From: Bill Burbank, CISSP, CISM, CISA

Date: November 5, 2021. Updated 1-31-2022, Updated 10-23-2024.

Subject: Security Tips for Home: 3rd Edition

I originally wrote this document for a friend from the gym. This friend is highly successful, and skilled at his craft but like many does not have an IT or cyber background. He was ill prepared when his wife's accounts were compromised, placing his family at risk beyond the initial loss that was recovered. Subsequently, I have helped many friends and family recover from cyber incidents, and I casually advise friends with small businesses. I am currently assisting a lifelong friend who has been repeatedly victimized since January of this year when her Municipality and School district were hacked. Recently, they have had their lives turned upside when their son's local scholarship money for academic performance was lost due to EFT Cyber Fraud. It was not until after the funds were recovered did the local authorities disclose that she is also a victim of Identity Theft. They will now have years and years of negative ramifications associated with the theft of her identity.

Cyber Criminals (Hackers) operating from around the Globe are constantly engaging in a variety of Cyber-attacks on both Businesses and Individuals. These attacks range from Phishing, Email Compromise, Vishing, Unemployment Fraud, Credit Card Compromise, actual and perceived Ransomware/Virus attacks and various Web Site attacks including redirection.

In 2019 I found it curious that that there had been such a large volume of cyber incidents without mass monetization of the Personally Identifiable information disclosed during the breaches. At the time I surmised that the Fraudsters in bad guy countries were trying to compile enough information to become you. "The Fraudsters want your PII data; specifically, emails, challenge questions, birthday and passwords. The fraudsters want enough data on your customer, so they can execute smaller number of identity fraud attacks with a larger ROI."

It was not until recently that the perfect storm materialized; the acceleration of AI, willful disregard of rule of law from Fraudsters in Bad Guy Countries and volume of PII disclosed in data breaches has contributed into a very active environment. It is open season on Cyber Fraud for individuals who have been involved in a data breach (EVERYONE) and there are bad guys operating with impunity in countries that do not participate in the Convention on Cyber Crime. **Between now and Christmas, you will either have an incident or have a friend or family member who has a minor incident like successful phish or account takeover or a significant one (Lose of funds or identity theft).**

This memo is written as a proactive plan for you to better secure your data, finances and identities. I approach this with the mindset of tenant one of ISC2 Code of Ethics. That being said, I make no assurances, no warranties and no guarantees in this document, securing your accounts comes at a risk but so does doing nothing. Additionally, some of my guidance could be perceived as vague, but I will provide the guardrails and "what" but not necessarily the "how". I will not provide detailed vendor evaluations or prescriptive runbooks at the desktop level for execution. I will give you some simple tips and tricks that your parents might be able to do, if not with a little help. Remember you can go back to the old way of doing things, you can have a passbook at your local bank, a checkbook, send payments via the mail, have a simple basic cable service and pay as you go cell phones and rechargeable Visa cards. Most of us will not do this, however, with an aging parent or family member it might be advisable. The elderly are prime targets, its deeply saddening and terrifying to hear about the victimization of this demographic. It's especially despicable when it happens to people who have spent their entire lives in selfless public service to others like medical professionals, Police officers, Teachers, Firefighters, Librarians, aid workers, and professional and civilian military. ISC2 Code of Ethics has the following.

Protect Society: Protect the common good, public trust and infrastructure.

Before we get started, I want you to think about your digital life and get a Notebook and pen/pencil, yes, a Notebook. Start thinking about your assets or your "Install Base". This would include the following, but each family might have more or less of an Install Base or digital footprint. With each action item keep track of what changes you are making, as you are going through this process. You will have a realization that all the information you are writing down at your desk is in the Cloud, accessible from all over the globe. Our goal is to implement security controls to keep your data out of reach of the Bad Guys in Russia, Nigeria, Vietnam, Singapore and South Africa and other countries who don't participate in the Convention on Cyber Crime.

Before you get started homework:

- Are you a Mac, Windows or Google Family, or a like many a hybrid.
- Who is your internet provider?
    - Do they also provide email accounts associated with the service?
    - Who is authorized to make changes to the account?
- Who is your cellular provider?
    - What are the active and inactive devices associated with the account, have you named the devices?
    - Who is authorized to make changes to the account?
- What do you have for Computers, Tablets, Phones, peripherals?
- Make a full list of your financial accounts, including, bank account, retirement accounts, and loans.
- What financial apps do you have Venmo, PayPal, Coinbase, Cash app, Zelle, apple pay, etc.?

ACTION ITEM #A: Collect all relevant **Identity documentation** and store them securely in a location you can remember and easily access.

- **Passports**
- **Birth Certificates**
- **Social Security Card**
- **Driver's licenses (Old and New)**

Goto to https://www.irs.gov/ and https://www.ssa.gov/ (Social Security went paperless, statements are now here), setup your accounts.

As part of this process, you will validate your identity at https://www.id.me/ .

Next, make your appointment for TSA pre check https://www.tsa.gov/ if you have not already and you don't have any felony convictions, or are already on the do not fly list.

IF YOU DO NOT HAVE THE ACCOUNTS ESTABLISHED ALREADY YOU SHOULD NOT HAVE ISSUES WITH THIS PROCESS.

ACTION ITEM #B: Determine **Roaming Cloud Profiles.**

Identify if you have any Roaming Cloud Profiles. Common ones are as follows.

- Apple ID (Safari)
- Google (Chrome)
- Microsoft (Edge)

Other than the Apple/Mac environment and you are logged in (picture is in top right-hand corner of browser). Are you browsing, saving payments and saving website passwords and do not have MFA setup or don't know what MFA is exactly…

STOP, PROCEED IMMEDIATELY TO NEXT STEP…

SETUP MULTI-FACTOR IMMEDIATELY, LOOK FOR UNKNOWN TELEPHONE NUMBERS, EMAIL ADDRESSES, UNUSUAL LOGIN INFORMATION. I DO NOT RECOMMEND USING ROAMING PROFILES UNLESS YOU UNDERSTAND ALL THE RISKS AND CAN APPROPRIATELY SECURE AND MONITOR THE PROFILE. THESE PROFILES ARE DIGITAL GOLD, IF THE BAD GUYS GET THE SECOND FACTOR AND THE BAD GUYS HAVE ACCESS TO EVERYTHING AND CAN BECOME YOU!!!

Identity Monitoring and Protection Services:

Everyone by this point in time has been involved in a data breach and received an offer for free credit monitoring. The terrifying fact is the Fraudsters sometimes use the information obtained in the breach to masquerade as credit monitoring services to steal more sensitive data. I strongly suggest that everyone purchase Identity monitoring services, everyone knows big players, and some are integrated with EDR or Anti-Virus. I prefer using services from Credit Agencies that don't include Anti-Virus and always purchase premium services. This is not a place to be pennywise and pound foolish. A good analogy is someone with AFib, or a heart condition not getting Apple Watch because they don't want to pay $30 bucks a month. These services monitor your credit, scan the dark web for leakage, alert to identity theft, monitor your children's identity until they are 18 years old, and some provide insurance with exclusions.

ACTION ITEM #C:

- Identity Monitoring Services can be free if you have been offered it by a company as a legal requirement after your data has been breached. If you want to take advantage of this offer, ALWAYs contact the company that has been breached using the company's website, learn about the offer to determine if it is a service you are interested in using.
- Otherwise research top providers and contract for the **PREMIUM** services, log in initially every day while you are securing your identity through executing steps in this memo.

Leaked Credentials:

There have been hundreds of Personally Identifiable Information breaches in both the Public and Private sector. These breaches will have email address, phone number (Cell and Home), home address, IP Address, passwords, socials, account numbers, challenge questions, etc. The information is then either utilized by the first party Cyber Criminals or sold off to the Dark Web. They then cross correlate publicly available information (LinkedIn, Google, Insta, Tock, X etc.) and couple it with Dark Web Data to construct attacks. Senior Level Professionals are a common target at home and at work, often using personal information as part of the work attack. Most corporations have a monitoring service that alerts the Security Team of new credential leaks. However, there are sites and services where anyone can determine if their credentials have been compromised.

ACTION ITEM #1:

Goto https://haveibeenpwned.com/
Enter ALL of your and your families' personal and business email addresses. Make note of the accounts, especially the ones that are active and used regularly.

Passwords:

Most people use a small number of words, numbers, special characters that they can easily remember, putting ease of use over Security. The Hackers then can use the Darkweb leaked credentials to create a very limited number of password permutations. Because of the limited number of passwords that need to be tried or tested ("Door Knocking"), the Hackers can then attempt to compromise the account without tripping password lockouts. They typically script this, use BOTS or AI, set it and forget it until they have successfully compromised an account. Now with the acceleration of AI technologies, executing these types of attacks is very easy, even if you don't have the right skill set to hack. **If your account is single factor, they are as good as in.** If you have multi-factor Authentication (MFA), they will trip the second factor if they get the first, and you may not even notice or ignore it. They will then know they have a valid first factor and will move on to more sophisticated attacks often enabled by AI.

Passwords should meet the following standard: some are dependent on the website or provider. If you are sophisticated enough to use a password vaulting solution, be very weary as they are under constant attack. If you use an apple generated password, make sure you are also well versed in the ecosystem and comfortable with the pros and cons of this approach.

- 12-16 Characters
- Contain at least one upper case letter
- Contain at least one lower case letter
- Contain at least one special character
- Contain at least one number
- **ALWAYS OPT IN FOR MULTI FACTOR AUTHENTICATION (MFA).**
- **NEVER EVER USE THE SAME PASSWORDS FOR WORK AND HOME.**

ACTION ITEM #2:

- **Review the haveibeenpwned.com list of leaked credentials.**
- **Identify the password(s) used for the compromised account(s)**
- **Never use those passwords again, create a Blacklist, your favorite words and numbers are retired.**
- **Ensure that all passwords go forward are unique, different for every account and follow the standards above.**
- **Always opt in for MFA when available**

Home Internet & WIFI:

Most people do not actively manage their home internet Router, Firewalls, SSID and corresponding encryption type. Lack of strong encryption couple with a visible SSID can make their WIFI an easy target. Most people think they are safe enough because it is just your neighbors in range. Hackers take the information obtained via credential leaks on the Darkweb, they have identified a victim's address, and then they use sites like https://wigle.net , to determine the victims SSID. Now the Hackers have a victim's favorite passwords and home address they can **War Drive a Neighborhood** (Yes, they do this all the time). looking for insecure SSIDs. Also, they can set up "Evil Twins" with a similar name or the same name because most people do not know that SSIDs are case sensitive.

ACTION ITEM #3:

- **Ensure that your encryption strength is set to WPA2-PSK (AES)**
- **Both the password for the Router and for the SSID should be completely UNIQUE and never used at any time in the past and not be a variation of other passwords.**
- **Hide SSID if you have the comfort level, but ONLY after you rename it in the rare chance it is available information.**
- **Secure your Smart TV, Gaming Accounts, and TV Apps by also having a Unique password.**
- **Turn OFF auto updates on your TV and gaming systems.**
- **Install your ISPs Mobile App, this allows the homeowner to name devices attached to WIFI, test connections & speeds and most importantly monitor and alert on devices attached to the WIFI.**
- **Using your inventory ensures that you review connected and authorized devices on your home network.**
- **You can also cap the number of Dynamically assigned IP addresses and authorize new devices connecting to the network.**

Anti-Virus:

Always, run next generation Endpoint Protection like Defender, Sophos, Avast, McAfee, Norton or equivalent, any of the top providers are fine and they all share threat intelligence as a community. The agent should auto update, be tamper proof once installed and offer some level protection if updates fail. Microsoft Defender is included with Win10/11 machines, and if you are happy with what came with your machine and it's working for you stay with it.

ACTION ITEM #4:

- **Ensure that you are running Endpoint Protection on all devices, that it is up to date and showing that you are protected.**
- **Schedule or manually run full system scans.**
- **Ensure your Windows Firewall is turned on, some Endpoint protection products require it to be installed.**
- **Ensure both Windows and Endpoint Protection are set to auto update.**

Phishing:

Phishing attacks can come via email, text, phone call or even a mailed letter, post card with QR code or fake invoice. Phishing attacks can result in email compromise, malware/ransomware attack, or trick a victim into sending something of monetary value to the Hacker. Most Phishing attacks follow the same pattern, as email gateways have technical capabilities to detect anomalies and ensure that it's coming from a legitimate source. The most common cyber attack that impacts the average person is a BEC or Business Email Compromise. This is when an email account from a trusted domain is compromised and used as a relay to send either bulk attacks or spear phish or whale with a custom attack. The domain is from a real business will be clean and slip right by all technical controls put in place.

Most Phishing attacks have some or all of these elements. Some attacks on Senior Level Professionals in Corporate settings are very sophisticated impersonating real people on LinkedIn and using look alike domains… Some are even using Deep Fake Phishing attacks; these attacks started during Covid and now have become more convincing. **These attacks are real, they are getting better and better, and they are terrifying.**

Signs of a Phishing Attack:

- Artificial sense of urgency or impending negative consequences, something needs to be done immediately.
- *Fake Display Name:* Display name says **Bill Burbank**, but when the address is hovered over it is **DrEvil@hackersinc.com**
- The Domain is a cloned Domain or look alike domains. For example, **Claireburbank.com (No dash)** has been changed to **Claire-burbank.com (Dash)**
- Poor spelling or bad grammar (Before AI) and now they are formal and with perfect grammar.
- Asking for account credentials on mobile phone via text. Not following the normal process of how you would normally interact with someone.
- Attachments or links, links are long when hovered over and are not from same domain.
- QR codes embedded in a document are a new favorite tool as the PDF document scans as clean, but the QR code has a malicious payload.
- Fraudsters once they have your first factor and know they are in your account, then apply various tactics to obtain the second factor. This ranges from impersonating someone in authority like Fraud prevention at your financial institution or other authorized person. Some of these attacks are coming from inside the US where educated Americans are risking it all entering the dark world of cyber crime and hacking. These are so dangerous because they are so convincing and can easily gain confidence of the victim, especially in the AARP 55 plus age range.

ACTION ITEM #5

- **Always call, log in online directly or visit the financial institution in person.**
- **DELETE SPAM, create rules to move to deleted items folder.**
- **Only unsubscribe if you are 100% sure it's legitimate, but as general rule DO NOT unsubscribe. Those links can be phishing attacks also, yes, they are unrelenting and clever.**
- **Always hover over or click on Display name on emails to determine if it appears to be from actual sender.**
- **In the event of a call or email from, for example a financial institution, always call back the number listed on the account statement or website.**
- **Watch out for cloned domains or look alike domains.**
- **If it has poor spelling and bad grammar it is most likely a Phishing attack.**
- **Even AI attacks have little subtle markers that are slightly off, they don't have the same "polish", but this is changing rapidly.**
- **NEVER click on links or enter credentials originating from an email. If you do a lot of the EDRs (Anti-Virus) platforms suppress and block malicious domains**
- **If it smells funny listen to your gut, whoever needs to contact you urgently can wait until tomorrow or later in the day.**

Home Email Accounts:

Home email accounts are a relatively easy target as the Hackers have already have a potential victim's email address(s) and the combinations of the most likely passwords. Most Email compromises are caused by a Phishing attack where an unsuspecting victim unknowingly provides their credentials to the Hacker. The Hacker then lays in wait with the ability to stay concurrently logged in, creates forwarding, compromises the account entirely or uses the email address to compromise other accounts by using it as the second factor for authentication.

ACTION ITEM #6:

- **Setup a unique Admin account for your email, do not use it for any other purpose but to administer the other accounts.**
- **Recovery Accounts and second factor accounts should not be the same as your general personal email account.**
    - **Never use challenge questions that are easily enumerated, like Wildcats for UNH or Blue Hawks for Exeter. Create deceptive challenge questions that will trip security alerts during an attempted compromise.**
- **Ensure Spam filters are turned on and report junk/spam.**
- **Some email accounts are better than others, be weary of yahoo, Hotmail, etc., as they don't scan attachments, so you will have to rely on your EDR or Anti-Virus. Just make sure you are aware of the risk and can spot phishing attacks, I understand it's really hard to move away from email address that you have had for decades.**
- **I recommend evaluating email services like Microsoft O365 or Google for Business that have better detective and preventative security controls. They also implement blacklisting of known attacks much faster than other email gateways.**

Device Management:

All devices come with a unique ID or MAC address. Though there are ways to obscure, randomize or spoof, you just need to know that you have a unique MAC address and machine name for all your devices. This includes your phones, tablets, PCs, gaming systems, TVs and Mesh Wi-Fi pods, and wearables, and even some cars. The important thing is to know what devices you have attached to your WIFI and your cloud accounts. Naming all your devices is ideal, if not knowing what your default device name is also ok, if you know for sure that it is your phone iPhone 12, Dell 5555. If you can find the MAC address, then you are able to rename the device.

ACTION ITEM #7:

- **Using your inventory, ensure that you review connected and authorized devices on your home network.**
- **Your Cloud accounts will list all devices associated with your accounts, review and remove any older devices that you have decommissioned.**
- **Install EDR on your devices, even IOS Devices, even though most "news" on IOS devices versions being vulnerable is click bait, you don't want any type of issue with your mobile devices or open yourself up to cascading attacks.**
- **Check your privacy settings on all your applications, only use locations while using or manually turn it on and off as needed, turn off Siri and the BIGGEST ONE… DO NOT LET SIRI learn from this app.**
- **Delete applications you don't use; you can always re-install them later.**
- **Buy a Faraday Bag kit with Laptop, tablets, phone and key sized bags.**

Private Browsing and VPN and Public WIFI:

Ever wonder why if you search for something on your phone and later that night you are served an ad on your computer or Tablet? Your IP address is internet facing or visible is on the world wide web. Apps and websites collect hundreds of data points, both PII and non PII, they can then correlate indirect PII to pinpoint exactly who you are and where you are at all times. They capture screen size, browsers, hashes, device information like name and Mac Address, and hundreds of other data points. Private browsing and VPN is important from both a security and privacy perspective. When you're traveling Evil Twins are everywhere, especially in major metropolitan areas.

ACTION ITEM #8:

- **Remember those "Evil Twins" … Never use Public WIFI unless you "Have to" and if you do always use a VPN. (Sometimes a strong cellular signal has better bandwidth than a WIFI with Quality of Service implemented).**
- **On your phone change your settings to always ask to join. Imagine an Evil Twin of Hilton honors, Omni, or Marriot. Practice hygiene around Wi-Fi settings on your phone or you could auto connect.**
- **Get a VPN, Privacy Browser and use privacy search engines like Brave, Avast, DuckDuck Go, Nord, etc. This is a double edge sword, the more private and more anonymous you become the more likely you will be blocked as this is an attacker technique used by the bad guys.**

Roaming Cloud Profiles:

Back to roaming profiles… So, by this point you could be feeling a multitude of ways ranging from feeling good & secure to being terrified or just overwhelmed and feeling like this new digital world is too much to handle. The issue is Roaming Profiles have your entire digital life if you are not careful, all your digital payments, all your passwords to all of your accounts, and access to your emails, **EVERYTHING!!!** And it contains all the information required to become you and steal your identity, if only for short periods, but the lingering effects can last a lifetime. So, you have three choices **Option 1)** Use a roaming profile but ensure that its secured **Option 2)** keep and use profile, but be very selective on saved payments, email address and passwords **Option 3)** do not actively use profiles, and do not save any passwords or payments to roaming profile.

ACTION ITEM #9:

Option 1: Cloud Profile: You are all over it, you have a MAC or just IOS devices or you are a savvy PC user, you are comfortable living in the digital world. You are using device-based authentication, know all your devices, have specific admin accounts for email, all your sites and tools use multi-factor authentication, and you store all your payments and passwords in the cloud. You feel that your cloud compromise risk is relatively low.

Option 2: Selectively Use Cloud Profile: You have a google or Microsoft account all your sites are multi-factor authentication, and you have minimal payments and passwords stored in the cloud. You feel that your cloud compromise risk is acceptable in the medium range but don't want to invest in a Mac or spend the time on active learning. You feel comfortable doing just enough and not actively storing sensitive information on a roaming cloud profile will keep you safe.

Option 3: Do not Use Cloud Profile: You may have Cloud accounts, but you have decided you will not use Cloud Profiles in integrated way through logging into your browser. You understand your three options while browsing 1) Cloud Profile storing passwords in the cloud 2) Locally browser saving passwords to your device 3) storing no passwords or other means of remembering passwords. This is the safest option as it prevents Fraudsters operating in bad guy countries reaching across the ocean and upending your life and stealing decades worth of hard work and sacrifice, disappearing as fast as they can hit enter on a keyboard.

Once you have decided your family's strategy for cloud profiles and protecting your identity, you will have to perform the remediation required to secure your account. The most important steps are detailed in Action Items A to C. In these steps you have started to secure your identity, ensured you have multi-factor on your Cloud profile (or confirmed you are not using one), established an administrative email account separate from everyday use and read this document. The next step is to not get overwhelmed, and go account by account, password by password and payment by payment and secure your digital life in line with your risk profile and option selected above.

If you have been targeted or compromised:

Victims of an email compromise or a network intrusion should react similarly as if they have lost a wallet. However, losing a wallet can be much easier to resolve than being the victim of a Cyber Attack. Victims must assume that the Hackers know everything about you, from your friends & family, all your email contacts, and most importantly where you're Banking and Retirement accounts are located**.** They can **camp out in your accounts lurking gathering information. This can result in Cyber-attacks for YEARS to come or worse, Identity theft**. The proactive steps in this document are meant to make it more difficult for Fraudsters to assume your Identity and upend your life. Also, if they are victim to EFT Fraud or other Financial Fraud, don't assume that Financial Institution is on your side, they are for profit business that relies on a fractional reserve system lending money they don't have. They also, for a variety of reasons, do not want a reportable incident.

Action Items for Incidents:

- **Time is of the essence, if you have an incident drop everything, grab a pen and paper and start documenting.**
- **Stay as calm as you reasonably can after the pit in your stomach subsides.**
- **Determine scope and size of the attack, accounts, dollar amount, etc.**
- **If it is large amount, Ransomware attack or a business you will need to determine if engaging the FBI immediately is appropriate.**
- **Contact the financial institution or provider using a secure device that you know is not compromised.**
- **Share what you know and look out for red flags for insider threats and or trying to shift blame on to you for the incident.**
- **Some level of law enforcement will eventually become involved, local, state or federal. Share absolutely all information and answer all questions. This is where your documentation of events and timeline will come in handy.**
- **Notify contacts, especially friends and family, business associates about the compromise. Alert them that they might receive Phishing or Ransomware attacks from cloned or look alike accounts.**
- **Make a list of all retirement, banking, crypto accounts, and force rank them. Double-check security of the accounts.**
- **Ensure your credit is locked and if you have not executed every suggestion in this memo do so immediately.**
- **Finally, if you are in over your head or need assistance do not hesitate contacting legal council and need technical assistance give me a call.**

ISBN: 978-1-949701-23-4

If you did not receive this personally from me or purchase this, please consider a donation to my cousin Nate Murray.

We love my cousin Nate, his dynamic personality, kindness and his deep love and caring for his wife, children, and his family & friends. Nate and I have found memories of holiday trips and vacations in Syracuse & Montario Point and when we both lived in Atlanta. Nate has been diagnosed with Thymus cancer in the chest. It's terrible that people to be getting cancer at a younger and younger age. It's also disturbing that we have normalize Gofundme for medical bills in America, when its life and death. Please pray for Nate, asking God to give him the strength to make a successful recovery with serenity and grace. Please give anything you can at all sharing love and well wishes, even if it is a small amount and anonymous or send as a friend of mine sharing support. "TOUT PREST" so Furth, Fortune, and Fill the Fetters. Nate, we love you, you know what to do, be strong, we love you and will always be here for you.

https://www.gofundme.com/f/donate-to-nate-murrays-cancer-recovery-journey