Protecting your Identity

Overview

April 2021

Downrange Technologies

305 Harrison St NE
Suite 1B
Leesburg, VA 20175
joe@downrange.tech

Contents

Preface

Maintaining personal privacy and keeping one's information safe while online has never been more challenging. Bad actors can leverage online communities of interest to facilitate their schemes, malware and its delivery mechanisms are more sophisticated, and the constant evolution of computer hardware and software often leaves users struggling to remain technically proficient. That said, a few simple practices and a safety-conscious attitude can reduce one's vulnerability.

Chrome/Firefox + Adblockers (Adblock + Ghostery)

Web browsers represent 90% of a user's attack surface. The vast majority of work performed on a modern computer is done through a web browser. Web browsers, in their default configuration, can leak a significant amount of data to second and third parties (e.g. sites you visit and the partners of the organizations that host the sites you visit).

To protect yourself, you should use, at a minimum, plugins/extensions that control and limit the data being leaked by your browser. Every user should install and configure the AdBlock and Ghostery plugins.

- **Ghostery** is a plugin that blocks ads and trackers. It focuses on privacy rather than security. The purpose of the plugin is to block "trackers" which exist on every site you visit on the internet. For example, when you visit cnn.com, your browsing habits are passed on, via a tracker, to third parties. These third parties are mostly advertisers and they pay cnn.com for your browsing information. Ghostery blocks such trackers.
- **AdBlock** is a plugin that blocks ads and prevents some types of browser code present on the website from running on inside your browser. This plugin protects you from ads and tracking code, but also from security threats.
- **WebRTC Limiter:** WebRTC is a new protocol included in all modern web-browsers. WebRTC is used to facilitate real-time communications between browsers without the use of a third-party server. This functionality is extremely useful, but it comes with a major drawback. The WebRTC library can be called upon by a website and ask the browser to describe the network environment of your computer to the web browser. In a perfect world, this is to facilitate communications between two browsers, but it can be used to obtain information about the local network environment, namely, the private IP address of your computer. An attacker or adversary can use this functionality to defeat the privacy afforded by a VPN client/service. The WebRTC Limiter plugin allows you to control the information your machine sends to servers/websites when WebRTC is invoked.

Below are direct download links to these plugins, organized by compatible web-browser:

- Firefox

    - Ghostery: https://addons.mozilla.org/en-US/firefox/addon/ghostery/AdBlock: https://addons.mozilla.org/en-US/firefox/addon/adblock-for-firefox/Disable WebRTC: https://addons.mozilla.org/en-US/firefox/addon/disable-webrtc/
- Chrome
    - Ghostery: https://chrome.google.com/webstore/detail/ghostery-%E2%80%93-privacy-ad-blo/mlomiejdfkolichcflejclcbmpeaniij?hl=en
    - AdBlock: https://chrome.google.com/webstore/detail/adblock/gighmmpiobklfepjocnamgkkbiglidom
    - WebRTC Limiter: https://chrome.google.com/webstore/detail/webrtc-network-limiter/npeicpdbkakmehahjeeohfdhnlpdklia?hl=en
- Safari (Mac)
    - Ghostery: https://itunes.apple.com/us/app/ghostery-lite/id1436953057
    - AdBlock:
    - Disable WebRTC: You cannot disable WebRTC in Apple's Safari Browser. For this reason, we do not recommend using the Safari web-browser.
- Microsoft Edge
    - Ghostery: https://www.microsoft.com/en-us/store/p/ghostery/9nblggh52ngz
    - AdBlock: https://www.microsoft.com/store/apps/9nblggh4rfhk
    - Disable WebRTC: There is no way to completely disable the functionality, but you can tell Edge to simply not reveal your Local IP address. Directions below:
        - Navigate to "about:flags" using the address bar.
        - Check the box next to the "Hide my local IP address over WebRTC connections" option.

Spammers, criminals, and nation-state services use the same "tracking" methods to attempt to gain access to your system. AdBlock and Ghostery will not protect your system 100% of the time, but they offer excellent privacy and reduce your attack risk significantly.

