Expedient Digital OPSEC for Travelers

Richard McNally, MSgt, USAF
Updated January 2024

Thank you for getting this far; you are reading a short tutorial on digital security. This is a step beyond the normal lifestyle of using cellphones and computers. You are tipping the scales of power and taking control back from your devices.

Let’s start by agreeing that this isn't a brochure on operations security (OPSEC) or clandestine travel. Rather it is a listing of best practices for using digital devices in a more private and secure way. Let’s cover some terms, and these are my own verbiage, not extracted from any textbook. I coach individuals new to digital privacy and security. My definitions work for them, so I hope they work for you.

Your Threat Model

Before you travel anywhere, it pays dividends to develop a threat model. This is your attack surface combined with your threat profile. It determines how much effort is required to defeat adversary tactics.

Attack surface: those components of your physical and digital environment which offer vulnerabilities to a threat. We'll focus on the digital ones. Every device you carry, every app you use, and every means by which you use them presents a possible vulnerability, and a cursory look at the news will reveal many.

Threat profile: those elements in your life that intend to do you harm. Notice that this requires intent; virtually anything has potential to harm you based on your attack surface, but specificity will focus your efforts best. For example, a student's threat profile is malware or malicious actors attacking a university's network, or operating rogue Wi-Fi at the local cafe where they study (again, focusing on digital attack surfaces). A police officer may find threats from organized crime or doxing campaigns more serious than a hacker at a cafe. An ambassador may find greater challenges combating nation-state intelligence agents or trans-national terrorist groups using breach data to find them or their loved ones. Your threat profile is unique to you, and you know best who your greatest threats are.

Think of how your biggest threats can possibly take advantage of your data and devices - you are analyzing your threat profile and your attack surface. Add them together - this is your threat model. That student's threat model is most likely low-level social engineering to steal login credentials for bank accounts or university portals, or maybe their cryptocurrency wallet keys. That police officer likely has their social media lurked for clues about their home address or patrol route. The ambassador's phone records are probably right now being sold to adversary agents looking to develop a pattern of life, social network analysis, and some form of covert access for intelligence, or something far more potent. Use your imagination or go watch old episodes of Alias. Say what you want; this was Jennifer Garner at her best.

Using your newly minted threat model, focus on that attack surface and hit the most glaring vulnerabilities. The following is my baseline recommendation for anyone traveling, whether domestically or abroad.

One-Time Steps

Account and Password Protection

Your adversaries, be they malicious hackers, foreign intelligence, or fraudsters, all want access to your stuff. Access means money and knowledge. If I had your bank password, I can have your money. With your IRS or social security accounts, I can have your identity. Give me your Facebook password, and I can know everything else.

The best way to protect these is by keeping them secret. We cut corners and get that wrong all the time. These are the most egregious of password security and secrecy violations:

- Reusing them
- Keeping them written or displayed out in the open
- Giving them to others
- Passing them over text message or email
- Passing them over social media
- Saving them on web browsers

There are good ways to stop these bad practices. The best and easiest are using multi-factor authentication (MFA) and password managers. These are examples of protecting *data in use*—every action you take on your device falls in this category until it either leaves your device for the intended recipient and/or arrives to a storage container.

Multi-Factor Authentication

MFA is a method of adding another factor of authentication to a first one. Authentication is based on proving you are who you say you are. This is done by providing any one or number of five categories of items:

- Something you have – a smartcard, hardware token, one-time pad (OTP) application
- Something you know – a pin, password, or passphrase
- Something you are – face, retina, fingerprint, voice
- Somewhere you are – IP address, geographic data
- Something you do – Role-based Access Control; time of day, location, data requested based on your role or function

Any one of those is a single factor of authentication. Adding another from **a different category** produces multiple factors of authentication. If you provide a password and then a one-time pad, either from an app, token, or text message, you're utilizing something you know and something you have. If you insert a common access card and provide a pin, this is something you have and something you know. If you enter a pin and scan a thumb print, this is something you know and something you are. Have you ever needed to log into your bank while traveling, and unexpectedly got prompted to enter a one-time pad from an email or text message? Your bank is combining something you know with something you have, because the usual somewhere you are does not match anymore.

