Ten Day Security

V3.2025

Difficulty: Basic

This ten-step security guide provides recommendations and steps for improving your digital hygiene and personal cyber-security. At IntelTechniques we often work with clients and colleagues who exist in high threat environments and thus require more extreme measures to reduce their risk of compromise. For those teams and individuals our "extreme privacy" resources are appropriate, but for most people those advanced tactics would be excessive and unnecessarily complicated. This guide was originally created for friends and family, who want to improve their security without having to turn their lives upside down. These are recommended steps that most everyone should address if they have any concerns about privacy or digital security

This is 100% a game of prevention vs reaction. If you wait until a cyber-incident occurs, then it is probably too late to mitigate much of the damage. As someone who works with victims of cyber-crime daily, the damage tends to be long lasting and much more exhausting than the preventative steps listed here. Most cyber-attacks are broad spectrum, targeting those with weak or no defenses, so this is a game of just making sure you are not as vulnerable as the next person.

Although laid out as a ten-day exercise, take it at your own pace and spread out the work in a manner that allows you to be successful without feeling overwhelmed. Some may choose to power through everything in a day (this is not recommended), while others might pick away at it over a series of weeks. The goal is break security down into actionable steps. Bite sized pieces that anyone can work into their busy lives.

This not "all or nothing". If any step is a deal-breaker, skip it with the understanding that doing so may leave a vulnerability in place. We all have lives to live and it is understood that some of these methods may not work for everyone's lifestyle. This effort is about just making ourselves more secure, so any steps you do in this guide will help. Do not feel like you have to do any steps that you are not comfortable with. We are just giving you options and sharing advice based on our experience investigating cyber-crime. Privacy and security are very personal things so do what is right for you and your family.

If you finish these steps and find yourself wanting more, consider moving on to a more in-depth privacy campaign. Some find "disappearing" in the modern age of technology a rewarding long-term challenge. For those, I recommend Michael's most recent privacy book: Extreme Privacy: What It Takes to Disappear (5th Edition). This book and the steps in it are very, very advanced so only go down that path if you are ready for a challenge and/or have a particularly high threat model. For the rest of us, the following steps will put you well ahead of the crowd in regard to security and privacy. We always say that when hiking

in bear country, don't be the slowest runner in the group. We will never be completely invincible to attacks, but once you complete these steps you will have mitigated a good portion of the most common cyber threats.

In addition to our books we have several free guides available at https://inteltechniques.com/links.html. You are welcome to share these with colleagues, family, and friends. In particular, freezing your credit is a great defense against identity theft. Help your family and friends reduce their own attack surface. A great approach to privacy and security is to look at it like physical fitness. Just like working out and eating well, you'll gain the most from your security efforts if you make it long term lifestyle vs a short term obsession. We should never feel self-conscious about wanting privacy. It is not about having something to hide, it is about having something to protect.

The Most Common Attacks

- **Social Engineering –** This a component of almost all attacks. The perpetrator collects intel on you and your loved ones and then uses it to manipulate you via text messages, calls, or emails. It is the modern version of conning or grifting someone.
- **Phishing** – Be very suspicious of emails and texts that ask you to click on a link or open a document. The more accounts you have which show up in breach data (see Haveibeenpwned in the next section) the more phishing attacks you will face.
- **Credential stuffing -** Cyber criminals collect your old passwords from breach data and try them on all of your current accounts. This is why we should never use old passwords and never use the same password twice.
- **Ransomware** – This is a popular "payload" or malicious code delivered to your devices as part of an attack. If successful it encrypts your data and hold's it hostage.
- **Spyware or "Stealer" Malware** – Similar to ransomware but instead of locking your data, it collects your documents, photos, videos, etc. and sends them to the attacker. Some ransomware attacks do both and exfiltrate your files before locking them.
- **Extorsion. Doxxing, & Reputation Attacks** – Attackers collect your personal data and then either share it publicly or threaten to do so.
- **Zero Day Exploits** – This occurs when an unpatched device connected to the internet is exploited due to it's code or firmware being out of date.

Threat Model

Threat model is combination of how attractive of a target you are with the level damage that could be carried out if you are successfully compromised. Thus people in the public eye, military/law enforcement/government employees, and those who work in finance likely have higher threat levels. If you are in one of these categories you will want to complete most steps in this guide and possible more. Also note, people with unique names are much easier to stalk, so a unique name put's you at greater risk.

Exposure

Another important factor is how exposed you are. How easy is it for a criminal or other adversary to collect your personal data and then use it against you?

- Conduct reconnaissance on your online presence and identify all phone numbers, email addresses, and accounts (including social media) that are easily accessible to anyone using a search engine.
- Check your email addresses on https://haveibeenpwned.com/ to see a list of accounts associated with the addresses where hackers already have your passwords, which they have collected from breaches at the corresponding companies.
- On a trusted personal computer use our search tools (https://inteltechniques.com/tools/Search.html) to see where on the internet your email addresses, phone numbers, street addresses, family members, and social media are publicly listed. We are hunting ourselves so that we can see what potential attackers are likely to find. You may want to make a list of all the sites that expose your personal information, because later we will talk about trying to get some of that removed.
- Are the people in your life sharing your personal information? Most families have in them people who are over-sharers and who because they don't care about privacy are more likely to share your personal details online. This obviously increases our exposure and we may want to talk to these folks and explain our concerns.