There are numerous privacy-oriented web browsers. These browsers are popular and very effective, but often lack compatibility with powerful extensions and plugins. If you want to try your hand at a more privacy-oriented browser, I highly recommend the Brave Browser (https://brave.com/). It is based on the Chromium engine (which is what Google Chrome is based on) but adds numerous privacy features and turns them on by default.

VPN (ExpressVPN, TunnelBear)

A Virtual Private Network, or VPN, is a network service that allows a user to redirect their internet traffic through a third-party server to obfuscate their location from sites they visit on the internet. This protects your internet traffic from individuals on your local network trying to snoop or interfere with your connection, as well as prevents your internet traffic from being attributed to your physical location or device. There are numerous commercial VPN providers. The technology they employ is effectively the same, with a few differences:

- **User experience:** The quality of the software client and number of platforms it supports.
- **Exit points:** Better services have more servers in more countries, and with faster bandwidth.
- **Privacy:** When you use a VPN, you are sending all your internet traffic to a third-party and trusting them to not-retain or track you. Not all VPN providers are trustworthy. Some providers are in fact advertisers and their business model is to collect information about you and siphon off and log the information you send through their servers. Moreover, some are run by nation-states and our adversaries. Only a small handful of VPN providers are trustworthy, affordable, and reliable (see *Recommendations* below).
- **Cost:** A very low-cost VPN provider may intend to use your data for commercial or nefarious purposes. Beware of "lifetime" accounts or companies that do not publish Privacy or Retention Policies. The cost to run a VPN is somewhat fixed and the "loss leader" business model is not feasible. Likely, a low-cost VPN provider is using your data for profit.

Recommendations

Below are some recommendations on the best-in-class VPN roviders.

1. TunnelBear (https://www.tunnelbear.com)
    - Cost: $9.99/month, or $59.99/year.
        - You can get 500mb/month for free, but you still need to sign up.
    - Platforms: Windows, Mac, Android, iOS, Browsers
    - Based out of Canada, owned by a US Company (McAfee)
2. ExpressVPN (https://www.expressvpn.com)
    - Cost: $12.99/month or $99/year (3 free months boosts this to 15 months)
    - Platforms: All major platforms and many minor platforms, to include routers
    - Ownership:
3. PrivateInternetAccess (also known as PIA) (https://www.privateinternetaccess.com)
    - Cost: $6.95/month or $39.99/year
    - Platforms: All major platforms and most minor
    - Ownership: US-based
4. NordVPN (https://nordvpn.com)
    - Cost: $11.95/month or $95.75/year. Multi-year deals available.
    - Platforms: All major platforms and most minor
    - Ownership: Panama

5. Mullvad (https://mullvad.net)
    - Cost: $5/month, no annual plans.
    - Platforms: Windows, Mac, and Linux. No mobile app, but it can be made to work.
    - Ownership: Swedish, privately-owned

- **Note:** Each VPN provider has a different VPN Client and the user experience for each one is unique. There are some considerations to take into account when using a VPN on your mobile phone and when traveling.

Features to look for in a VPN Client/Provider:

- **Network Lock:** Block outgoing internet traffic when the VPN is down. This function helps prevent accidental spillage of user data when the user is unaware the VPN is temporarily unavailable.
- **DNS Privacy:** Use VPN-provided DNS servers instead of what your ISP offers. This is another way you can be tracked and is often overlooked.
- **Robust Locations:** You should use a VPN provider with exit-points in at least 10 countries. It is trivial to host servers in this number of countries and therefore a VPN provider with a small footprint is likely not mature.
- **Mobile Support:** Mature VPN providers offer support for mobile platforms, e.g. iOS and Android.
- **Payment Options:** If a VPN service accepts Bitcoin as a payment method, then the service is likely privacy oriented. If possible, avoid using a credit card, as this increases the likelihood for attribution*.
- **Logging:** Pay attention to what the provider says about their logging policies. If they do not make any statement at all about logging, i.e. about recording and retaining users' internet traffic, this is a strong indicator that customers' browsing data is being used for advertising or sold to a third-party.