Many of your online accounts offer MFA. Some accounts use apps like Authy, Google Authenticator, and Microsoft Authenticator for OTPs. Many services will offer to send OTPs via less secure methods, like email or SMS. Some of you may be familiar with Yubico's YubiKey, a USB plug which sends a private authentication key as a second authentication step if your service supports it (Microsoft and Google do).

Authy is a very good example of a software MFA service - let's walk through very briefly how to set it up if the account your securing supports it.

1. Go to https://authy.com and download it for your device
2. Create an account
3. When your are set up, log in to your account and explore the settings of the service to confirm if MFA is supported, specifically Authy or another software MFA service
4. The instructions usually have you scan a QR code with your mobile phone or tablet; alternatively, you can hand type a 6-8 digit code – this associates your account with Authy
5. Henceforth, every time you log into this account, you'll be prompted to enter Authy's 6-digit OTP, which you get by logging into Authy, finding the associated account entry, and pasting the OTP

6. Be sure to have Authy installed on more than one device – if not, and you lose the one device which has Authy downloaded, you won't have access to any OTPs until you sign into your Authy account on another device and download the app again

I urge you to do this for as many accounts as you can. Also be aware that not all MFA is created equal. Some methods are better than others, and this is my recommended hierarchy from best to least good, though anything is better than nothing:

1. Hardware token (YubiKey, smart card)
2. Software token (OTP service like Authy, Google Authenticator)
3. Email messages
4. SMS messages

Password Managers

These are applications which store your passwords and help you create new ones. Password managers store your account credentials as separate entries per account, linking a username, password, web site URL for the account, and any other information in one place. The biggest benefits are:

- Access to the password manager with one master password – now you only need to remember one password or passphrase to access however many credentials you choose to store
- Each entry links credentials with an account login site, and does not allow username/password auto-population if the URL is incorrect – this is good protection against fraudulent websites
- Most password managers allow you to generate random strings of characters for use as usernames or passwords, making them much harder to guess or predict
- You can store contacts and sensitive notes in them as well as separate entries – not just passwords
- Some password managers are web-based, which lets you access them from a web browser from anywhere (Bitwarden is a good choice); others are offline and operate like databases disconnected from the internet

The most important thing to remember about password managers is the safety, security, and secrecy of the master password – this is the one item of information you must take measure to protect. If you lose it, or it is compromised, you could lose your entire credential database. Here are some tips for a very good master passphrase:

- 18 characters or more
- Upper and lower case, special characters, unpredictable
- Make it a phrase that make no sense to anyone but you i.e. '5Recorders)Faraway(4*Cornhusk&Dreaming^'
- Enlist your password manager to generate this or parts of it for you

The second most important thing to remember is making password manager backups. Store these as you would store your sensitive financial or personal identity documents. If you lose your master password, these backups will allow you to recover your passwords. Here are some backup tips:

- Do not store the backup unencrypted on your computer or phone
- AESCrypt is a good app for both Windows and Android that can encrypt your backup—you might as well use your same master passphrase
- 7-zip will compress and allow you to add a password too
- If you typically keep passwords printed in a safe place in case your family or legal representative needs access to any of your accounts, a printed password manager backup is a convenient measure

Hardening Mobile Devices

The best way to treat your phone is like a game of hangman. Every time you tap it, type on a keyboard, open an app, select a setting, or even power it on, you get one step closer to the gallows. I know, that's a very dire metaphor, but it helps to visualize that every action on your pocket tracking device is recorded, and potentially used against you. If you implement some of the software and hardware soon to be recommended, you curb some of the most pervasive collection.

Here are some fun facts - a typical iPhone sends about around 50 KB of data to Apple servers at startup, normally containing the phone's IMEI, dialed number, advertising ID, unique wireless MAC addresses, and telemetry and diagnostics useful for quality of service. When idle, your iPhone sends this same data plus a few megabytes (MB) of app usage statistics, any nearby device info (if certain apps or services which detect them are enabled), time up, time active, time idle, battery status, and some other bits. Your typical Android will send nearly 4 MBs of data at startup - much more than iOS, but sends about the same information when idle. Both OSes will beacon to their support servers about every 4.5 minutes if idle. When in use, the connection requests and data transfer is manifold, with hundreds of requests to report every minute. It makes little sense to dig into the data sent and where they go, but just to inform the users that their hangman game is very chatty and there is little they can do about it without taking some steps.