Improving Your Privacy/Security in 10 Steps

- ☐ Start Your Security Journal
- ☐ Secure Your Passwords
- ☐ Secure Your Mobile Devices
- ☐ Secure Your Accounts
- ☐ Secure Your Computers
- ☐ Secure Your Network
- ☐ Secure Your Credit/Identity
- ☐ Remove Yourself from Online Databases
- ☐ Disinformation Campaign
- ☐ Inform and Assist Your Friends & Loved Ones

You may wish to print out this guide and use it as a checklist as you complete each phase of your privacy/security. Although this is the recommended order of progression for most people, feel free to lay out your own path if you wish. Also, we encourage you to do some of your own research. Multiple opinions and perspectives are always a healthy thing. We have also listed some recommended channels and resources at the end of this guide.

Ten Day Security - Day One

Start Your Security Journal

We are going to start off this effort by taking the time to make a solid privacy & security plan. The following steps may seem simple, but they will set us up for success as we move forward with more specific action items. This does not need to be complicated, and operational security always benefits from simplicity. Therefore, we will start out with a planning stage that should only take matter of minutes to complete.

Security Notebook

1. You will need a paper notebook or binder to store notes related to your privacy-security work. It does not have to be fancy and I do not like using electronic formats for such sensitive information.
2. Find a secure location to store your notebook and make sure it does not leave your home. In my case, I chose to use a simple Moleskin journal which lives in the fire-safe in my office. A three ring binder also works well if you intend to print out this guide and include it with your notes. I only work with this notebook in my home office and it never leaves that room. Make a strict rule regarding where this notebook will live and how it will be accessed. Paper is just about the most private method of data storage if it stays in a secure and private environment. This journal is for sensitive, infrequently accessed information so a secure, private location is the important thing. If you are questioning storing these details on paper, I can tell you from my LE experience, if your home is burglarized, they will be going after your prescriptions, cash, jewelry, and electronics, not your notebooks and journals. The likelihood of a digital compromise is exponentially higher than someone breaking to steal your physical notebook.
3. Find a reliable pen that will live with your journal and write your start date on the inside cover. Although this is specifically for our 10-day effort, many people go on to use this notebook as a long-term security journal.
4. This is also where I store additional sensitive information such as the configuration details and credentials for my home network and backup codes for accounts that support a master password or recovery key.

That is it, you are done with your first task. Step Two will be a little more involved, but we will use our journal throughout our security make-over, so it was important to establish a secure place to store our analogue notes. Just like our offensive intelligence work, taking the time to construct an actionable plan will reap rewards in both effectiveness and efficiencies further into the process.

Setup Secure & Private Email

Email is very important because most of our accounts use an email address as the control mechanism. It is how we typically reset passwords and verify authenticity for our accounts so we must have a secure and private email option. In this step we are going to setup a secure and private "control account". This is the email address we will use for anything important or sensitive, such as our password manager. We need to compartmentalize our secure email addresses so we will not being using this address for entertainment purposes or anything trivial. This is the address you will use for personal security and any sensitive accounts. Here are the recommended steps and considerations.

- ☐ Set up a free or paid tier Protonmail account. The free tier is enough for most people and although we typically avoid free services, Proton's free tier does not have any of the usual privacy trade-offs and they are very well vetted. https://account.proton.me/mail/signup
- ☐ Use a strong passphrase for this account save it to your journal.
- ☐ Set up MFA on this account. https://proton.me/support/two-factor-authentication-2fa and review Proton basics https://www.youtube.com/watch?v=K2vzs6Q39Zc.
- ☐ When you get to phase three use this address to setup your password manager.
- ☐ Proton also has a masked email feature which you can use to create temporary forwarding addresses. This prevents you from having to give out your real address to any contacts or businesses who are not completely trusted. https://proton.me/blog/hide-my-email-aliases
- ☐ If you get a paid tier account you also can create additional addresses. This is super useful for compartmentalization. For example, I can create one address that is just for finances and another that is used for sensitive utilities/services, such as my password manager or web hosting. This limits exposure and damage should one of your addresses be targeted or compromised in the future.
- ☐ When you get to the accounts phase later in this guide, you will move any important account over to this email address.
- ☐ You no doubt have current email accounts which you have used for years. Consider these un-secure but you may continue using them for personal correspondence and other non-sensitive communications. When you get to the accounts phase change your passwords on these older email accounts to something new and strong. At that time you will add MFA to these accounts as well when we get to that step.
- ☐ Compartmentalization is the key. We don't want to use the same email address to setup accounts as we use for personal correspondence or to sign up for other things online. I also avoid using the same address for finances and social media. Social media companies abuse and leak our addresses so the best case scenario is to have a few addresses that are each used for specific areas of your life: social, sensitive accounts, business correspondence, etc.

Ten Day Security - Day Three

Secure Your Passwords and Setup MFA

Weak and recycled passwords are the most common vulnerability for most people. A weak password is anything under 12 characters and a recycled password is one that has been used on more than one account. If you have not yet completed the video course, the sections covering passwords and breaches explain in detail why this step is so important. Our end goal is to have a unique long passphrase (something closer to 30+ character in length) for each of our accounts.