There is a considerably complex discussion related to the attribution of online activity and the legal implications of using a VPN. If interested, conduct some research on "Warrant Canaries". Contact me for more information.

Testing your VPN

After you connect to the VPN, you should always perform a manual test to confirm that your VPN is working and protecting you. The easiest way to do this is to connect to a website that will show your public facing IP address is. The website IP Echo (https://www.ipecho.net) will give you, without any ads and in a very simple way, your public IP. This is the IP address that websites will see when you visit them.

The website IP Leak (https://www.ipleak.net) will provide a significant amount of information to you about your browser, including a good deal of unique information about your browser.

Webcam Cover

You should definitely be using a Webcam cover over any webcam on your devices. The best kind of cover is one you can slide open or closed to allow for use of the camera when needed. Placing a piece of tape over your webcam and removing it to use the camera is a fine alternative except that you may not remember to replace the tape when finished.

If you need a webcam cover, please contact me. I give these away for free.

Encryption at Rest (FileVault/BitLocker)

In the event your laptop, phone, or tablet is stolen, the information you have on the device will be protected only if you have previously encrypted it at rest. This means that the data is in an encrypted state when the system is off, or "resting". When a device is encrypted at rest, the data cannot be read by a third party without the password or key. If this feature is not enabled it is very easy for an adversary to steal data from your system or to install additional software without your knowledge. A technically savvy adversary could gain access to your unencrypted system and data within approximately three minutes if your laptop/phone were left unattended. Mac, Windows, iOS, and Android come with encryption at rest capability, but in most cases, it is turned off by default

Mac / Apple OSX:

On the Mac platform, the encryption feature is called *FileVault* and it is located in Settings > Privacy > FileVault. During setup, the program will ask if you want to store the recovery key in your iCloud Keychain or if you want it to be displayed/shown. This is a major decision.

- If you choose iCloud Keychain, anyone with access to your phone or other iCloud device can recover your key and use it to unlock your device. If you feel confident you can adequately lock down and protect those devices and accounts, you should choose the iCloud option.
- If you choose to have the key displayed, you will never be shown that key again. If the key is lost, you will not be able to recover your system if you forget your system password. If you decide to not use the iCloud storage option and instead use this second option, my recommendation is to take a photo of the key, print it, and store it in a secure place, such as a safe, where you would store other sensitive information.

Please see the included attachment entitled "*Turn on and set up FileVault on Apple OSX*" for detailed instructions on how to enable this capability.

Windows

Through its Windows operating system, Microsoft offers a reliable encryption at rest feature is called "BitLocker". To turn on BitLocker, you will need to be running Windows 10 Professional, and this is a paid upgrade. If you need help upgrading, please contact me. You can upgrade manually and instantly, and the cost to do this, via Microsoft, is $99.

Please see the included attachment entitled "*How to turn on BitLocker in Windows 10*" for detailed instructions on how to enable this capability.

Mobile Platforms

- **Android:**

On the Android platform the implementation varies based on the hardware manufacturer but the option for encryption is usually located in Settings > Security. If you protect your phone with a PIN, it is likely already encrypted.

- **iOS:**

A note about privacy, encryption, and TouchID and fingerprints:

Most modern devices now contain a feature that allows a device to be unlocked using a fingerprint. This functionality is advertised as very secure. However, there are two key details to take note of:

1. Your fingerprint is not protected by the Fourth Amendment. This means you can be compelled to unlock your phone with your fingerprint. Yes, your phone is still encrypted at rest, but if your phone is turned on it is not "resting" and therefore your data is open and can be unlocked with your fingerprint.
2. A PIN or Password is protected by the Fourth Amendment. This means that if you are stopped by authorities and your device is compromised or taken, the choice between volunteering access to your device to a third party or protecting yourself from an unwanted search would be in your hands.

The key point here is that when your phone is first turned on (Android and iOS are the same in this regard), you must input your PIN/Passcode for the device to continue to boot. The pro-tip here is this: If you feel your phone or device is in danger of being compromised or searched and you want to protect your data, **simply turn off your phone**.