In the end, today's mobile devices (smart phones, tablets, and laptops) are a minefield, but there are ways to tame them just enough to delay an investigating adversary or throw them off your digital spoor. These are your protections for *data in motion*—when you are done creating or consuming information, it goes somewhere else, and every trip your data take puts it at risk of interception, corruption, or loss.

End-to-End Encrypted Chat

Cellular providers require money to give you service. You can buy SIM cards that work wherever you're going, but Wi-Fi is free, and a trusted encrypted chat app will serve you well if using insecure and untrusted W-Fi networks. Make sure it has a VoIP component for calls too.

Signal, by Whisper Technologies, seems to be the app of choice amongst many. It requires registration via the device’s phone number, but you can get around this by using a VoIP number. Another option to maintain anonymity is activating a SIM card from a pay-as-you-go service, using that number to register Signal, and then ditching that SIM card. As long as the Signal account using that number stays active, it is yours, and the next owner of the registered phone number will not be able to use it to open a Signal account.

Wire is good too since it does not require a phone number for registration. You need only an email address; any one you own will do, not necessarily your main email address. Another that follows this anonymous registration model is Session, by Oxen. This app uses the “Onion” network for communication, further obfuscating activity from observers, but opens Sessions to issues with speed, reliability, and transmission of larger files.

Remember, you and your important contacts need the same app to stay within the encrypted ecosystem. If your network uses WhatsApp, then by all means use that too, whether it is the best option or not. The benefits of using an app that all your contacts use too outweighs the risks of Meta/Facebook collecting your usage statistics. Having your entire community switch apps because you ask them to is an uphill battle, and we should avoid app fatigue if possible.

Virtual Private Network (VPN)

VPNs do not hide your identity, protect you from hackers, or make your devices more secure. VPNs serve a single purpose – they allow you to use a proxy server for all internet communication. In plain language, all of your internet traffic will appear to be coming from and going to a location other than your true one. This means your activity will display a different IP address to the internet. The benefits are that you can appear to be active in other countries, circumventing some app restrictions, and all the traffic moving between your device and the proxy VPN server is encrypted.

For home usage, VPNs will deny your internet service provider any of your internet usage information, which is good for privacy. If using a VPN while traveling, anyone trying to snoop on your traffic will just see encrypted data. This is useful for open, unsecured Wi-Fi networks.

This is an example of protecting data *in motion*.

If your work provides you a VPN client, then you're set to work remotely, using your corporate network as the VPN proxy. If not, use a reputable one and remember that you get what you pay for. I tend to avoid making recommendations to my students, as I am not an expert on VPN technology. I just know what works for me and tell whatever stories that seem relevant to help them decide which they like. I have had good results with Mullvad, Proton VPN, and Private Internet Access (PIA).

Again, be aware that VPNs are not an anonymity solution, just a data security measure. Once your traffic has left the VPN server, it is still most likely encrypted using Transport Layer Security protocol (TLS), but as mentioned, the destination sites and servers still know it’s you.

USB Data Blocker

Also known as a USB condom, these handy gadgets slide onto your USB charging/data cable and add a data-blocking barrier, thus allowing you to plug in anywhere to charge and allegedly alleviate the danger of covert data access to or from the device. I recommend at least two in case one falls down the drain of your hotel's sink. I speak from hard-gained experience.

Faraday Bag

I didn't always recommend one of these, but the amount of data exfiltrated from mobile devices, even when idle, convinced me of their utility. If that weren’t enough, some sources purport that smart phones are not completely "off" when you turn them off, and places all over the world collect air interface packets from any device with a network interface controller in it (cellphone radio, Wi-Fi, Bluetooth, etc.). Also, many of us like to carry our vehicle key FOBs everywhere. After dabbling in some vehicle penetration testing and seeing how open they are to replay attacks, I now store my FOBs in a RF-blocking container. For travel, a Faraday bag big enough for your mobile phone and key FOBs is a good choice. Unless being actively used, keep them in there.