Password Manager

1. If you already have a password manager that you are comfortable with go to the corresponding website and review the privacy/security policies. Your existing password manager must support multi-factor authentication. Using SMS (a text message) for authentication is better than nothing, but the popularity of "SIM-jacking" or cloning cell numbers is a major weakness. Whenever possible using an authenticator such as Authy or the Google Authenticator is advised.
2. If you do not yet have a secure password manager, subscribe to one of the following. They are companies with good track records, which offer multi-factor authentication. The benefit of using a popular, mainstream manager is that the company has a lot to lose if it messes up and has a high level of resources to put into securing your data. Multi-factor authentication and heavy encryption are key. We always warn against using free products for security as they typically mine your data. If you wish to test a trial version of these products, they are an exception to that rule, although we recommend moving on a paid plan. Your security is worth it. Here are our recommended managers from most to least private/secure.
    a. Bitwarden https://bitwarden.com/
    b. 1Password - https://1password.com/
    c. Dashlane - https://www.dashlane.com/
    d. Keypass XC https://keepassxc.org/ (this is an advanced offline option)

    Note: Keepass is the most secure option in that it is well encrypted and offline. It is also free and open source. The downside is lack of convenience, such as no syncing feature. https://keepassxc.org/docs/KeePassXC_GettingStarted.html

If you are unsure of which password manager to use, Bitwarden is the best option for most people. It has all of the modern conveniences, with good security, and a solid privacy policy. This is what I use for my family, so it is fair to say that I trust Bitwarden.

3. Set-up your password manager based on security best practices
    a. Turn on multi-factor authentication (MFA or sometimes referred to as 2FA)
        i. Bitwarden – https://bitwarden.com/help/setup-two-step-login/

ii. 1Password – https://support.1password.com/two-factor-authentication/
iii. Dashlane – https://support.dashlane.com/hc/en-us/articles/202625042-Protect-your-account-using-two-factor-authentication#title3
iv. KeepassXC – Being offline, KeepassXC is much less dependent on MFA safeguards, but if you choose you add a YubiKey or other hardware key as secondary security measure https://keepassxc.org/docs/#faq-yubikey-2fa

b. Syncing your password manager to the cloud is not as secure as only using it offline, but for most of us "online syncing" between devices is necessary functionality. If you choose to enable cloud sync, ensure that you have MFA in place. Now install the associated extensions and apps on your browsers and devices. The reason we do not push harder for using offline password managers is that we have found that if your system for integrating password management is too cumbersome, most people will avoid using it which is much worse.
c. The master passphrase that is used to secure your password manager must be strong. Use a long phrase that has at least 20 characters. Example: Doritosworkwhenyurhungry#89 Write this master passphrase down in your security notebook (remember this is living at home in a secure location).
d. Some password managers will also allow you to generate and download a recovery key. Print this out and put it in your journal. This can be used to unlock your account if you get completely locked out.
e. Many modern managers, such as Bitwarden, will let you import and export your account credentials, which makes switching password managers easier.

4. Password Migration & Audit
   a. Collect your account logins from any current sources: other password managers, notebooks, post-it notes, etc.
   b. As you enter accounts, log into their corresponding sites, and update the passwords to "passphrases" using the generator in your password manager. Remember, a password is short, a passphrase is exceptionally long. The manager is storing it for you so there is no reason to use anything less than 30 characters unless the site hosting your account limits your options.
   c. Most password managers have an audit function where they will look at all your entries to ensure that no passphrases are repeated or too short. It is good to run this audit periodically to make sure all your accounts are squared away.
5. Multi-factor Authentication (MFA)

   As mentioned in section one, MFA is essential to protect your password manager so the master passphrase to unlock your password manager must

be reinforced by multi-factor authentication (sometimes referred to as 2FA which means specifically two factor authentication). In addition to your password manager review any critical accounts such as banking or social media and add MFA. Authy has a great guide on enabling MFA on various platforms https://authy.com/guides/. If you want to take it a step further, consider using a hardware key as your second factor, such as a Yubikey https://www.yubico.com/why-yubico/for-individuals/.

6. Passkeys

   Passkeys are a new credential management option available on most major platforms (Google, Microsoft, Apple, etc.). Passkeys allow you to use a system managed passkey instead of a memorized password. At a very basic level passkeys require you to be on a trusted device instead of having you type in your password. Are passkeys a good option? For most people yes, but we encourage you to do a little reading on the topic prior to using this option for your accounts.

   - https://www.eff.org/deeplinks/2023/10/what-passkey
   - https://bitwarden.com/passwordless-passkeys/
   - https://1password.com/product/passkeys
   - https://www.dashlane.com/blog/what-is-a-passkey-and-how-does-it-work
   - https://www.consumerreports.org/electronics/digital-security/should-you-use-passkeys-instead-of-passwords-a1201817243/

Note

This step can be laborious if you have not used a password manager before. If need be, take care of your most sensitive accounts first, such as financial, and then revisit less sensitive accounts in another sitting. Some sites, such as banking portals, restrict password length so you may need to adjust your password manager for those sites where they may limit the number of characters you can use.