Note: Encryption models on Android and iOS are very different. iOS offers the most robust encryption implementation (there are multiple layers of encryption vs. a single layer on Android). My

recommendation for all users who travel overseas frequently or who feel they are at risk of having their phones compromised or stolen is to use Apple devices.

Power States:

An important detail to know is that when you close your laptop, or your device goes to "Sleep," your data is still open and unencrypted. On Mac's and Windows-based laptops, there are at least four different power states, as follows:

- **Powered off:** Keys are safe and not in memory.
- **Sleeping:** When your system is powered on and then goes to sleep, your files are still open. This is important to note because the device is still responding to external events, such as someone inserting a disc or USB-device in the system.
- **Hibernating:** Slightly different than sleeping in that the device does not respond in the same way to external events, but some data is still held in memory.
- **Powered on:** Data is held in memory.

As the user, it is not easy to determine what power state your device is in, namely Hibernate vs. Sleeping. Why am I mentioning this? If you are planning on leaving your laptop unattended for any period of time, and someone not 100% trustworthy may have physical access to it, you should fully turn off your device while it is unattended. This ensures there is no open data on your system and the only external event it will respond to is someone pressing the power button.

Encrypted Backups:

If you are using Apple's Time Machine or Window's Backup functionality, you should always utilize encrypted backups. If you are doing everything you possibly can to secure your system, but you are making backups that are not encrypted, then an adversary only needs to steal your backup to get access to your data. The best practice here is to use an offline key, physically print it out, and then store that key in a secure place, such as a safe or safety deposit box. Note that without that key, a backup is useless both to you and an adversary. Therefore, don't lose the key!

Two-factor Authentication on All Accounts

Many services offer two-factor authentication and I cannot stress enough the importance of using this feature whenever possible. If a service offers the option to set up two-factor authentication, you should turn it on immediately.

Usually, the second "factor" in a two-factor authentication setup is a code, provided by a text message or an "authenticator" app. Whenever possible, use the authenticator app over SMS, as this

is significantly more secure than using a text message as a second factor. Text messages are not a secure method of communicating, especially while traveling overseas. Using an authenticator app means you can get that second-factor code while your phone is offline and/or not connected to the internet.

I recommend using the authenticator app called **Authy**. It is more powerful than Google's authenticator app because it allows you to back up your codes. If you upgrade or replace your phone, those codes do not carry over, and therefore creating a backup is a major timesaver. If you are already using Google's Authenticator, it is adequate, but if you upgrade your phone and need to start over, consider using **Authy** on your new system. Microsoft also has its own authenticator application. These applications can all be installed and run in parallel. You do not need to decide on a single app to store your 2FA codes.

Links

- Authy App
  - iOS: https://itunes.apple.com/us/app/authy/id494168017?mt=8
  - Android: https://play.google.com/store/apps/details?id=com.authy.authy&hl=en_US
- Google Authenticator App
  - iOS: https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8
  - Android: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_US
- Microsoft Authenticator
  - iOS: https://itunes.apple.com/us/app/microsoft-authenticator/id983156458?mt=8
  - Android: https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en_US

Below are pictures of what the above applications should look like in their respective "App Stores"

Authy	Google Authenticator	Microsoft Authenticator
		

Setting up Two-Factor Authentication

The common process for enabling two-factor authentication is as follows:

1. User logs into their account and goes to the "Account" or "Security" page, usually within Settings.
2. Starts the 2FA (two-factor authentication) enrollment process.
3. The website provides the user with a QR-code to be scanned into their Authenticator app, or
4. The website asks the user for their mobile phone number, and a text message is sent.
5. User enters the code and Two-Factor is then turned on.
6. At this point in the setup, if the website provides additional methods to set up, you should set them up now (backup codes, hardware dongle, etc).

Within the Authenticator app of choice, there is usually an "add a barcode" or "add a site" option, which, when selected, turns the phone into a camera and allows the phone to scan the code on the screen. Once this has happened, a six-to-eight-digit code is shown on the screen. This code usually rotates at some interval, usually around 30-seconds.

When the SMS option is enabled, a six-to-eight-digit code is sent to the number.

From this point, the user is required to enter that code into the website. Once that happens, the account is then protected with 2FA (two-factor authentication).