Mobile Device Best Practices

For mobile phone usage and settings, let's instill some small changes in lifestyle where that game of hangman is ever looming large in the background - I offer four very basic suggestions unlikely to leave a bad taste for mobile security and privacy:

1. If it is not in use and you don't need it on to receive communication, leave it off, preferably in your new Faraday bag. In fact, restart at least 1x per day for the health of the device and to burn off the less sophisticated malware.
2. Be aware of your Wi-Fi, Bluetooth, and Location settings; be deliberate about toggling them off when not in use.
3. Take a lunch break and review all your app permissions; ask yourself if that fitness app needs to know your contacts, or that email client needs access to your location.
4. Every app is another way someone like me can find you or even control your device, so be very, very stingy about the apps you have.

A Word on Malware

Recent news of Intelexa’s Predator spyware, the now defunct NSO Group’s Pegasus spyware, and other remote access trojans (RAT) for mobile phones is prompting a surge in awareness toward mobile device malware, but also fueling some paranoia from users. To be clear, your Threat Model will dictate how susceptible you are to being a victim of sophisticated spyware like those mentioned.

Low level malware, on the other hand, is typically less discriminate and will infect more devices. These are advertising cookies, automated spyware, stealer malware, and crypto-mining bots. Each of these will access and report most of your phone’s details to whichever third party controls the malware, with varying levels of intrusiveness.

The good news is that most of them can be burnt off of the device with a power cycle (restart). Since these common pieces of software operate at the application level of the device, not the kernel/operating system level, a power cycle will reset all applications back to a last-known trusted state. Advanced spyware like Predator and Pegasus operate at the kernel level, and will persist past a restart. These infections are only cured through a factory reset of the device, or in some cases, replacing the device altogether.

These are some quick steps to detect and mitigate most common malware:

1. Disable password, address, and credit card data storage, typically used for auto-fill, from mobile web browsers, then back up any that are stored to a password manager or other secure space and delete from your browser—this defeats stealer logs and spyware cookies
2. If the device runs hotter, uses battery much more quickly, or runs much more slowly than usual, perform a power cycle and confirm if the behavior continues—this indicates malware using your phone’s data connection to exfiltrate stolen data
3. Search for new or unknown apps and investigate them; remove those you do not know or need
4. If language settings change, GPS or locations displayed in other apps are false, or your search engine’s homepage indicates a location not your current one, perform a power cycle and confirm the issue is resolved—this indicates internet connections to foreign servers which alter your phone’s settings
5. If you receive warnings from accounts or services you use that login or password change attempts have been made, unknown to you, confirm the device making the attempt is possibly your mobile phone—immediately secure these accounts with password changes and MFA activation (if not already). Then uninstall any associated apps from your phone. In some cases, the damage may already be done if you had auto-login or no login security for the app in question.
6. If any of these events occur and mitigations do not work, perform a factory reset and do not use the device for banking, shopping, or sensitive activity until you no longer detect any of the malware symptoms. Meanwhile, be much more vigilant over your email inbox, online accounts, social media, and received phone calls/SMS, looking for fraudulent attempts to get your login credentials or pass any other sensitive data.

Hardening Tablets and Computers

First and foremost, I discourage medium- and high-risk travelers from carrying these while traveling if they don't need them for specific tasks. The potential for loss or seizure is high, especially when traveling through airports or border crossings, which we’ll cover later. Don't assume that Allied countries are not interested in your electronics either. My phones and laptops have been more scrutinized in Atlanta and Frankfurt than Baghdad and Kabul.

Every one of these requires a baseline of full disk encryption (Bitlocker, Filevault, etc). Now we’re protecting *data at rest*—if it is not being created, being consumed, or moving somewhere over copper, fiber, or airwaves, it is in storage, be it on your device or someone else’s. In those cases, we need to ensure it is safeguarded. Since Androids and iPhones now have full disk encryption (FDE) by default, we’re not as worried about those. Computers and some tablets may not.