Ten Day Security - Day Four

Secure Your Mobile Devices

Mobile devices are one of the biggest threats to our digital privacy. It is the ultimate surveillance device and it lives in our pocket. It has a camera, microphone, GPS tracker, personal photos/videos, our schedule, and contact information for every person in our lives. We need to limit access to the contents of our phones and also limit the phone's access to our critical and personal data. Consider disabling any new "AI" features as almost all of these upload our data to third parties.

Passcodes

Change your unlock/passcode to a stronger setting. Biometrics are not recommended because if someone steals your biometrics, you cannot get new ones.

1. iOS Passcode Settings
    a. Apple Account Passcode: Settings > Select your Apple ID at the top > Sign-In & Security > Check your trusted devices under two-factor authentication and consider updating the password for your apple account to something very strong (this is your Apple account passphrase, not your device passcode) if you change this put the old and new passcodes in your security journal and/or password manager. Consider setting up a recovery key which is an option in the same section. Put this key in your password journal.
    b. Now back in general settings update your device passcode: Settings > Face ID & Passcode > Change Passcode > Passcode Options > Custom Alphanumeric Code (this is the strongest option). You may be prompted with a security delay which requires you to wait for an hour or so before making changes.
    c. Write down your device passcode and your apple ID passcode in your security journal or somewhere safe.
    d. If you go into the Privacy & Security section of settings, there are some additional options you may wish to review. For example, turning on App Privacy Report will generate a report once a week detailing which apps are accessing your data. Reviewing "Location Services", "Tracking", "Analytics", and "Advertising" options would also be a good idea. Just look at each setting and use common sense. We're not making your phone impenetrable; we're just making it a little more private and secure.
    e. Consider going into the photos settings and turning off "Enhanced Visual Search". This was a feature that Apple quietly enabled which sends them our photo data.
2. Android
    a. Android has many flavors based on brand so there is no one set of steps for all phones. So if you had a Pixel 8, you may want to Google something like "Google Pixel 8 privacy settings to change".
    b. Remember that with the constantly changing security settings, the best approach is to go through every setting in the privacy tab: Settings > Advanced > Privacy
        i. The selections are logical, uncheck everything that shares data out and stop sharing your location, no personalization, no sharing of diagnostic data. Make sure to expand the "advanced" section to see options that are otherwise hidden.
    c. Delete any apps that you do not need and check permissions on any you keep. Most phones ship with extra garbage apps and we want to remove any

that we do not use if the phone lets us. Depending on manufacturer some apps may be locked so just remove what you can.

d. A good guide can be found at https://restoreprivacy.com/secure-android-privacy/

Device Settings

Apple is constantly changing iOS device settings with each update and Android settings may differ across manufacturers. That is why it is important to browse through all your device settings to familiarize yourself with the current options. Pay special attention to anything related to privacy, security, location, and applications. As you work through these steps, Apple may have just dropped an update that changes settings options, so it is a good practice to do an online search for recent articles. Browse to Duckduckgo.com on your privacy focused browser (Firefox or Brave) and search for "iOS security settings". Change the date filter to "Past Month" and the phone type to suit your situation. https://duckduckgo.com/?q=ios+privacy+setttings&t=hk&df=m&ia=web

Apps

The number one threat on most mobile devices are the apps, especially free apps. With few exceptions free apps are mining your data and selling it. One possible exception are apps that accompany a paid product such as a companion app or a "try before you buy" product.

1. Remove any unused or blatant privacy offending apps from your mobile device.
2. Review application permissions in your device settings and restrict data access as much as possible for any applications that you choose to keep. Top offenders often have access to contact, camera/microphone, and geolocation data.
    a. On iOS – Settings > Privacy > (review each data type: photos, contacts, etc.)
        i. Consider turning off Location Services completely. You can always turn it back on if you need to fire up Google Maps for navigation and then turn it back off again.
        ii. An article with additional recommendations: https://www.igeeksblog.com/how-to-change-iphone-privacy-security-settings/
    b. On Android – Settings > Apps & Notifications > Advanced > Permission Manager (review each data type to see which apps have access and toggle those permissions accordingly)
        i. An article with additional recommendations: https://tuta.com/blog/android-settings-increase-privacy

Ten Day Security - Day Five

Secure Your Accounts

As you work through your accounts, double check that you have updated passphrases and entered them into your password manager. Also make sure that you have enabled multi-factor authentication for any accounts that offer it. This effort can take considerable time so I like to triage my accounts by placing them into categories by

Social Media

1. **Remove Unwanted Accounts** - Properly close any accounts that you no longer wish to maintain, do not just abandon them. https://www.accountkiller.com/en/home or https://justdelete.me. If as site requires a written request, you can prepare something similar to the template at https://www.wonder.legal/us/modele/personal-data-deletion-request.
2. **Settings** - For your remaining social media accounts go into settings and review the privacy/security options. Like mobile devices, these tend to change over time, but most of the choices are intuitive, it's just a matter of looking at them periodically, which most people do not do. https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/
3. **Review photos & videos** – Consider removing images showing your face from profile photos as those are often public. Are there any photos on your account that unintentionally share private information, such as an address or other visual overshares in the background? Are there any photos that you would not be proud of if an employer were to see them?
4. **Friends** – Check your friend settings to limit who can see what and who can contact you. If only friends can message you, then an extortionist will not be able to send you that scam message.
5. **Social Media is Public** – Assume everything posted to social media will eventually become public. Social media is one of the first places that people will look to find information about you, whether for good purposes or bad. Criminals, employers, and acquaintances will all eventually scour through your online profiles, so always keep that in mind when posting and sharing personal information online. We not only want to reduce our attack surface but also control our online reputation.

