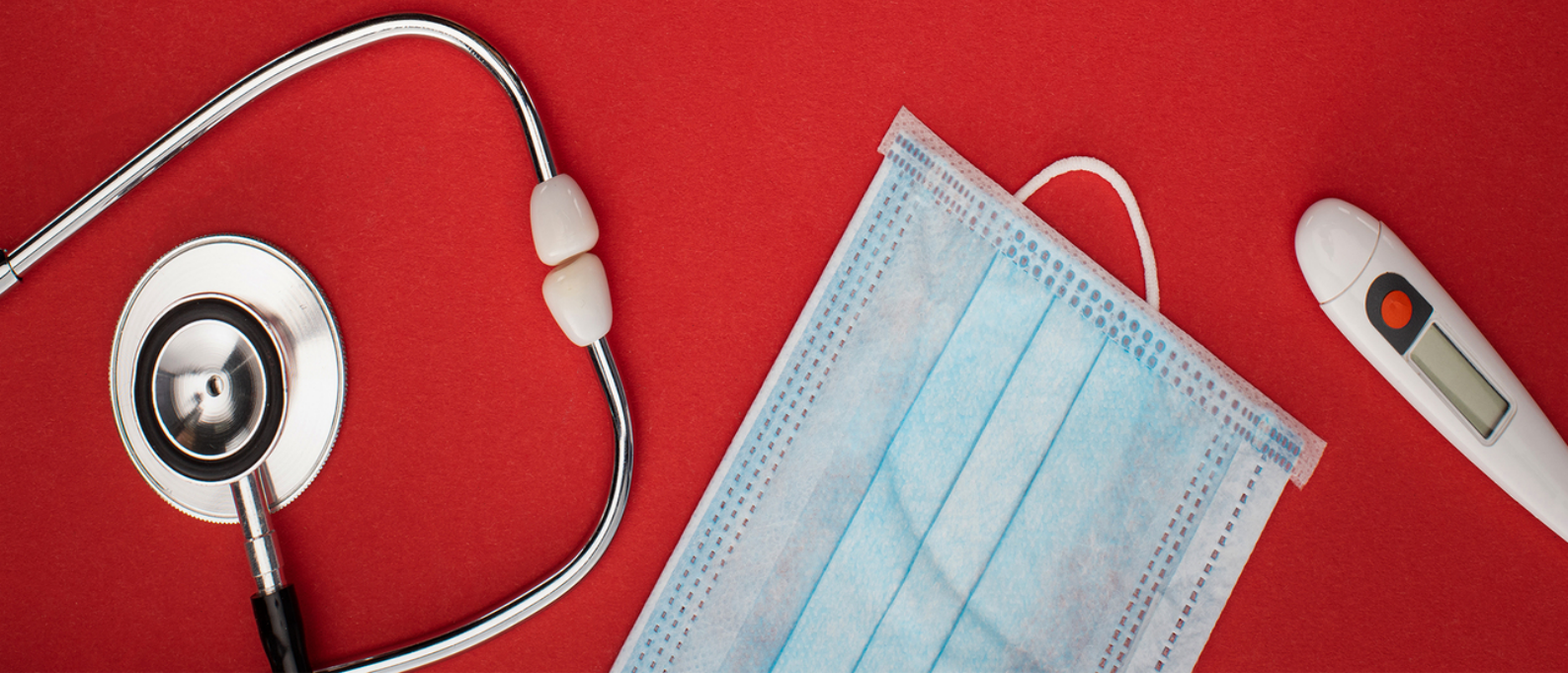
LEVI WEST

THE CORONAVIRUS CYBERSECURITY SURVIVAL GUIDE

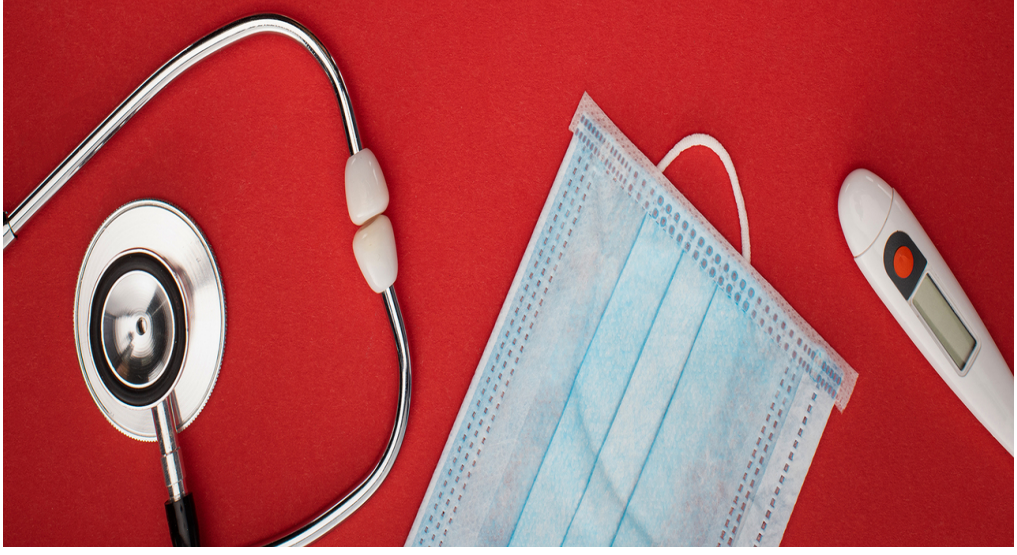
TOP TIPS TO PROTECT YOU FROM A CYBER ATTACK