Applying Encryption - Bitlocker for Windows

Windows Professional Edition offers Bitlocker, which is a very robust encryption program for your PC and laptop. You can apply Bitlocker to USB drives or external hard drives too.

- Hit the Windows Menu button and type “Bitlocker” – select Manage Bitlocker
- Options to encrypt an operating system drive and removable drives appear – if it is your personal laptop or Windows tablet I recommend encrypting the OS drive(s), but ask permission first if it’s an issued device
- Plug in your USB drive or external hard drive, wait for it to appear as an option under the Removable data drive = Bitlocker To Go list, and select the drive to turn Bitlocker on
- In the new Bitlocker Drive Encryption prompt, you may enter a new password or choose to use a smart card to lock/unlock the drive once encrypted – **KEEP THIS PASSWORD SAFE** and separate from the device itself
- Windows will present you with the Bitlocker *recovery key* to either print, save to your Microsoft account, or save on a separate device – this is your emergency decryption method if you happen to lose the password or the operating system is damaged somehow – **KEEP THIS KEY SAFE** and saved in a place no one else can access unless permitted by you
- You are now given a choice to encrypt only used space or an entire drive. Choose which ever option fits your drive; neither is better or worse
- Choose compatible mode for the encryption mode
- You are ready to start the encryption process

Bitlocker-encrypted external drives can be opened on Macs and Linux devices too, using the password you set.

Applying Encryption - FileVault for Mac

MacOS offers FileVault 2 in OS X Lion or later. When FileVault is turned on, your Mac always requires that you log in with your account password.

- Select the Apple menu > System Preferences, then click Security & Privacy
- Click the FileVault tab
- Click 🔒, then enter an administrator name and password
- Click Turn On FileVault

Follow the same advice as Bitlocker for your password and recovery key security. Since FileVault requires the admin password, you are in a sense killing two birds with one stone here by knowing the device password anyway.

Encrypting external drives using FileVault isn’t so easy; you’ll need to reformat the external drive to MacOS Extended (Journaled) file system, which means you either need a clean drive or have to save everything to a temporary space first, reformat and encrypt the target drive, then re-save everything back to it. Yes, that is a pain.

Applying Encryption – VeraCrypt for all Platforms

While the popular operating systems have their native options, a third-party application called VeraCrypt creates encrypted container on any drive, internal or external, on most operating systems out there. I’ll skip the step-by-step tutorial since the program walks you through the process pretty clearly, but here are some useful pro tips:

- Choose AES for your encryption standard as a default, but Twofish is another great option in case AES isn’t your jam
- Creating hidden volumes is useful if you are expecting device seizure or high threat of loss/theft, but is a more involved process

- As with Bitlocker and FileVault, **keep your password and recovery keys very safe, very secure, and separate from the device**

Out and About

Physical Security

Physical security is typically overlooked by digital security heavyweights. After all, I just want to know how to secure my internet from hackers—I already know how to lock my door and keep my car keys safely in my bag or pocket. Maybe, but I argue that it is inextricably linked to digital security in many ways. Your internet habits and wireless pattern of life can prove useful to someone who wants to find you physically. The less you give away on social media or to big data corporations, the harder that becomes for your adversary.

In more extreme circumstances, I present three scenarios that are common to U.S. travelers overseas, and government affiliates in particular.

1. Your device is lost or stolen while out of your possession – the bad news is that this phone or tablet is likely on its way to a chop shop to be dismantled and sold for parts on the internet. The good news is that your data protection measures, particularly that 6-8 digit pin, full disk encryption, and avoiding keeping sensitive items saved on it unprotected, will 99.99% of the time keep those data inaccessible. Nowadays only the most sophisticated software, or hardware manipulation, can retrieve data on modern, typically encrypted-by-default devices. If your location was turned on and you enabled your provider's find-my-phone feature, you may even get to track where the device is.

2. Your device is seized or otherwise taken by authorities at a security stop – this is a tough spot to be in, especially if the authorities start demanding you unlock your device for their inspection. Keep your devices turned off (in a cold state) when moving through security bottlenecks. If you keep them on your person and not in your bag, a bag search will mean nothing. If they require you to turn anything on and unlock it, refusal is fine but might delay you some hours. The point here is that pins and encryption might be defeated if your new friends put enough heat on you, and your next steps in life are dependent on how judicious you were with saving documents, photos, locations, contacts, and messages on the device. While most agencies won't take the time to manually investigate your phone or tablet, they may instead hook it up to a forensics collection kit and clone it. This gives them a searchable copy. If your device was never unlocked, this copy gives them very little. If you unlocked it for them, they can access most data on it.

That said, I have successfully forgot to mention one or two of my cellphones in a duffel bag side pocket when undergoing the occasional electronics inspection. A laptop is harder to overlook. If you must carry one, keep it as close to factory settings as possible. If you can get one issued from work, and they are aware of your travel plans, the one issued should be newly imaged and devoid of any sensitive data. If not, then I recommend the following three tactics, listed from least difficult to most:

1. Factory reset the tablet or laptop and carry a small USB drive with anything sensitive you'll need to do your job, live your life, etc. Use that drive as if it were the only storage you have. Before traveling again, stow the USB drive and repeat the factory reset for the computer.

2. Install a tool like Veracrypt and utilize the hidden container feature to store anything sensitive. Minimize clutter, apps, or anything else on the unencrypted user space. This reduces you from two to one objects to carry, and adds another encryption layer.

3. Same profile as 1, but have a bootable USB drive with your OS. Boot from it and operate on that platform each time. This leaves much less forensic data on the device.

These procedures require some learning and practice, and are on the more extreme side of operations while traveling, but keep them in your back pocket.

3. Your device is taken from you while unlocked and in-use – now a thief has your phone with almost no protections in place, unless you placed pin or password gateways on individual apps like your chat, bank, email, and (ahem) password manager. I highly recommend this when traveling anywhere, not just overseas. The market for stolen phones is lucrative enough that the common criminal has no time or care for reading your email and chat; they want to use the phone to buy things, access your bank and maybe steal some cash, find any personally identifiable info for identity theft, and scrap the phone for parts, in that order. An adversary looking to compromise a U.S. government employee is the opposite. They want your communications, pattern of life and travel, and contacts. With your phone unlocked, they can get most of this. Both criminals and nation-state adversaries would know enough to immediately disable your pin, biometrics, or other device lock feature, thus keeping the device accessible indefinitely. This is where those app-specific security features come into play.

- Remember your password manager with its very secure passphrase can also be used to store your contacts and sensitive notes
- Encrypted chat apps like WhatsApp, Signal, and Wire offer a pin or password unlock feature
- Many email apps offer that too, as well as social media apps, though I highly admonish against having any social media apps on your daily device when traveling overseas until you get well-accustomed to the area and can afford the distraction
- Banking apps universally require a pin or password to enter the app; make sure they are activated
- Most of the aforementioned apps support MFA too, and your MFA service (Authy, Google Authenticator, etc.) should be pin or password protected as well

Let's review—your phone was unlocked and you may have had an app open. If you other apps were pin or password-secured, and required MFA, plus your MFA app was pin-protected, then you have 2 more layers of defense on your data even if your device was unlocked. You stand to lose integrity and control of the device itself and one app you had open, but that is a far less steep hill to climb than losing control of all your apps on the stolen device. It's now time to take account of what could be compromised, and be diligent about changing passwords of what services may have been exposed. Change your phone number if needed, and alert anyone who may have the stolen one that it is, in fact, no longer yours.

To cap the physical security topic, avoid getting buried in your device while out in public. If you need to take a call, reply to a message, or check a map, stand or sit off to the side with a wall or fence to your back. Keep looking up and around to maintain situational awareness. Keep the device usage to a minimum as much as possible. Your appearance as an alert and resolute traveler will deter the vast majority of potential device thieves.