Providers do not usually allow users to add more than one phone number or device to an account but there is a workaround. If you have two people (or devices) that need to gain access to the second factor, you can register more than one phone using the QR-code **at the time of registration**.

Some Helpful Tips:

1. Practice what happens when you do not have your primary second factor available:
    a. Phone is off
    b. You have no cell service (flying, out of the country, etc)
    c. You are setting up a new phone
2. Make sure you have more than one backup method setup

Links to get started with Two-Factor Authentication

- Office 365: https://support.office.com/en-us/article/set-up-2-step-verification-for-office-365-ace1d096-61e5-449b-a875-58eb3d74de14
- Google: https://www.google.com/landing/2step/

Hardware Dongles

The use of a hardware dongle is much more secure than the use of an application. Dongles come in many configurations, including USB, USB-C, NFC, and Bluetooth. The following two hardware dongles (or "keys") are the most popular and secure.

- Yubico's Yubikey 5 series: https://www.yubico.com/products/yubikey-5-overview/
- Titan Security Bundle (Google preferred): https://store.google.com/us/product/titan_security_key_kit?hl=en-US

Google

Google offers an "Advanced Protection Program" whereby your second factor can *only* be a hardware dongle. This makes your account extremely secure, but it comes with limitations. For example, an account enrolled in the Advanced Protection Program cannot sign into to third-party websites using the Google Service. Secondly, users can only use Google-approved applications to use the Google services (such as Google Mail, Calendar, and Contacts). Lastly, accounts are difficult to recover in the event your hardware dongles are lost.

For more information, browse to the following link: https://landing.google.com/advancedprotection/.

Wireless Security at Home

I recommend the following best practices for wireless security at home:

- Ensure you are using WPA2-Personal encryption on your router and are using a key that is not easily guessed.
- Your router's firmware should be up to date.
    - Set your router to automatically update its firmware, if possible.
- Change your wireless key/password periodically. I change mine monthly, but every 3-6 months is adequate.
- If your router allows for a "guest" network, use it. This keeps guests from accessing any of the other devices on your network. If someone introduces a compromised device to your network, it is likely that it will attempt to access other devices on your network. Having a guest network prevents this type of activity from occurring.
- Do not use identifying information in your wireless network name. Wireless survey data with geotags are publicly logged and searchable online. If you name your network "SMITH-RESIDENCE" and someone wants to find your house, they can look for that name within a geographical area and find your address. It might seem far-fetched, but it happens.

Wireless Router Best Practices:

If you are using the wireless router provided by your ISP, it is a good idea to utilize your own router behind that router. Your ISP maintains access to your router, and they can see any device that is connected to it via wireless or hard wire. If you use your own router, then the only device the ISP can see is the router they provided. Additionally, the routers provided by your ISP are typically not that great. Usually they have only embedded wireless antennas and their performance is good-to-poor. If you are in the market for a good wireless networking system, I recommend Ubiquiti AmpliFi (link: https://amplifi.com/) or the Linksys Velop system (link: https://www.linksys.com/us/velop/). These systems include mesh repeaters/extenders that are easy to install and configure for good wireless connectivity throughout the home or office.

The Velop system should be used in environments which already have ethernet wiring within the building/house. Velop allows for the interconnection of the devices over ethernet, resulting in a significantly faster wireless speed.

Password Managers (1Password)

I cannot stress enough how important it is to utilize a password manager of some kind. Like VPNs, there are many password managers on the market, but their quality varies significantly. My recommendation is **1Password** because they are cross-platform and mobile-friendly. The passwords are encrypted at rest on their servers and their user interface is excellent. Unfortunately, their software is not free. However, once you use the application and integrate it into your systems, you will find the convenience of having all your passwords readily accessible, and each one unique and super-strong, to be worth the price. One can argue that putting all of one's passwords in a single place is a risk, and it is, but it's a much smaller risk than re-using weak passwords that are easily guessed and keeping them on sticky notes.