LEVI WEST

THE CORONAVIRUS CYBERSECURITY SURVIVAL GUIDE

TOP TIPS TO PROTECT YOU FROM A CYBER ATTACK



The Coronavirus Cybersecurity Survival Guide

Top Tips to Protect You From A Cyber Attack

by

LEVI WEST

CONTENTS

Introduction

Coronavirus pneumonia (COVID-19) has gripped the world scene. At the time of this writing, most major countries have confirmed cases, and many deaths have been recorded.

Criminal hackers and underground networks have taken advantage of this situation to profit off vulnerable citizens and infrastructure systems. By shifting to teleworking and work-from-home business models, companies have inadvertently created a wider attack surface for cyber threat actors (CTA). IT departments at hospitals and other sectors are staying vigilant because at the most basic level, malware and hacking tools have also become more easily available, allowing those without a coding background to understand and use them.

Coronavirus scams are on the rise. These include many of the same scams cybersecurity professionals have seen before. They may seem new, but they are in fact the same. The main difference is that they are corona-themed. This includes a wide range of schemes such as phishing, ransomware, and fake advertisements. Governments, businesses, and individuals need to figure out ways to stay safe.

Due to this storm, you are a target. You have a lot of valuable information that hackers seek. Protect it, safeguard it, and find ways to bolster your security.

In this book, I will give you dozens of ways to protect your Internet network and devices. This book covers topics such as email, passwords, and software security. It may seem too general, but all of these tips are excellent at defending against corona-themed scams/exploits/attacks. In fact, whether for COVID-19 or another emergency, these suggestions reinforce good security practices and habits.

You can choose to implement any number of these tips or at least understand the reasoning behind them. These suggestions focus on practicality and things you can do right now.

This is a general guide meant to capture the essence of what you need. Pursue further research if you must. The

responsibility lies on your shoulders.

And finally, stay safe out there. Be well and take care.

1. Adopt Strong Passwords, Part I

Why it's important: Weak usernames and passwords are often one of the best ways for hackers to get into vulnerable accounts. You wouldn't believe how many people use "1234" or "111111" as their password. These weak passwords can be guessed or brute-forced (systematically guessed via computers).

What can you do? Think of establishing your own system for creating new passwords. Throw in special characters, numbers, and case sensitive letters to add complexity to your account. In addition, try to not use the same passwords more than once. That way if one account is breached, the others won't be comprised as well.

Common Passwords:

1. biteme
2. qwerty
3. password
4. 111111
5. sparky
6. access
7. yellow
8. 12345678
9. abc123
10. 1234567
11. computer
12. password1
13. sexy
14. 12345
15. Cheese

2. Adopt Strong Passwords, Part II

Why it's important: I cannot stress enough the importance of strong passwords. Many accounts have already been compromised, perhaps even yours. Many large-scale breaches have occurred and compromised. Companies like Target, Yahoo, and Marriott have been the victim of hackers. Don't be surprised if your favorite company has suffered a cyber attack.

What can you do? Become familiar with the term "pwned" when it comes to cybersecurity and passwords. It means that those passwords have been compromised. Consider going to the website https://haveibeenpwned.com/Passwords and see if your email address has breached.

3. Analyze Privacy Policies

Why it's important: Websites are constantly changing the ways they collect and store your data. With the General Data Protection Regulation (GDPR) and

other legal frameworks, many companies have had to update the way their collect your data. Websites will examine your data to identify trends and predict user behavior.

What can you do? Every time you connect to a website, visit their privacy page. Read their policies on how they collect your data and what they do with it. Look for the specifics and technical jargon. If the websites you are visiting and shopping on don't have a privacy policy, consider that a potential red flag.

4. Anticipate Cyber Attacks

Why it's important: Hackers are constantly looking for ways to get into your system. Cyber attacks happen every day. A lot of this occurs via computer automation.

What can you do? If cyber attacks can occur at any time, then you must update and defend your systems as soon as possible. Run antivirus software on an automatic basis. Scan all new files that you download to make sure they are malware free. Never install anything you aren't comfortable with.

Lock up your valuable information via password protection. All operating systems allow you to hide files as well.

5. Avoid the Shady Salesmen

Why it's important: Con artists create a sense of urgency and scarcity to get users to buy fake products, download free infected software, or enter their credit card information on fake websites.

What can you do? Don't panic buy. Websites and vendors are being setup with "new" goods that don't exist. They may create fake testimonials and have no real record. They may even promise a cure to the COVID-19. Don't give in and do careful research on any new products that surface. Be wary of suspicious ads and promises that are too good to be true.