Public Wi-Fi

I default to mobile data (LTE, 5G) when not on a trusted Wi-Fi network. Successful attacks against mobile data are much rarer than against Wi-Fi. If you need to use public Wi-Fi, try to do the following:

1. No online banking
2. No online shopping
3. Use a VPN if available
4. Be very suspicious of any emails, SMS, or chat messages received asking to log into anything or pass any sensitive or private data—this is how attackers use unencrypted wireless data to craft convincing emails or messages to you and steal your data

Hotel Internet

When staying at commercial lodging during travel, most offer free Wi-Fi. Commonly you'll need to enter your last name and room number in a captive portal before getting to the internet. This is not real authentication, and talented attackers will get these names and associated room numbers uncomfortably easily. If given a password for the Wi-Fi, be aware that all the other guests likely have the same one and you are all sharing the same network.

I mitigate the dangers of these public networks with progressively more secure (and complicated) strategies. They are listed here from easiest and least level of security to most complicated but most secure:

1. Default to Ethernet—with your computer plugged into a RJ-45 port via an Ethernet cable, you mitigate the wireless attack surface. Leave your mobile devices on mobile data.
2. Use a VPN—your device is seen on the network, and through the captive portal, associated with your name and room number, but your internet activity is inside the encrypted VPN tunnel and protected from snoopers on the same network.
3. Use a travel router—these handy devices are small routers often with both Ethernet and Wi-Fi capability. If plugged into Ethernet, you have turned your hotel room into your own Wi-Fi network, complete with strong password, firewall, and VPN software if desired. There are some challenges, though, if the hotel requires a captive portal to access the web, and that may stop this strategy in its tracks. Here is how to possibly work around that:
    a. Log on to the network with your laptop and access the captive portal—do not do anything else with it yet.
    b. When past the captive portal, find your laptop's MAC address (they are different depending on whether your connection is Ethernet or Wi-Fi)—you can find the MAC address in your operating system's internet connection settings and will look like this, with each 'x' being a letter or number: xx:xx:xx:xx:xx:xx.
    c. Log into your travel router's administrator portal, and find the setting to change the router's MAC address—some models will offer a 1-click option to duplicate a connected device's MAC address. If so, choose the laptop you used to pass the captive portal and save yourself a step.
    d. With your router's MAC address the same as your laptop's, log into the public network with the router, and it should successfully connect—you have just spoofed a trusted device, using a "whitelisted" MAC address to bypass the hotel's poor authentication process.
    e. If this works, connect your devices to your router and enjoy your own personal network. While logged into the router's admin portal, lower the power output to the lowest setting, enable or disable guest networks, ensure the network's password is strong, and check if the router's firmware is up to date.
    f. If this does not work, fall back to strategies 1 and/or 2.

Rental Vehicles

Few people really think about it before they link their phones to a rental car's USB port and Bluetooth. The reality is that modern cars are very well connected, many having their own dedicated 5G cellular radio chains keeping the vehicle constantly talking to manufacturer and third party app servers. With the advent of Smart Cities, vehicular connections to wireless infrastructure will become much broader.

When you connect your device to a car, you may get prompts asking to allow access to calls, contacts, and messages. It is your choice to allow these for the convenience of hands-free operation, but bear in mind that these data now can be shared with those servers via the vehicle's cellular connections. If you use your phone for GPS navigation and integrate it into the vehicle's on-board infotainment system, those same servers now know your particular pattern of travel. Granted, connected cars already track and report location, speed, operating details, temperature, and many other factors, but now with your personal device linked and feeding GPS data, all these bits of information are associated with your identity.

This is not a huge threat for the typical rental car user, but consider the second and third order effects of allowing access to calls, messages, contacts, locations, and other app data, then leaving the vehicle at the drop off lot without forgetting your device and erasing the saved data from the vehicle's memory. For those conducting sensitive travel, this is a treasure trove of information about the renter.

While each car is different, it shouldn't take longer than a few minutes to navigate to and factory-reset the connected devices settings. A great resource to ease this process is Privacy4Cars (https://privacy4cars.com/personal-use/). To avoid this process altogether, consider the following strategies in lieu of connecting your phone to a rental car:

1. Use a standalone GPS navigation device, like a Garmin—I keep one specifically for travel and update the maps before leaving for trips.
2. If you must use the phone for navigation, keep an air vent clamp or dashboard stand handy to most easily view the phone's screen
3. To power and charge your devices, be sure to use the aforementioned USB data blockers to keep the charge flowing, but deny any data exchange between the vehicle's USB port and your device. A better solution is the 12 volt "cigarette lighter" port which most vehicles still have. You'll need a USB port adapter for it, which I advise as a staple for a travel kit.
4. Use a hands-free Bluetooth speaker for calls and music, sitting in the center console or the passenger seat (if empty).
5. If you don't need hands-free phone capabilities, but enjoy listening to music, audiobooks, and podcasts, consider carrying a 3.5 mm headphone cord while traveling. Bear in mind that some of the more modern vehicles don't have headphone jacks anymore. If this is the case, make sure that portable speaker from step 4 has one.

Putting It All Together

Some of this may seem too extreme or solutions looking for problems. That's understandable. I would agree that there is little need for much of what we've covered. The point of this digital device protection survey is more to give an idea of what's available to you if the needs arise. That decision is based on your threat model. If your life is anchored in a safe place where you live, work, and enjoy the company of friends and family, you may not need most of what we discussed. Now consider the Foreign Area Officer constantly uprooted to myriad cities to meet multitudes of unknown people from all over the world.

No one tactic is a one-stop turnkey solution of protection, but any combination of these measures build those layers needed to slow and stop your adversaries. Each one is another obstacle against your threats, and act as deterrence measures. No system or device is unhackable, but if I, as an attacker, run into enough countermeasures while assaulting your digital ecosystem, I may just give up and find a softer target. In other words, you need not be the fastest to outrun the bear—just not the slowest.

Having set up and used any of these tools and tactics is a good start. As you experience them and decide what works and what doesn't, learning is happening, and possibly some teaching. Be mindful that your digital protection profile and threat model are not universal; everyone needs a different plan and set of defenses. Once yours is in place and ever developing, guide others who may need it towards their defense plan.

Further Learning

About 25% of my time is spent on reading, attending webinars, watching experts' videos, and listening to podcasts. This is how I keep up with the latest news, best practices, and constantly alter my threat model.

Books:

Parker, Carey. ***Firewalls Don't Stop Dragons: A Step-by-Step Guide to Computer Security and Privacy for Non-Techies, 5th Edition.*** Apress, 2023.

- Easily the most accessible guide to digital security for the average citizen, and updated for most household tech up to 2023
- This is my top pick for those relatively new to enhanced digital privacy

Hypponen, Mikko. ***If It's Smart, It's Vulnerable***. Wiley; 1st edition, 2022

- This is not a tips and tricks workbook, but surveys the current technological landscape and dissects the dangers of data as a monetized commodity, data as a weapon against people, and awareness of your devices' handling of your data

Bazzell, Michael. ***Extreme Privacy: What It Takes to Disappear, Fourth Edition***. Independently published, 2022.

- This book is thick and intense; do not read it cover to cover, but rather reference it for specific topics on advanced-level privacy once you have a decent foothold on the basics

Podcasts - If you are an audio learner, these podcasts keep me updated on a weekly basis:

Hacking Humans. Bittner, David and Kerrigan, Joe

- https://thecyberwire.com/podcasts/hacking-humans
- This weekly show is my top pick, covering digital and phone fraud, scams, and social engineering tactics, while being lively and highly entertaining

Firewalls Don't Stop Dragons. Parker, Carey

- https://podcast.firewallsdontstopdragons.com/
- This is a companion show to the book, with weekly interviews with industry experts and the latest news; this is where I discover many of the digital tools I test and recommend

Security Now. Gibson, Steve and Laporte, Leo

- https://www.grc.com/securitynow.htm
- This weekly show is a long one, typically over two hours, but well worth the listen to stay on top of current trends in technology and how it affects our security and privacy

Contact Me

Feel free to send me an email if you have questions or feedback. I am also open to experiences with your travel, whether they are successes or failure, so that we can teach others.

richard.mcnally@us.af.mil

mcnallyusaf@protonmail.com

Thank you again for reading and taking a step to protect yourself in cyberspace.