Financial

1. Every financial account must have a strong passphrase and two-factor authentication enabled. If your financial institution does not support both functions, find a better company to work with.
2. You may wish to only save your most valuable account credentials in your offline security journal vs your online password manager. This is personal choice based on your own threat level and desired level of privacy/security.

Everything Else

For most people this will primarily be entertainment accounts such as Netflix, but also things like e-commerce. The possibilities here are far too numerous to list, but a good approach is to look at your password manager for an idea of what sites you might need to adjust your privacy/security settings. Remember that above all else, email accounts tend to be our most critical accounts as they often allow access and control over our other accounts. Secure you email, business, and financial accounts first and your entertainment accounts last.

Ten Day Security - Day Six

1. Secure Your Computers

Like our mobile devices, when it comes to personal computers, we want to limit who can access them and what personal details they collect. Think of it as your digital house: you want to keep strangers out and even if you invite someone in, you do not want them to be able to see straight into your shower. We need to keep malware out of our computers to avoid high impact threats such as ransomware and "stealer" attacks which can copy and exfiltrate sensitive data and documents from our workstations.

All operating systems

- Patch/update your operating system regularly. This reduces the chances of falling victim to a "zero day" exploit. https://en.wikipedia.org/wiki/Zero-day_vulnerability
- Be mindful of downloading files and documents from untrusted sources, especially those receive via email or found web sites. Remember, anything digital that is offered to you for free or that seems too good to be true, may contain malware.
- Every week run a full anti-virus scan with your scanner of choice (recommendations included in the instructions below).

Windows OS (PC)

Windows is arguably the least secure operating system and requires the most care to secure.

1. When you install Windows, uncheck any settings that give Microsoft your data. Consider NOT using a Microsoft account but rather create an offline login only. https://www.makeuseof.com/tag/complete-guide-windows-10-privacy-settings/. This becomes more difficult with each new version of windows as Microsoft attempts to force us into using their accounts, but not everyone needs to be this strict about their privacy. If you prefer to use a Microsoft account, that is fine, just understand that they are collecting telemetry on your behaviors.

2. If you are using a Microsoft account associated with your PC control what Microsoft collects: https://support.microsoft.com/en-us/help/4027945/windows-change-privacy-settings-in-windows-10 or for Windows 11 (every new version of Windows has worse privacy than its predecessor) https://www.howtogeek.com/893162/11-windows-11-privacy-settings-to-change/.
3. Anti-Malware - Windows has Windows Defender built in. Additional layers of protection can be obtained using Malwarebytes. This is my preferred paid option if you would like something more than Defender.
4. If you are using a laptop, full disk encryption is a must. If your laptop is stolen it will nearly impossible for the culprits to get at your data if you have encryption and a good laptop passphrase. Windows has Bitblocker built in and the wizard will walk you through encrypting your drives. Make sure to print and save any keys. https://support.microsoft.com/en-us/windows/device-encryption-in-windows-cf7e2b6f-3e70-4882-9532-18633605b7df

Mac OS

The good news is that Apple products tend to have better security and privacy out of the box. For friends and family who are less technical I generally recommend Apple products because they require less work to reduce your exposure. If you would like to take some additional steps to secure your Mac computer, you might consider some of the following steps.

1. System > Privacy & Security > Turn off Location Services
2. System > Privacy & Security – Check each app to see what it has access to and disable access to contacts
3. System > Security & Privacy: Photos, camera, and microphone; examine each category and remove access accordingly
4. System > Privacy & Security > Analytics & Improvements – disable all
5. System > Privacy & Security > Apple Advertising – disable personalized ads
6. System > Privacy & Security > FileVault – Turn on to Enable Encryption
7. (Optional) System > Siri: Disable Siri to reduce data sent to Apple
8. (Optional) Premium Anti-Virus https://www.malwarebytes.com/mac/
9. Apple Security Reference: https://www.apple.com/macos/security/

Linux

If you are using Linux as your daily driver you are likely already a power user with a higher degree of technical experience. Linux is a smaller target for things like Malware, but you will still want double check to ensure that your privacy and security settings are suitable for your specific needs. There are many, many different flavors of Linux so we will stick to some general considerations versus specific settings.

- Not all Linux distributions are created equally. Some distros such as Tails (https://tails.net/install/) and Qubes (https://www.qubes-os.org/doc/installation-

guide/) have good privacy settings out of the box, but they can be difficult to setup and use so we recommend them only for more advanced users.

- Pop!_OS (https://pop.system76.com/) is a pretty good option for using looking to balance privacy with ease of use. If I were new to using Linux I would probably start there and then move on to more complicated Linux operating systems in the future.
- When installing a new Linux operating system, pay attention to the options and be mindful about unchecking any "opt-in" information sharing such as location data or general telemetry. Once installation is complete, review all of your system settings, especially in the privacy, security, and power tabs.
- Linux builds often do not have anti-virus built in, so you may wish to install something like ClamAV, which is an open-source anti-virus program. https://docs.clamav.net/manual/Installing.html
- There are many different Linux distributions so your best bet for guidance is to look for an online guide for your specific flavor of Linux.