Using a password manager is good idea for the following reasons:

- Assists you with your digital "inventory" of your online accounts.
- Helps you identify passwords that are weak, used across multiple services, or have already been compromised.
- Let's you load other data in the manager, including secure notes, passport data, miscellaneous accounts, etc.
- Automatically captures usernames and passwords from websites when you log in. When it detects that you have logged in, it will prompt you to save the username and password, then will allow you to click a button to auto-fill those fields when you visit that site in the future.
- Includes numerous other benefits!

Keep your Software Up-to-date

You should keep all software up-to-date at all times. This is especially critical for the following software and hardware packages:

- All your web browsers
- Microsoft Office
    - Set it to Automatically Update and Install new versions
- Adobe Acrobat Reader
- Your Operating System
- **Your Phone**
- Any other software you use frequently

Almost all software has an *Automatic Update* feature. You should utilize this whenever possible. Look for it within your application's "Settings" option.

Backup your stuff!

A note about updating your phone:

Apple:

Over the last year or so, the stability of iPhone operating system updates has been terrible. The updates often introduce features that are unwanted and that modify the known/default behavior of the phone. This causes numerous disruptions to workflow and can be very irritating. My advice is as follows:

- When a minor upgrade/update is available, perform the upgrade immediately. Such updates are almost always security-related. An example of this is when you have an iPhone running iOS version 10.11.3 and the update is for 10.11.4.
- When a major upgrade is available, wait and perform the upgrade within a week or so. Usually, the upgrade is either a critical success or contains a bug that is immediately identified by the hundreds of thousands of users who upgrade immediately.
    - In this case, waiting a week or so usually allows Apple to release a patch to the update.

Android:

Android updates are much less frequent but are tested much more thoroughly. They are often released by your phone carrier and are done so in a staggered schedule. When you see an Android update, do it immediately. You can rest assured that it will not break anything. This is because the update is controlled by your carrier and not the phone manufacturer. In Apple's case, the carriers are not involved in the update process.

Lock Down Your Credit

If you have had your credit stolen or your identity information leaked, you can lock down your credit at each credit bureau. You can also lock your credit down proactively if you do not want others to be able to open new accounts in your name. Locking your credit profile prevents an identity thief from opening an account in your name or accessing your credit report (e.g. determining your credit worthiness). When someone attempts to open an account in your name, the vendor will usually do the following:

- Pull a credit report to determine your credit worthiness. Traditional credit monitoring services watch for this event, then call you to ask if you have requested a report.
    - If you say Yes, they release the report to the requestor.
    - If you say No, they deny the report and the person originating the request is notified.
        - This notification is often misinterpreted as having "bad credit", specifically by employees/sales people who are unfamiliar with how the credit reporting system works.
- If they deem you to be worthy, they will open an account and notify the credit bureaus so they can track the activity.

If you lock down your credit, you are stopping both of these events from happening.

When you first go to lock your credit profile, you will be required to set up an "Unlock PIN". This PIN is used when you want to unlock your credit later.

It is imperative that you set this PIN to something that cannot be easily guessed and that is not used elsewhere (See the section on *Password Managers*). Without that number, a criminal will not be able to open accounts using your identity. Also, if you forget your PIN, it is extremely difficult to unlock your credit. Not impossible, but very difficult. Usually this involves something being mailed to you, which could take at least a week.

The downside to locking your credit is the cost – typically $10 per bureau. Some bureaus do not charge you until you go to unlock your credit. The cost varies per state. Another downside is that

having a locked credit profile can be irritating when you are legitimately trying to do something credit-related, such as open an account somewhere or prove your credit worthiness.

Pro-Tip: If you lock your credit, and forget that this has happened, and then go to open an account, the representative may ask you to simply provide your unlock PIN. This process is not a "one-time unlock". It's a permanent unlock. This may or may not be appealing to you. Just know that if you do provide it to them, you will need to go back and lock your credit again.

The credit bureaus have made the function of temporarily unlocking your credit significantly easier. For example, you can now request a temporary unlock and your credit will re-lock itself on a specific date you choose.

I recommend going through this process for every individual in your household. Your family members' credit worthiness affects your credit, too.

Below are direct links to the three major credit bureaus' "credit freeze" pages:

- **Equifax:** https://www.freeze.equifax.com/
- **Transunion:** https://www.transunion.com/credit-freeze
- **Experian:** https://www.experian.com/freeze/center.html

Identity/Credit Monitoring Service (IdentityGuard)

Identity monitoring services provide a lot of useful information, including:

- Questionable activity involving your email address, usernames, or passwords;
- Sex offenders in your area;
- Credit score changes;
- General security news and notifications;
- If your email address has been seen in a data breach.

Some of these services also offer insurance, at no additional cost, in the event your information is compromised. This helps offset some costs in the case of identity theft.

There are free services that will monitor your email address in public data breaches. These are useful, cost nothing, and don't require a username and password. You simply give them your email address and they will send you a notification if they see that particular email address in a breach. Two popular free services are HaveIBeenPwned.com and SpyCloud.com.

Downrange recommends the commercial service *IdentityGuard*, specifically, the "Individual Total" plan. You can view and compare their plans at the following location: https://www.identityguard.com/compare-plans.html. The cost is typically $55 per year. This is the service recommended by the USG following the massive OPM hack which occurred in 2015. *IdentityGuard* also offer family plans.

Locking down your Utility Accounts

It is highly recommended you take inventory of any online account you have that controls or influences your basic utilities and household services. Examples include your power bill, internet/ISP account, cell phone provider, mortgage account, and banking accounts.

You should identify any and all accounts you have *or could have*, systematically log into each account, and then do the following:

1. Change your password to something unique, i.e. password not used on any other account, and one that is not easily guessed (See the section on *Password Managers*).
2. If possible, enable two-factor authentication.
3. Look for "Notification" settings, where you can be emailed/notified when someone logs into the account or makes changes to the account, such as changing a password or turning off service.
4. Ensure the email address associated with the account is protected by two-factor authentication.
5. Ensure any PIN number or "passphrase" (e.g. what is your dog's name) used on the account is unique and not easily guessed.

The important thing to realize is that the people who take customer support calls for these types of services are not typically security-oriented or well-trained. And they often hate their jobs or are simply not good at them. This means it is easy for a clever or determined hacker/adversary to socially engineer such support personnel to give them access to your account.

A well-known and highly effective attack vector is known as "SIM Hijacking". This occurs when an attacker calls or visits your mobile phone provider and requests a new SIM card, under the pretense that they are you and you/they have lost your phone. The provider issues a new SIM card to the user and thereafter all phone calls and text messages would be sent to their new phone. Consider the implication of SIM hijacking as it pertains to Recovery information on your accounts and two-factor authentication being enabled and using an SMS message.

In all of these scenarios, you may not be able to stop your adversary. But if you lock down your accounts adequately, or set up notifications and security settings, it is possible for you to identify and detect this type of attack ahead of time and then prevent it or shut it down quickly.

Anti-virus Services (BitDefender)

You need an anti-virus (AV) software suite. There are hundreds of AV vendors on the market. Mac does not come with a default anti-virus program. Windows comes with Windows Defender pre-installed. It is not terrible, but it is not comprehensive enough. I recommend **BitDefender** (https://www.bitdefender.com). Downrange Technologies is an authorized BitDefender Managed Service Provider (MSP) and we offer this software to our customers at a very steep discount.

There is no anti-virus for iOS, regardless of what you may read or hear. The iOS operating system does not allow an app to communicate with another app except through the iOS constructs. This means it is impossible for any app you download from the App store to introspect the operating system in any way. And because iOS is entirely closed, there is no way to introduce other software on the phone without significant technical means.

Android has several apps available, and my recommendation is **Lookout**. The cost for the Premium version is $30 per year.

Secure Messaging Applications

There are numerous ways for users to communicate using text messaging. Standard SMS messages are not encrypted and are easily intercepted by adversaries monitoring the network. Additionally, the network provider that is offering your phone's network service, regardless of whether that network provider is your actual carrier, can see your messages.

It is important to know that your phone has two channels by which it can communicate with a cell tower: The data channel and the voice channel (please note: this is a major oversimplification of a very complicated topic). Phone calls and text messages occur over the voice channel. This channel is easy to intercept, and the equipment needed to intercept such data is available on the commercial market. The data channel can also be intercepted but it is significantly harder to collect data on it.