Clickbait is one of the cheapest ways for hackers and vendors to harvest your information. They will often present themselves as hyper sensationalized links.

6. Backup Your Data

Why it's important: Murphy's Law states that anything that can go wrong probably will. As a consumer, you should have a reliable copy of your data lying around somewhere in case something goes wrong. The number of reasons could range from physical destruction of your device to hardware failure to cyber attack. You never know when your smartphone or computer hard drive could die. A second life will remedy this situation fast.

What can you do? Think about the data you have and what's important. Rank them from most to least important to figure out what to backup first. Once you've done that, store your data on a reliable cloud network system and another device medium/system that you have. Make sure they are convenient to you.

7. Backup Your Data Regularly

Why It's Important: Backups must be done on a continuous basis. Having a historical copy is good, but even in this emergency, you are creating new data and records that are important. You never know when you could make a mistake and suffer a setback.

What can you do? Depending on the backup system you decided to use, see if automatic backups are enabled. Determine if there is a setting that will allow you to backup the device on at a specific time. Don't be afraid to develop your own policies.

8. Beware of Phone Fraud

Why it's important: Your phone is one of the most common attack vectors for adversarial actors. This is because the phone number format is predictable. This means that there is only a finite number of phone numbers that can be used. Many people use more than one number as well. Hackers and spammers will send phone lists and may call you even if you did your best to secure your number. They may pretend to be a government agency or send you malicious text messages. It only takes a single misstep to compromise you.

What can you do? Do not click any unsolicited links via text messages and do not answer phone calls you think may from scammers. If the scammers did their research, they may have some intelligence information about you. Do your best to not react to it, and never give any money to them.

Consider investing in a reverse phone lookup service.

9. Beware of Phishing, Part I

Why it's important: Phishing is another popular tactic used by hackers to grant them access into a victim's system. Phishing involves masquerading as a trustworthy party in an attempt to steal your information. They may pretend to be your favorite company, boss, or even your friends. The most popular delivery method is by email, but it can happen through any form of electronic communication.

What can you do? If you see something strange, see how it was vetted. Is the quality of the email the same? Is something off about it? A lot of phishing emails will ask you for personal information and to reply back. Reputable companies do not ask for this information in an email. Never respond to these communications.

Phishing is simple but is one of the most dangerous types of attacks.

10. Beware of Phishing, Part II

Why it's important: Phishing has different types of forms. Due to the low cost of sending it, hackers routinely send out phishing schemes to catch their victims. I'd like to take a moment to go over the most common forms.

What can you do? Realize that attaining domain knowledge over phishing takes lots of reading and time. No way around it. A good resource to learn more is https://www.us-cert.gov/report-phishing. Till then, I will go over several of the most common forms of phishing.

Spear Phishing. This is a sophisticated type of phishing that targets a specific person and email account. In this particular situation, the hacker knows all about the would-be victim. They have accumulated the targets personal information and digital footprint. They may even study the victim's behavior and determine the best time of day to catch them off guard. When a spear phishing attack is launched, it will appear very real and relevant.

Whaling. A type of phishing that takes aim at the management and leadership levels of an organization. Hackers will do their research on social media platforms like LinkedIn and identify partners they work with. Conjointly, when they send the email, the hackers may also embed links or attachments relevant to the daily operations of an organization. When opened, it will compromise a system through malware (like a virus or keylogger).

Smishing. Like spear phishing, smishing is similar in scope and targeting. However, smishing involves text messages sent to your phone. Hackers have been known to spoof your area to make it legitimate too. The skepticism that you use for phishing should be adopted here as well.

Restrict your private information when you can.

11. Bluetooth Vulnerabilities Exist

Why it's important: Users often have their Bluetooth connections widely accessible. Hackers can steal a Bluetooth connection and use it to siphon off data. They can also force your smartphone to connect to something it doesn't want to.

What can you do? A world without Bluetooth may seem impractical. However, what you can do is turn off Bluetooth when it is not being used.

Balancing security and convenience is a tough juggling act.

12. Check Emails Twice

Why it's important: Cybercriminals know that their potential targets could succumb to panic and impulse. Due to this possibility, they know that when they send a malicious email, there is an increased chance of it being opened.

What can you do? Whenever you get an email into your inbox, check the sender and the email address they are using. Make sure that the "send" email address has sent you emails before. Cybercriminals may register a fake domain and add characters to appear legitimate. For example, user@un.org is the official domain for the United Nations. They are not likely to send you emails from the email addresses user@un-safety.net or user@un-usa.com .

13. Check Spelling and Grammar

Why it's important: It may seem obvious, but a lot of hackers make spelling and grammar mistakes when communicating with potential targets. A lot of hackers are international and learned English as a second or third language. Many of their threats may be oddly worded or include phrases that a native speaker would seldom use.