Backups

One of the best defenses against ransomware is to back-up your most valuable data to offline storage. I recommend backing up to an external hard drive and these can be fairly inexpensive these days. Use your operating-system's built-in backup functionality to save documents, photos, and anything else irreplaceable.

1. Windows - https://support.microsoft.com/en-us/help/4027408/windows-10-backup-and-restore
2. Mac - https://support.apple.com/mac-backup
3. Linux – One option is Rsync https://www.howtogeek.com/427480/how-to-back-up-your-linux-system/
4. Manual Backups – A simple option to backup just your files (not your operating system) is to copy any key directories over to external storage. Large external drives from companies like Western Digital are very affordable these days and can be used to manually backup documents, photos, videos, etc. each month or as often as you like.

Browsers

Browser security can be quite complicated so we were going to stick to some basic steps to make us a little more private and secure.

1. Chrome is powerful but probably has the worst privacy of any browser. Microsoft Edge isn't much better. Consider using Brave (https://brave.com/) or Firefox (https://www.mozilla.org/en-US/firefox/) for your personal browsing. Brave is built on the same code at Chrome but has all of Google's tendrils stripped out.
2. For each browser go to the menu on the top right and select settings. Go to the privacy/security tab and review all settings. Adjust anything that is using or shares your personal data or location.

3. Install a privacy addons: There are many browser extensions that can improve privacy. Our recommend addon is uBlock Origin (https://ublockorigin.com/) which blocks malicious code on webpages. Another popular option is https://privacybadger.org/.
4. If you are determined to use Chrome as your browser just know that using your Google account in Chrome is convenient, but a huge drain on your privacy as it is literally them building a profile of all your behaviors. Do what works for you but just know that Google collects everything.
5. Compartmentalize – You may want to use multiple browsers. For example, Firefox has better privacy so it might be a good fit for logging into your social media and other accounts. Then maybe you have Chrome on hand for anything that does not run well in Firefox. For example some meeting services such as Microsoft Teams may not run well in Firefox and this is because Firefox is more locked down.

Note: Compartmentalization is a key component of both security and privacy. We want to draw distinct lines between devices, accounts, and services used in different portions of our life.

Ten Day Security - Day Seven

Secure Your Network

Your mobile devices and your personal computers undoubtedly connect to your home network, so let's take some time to update our network. Out of the gate probably the most common two mistakes are:

- Buying a new router and leaving the default admin login. Don't do this, go in and change the credentials.
- Failing to regularly update/patch your router firmware. These patches often contain security updates to protect your device. Remember your router manages the traffic on your network so you really, really do not want it to become compromised by cyber-criminals.

Modems/Routers

Your modem connects to your internet service provider via cable, fiber, satellite, or cellular. Your router manages the traffic on your network. For some of you these are separate devices, but if you are using a single box supplied by a cable or fiber provider you likely have a hybrid modem and router in one enclosure. For security we are primarily interested in the router functionality as many ISP supplied devices will not easily allow you to access the settings of the modem functionality. So if you have one box that provides the internet for your home, it is likely a modem/router combo. Many all-in-one boxes also provide wireless, which we will cover in the next section.

Protecting your router:

1. Log into your administrative panel using the information provided when they installed your internet access. They will have given you an IP address which you enter into a browser to login. You must be connected to your network so using a home desktop or laptop is recommended. It will look something like 192.168.0.1 (although your numbers may differ). If you do not know the login, sometimes it is on a label on the back or underside of your router. If you bought your own router and never changed the default login, look up the default login for your routers make and model in a search engine.
2. After using the credentials given to you by your ISP or the credentials you previously setup to login, go to the administrative tab and choose to change the admin login. If it allows you to change the username from "admin" or "root", make it something unique such as "routercontrol". Next change the password from the default to a strong passphrase. Write this down in your security journal for safekeeping along with the IP address of your admin page. Hit save and it will likely force you to log back in with your new settings.
3. Again, on the administrative tab, go to the firmware section and have it check for updates. If any are available update your router and you will have to log back in once it is complete.
4. Next, we will secure the WiFi which will either have its own tab or on some units it is under "Status", "Setup", or "Wireless. Once there move to the next section for instruction on setup.
5. The browser page for your router admin control will be unique to your brand of router so the tabs, sections, and options will vary. If you get lost just google the make/model and look for a video or article explaining how to navigate the graphical interface.

Access Points (WiFi)

A wireless access point is how you connect to WiFi. This might be a function of your main router, or a second dedicated box that only controls wireless access. Either way the settings are the same. Most modern units will come preconfigured with a primary network and guest network. Often in cases of network intrusion, the suspect ends up being a neighbor or someone else in proximity to your WiFi signal (especially in apartment buildings).