Even if the channel is collected, most applications utilize encryption (SSL/TLS), making exploitation harder. Not all applications use these protocols.

Regarding Messengers applications, all "secure" messaging applications use a phone's data channel and offer some level of encryption. The key to these applications is how their encryption happens (i.e. the nature of the encryption algorithms) and where the private keys for the encryption are stored and generated. For example, WhatsApp generates keys on the server-side and then pushes them down to the client. This means that, yes, while the data is encrypted in transit, WhatsApp can decrypt the messages if they want or a hacker can break into WhatsApp and steal the keys.

There are only a handful of ways to properly secure text messages between you and another person. Apple's iMessage advertises a "zero-knowledge" model, meaning they cannot read the messages being passed on their network. However, we can only take them at their word because the iMessage protocol is private and closed source. The iOS Messaging application automatically determines if a user you are messaging also has iCloud and, if so, uses the iMessage protocol across the data channel. If the user does not have an iMessage account, then it sends a normal SMS message. You, as the user, can tell which type of message was sent to the user based on its color. iMessage's are shown in blue and regular SMS messages are sent in green.

For Android, the best secure messaging application is the Signal app. Signal uses very strong encryption algorithms and also generates keys on the client (phone). This means that while the messages pass through the Signal servers, they cannot be read by the people running the servers. Additionally, the application is open source and has been audited by third-party security organizations. The Signal app on Android also allows for seamless integration as the default SMS messenger on your phone, making it quite easy to use and replace your existing Messenger. Whisper Systems, the maker of Signal, have also released Desktop versions of the Signal application, so a user can perform secure messaging using their account without their phone. iPhone users who regularly text with Android users and wish to secure their messages should consider using the Signal app for such communications.

Threat Awareness While Traveling

There are a few important things to keep in mind regarding internet privacy while traveling:

- Using open wireless networks is a very risky behavior, but sometimes cannot be avoided. Use a VPN whenever you must use an open network.
    - A wireless network with a publicly posted key is equivalent to a wireless network without encryption.

- Always use a VPN when you are:
    - Using a network that is untrusted.
    - Using a public network of any kind.
    - Using a network that has no encryption.
    - Using a network that has encryption, but the key/password/passphrase is widely known.
- A VPN client's "Network Lock" feature can be your best friend or your worst enemy. Such a feature automatically stops all traffic from entering or leaving your device if you are disconnected from a VPN server location.
    - Know how to identify when it has been activated. If you don't know when it has been activated, you may think your internet is simply not working.
    - The feature is not found in many clients. When it is present, it generally works well.
- Make sure you have recovery information in your Google account.
    - Whichever phone number and/or email address, you have set up as your Recovery Contact Information, should also be adequately protected.
    - If an adversary has access to either of those resources, they can easily take over your account without your knowledge.
    - Most criminals will do this when they know you are not checking your email (usually while sleeping) so that any notification sent to you is not seen until later, or not at all.
- Use a PIN or TouchID on your phone.
    - Please go back and re-read the section about regarding privacy and the Fourth Amendment.
    - TouchID is an adequate security measure and provides ease of use for everyday operations on your phone. Simply put, you should understand the implications of this feature as it pertains to search and seizure.
- Understand the implications of encrypting your phone and laptop.
    - Remember that without the recovery key, you cannot recover the information on your laptop if you forget your system password.
    - Also understand the differences between *powered on, sleeping, hibernating, and powered off.*
- Use Signal/iMessage whenever possible. These applications are encrypted end-to-end and your messages are protected from adversaries with access to the network components between you and your message recipients.

Other security best practices:

- Avoid TOR. It is used mainly by criminals and offers no anonymization whatsoever.
- Use, or have available, more than one VPN provider. Network providers (ISPs/nation-states, etc.) do not like people using VPN, so they put blocks on the network to stop your client from working. Utilizing multiple clients means you have more than one way to connect. TunnelBear, ExpressVPN, and NordVPN are all good services.