What can you do? If you get anything suspicious from your friends, co-workers, etc., consider the phrasing. Is it awkward? Was it sent at a weird time? Do they normally communicate with you in this way? Some hackers have a tough time replicating the way your associates talk to you or even their writing voice. The English language is complex, and in this case, that's a good thing.

No one's perfect. That includes hackers.

14. CISA Provides Alerts

Why it's important: The Cybersecurity and Infrastructure Security Agency (CISA) is one of the foremost agencies for providing updates to the American people. They help bridge the gap between the federal government and the local and state governments. They are continuously monitoring the situation for disruptions and emerging threats.

Why can you do? Visit the website https://www.cisa.gov/coronavirus for ongoing developments. Updates are posted there, and it is very comprehensive. There is a lot of documentation on social engineering, teleworking, and risk management.

Another website for staying up to date is the CDC's website for Coronavirus (https://www.cdc.gov/coronavirus/2019-ncov/index.html).

15. Coronavirus-themed Domain Registrations are Up

Why it's important: Hackers are setting up shop with websites that promise to have something related to the coronavirus in theme. This is meant to catch your attention and then exploit your computer.

What can you do? Make sure that what you are visiting is in fact safe. There are quite a few cybersecurity companies that will perform website security checks. Search for URL and website scanner. When it doubt, check. Bookmark your preferred sites to avoid going to sites that aren't familiar with.

16. Criminals Wield Shame Like a Weapon

Why it's important: Criminals want to make you feel vulnerable. They may use scam letters, send compromising videos and photos of you, or hack your web camera to make you feel scared.

What can you do? Don't fall for any of it. Report it right away to the appropriate law enforcement authorities. If they ask you to wire money, buy a gift

card, or send them Bitcoin, ignore it. They want emotion to take over, don't let them win.

Hackers often don't have the level of access that they say they do.

17. Cyber Threats Evolve

Why it's important: The landscape changes every day. Viruses undergo evolution and natural selection. Cyber threats are the same way. New ways to perform social engineering, ransomware, and data breaches, are found every year.

What can you do? Find strong sources of news for cybersecurity issues. Find a blog or subscription to one of the leading experts that advise on these matters in academic journals and at conferences. Read as much as you can. Finally, if you haven't already, make friends those who are familiar with computers and IT.

18. Disconnect When Appropriate

Why it's important: Sometimes too much information is a bad thing. With all of the available sources, it is easy to get overwhelmed. A reset from all electronics can be the best thing to do.

What can you do? Turn off everything for thirty seconds and take a stretch. When you're done, you can get back to it. Taking breaks often is highly appropriate.

19. Dispose of Confidential Information When Possible

Why it's important: Today or tomorrow, you will have to create new records. You might create these new records on a sheet of paper or notepad. This leaves a new trail for hackers to pick up. The fewer records there are, the easier it is to keep your information safe. Physical evidence of name, address details, passwords and other identifying information can compromise internet security.

What can you do? Shred anything that you can. While uncommon, some hackers will go through people's trash. In addition, they may analyze Wi-Fi networks in neighborhoods. Depending on what they find, they can get an edge of your network's security (passwords, name, unique identifiers) and what type of information you may be trying to protect (billing and personal information are good examples).

Delete any user accounts you don't use anymore. Old services that have run their use are a good example. Unsubscribe to email newsletters and updates that you don't need and clutter your inbox. Some companies publish too much of your information in these things and give attackers another way to snoop on you.

Wardriving is a tactic where hackers will driver around in their vehicle (usually a car) searching for Wi-Fi networks to infiltrate. Laptops are a favorite in this scenario, but they may also use smartphones and tablets.

20. Dodge Fake Coronavirus Maps

Why it's important: Maps and graphics are one of the best ways to tell a story. Whenever the media is trying to paint the current status of the virus, they will often point to a geographic map or data visualizations to give you a snapshot of what's going on. Due to the reliance of these, hackers have copied the framework or embedded malicious links to harvest information from you.

What can you do? Bookmark official and well-known sources so that you can refer to these when needed. Reputable news organizations and universities should be your go-to source. Never underestimate a hacker's creativity.

21. Don't Open Suspicious Emails

Why it's important: Unsolicited emails are sent all the time. It may seem obvious to not click on suspicious emails, but it happens all the time and can happen to anyone. Opening them up can reveal information to the hackers, even if you are just curious. For example, they can learn where you are and geolocate you!

What can you do ? Stay vigilant. Report any emails that come into your inbox that have any sign of suspicion to law enforcement and your email service provider. Your email account is one of your most prized assets.

Set up another email account to use as a buffer between you and your primary account. Upon setting that up, enable a preview email feature that isolates the content from your system. You have a long history in email!

22. Don't Click on Suspicious Links, Part I

Why it's important: Even if you open an email from a trusted contact or source, hackers can still compromise you. In fact, they often compromise friends or family first because this raises the chance that you will read their emails. However, it may be hard for them to compromise those accounts. What they might do instead is redirect the web hyperlinks (the blue links) that you see in emails to another location that they control. A fake website account of a social media company or your bank for example.

What can you do? Avoid clicking direct links that embedded in emails. Copy the link, otherwise known as a Uniform Resource Locator (URL) and put it through a URL scanner. Sites like virustotal.com and sucuri.net are popular for this reason.

Malicious links are one of the most common vectors to trick victims.

23. Don't Click on Suspicious Links, Part II

Why It's Important: Links are a common denominator for hackers to gain unauthorized access. Hackers will often use shortened links that redirect to malicious websites. Shortened links use a number of characters that are very small

in length. However, hackers have also figured out that it is hard for someone to see and verify a link because these links give them a layer of obfuscation.

What can I do? When you receive a link, examine each one of them. Use URL scanners to scan them and check if it is malicious. Despite its form, at the end of the day, it is still a link. If you must, open the email before you copy and paste the link into the URL scanner to determine if it is safe.

24. Download Security Tools

Why it's important: A security apparatus is necessary for protecting your information systems. This apparatus should include a suite of defenses like anti-virus, anti-spyware, and a strong firewall. Each is a necessary part of your defense.

What can you do? Find out what you can afford and pay for. There are a lot of good anti-virus and anti-spyware tools that are free, but many of the most robust and updated tools require a subscription. Your balance and comfort level will help you determine which is best.

25. Email Attachments can be Dangerous

Why it's important: Malicious attachments are an effective way of infecting a user's systems. Attachments, while plain, can host and executive malware that can compromise your information fast. It doesn't matter if it's a document, spreadsheet, or even a picture. All of these things can be detrimental.

What can you do? If you have a setting to automatically download attachments, turn it off right away. Make sure any attachments you receive are expected. For example, if a coworker said a specific file was sent, then you know it is coming. Still, scan each file as it arrives to give you the peace of mind you need.

Trust Your Instincts.

26. Endless Ransomware is Here

Why it's important: Ransomware is one of the top cyber threats being used to threaten victims. Ransomware is a type of malware that locks all of a victim's data and encrypts it so that they cannot get to it. It infects computers in many ways, but opening email attachments or visiting already infected websites are two of the top ways. Once infected, hackers will then demand money (USD or cryptocurrency usually) or they will publish the data publicly or delete all of it.

What can you do? Do you remember how I told you to backup your data? Fresh backups are one of the best defenses for your data. If they delete your data, you can then revert to your backup and continue operations as normal.

Ransomware is a type of threat is highly effective. Treat it very seriously.

27. Ensure the Latest Firmware is Installed

Why it's important: Firmware is software that is embedded on your hardware to help it run. Many Internet users do not update the firmware on their router. This exposes their network to security flaws that may be used by attackers who are exploit remote users.

What can you do? Connect to your Wi-Fi management software and run an update on your router. Install the latest software if you are out of date. Check to see if your router updates automatically or if you can set it do automatic updates. In addition, call up your Internet service provider for additional tips on your router and Wi-Fi network. Expand to other devices as needed.

28. Expect Social Media to be Overwhelming

Why it's important: We live in an information economy. We are dependent on the Internet to understand what is going on. The first thing people often go to is social media. Social media is the widest vector to infect media users. Lots of accounts are fake (run by computer bots) and there's a lot of distracting news that will take away from key time you need to prepare. Moderators on this social media sites will likely have to spend a lot of time keeping the bots at bay.

What can you do? Minimize retweets and posts to only relevant details. Follow only a limited number of sources for news. Flag and report any fake accounts. Familiarize yourself with the terms and services on these sites as well. It may be long and complex, but it is worth it.

Many provocative accounts are run by bots and these bots "argue" with each to stir up controversy.

29. Fake Videos Via DeepFakes are Here

Why it's important: Streaming is a double-edged sword. On one hand, data science and machine learning has allowed us to quickly find videos that we think are relevant and informative. However, hackers and social media manipulators have also created fake videos called deepfakes.

A deepfake means that a video is altered in such a way that it appears to be an authentic video. For example, a person's face in one video is switched with someone else's face. Due to encoding, this means that the videos are very convincing and real. This allows hackers to control the national conversation and debate online. It's deception at its best.

What can you do? In videos that are suspicious or seem unreal, think twice. Check the video to see if there is lighting that isn't right or if the video is out of sync. Many deepfake videos are close, but not exact. There's usually something wrong as the algorithms that make these videos aren't perfect.

When in doubt, dig deeper.

30. Fake Census Letters may Come

Why it's important: The 2020 Census has arrived. You may get a letter in the mailbox. Scammers may also send mail at the same time to confuse individuals.

What can you do? If you get one of these letters, examine the contents. See if there's anything off or inaccurate. You can also go to the U. S. Census Bureau website https://my2020census.gov/ to verify the 12-digit Census code that you should have gotten in the mail. Visit the website https://2020census.gov for more general information.

31. Fake Charities also Exist

Why it's important: New websites posing as charities are being registered with a combination of words such as, "relief," or "victims." These words are meant to illicit emotions from users. Many of these domains are malicious and will drop software onto your computer to spy on your accounts and web activity.

What can you do? If you are going to donate for emergency relief, verify all charities before doing so. Do extensive research on potential charities you may donate to. Examine their record to see their reviews and look for clear documentation on their history.

32. Fend off Cyberbullies

Why it's important: The Wild West atmosphere of the Internet has given bullies a new way to harass others by posting hurtful information anonymously. Sometimes these comments can turn physical and have real-life consequences.

What can you do? If you find yourself dealing with a cyberbully, there are a number of things you can do. Limit your personal information so that it is hard for them to dox you or expose you online. They will often Google you or look on white page websites to find out who you are in real-life and post it online for everyone to see. Whatever you do, do not escalate the situation by responding with hostility. Finally, document and record all the activity that you are experiencing. This will help with legal action and reporting should you choose to do so.

Don't be afraid to document in abundance.

33. Filters are Your Friends

Why it's important: Some people receive dozens or even over a hundred emails per day. If this is you, then implement filters to help you cut through the noise. This will also help you spot strange emails easier.

What can you do? Organize a list of folders for you to sort emails. This will help you white list and black list websites that are sending you emails. Dump subscriptions, deals, and notifications into a number of specific folders. Keep track of what you are subscribed to, and make sure to unsubscribe from odd lists. If you continue to receive emails that you don't want, implement a new rule to dump those straight to the trash bin.

Customization gives you strength, power, and efficiency. Default settings are often not enough and can constrain your interests.

34. Get Familiar with Jargon

Why it's important: In today's world, you need to stay up to date on new technological terms. You may feel that it is scary or pulls you out of your comfort zone. Embrace it, don't fear it. Every new word you learn builds your knowledge bank.

What can you do? Study! Study as much as you can. A full glossary of terms is available at the National Institute of Standards and Technology (NIST). I provided the link to their glossary here: https://csrc.nist.gov/glossary?index=O .

35. Identity Theft will Always be Real

Why it's important: Millions of people have been affected by identity theft. Theft of personally identifiable information (PII) like contact details, travel documents, and date of birth, provide a rich number of ways for cybercriminals to make money. When you type in details in any information system, you risk a hacker sniffing out your information and using it for fraudulent means.

What can you do? Avoid giving out any PII unless you have to. The less of a digital footprint you leave, the better. It is hard to determine how safe your information is at your bank, grocery store, etc. You only have one identity. You might as well protect it.

Monitor your credit and prepare to freeze it at any moment.

36. Implement Two-Factor Authentication

Why it's important: Two-factor authentication is a mechanism where two different types of information must be presented in order to be granted access into an account. For example, in order to get into your bank account, you may have to provide as password and a special one-time code that is delivered to your phone. This added layer of security makes it hard for your account to be compromised even if your password is listed somewhere on the Dark Web.

What can you do? Go over all of the applications and services you use, especially ones related to financial information. Check to see if each of these has two-factor authentication. Try to enable it on as much applications as you can. It may be an inconvenience and add time to your day, but it is well worth the trouble when it stops a hacker dead in their tracks.

Beyond two-factor authentication, there's three-factor and four-factor authentication.

37. Invest in a Privacy Screen

Why it's important: A privacy screen is a layer of protection that you put over your device's screen. They obscure the view of your screen, especially when someone tries to snoop on what you're looking at from the sides. Privacy screens also provide protection against scratches and dents.

What can you do? Buy a few if your budget can spare. Visual hacking is a real thing. If you end up going out in public with your device, it will be hard and impractical for snoopers to see your username and passwords that you type in. They will also have a hard time seeing anything you do for that matter. Privacy screens are considered low-tech, but they truly live up to their name. Privacy screens also protect against glare and reduces blue light.

38. Jailbreaking Can Leave Your Phone Less Safe

Why it's important: By definition, jailbreaking is an exploit that removes your phones operating system. You get to exercise more control over your phone, such as download an app you couldn't before, but you also lose some flexibility as well. Risky maneuvers have a trade-off.

What can you do? Jailbreaking makes it hard for the official company to push updates to your phone. You run a greater risk of exploits that can take advantage of you. Your settings may also change. Always look at your security settings, and make sure they are set up correctly if you do decide to jailbreak.

Know the amount of risk you are comfortable with.

39. Juice Jacking is a Thing

Why it's important: Juice jacking is a type of data stealing tactic where a power plug has two purposes: charge a device and steal data or install malware. Plugs at airports, coffee shops, and other public areas are vulnerable to this. If you end up going out, be careful where you plug your device.

What can you do? Keep your devices fully charged at home. Consider investing in a spare battery or even a solar charger if that is possible. Whatever you do, be mindful of where you charge your devices. The most common vector for conducting juice jacking is via USB cable.

40. Learn About Scareware

Why it's important: By definition, scareware or deceptive software is a type of malware that is meant to capitalize on a user's anxiety. Scareware does this by flashing a terrifying message that will often threaten a user into doing something against their interest. The bad guy will either demand money in exchange.

What can you do? Antivirus is good for scanning for type of threat. Scareware is a known threat, and reputable antivirus companies have built defenses against this type of threat. Make sure to only visit the websites you trust and don't give into the fear. A lot of scareware has been reused over and over again. It's predictably makes it vulnerable.

41. Learn From Other Victims

Why it's important: For years, victims have fallen to the many of the same types of malware that have plagued the world. Some of these have included

Emotet, HawkEye, and Agent Tesla. Each of these has been documented, including the technical details and the methodology on how it is deployed to a system.

What can you do? Research the top malware families and become familiar with each. Realize that if you are doing many of the same things said in this book that you will be protected from a lot of ways these things can affect you. Still, realize that these are effective and relentless pieces of malware that are unlikely go and last beyond this emergency.

42. Logout Frequently

Why it's important: Personally, I dislike staying logged into anything too long. I like to end my session and wipe my credentials when I am done. This helps me narrow the gap and attack window a hacker has. In fact, a lot of hackers use session hijacking (credentials stored for too long) as a way to steal someone's identity.

What can you do? Log out of any services you do need when you are done, especially for financial information. Automatic login features that save your accounts should be turned off. Whether on your laptop or online, this type of feature gives attackers an edge if you end up losing control.

43. Maintain Communication with your Employer

Why it's important: This one is more is more for those working from home. If you are still working, it is best to not isolate yourself from ongoing developments and policy changes. Developments are flooding in every minute.

What can you do? Draft up a list of contacts at your workplace. Get their email, phone, and other contact details. Keep a list of all questions you have. For example, seek clarification on how to record hours and what is considered work-from-home. Also find out who is the designated contact for specific issues, such as help desk matters. Volunteering for meetings and staying abreast of IT issues will give you a rhythm for what is normal and not.

Remote work can expand the attack surface a hacker can exploit.

44. Mobile Malware Has Risen

Why it's important: It shouldn't be of any surprise that the same type of viruses and trojans that can affect your computer can affect your mobile devices. Hackers have been shifting their focus towards mobile devices. Whether it is smartphones, tablets, or even watches, these systems rely on software and digital systems to run. This fact has also given them time to develop new malware variants and catch consumers by surprise.

What can you do? If your phone is running slower than usual, find out why. Double-check all of the apps and updates running on your phone. Enable additional security and privacy settings. Make sure that whenever a new app is installed on your device that you have to manually enable permissions for it to run.

Drive-by downloads are a favorite of hackers. It can happen when you visit a malicious website. This type of threat can install a wide number of threats on your phone like adware and spyware.

45. No is an Option

Why it's important: There's a lot of pressure to take action during this time. Hackers want you to react to what they're sending you. They want to capitalize to on anxiety and panic because they think it gives them an edge.

What can you do? Decline when you feel the need to. You don't always have to say "Yes." "No" is sometimes the right answer. The choice is yours.

46. Not All VPNs are Safe

Why it's important: Virtual Private Networks or VPNs, are a common way to encrypt an Internet traffic. Due to the need to work-from-home or protect information, a lot of news articles suggest using a VPN. The problem is that not all VPNs are safe. A lot of them are run by hackers.

What can you do? If you decide to use a VPN, make sure it has been reviewed by others. Some of the better VPNs have hundreds of reviews, even awards. You may have to pay for their services if you want quality service.

Research, research, research!

47. Personal Information Must Be Protected

Why it's important: I cannot stress this enough. Your information is worth a lot of month. Beyond PII as mentioned before, your posts on social media, usage on social media, and just about everything you do is worth something. This is more than your social security number and bank account number. You only have one identity, please take care of it.

What can you do: Restrict as much information as you can, expand the scope and meaning of personal information. Only give off the information that you deem to be necessary. Don't be afraid to ask twice or ask for specific information. Never overshare on social media and be careful of who follows you.

Social media is not meant to be a soap opera.

48. Public Wi-Fi Networks are Vulnerable

Why it's important: Whenever you connect to a public Wi-Fi network, you are exposing your data to someone else. Unlike the home network you use at home, you won't know who is connecting to any particular public network at any time. Hackers can snoop on your connection and steal your information.

What can you do? Generally speaking, avoiding public networks is the best way to go. You simply don't have enough control over them to know what is going on. However, if you are forced to connect to one of them, it is best to not go to

websites that are sensitive to your online identity (online banking, social media accounts, etc.). Disable file sharing and make sure to log out of all accounts when you are done.

49. Realize Fake Non-profits are Out There Too

Why it's important: There are bound to be fake non-profits that ask you for money. It's not just charities. In fact, cybersecurity companies have already reported on these supposed helpers-in-need. These non-profits may use catchy ads and well-crafted emails to illicit emotions from you and catch you.

What can you do? Research all non-profits before giving any money or information to them. Do not enter in any information, unless you are sure it is the right thing to do. Search for a watchdog report, a company that reports on non-profits, and see if they reviewed them.

50. Scan New Files

Why it's important: I've stated this with email attachments, but the same concern also extends itself to all of the new files you get onto your system. It could be from the Internet, but it could also be from a USB or CD drive. All new files should go through the same process.

What can you do? As soon as you get a new file, isolate the file and scan it. If you've been downloading and using your security tools, then you can right click on the file and scan it. Make sure your virus software is up to date to ensure it is effective at detecting any known malware signatures.

Better safe than sorry.

51. Stem the Spread of Misinformation

Why it's important: We are all being bombarded by information and misinformation.

What can you do? Be ready to flag, downvote, and tell others about inaccurate information on the Internet. Forward dangerous information to the appropriate channels to see if action can be taken. There are lots of private sector companies that will be quick to respond and readily take in your information. Think about volunteering online for a moderator position and/or joining a membership organization to provide your assistance.

52. Stay Up to Date on Software and Patch Applications

Why It's Important: Cybersecurity and tech companies are still working in this emergency. They are patching and analyzing software vulnerabilities. A lot of these companies had people working-from-home well before this emergency.

What can you do? Write a list of all your devices. Then, examine each of the devices to make sure they update automatically and see what they are updating. Some updates are optional, consider getting those as well.

Software is like teeth. It must be cleaned regularly.

53. Take Security Awareness Training

Why It's Important: While security awareness training can seem laborious, there is a real benefit to them. They bolster your foundation for tackling these threats in a formal way. There's always a new trend emerging in the battle for cybersecurity, and you should take notice when they surface.

What can you do? Search online for reputable companies and vendors offering awareness training. A lot of training is being offered for free, especially with many students at home. Think about the amount of time you can dedicate and if it caters to your knowledge level. Pick one or two training courses to contrast them both to find out the best practices you need.

54. Take Up a Password Manager

Why it's important: A password manager is another tool that you can download to help you keep track of all of the different passwords you use. It's not a be-all and end-all solution though. Users will have well over a hundred passwords in the course of their lifetime. Super users will have hundreds of passwords. Password managers organize your passwords and streamline your accounts for you. Easy peasy.

What can you do? Examine free and paid password manager tools. Free one's won't offer the number of robust features that paid one's will, but you will be able to get it fast and it won't break the bank. Paid password manager companies often have a free option available. Use what works for you.

Passwords managers are vulnerable too. Never put all of your eggs in one basket.

55. Verify New Apps

Why it's important: Like regular files, all new apps you download on an app store must go through a screening process as well. Apps, especially new ones, may have malware embedded in them. Apps need a lot of files, permissions, and resources to run.

What can you do? Scan new apps with antivirus software. Delete these apps if they don't pass these tests. Right when you get a new app you should also restrict it. Be hesitant on any permissions you give these apps. The more permissions, the more access you give it.

Cyber Truth: Some third-party app stores have been known to host apps with malware.

56. Warn Others

Why it's important: From time to time, you may see something that is suspicious online. While you may not fall victim to it, expect that others may. You're in a position to make a difference.

What can you do? Report anything you think is suspicious to the appropriate channel. If it arrived via an email, report it to your email provider. If it is via social media, report it to the tech company that manages that service. Better safe than sorry.

Billions of records have been stolen and compromised. This number will continue to grow as Internet dependency increases.

57. Watch for Price Gouging

Why it's important: Many goods and services that were readily available are now scarce. This has created a market with predatory price practices. Some vendors are selling toilet paper for hundreds of dollars. Due to this dynamic, hackers have setup websites will attempt to lure buyers in buying goods that don't exist. These are called nondelivery scams.

What can you do? Research all websites before putting in any of your information. It is probably a good bet to only go to vendors that you have shopped with before and trust. Know that some of these suspicious vendors may never deliver the goods that you are seeking.

58. When You Can, Encourage Good Habits

Why it's important: You are constantly learning a lot of great things in this book and from your experiences. You have a wealth of knowledge to provide to others. Let others benefit from it.

What can you do? When discussing with others about how to be more secure, see if there's something you can help out with. Don't be afraid to give them some of the tips in this book. Knowledge is power.

Closing Note

You cannot escape the responsibility of tomorrow by evading it today.

—Abraham Lincoln

By following the tips outlined in this survival guide, it is possible stay ahead of hackers and thwart them before they even stand a chance. Whether for general cyber threats or corona-themed cyber threats, you can have the peace of mind you deserve and have the confidence you need to survive in this changing time.

You will be prepared in advance. This is because you will have updated software that will scan for threats as they come in. The computer you use will utilize detect anti-spyware and anti-virus protection to quarantine and isolate files that are intended to harm you.

You will be hesitant in giving your personal and financial information to others. The identity you have is valuable and identity theft is something you will always be vigilant about.

You won't dread when you're dealing with email because you know of the various ways hackers can get you. Whether it is through spear phishing, embedded links, and malicious files, you are ahead of the threat.

You will have the ability the assist others in their time of need. Whether it is through mentoring and reporting fake news, you are armed with the necessary information to spot manipulation.

And perhaps most important of all, you will be inspired to learn more about cybersecurity. Your view on technology and appreciation for it has grown and gained all this in a fast and concise manner.

Thank you for making the Internet a safer please! Get out there and make a difference.