1. **Primary Network** – this is for your trusted devices belonging to people who live in the home.
    a. On the setting tab change the "SSID" to something innocuous and unique. So, if the default is "Comcast WiFi", change it to something like "potato12_nomap". Putting _nomap on the end prevents Google from adding you to their mapping when the Google cars scan your neighborhood. Yes, Google cars are scanning your WiFi as they drive past.

b. Change the SSID so that it is not broadcast (make it hidden). By doing this you will need to enter the SSID manually when joining WiFi from a device. It is not completely hidden but is less publicly visible to strangers. You will no longer see it in WiFi lists on devices and will need to choose "Other Network" when joining for the first time. Security is almost always a trade-off with convenience.

2. Guest Network – This is for guests and untrusted devices such as IOT and security cameras.
    a. Repeat the above steps but name the SSID for this network something logical such as "potatoguest_nomap".
    b. This network provides internet access but somewhat inhibits connected devices from accessing your trusted phones and computers on the primary network. You do not want that cheap insecure smart thermostat getting hacked and being used to access your computers or phones.
    c. If guests complain about the extra steps to connect, they are welcome to use their own cellular connection. This also reduces the instances of children giving the login out to their friends.

Internet of Things (IoT)

Most home electronics now offer "smart" features and require an internet connection. These tend to be inherently insecure and are the most common source of compromise on a home network.

1. Avoid connecting smart devices to your home network, but if you must, put them on your guest network.
2. Consider putting these devices on an entirely separate router/access point to further isolate them from your primary devices and sensitive data. This obviously requires a little more trouble and skill, so if this is not an option just use your guest network for IOT appliances.
3. (Optional/Advanced) The best option, if you absolutely must use IoT devices on your network, is to install a firewall to monitor and control the traffic. This is not for everyone as it does require some technical experience and maintenance. If you do want to go this route, we recommend using a Protectli box and PfSense which are both covered in our Extreme Privacy (https://inteltechniques.com/firewall/) and you will also be able to find video tutorials online that will walk you through building a Firewall at home.

Additional Resources

1. https://routersecurity.org/checklist.php – Very detailed descriptions and additional steps for securing your network.
2. https://portforward.com/router-password/ - List of popular router brands, default logins, and instructions for resetting credentials.

Ten Day Security - Day Eight

Secure Your Credit

The best way to protect yourself from identity theft and other electronic fraud is to establish fraud alerts and/or a credit freeze with the major credit agencies. Keep in mind that a freeze may be a non-option if you have a forthcoming large purchase such as a home. A more in-depth guide can always be found at https://inteltechniques.com/data/workbook.pdf

Fraud Alert

Fraud alerts establish notification prior to the major credit agencies authorizing any significant line of credit. Anyone can get a 1-year fraud alert for free and identity theft victims can request a 7-year fraud alert.

https://www.consumer.ftc.gov/articles/0275-place-fraud-alert

https://www.identitytheft.gov/Know-Your-Rights

Credit Freeze

A credit freeze restricts access to your credit report; therefore identity thieves are prevented from opening lines of credit in your name. In some ways it is less valuable in that it lacks the notification on fraud attempts. Credit freezes are now free by law so you should not pay a third part to do them for you. You should freeze your credit with at least the three primary credit companies. Have your security journal handy as you go through this process as the companies will issue you pins that will be necessary when it comes time to later unlock your credit.

https://inteltechniques.com/freeze.html

https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs#place

https://www.optoutprescreen.com/

Government Sites

A recent criminal trend is the use of breach data to open federal IRS and state benefit accounts using your identity. One strategy to combat this is to "squat" your own Social Security Number (SSN) by opening an account before the criminals can. Most government systems will not allow two accounts with the same SSN. The obvious downside is putting information in another government database and having another login to manage. The IRS already has most of our information, so it may be worth it to go ahead and claim your account.

1. **IRS** – The IRS system is very particular about the phone number you use and will not accept VOIP or other virtual numbers.

https://www.irs.gov/payments/view-your-tax-account

2. **State Benefit Accounts –** (Optional) Use Duckduckgo.com to research the state employment benefits sites in your state. See what information they require to create an account. require. If they require only an address, SSN, date of birth, and name, it will be quite easy for someone else to use your identity to create an account. This was very common during COVID when cybercriminals impersonated people on state benefits sites to fraudulently request benefit payouts. You may want to consider signing up yourself to "plant a flag" on your social security number in the state system . Use a Protonmail or other secure email option, multi-factor authentication, and store any credentials in your security journal, but understand that government agencies are horrible at protecting your data, so expect the email address you use to become publicly visible. For this reason you may want to use a masked email address, which ProtonMail supports.

Ten Day Security - Day Nine

Remove Yourself from Online Databases

The process is often referred to as "opting out" and involves removing your personal data from online search engine results and data brokers.

Stalk Yourself

You need to locate the data so that you can submit removal requests to the correct companies. The following resources reflect how most "stalkers" will start looking for you. Refer to the online OSINT training if you would like to improve your research skills and bring them up to par with more sophisticated cyber-criminals.

1. Download/print the workbook: https://inteltechniques.com/data/workbook.pdf
2. Google your name and employer or name and city. Example search: "Jason Edison" AND "San Diego". The first page of Google results is your top concern, especially if anything lists your phone number, home address, or immediate family.
3. Use other OSINT tools and people search engines to search for your name, address, and phone numbers for publicly viewable personal data and associations.
4. As you locate information in online databases look up the sites in the workbook. If you find sites that are not listed, consider a duckduckgo.com search of: `sitename opt-out removal` for example: `whitepages.com opt-out data removal`
5. Create a new "burner" Protonmail.com email account and MySudo phone number for use in submitting opt-outs. (or your private email/phone number of choice)
6. Note your progress in your security journal. That is also where I like to keep any paper correspondence or printouts related to my privacy campaign.

Ten Day Security - Day Ten

Disinformation Campaign

This step is not one that can be completed in an afternoon and really it is more of a lifestyle change. A disinformation campaign is all about using the data-brokers' and marketers' own tactics against them. They are constantly mining and stealing our phone numbers, email addresses, etc. and we are going to start feeding them incorrect data. For any mass marketing or spammy information requests, we are going to give them one piece of real information matched with misinformation.

Example: Value Cards

If your grocery store requires a value card to get sale prices, request an application the next time you check out. On the application put your real name, but for the address and phone number use details from a library, post office, or other public building. Next time use an incorrect name and address, but a real cell number. The idea is that we are filling these sales databases with disinformation. One piece of real information is being submitted along with multiple pieces of incorrect data. When they resell my data, I don't want my real home address or phone number to end up online along with my name.

For any sign-ups that require email or phone verification, consider using a masked email service (simplelogin.io) or burner phone number (mysduo.com). Using masked or "burner" email addresses and phone numbers for anything likely to result in marketing or junk messages will start to become second nature. Typically we never want to give sketchy companies our real phone number or the email addresses that we use for important business, such as managing our finances. Ideally you will never give a company or random third party your real cell number unless you are purposely sharing it along with an incorrect name to create even more disinformation.

Important: We never use the complete details of another real person when associating disinformation with our identity. Using someone else's name, address, phone number, or photograph could be considered identity theft and a crime. We also never give fake details to government agents or use them to commit fraud, such as buying pharmaceuticals. The tactic described in this section is for coupons and signing up for deals, it is not for legally binding contracts or dodging legal responsibilities. DO NOT COMMIT FRAUD.

Ten Day Security – Extra Credit

Help Others Improve Their Own Security

Awareness is the single best weapon against physical and electronic threats. The weakest link theory absolutely applies to your digital life. We need to help our friends, colleagues, and loved ones up their security game for their own benefit, but also so they are not exploited as a point of weakness by our own adversaries. When we in Law Enforcement

hunt elusive fugitives, we are often successful in compromising them by way of someone in their life who has weaker security awareness. Criminals use the same tactic when targeting us. If they cannot get to you directly, they will exploit people in your social, professional, or family circle to gain access.

Map Out Your Circle

Your "circle" is the collection of people who have physical and digital access to your life. We always like to approach security efforts methodically, so it is useful to make a list of the people close to you, starting with anyone sharing your home. Try to put yourself in the shoes of a cyber-stalker bent on infiltrating your life. From that perspective, who are the individuals and groups that you would target as a potential point of weakness. Typical considerations are:

1. Everyone in your household, children, spouses, & romantic partners
2. Children, siblings, and parents with separate residences (i.e.: daughter away at college, sister in another state, and so on)
3. Roommates and close friends
4. Close friends (especially those associated with us on social media platforms)
5. Co-workers and colleagues (again shared social media increases their likelihood of being a target)
6. Groups – Sports teams, clubs, school associations, and other interest groups

We want to raise the level of awareness amongst the people close to us. Do not be pushy and provide them with practical examples of common threats. Cyber-crime and other threat vectors are very much in the news which works in our favor. Talk about the best practices listed in previous steps and make yourself a resource. Above all else, please teach your loved ones to listen to their instincts. If something feels wrong, it probably is.

Keep Learning

Read books, join online security-privacy communities, listen to podcasts, and stay updated on the latest trends and threats. Like all efforts, the most benefit is realized when you make security and privacy part of your lifestyle. Make a game of it and challenge yourself and your family to give away as little of your personal information as possible. Keep in mind that it is a marathon, not a sprint. At times you will feel frustrated and overwhelmed but just take a break and come back to it once your batteries are recharged a bit.

Ten Day Security – Checklist

Tracking Your Progress

Some items are not steps that you truly "finish", such as the misinformation campaign. Mark these complete when you feel satisfied that you have successfully started down that particular road and then settle into a routine of picking away at it when you have time. Any "all or nothing" approach is the enemy and we want to have a mindset of doing what we can and ending up better off than when we started. You will never truly be done working on your security and privacy, but you can be in much better shape than just about everyone you know.

Consider printing out this guide and including it in your security notebook. You can find our other privacy/security guides at https://inteltechniques.com/links.html. This resource page is open to the public so you may share it with colleagues, family, and friends. Attackers often go after the people in our lives so it is a bit of a "weakest link" situation. Helping those close to us also improves our own cyber-resilience.

	Task	Date Completed	Notes
☐	Security Notebook		
☐	Password Manager & MFA		
☐	Mobile Device Settings		
☐	Accounts		
☐	Computers		
☐	Network		
☐	Credit Freeze		
☐	Online Data Opt-Outs		
☐	Disinformation Campaign		
☐	Help Loved Ones		

Additional Notes: