Good practices

Information security is the ever evolving process of using the best tools at your disposal to protect your data. Privacy is about having control over how that data is stored, used, or shared.

What follows is a list of measures you can consider adopting in order to better address these important aspects of your life in the information age.

Index

1. Software updates

Software is complex, flawed, and ever evolving.

One of the most important things you can do to protect your information is to keep your software (like your apps and operating systems) always up-to-date, making sure at the same time they are recent enough to still be supported by their developer (it being an indie developer, or a big company like Facebook, Apple, Microsoft, Google, TP-Link, and Samsung).
By doing so you'll not only make sure that you have access to the latest features and fixes, but that you'll also be running the most secure version of any given software product, at any given time.

Keep in mind that it's not only your phone, tablet, laptop, and desktop computers that rely on software updates and firmware updates to function securely, improve over time, and introduce new features. Routers (which are at the heart of any local area network like your home network) and IoT devices such as smart speakers, lights, fridges, doorbells, TVs, TV remotes, etc. also rely on regular updates for the very same reasons.

In the words of EFF's Gennie Gebhart (which I edited for clarity): "All code is sketchy, some code is just less sketchy than other. Running on your devices there's a lot of code and it has problems in it. It is written by humans and humans make mistakes at some point. You have (ideally) teams of engineers constantly working behind these OSes and apps to find the mistakes and fix them. All they need you to do is click "Update" and maybe restart. If you don't do that, that means that there is a way out there to exploit your device or your software that the world kind of knows about. Until you click "Update" you are easier and cheaper to hack."

2. PIN

You can help avoid other people having access to your personal data (as well as the personal data the people in your life might be sharing with you) by setting up a unique PIN (sometimes referred to as a passcode) on each of your devices.
Think about the personal information you're storing on them (things like notes, contacts, private conversations, photos and videos, web browsing history, etc.), as well as the personal information accessible through them (things like files uploaded to cloud storage solutions, email inboxes, financial information, and your other online accounts). You probably wouldn't want all of this to be left unprotected every time you leave one of your devices unattended, or in the event you lose one of them altogether. The people sharing personal information with you probably wouldn't want this either.

Once you're using a PIN, it might be possible (based on the device you're using), to set up some form of biometric authentication. In this case you'll also be able to unlock your devices by way of scanning parts of your body such as your fingerprints, your face, or your iris.
This can help you make the action of unlocking your devices quicker and easier while at the same time empower you to use PINs that are stronger and to reduce the time window between when you lock your devices and when a PIN or biometric factor is required to unlock them (since the friction of having to frequently type your way into your devices will no longer be there). It can also help you keep your PINs private when using your devices in font of other people (such as in public venues) or in places employing video surveillance.
If for any reason biometric authentication is not an option for you, consider changing your PINs either regularly, or upon indication or suspicion of compromise.

A good way to go about creating strong, unique, and memorable PINs is using passphrases composed using the Diceware method or similar methods.
Many password management solutions (more on this in the Password manager chapter) include a password generator able to generate those for you. This is the quick way.
Alternatively you can get some dice (ideally five, but one will also do), a word list like this one from the EFF or these ones from Arnold Reinhold, and then pick one of the following

guides on how to proceed:
• How to Make a Super-Secure Password Using Dice / EFF
• EFF Dice-Generated Passphrases / EFF
• Passphrases That You Can Memorize — But That Even The NSA Can't Guess / The Intercept

A note: You should not (in most cases) share your PINs with other people.

3. Device encryption

You can turn on device encryption on both your devices' internal storage and on any other external drives you may be using (such as SD cards, Hard Disk Drives, Solid State Drives, and USB flash drives) to make it harder for anyone to extract data from them.

Data stored in iOS devices like iPhone and iPad can be easily encrypted by setting up a passcode (optionally coupled with TouchID or FaceID).
A few Android devices (such as ones in the Pixel line and some in the Nexus line) are encrypted by default. Users should also be able to enable device encryption on most 3rd-party Android devices by visiting the Security (or Security & Location) section of the Settings app.
Windows devices can be encrypted using the built-in BitLocker feature (available to consumers as part of Windows 10 Pro, but not available to Windows 10 Home users), and macOS devices can be encrypted using FileVault, a feature that is part of the OS and available via System Preferences.

Keep in mind that encrypted devices might need to be powered down for the data they contain to be fully encrypted.

Here are a few resources, if you need a little help:
• How To Encrypt Your Devices / DuckDuckGo
• How to Encrypt Your iPhone / EFF

4. Find my device

You can turn on features such as Find My Device (available on Windows and Android devices), and Find My iPhone/Mac (available on iOS and macOS devices) to have remote access to at least some of the following actions and information (the availability of which may vary based on the type of device in question):
• Locate your device on a map.
• Remotely make your device ring (even if set to silent).
• Remotely lock people out of your device and display a custom message on the screen.
• Remotely erase all the data stored on your device.
• Protect your device from being used by people other than you even after being reset to factory settings.

Note that by enabling this you will be regularly sending your location information to a company such as Microsoft, Google, or Apple (depending on the device in question).
You should therefore balance the benefit of locating your devices and remotely erasing the

data stored on them, with your willingness to disclose such personal information to a third-party.

Keep in mind that this is not the only way your devices may be broadcasting your location. Mobile phones transmit this kind of information to mobile network operators as a matter of course, for instance.

5. Password manager

You can use a password manager (which is an encrypted vault) to drastically improve the security of your accounts and make the whole process of managing such sensitive information easier.

Well-regarded options when it comes to choosing one are:
• 1Password – Downloads page, Beginner's guide
• LastPass – Download page, Beginner's guide
• KeePassXC – Download page, Beginner's guide

Start using a password manager means you can start randomly generating long, complex, unique passwords and not have to worry about remembering them.
Picture a string of 30+ characters (or as many characters as you want, really) made up of randomly generated letters, numbers, and symbols: That's a password! 123456, dictionary words, movie titles, dates, etc. are not passwords…
You can approximate the strength of your passwords at PasswordSecurity.info

Password managers usually come with the ability to copy/paste things like usernames and passwords and in some cases to auto-fill them where needed as well.
One thing that could make the overall experience even more convenient on your tablet, laptop, or desktop computer is a password manager browser extension, which password managers also usually provide. Look for it in their various download pages, or in your web browser's extension store.

Creating and maintaining an encrypted and possibly well organized list of all your accounts' information (and any other kind of sensitive information you might want to store there) is a big plus for both security and convenience.

Even when using a password manager you'll probably need to create a few strong and memorable passwords for things like your password manager's master password and maybe a few of your main accounts. A good way to go about facing this issue is (as mentioned in the PIN chapter) using passphrases created with the help of the Diceware method or similar methods. Hop there for more information about this.

Even though a password manager is the best solution for most people, there will be cases in which (for whatever reason) a software solution is just not viable.
If this is you, keep in mind that managing your credentials with a physical password book that you keep someplace safe might still be better than not managing them at all.

Once you've set up strong and unique passwords (or passphrases) for your accounts, you're pretty much done with them. Companies and services that follow modern security practices should only require a password change upon indication or suspicion of compromise.

A note: You should not (in most cases) share your passwords and passphrases with other people.

6. Multi-Factor Authentication

You can enable Multi-Factor Authentication (Two-Factor Authentication, 2-Step Verification, etc. are all forms of MFA) to improve over sign-in processes that only require you to provide username and password.

You've probably already used some form of MFA before. If you own a credit card when you go to an ATM you put in your card, and then you provide a PIN: that's MFA!
These factors are generally something you know (like a password or a PIN), something you have (like a phone or a credit card), and/or something you are (via a fingerprint, face, or iris scan).

The flavors of MFA available (as well as how such features are referred to) usually varies from service to service (if they support MFA at all, that is).
This means that even though any kind of MFA (even SMS, an easy to social engineer, spoof, frequently non-verifiable, insecure channel) is usually better than no MFA at all, you might not have much of a choice when it comes to picking the method that best fits your needs. It also means that in your quest to MFA All The Things very similar things will have pretty different names.
Here's some help: Turn On 2FA

In the case of the online companies and services that do offer MFA (such as Facebook, Twitter, Google, Microsoft, etc.) the second factor is usually a one-time verification code delivered to your phone (something you have) via SMS, or generated by a software token (a code generator app) installed on your phone (again, something you have).
Less frequently you'll also be able to use a hardware token like a YubiKey that you'll need to physically plug into the device to log in. This is currently (as far as I know) the most secure option currently available.

Popular software tokens are LastPass Authenticator, 1Password, Microsoft Authenticator, Google Authenticator, FreeOTP, and Authy.

The fact that you'll have to demonstrate not only that you know your log-in credentials, but that you also have access to the device you've set up MFA with, significantly increases the security of your data against all sorts of attacks.

Here are a few resources that can help you choose the MFA method that's best for you:
• Decoding two-factor authentication: which solution is right for you? / Access Now
• A Guide to Common Types of Two-Factor Authentication on the Web / EFF
• Two passwords are always better than one / Jessy Irwin

PS: Apps like WhatsApp (More info here) and Telegram (More info here) offer MFA features as well. Consider enabling them!

When enabling MFA, you'll likely be prompted to save one or more recovery codes or backup codes. Those will allow you to get back into your account in case you lose access to your MFA device. Make sure you keep them safe in your password manager, or somewhere else that is safe.

Keep in mind that no matter how layered your security approach is, your accounts' security are only as strong as your "I forgot my password" settings are. That is to say that you might want to check those out as well…

7. Secure communication

You can prioritize the use of end-to-end encrypted communication tools like Signal (Beginner's guide), Wire (Beginner's guide), WhatsApp (Beginner's guide), or ProtonMail over less secure options such as regular email or phone calls, Facebook Messenger*, Telegram*, Skype*, WeChat, and SMS to help make sure (to a reasonable degree) that only you and the people you want to communicate with have access to the information you share. No third-parties like Facebook, Google, Microsoft, rogue employees, governments, or malicious actors will be able to access your conversations.

End-to-end encrypted communication services usually rely on a technology called public-key cryptography, where a public key and a private key are assigned to every user.
When someone sends a message to someone else (or a voice message, or an attachment, or a voice/video call, and so on) that data is encrypted locally on the sender's device using the recipient's public key and is then sent over the Internet to the recipient, where it's decrypted locally on their device using their private key (which, as the name suggests, is never shared). Voilà!

Public keys can also be used to make sure any given conversation is end-to-end encrypted and to verify that the person on the other end is really who they say they are.
Various services refer to this feature in different ways: Signal calls it Safety Number, Wire calls it Key Fingerprint, WhatsApp refers to it as Security Code, and ProtonMail as Address Verification.

In the case of WhatsApp you should consider enabling security notifications to make sure you're notified if your contacts' Security Code changes, disabling non-encrypted cloud backups (which as a feature defeats the entire purpose of providing end-to-end encryption in the first place), and understanding if you're comfortable with the amount of information WhatsApp (which is owned by Facebook) is able to collect about your activity (also known as metadata). This include things like who you are, where you are, who you communicate with and when, and how frequently you do so.
Signal, by contrast, has a much stricter privacy policy, various privacy-focused features (such as encrypted profiles, private contact discovery, and sealed sender) and an overall stronger commitment to transparency and accountability.

ProtonMail provides both end-to-end encryption and zero-access encryption. While someone's ProtonMail inbox is always protected with zero-access encryption (meaning no one except the user has access to it), the availability of end-to-end encryption depends on the email services used by all the people involved in a conversation. The easiest way to make sure your email correspondence is end-to-end encrypted is making sure all parties involved are using ProtonMail.

Here are some additional resources and articles you might want to take a look at:
• Secure Messaging Apps Comparison / Mark Williams
• Secure Messaging? More Like A Secure Mess. / EFF
• Where WhatsApp Went Wrong: EFF's Four Biggest Security Concerns / EFF
• Why I told my friends to stop using WhatsApp and Telegram / freeCodeCamp

* Facebook Messenger's Secret Conversations, Telegram's Secret Chats and Skype's Private Conversations features can be used to setup end-to-end encrypted communication channels with people, but being those opt-in features that are disabled by default means that users have to be aware of them and enable them for specific conversations on a specific device to benefit from actual private conversations.

8. Web security

A big part of web security is HTTPS (the secure version of the Hypertext Transfer Protocol, or HTTP).

When connected to a website over HTTPS you can be sure that the site in question is really who it says it is (proof of identity), that the exchange of information between you and that site is protected (confidentiality), and that the data flowing back and forth is not tempered with (integrity).

HTTPS improves upon HTTP in all sorts of ways. Unsecured webpages can and are used by malicious actors, governments, and ISPs around the world to:
• Gain access to the unencrypted data flowing between users and the webpages their're visiting.
Think again before typing login credentials, credit card information, or any other kind of sensitive or personal information into a page that is not secure. Keep also in mind that any unsecured webpage you visit can represent valuable information for ISPs able to use or sell personal information for advertising purposes, or for governments engaged in mass surveillance.
• Do targeted censorship.
In the case of secure webpages everything after the "/" (forward slash) is encrypted. This means that if you visit any Wikipedia page all a potentially malicious actor can see is: https://www.wikipedia.org. This also means that a repressive government (or an unregulated ISP) has to choose between blocking Wikipedia entirely, or not blocking Wikipedia at all. In the case of HTTP pages though, a malicious party could potentially censor pages in a selective manner, and even change the content of such pages.
• Alter the content of webpages in all sorts of ways and for all sorts of purposes.
This malicious behavior can range from injecting ads, malicious links, whole sets of UI controls (yep!), or completely replacing the content of a page (essentially blocking it), to

altering the content of pages with the purpose of redirecting traffic (something ISPs seems to be doing A. LOT), installing malware, or spreading phishing attacks.

You can make sure you're not on an unsecured website by keeping an eye out for the address bar: If you see a "Not secure" warning or you DON'T see a padlock icon , then the website you're visiting is served (at least in part) over a connection that is not secure. If this is the case you should avoid entering any private information on that website and, if possible, try not to use it in the future as well.
Some websites may be available both via unsecured HTTP and secure HTTPS. Browser extensions such as EFF's HTTPS Everywhere (which requires sites to use HTTPS whenever possible) can help here.

Keep in mind that in some circumstances the act of visiting a webpage could be in itself considered very personal information and that just because you deleted your info from a search box, an online form, or any other type of input field before submitting it doesn't necessarily mean the website in question has not logged what you entered anyway.

Also: The fact that a page is secure doesn't necessarily mean it is also safe.

Here are a few additional resources you might want to check out:
• How HTTPS works / DNSimple
• Here's Why Your Static Website Needs HTTPS / Troy Hunt
• Does my site need HTTPS? / Matt Holt
• HTTPS Is Easy! / Troy Hunt

9. Privacy settings

The apps and services you use come with a set number of default settings. Those can include permissions that grant the apps you use access to things like your camera, microphone, or geographic location; as well as settings that let companies like Facebook and Google access your personal data to target you with ads.

Since in many cases security and privacy do not come as the default, consider exploring such settings while at the same time asking yourself: What data about myself should the apps and services I use be able to access, store, and use?

Making sure you're comfortable with any of these settings could mean:
• Checking your apps permissions
How many of your apps really need access to your location, microphone, camera, or contact list in order to work?
• Checking other apps' settings
Maybe you want to protect your WhatsApp app with a PIN? Maybe you're not OK with iOS automatically backing up your messages to the cloud?
• Checking all the privacy settings of the services you use
Have you ever done a Privacy Checkup, or visited the Privacy, Apps and Websites, and Your ad preferences pages on Facebook? Or the Google Privacy Checkup and My Activity pages if you have a Google account? Or the Privacy and safety and Your Twitter data pages if you use Twitter?

• Quitting a service deleting your account
If you make this decision but want to keep you data remember that most services allow you to download a copy of your data.

Don't forget that when you sign up for a service you're most likely also agreeing to privacy policies, terms of service, and other similar documents that govern your relationship with that service as well as what you and the company behind it can and cannot do. Consider reading them.

If you're using browser extensions you might also want to check the permissions you've granted them. Browser extensions can do a lot of things, beside being useful: They could have the ability to access your browsing history, or to replace content on the pages you visit, or to access the data you input into any web page (including sensitive data like financial data, usernames and passwords, and private messages). If you're not okay with some of the permissions a given browser extension require, consider removing it and maybe find a replacement. If an extension doesn't come from a trusted publisher, it could cause a lot of damage.

10. Online tracking and advertising

Big tracking networks like the ones put in place by Google, Facebook, and Amazon are always trying to follow you around the web with the goal of collecting as much data about you and your behavior as possible, data they are then able to use to do things like targeted advertising.

Ads can be invasive, sometimes exploited for malicious purposes (like prompting you to install malware, or giving up personal information) and can negatively impact your browsing experience, your bandwidth usage, and your battery life.
Sites can even be hijacked to mine cryptocurrency without your consent. Which can be a very lucrative business for malicious actors.

To minimize this kind of behavior, you can try out browser extensions such as uBlock Origin, DuckDuckGo Privacy Essentials, Privacy Badger, and Ghostery.

Keep in mind that the vast majority of websites is ad-supported, so you might want to consider white listing the ones you want to support and/or the ones you trust to help them continue doing what they're doing.

11. Cloud services

Cloud services can be amazing tools. But they can also bring some important security and privacy trade-offs with them.

Mainstream and very useful products such as Google Drive, OneDrive, Dropbox, OneNote, Evernote and so on cannot guarantee that the user is the only party with access to their personal data simply because (for various reasons) they have access to users' data as well.

Although this can be fine in some scenarios, there are times when (even at the cost of losing out in terms of functionality) you might want to have more control over your data.

This is where services like Sync for cloud storage and Standard Notes for note-taking could come in handy. They both encrypt and decrypt your data locally, so as to provide a service in which you can be sure (to a reasonable degree) to be the only person able to access your data.

These kind of offerings are sometime called zero-knowledge.

12. Data breaches

Data breaches have become very frequent in recent years, and every breach adds to an ever growing pool of personal data about us that is publicly available (compromised). Think about the Equifax disaster that exposed personal data such as Social Security Numbers and dates of birth of over 140 million US citizens, or the Yahoo! data breach that exposed personal info of all of Yahoo's 3 billion registered accounts.
All of this compromised data will never go back under the control of the people who lost it, and in cases such as SSNs and dates of birth there's not much one can do. Those are things that just cannot be changed.

In a world that's increasingly reliant on digital means to store, share and collect all sorts of data (including personal data and sensitive personal data), in which personal information is frequently compromised in data breaches and/or voluntarily disclosed on social media and yet still widely used to identify and authenticate people (think about what "only-you-could-know" info your phone company asked you the last time you called their customer support to get info about something, change something about your contract, or block your SIM card and request a replacement) malicious parties can do real damage.

A very useful tool (both when it comes to security awareness and knowledge about data breaches) is Troy Hunt's Have I Been Pwned? project.
The easy to use website lets people check if their data was ever part of a known data breach via a publicly searchable database.

You can also subscribe to the service (it's all free) with the email addresses you want to keep monitored and (after having verified you're actually the owner of those inboxes) receive email notifications of both publicly searchable, as well as sensitive data breach information.

A number of companies are now starting to incorporate the useful Have I Been Pwned? tool directly into their products and services. This includes password managers such as 1Password, but also browser extensions such as PassProtect, which can help you avoid using passwords previously exposed in known data breaches by prompting you to change them in real-time.
1Password and PassProtect use k-anonymity, which means that your passwords are never sent to anyone.

13. Data protection and minimization

Try to be aware and mindful about which data you digitize and where you store it, as well as which data you share about yourself (including personal info such as your name and surname, date of birth, home address, etc.), with whom you share it, and how/where you share it.

Keep in mind that you're not probably dealing exclusively with your personal data, but with the personal data other people have shared and are sharing with you as well.

Personal info such as name and surname and date of birth, which are still used in many cases as only info required to authenticate people (looking at you telecommunication companies…), could be used to impersonate you and gain unauthorized access to all sorts of services you use. Moreover once such data becomes public there might not be a way for you to do much of anything about it.
You may be able to change your passwords, but changing things such as your date of birth, your name and surname, or your home address is much more difficult…

When signing up to a service try to get a sense of how that service or company will store your data and if they'll do so in a matter that protects your security and privacy.
Try to also think about what data any given service needs vs. the data it asks for, and try to find a way to only give up what's strictly necessary. For instance: If when paying for something you're given the option to pick a service like PayPal instead of your credit card, consider choosing PayPal. That way you'll not be giving your credit card info to that service.

Consider deleting data you don't need/use anymore.
This could mean deleting old files, Internet accounts (the Just Delete Me website or the accompanying browser extension can help you here), as well as wiping unused devices (like old phones or old Hard Disk Drives still full of personal data).
Keep in mind that aside from employing a trusted disk wiping tool, the best option to wipe devices like old Hard Disk Drives is usually that of physically destroying them.

As the UK's National Cyber Security Centre wrote soon after news hit of a previously undisclosed Google+ bug that could've potentially be exploited to access people's private information: "For any user of social media, this breach is a reminder that social media applications that you no longer use may still contain your data and this could potentially be leaked. It is recommended that any active or inactive users of social media platforms review their data held by such platforms to limit any future exposure to breaches. They should also review their privacy settings with companies, including Google, which have introduced further privacy checks with the introduction of the GDPR act."

Two products that can help you minimize the data about yourself you wittingly or unwittingly share with third parties are DuckDuckGo's search engine (a search engine that doesn't track users) and the Tor Browser (a tool that lets you browse the web anonymously).

In case you were wondering: Private Browsing is NOT an anonymity tool.

If you need to protect yourself from online harassment, then you might want to check out the following guide from Jaclyn Friedman, Anita Sarkeesian, and Renee Bracey Sherman:
• Speak Up & Stay Safe(r)

14. Social engineering

Even though popular email services like Gmail and Outlook.com already do a pretty decent job at filtering out most junk mail from your inbox and popular web browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge have the capability of warning you when you're about to visit potentially malicious webpages, keep in mind that such safeguards will not protect you against everything. And will not protect you against yourself.

Contemporary hacking usually involves the user's unwitting participation. This is because it is way easier (and cheaper) for someone to send a malicious link or attachment and have the victim do the work for them, instead of having to make their way through technical safeguards themselves (which could be possible too, just generally more expensive).

Think twice before opening suspicious email attachments or clicking fishy links. They could end up tricking you into unknowingly giving away personal information (phishing), into installing malicious software such as ransomware, or some other nasty thing.

Here are a few things you can look out for to protect yourself against these types of attack:
• Things that are too good to be true.
Such communications may involve free giveaways, large sums of money, or something along those lines…
• Messages that convey a sense of urgency and ask you to act promptly.
Such messages may involve communications about your accounts being compromised, and may ask you to put your info into a page that looks just like the original one but in fact is not.
• Shortened links.
Shortened links (like bit.ly's) can be used to hide links to malicious webpages.
• Email addresses that don't look quite right.
This may involve very long, apparently random email addresses as well as addresses similar to ones you trust but different in some little, less apparent way.
• Messages from and about services you don't use.
Such as an email about a bank account from a bank you don't bank with, or from a service you never signed up for, or about a package you never ordered.

15. Anti-malware software

When using anti-malware software (like anti-virus software) take into account the fact that for it to work it has to have deep access to a system. Vulnerabilities in such software would therefore greatly increase the surface for potential attacks.
This is not to say that you should downright avoid it, instead that you should be aware of the fact that poorly developed anti-malware software (particularly if provided by a third party, which usually needs to hack its way into a system in order to work) could add serious vulnerabilities to a system, instead of helping securing it.

Microsoft's Windows 10 comes with the Windows Security app as part of the operating system. Consider sticking with it.

Here are some more information on the topic:
• Protect my device with Windows Defender Security Center / Microsoft
• Should users disable Windows Defender on Windows 10? / Security Now
• Steve Gibson's position on anti-virus software / Security Now
• Disable Your Antivirus Software Except Microsoft's / Robert O'Callahan
• A Followup About AV Test Reports / Robert O'Callahan
• Steve Gibson and Leo Laporte talk about AV software / Security Now
• Next-gen security with Windows Defender Antivirus / Microsoft
• Disrupt the revolution of cyber-threats with Windows 10 / Microsoft

Whatever you choose to do, try also to be careful and mindful about what you're doing with your devices and in which context you're doing it. Anti-malware software can indeed help you, but it can't do much to protect you if you ignore common sense security practices.

Also, in case you were wondering: Yes, everybody has software vulnerabilities and (yes) there is malware for everybody. No system is immune and there is no such thing as a hack-proof system. That is where regular an timely updates come into play.

16. VPNs

A Virtual Private Network is a tool used by different people in different parts of the world to achieve different goals. Someone could be using a trusted VPN (the keyword here being "trusted") to prevent their Internet activity from being monitored or tampered with (whether because that's mandated by law, for profit, or for malicious purposes) or to access content blocked in their country by a content provider or the government, while someone else could be using one to get around pervasive surveillance and censorship and participate in the open Internet.

Using a VPN means all your Internet traffic is sent to one of your VPN's servers (VPNs usually have hundreds or even thousands of servers spread across the world) via an encrypted tunnel, and it then goes out to the Internet from there. This has two main positive implications:

• Anyone positioned between you and the VPN's servers will only be able to see that you're connected to a VPN, preventing them from having any kind of access to your Internet traffic. This can protect you from unregulated ISPs, mandatory data retention laws, bad actors in general, as well as give you peace of mind when connecting to Wi-Fi networks you don't trust (like that public Wi-Fi hotspot you find really convenient connecting to from time to time, or the Wi-Fi network from that friend that doesn't have a very good security hygiene).

• Anything you connect to on the Internet will only see the IP address of your VPN's server, effectively masking your devices' IP address. This means that your traffic will look to the services you're using as if it were coming from the VPN's servers instead of your actual physical location. This can help you avoid letting services know who you are and where you're visiting them from, but also access content that wouldn't normally be available in your country or region by connecting to VPN servers based somewhere around the world where that content is available.

Keep in mind: A VPN only protects the connection between you and the services you're using, it doesn't prevent you from visiting malicious websites or from voluntarily or involuntarily disclosing personal information to the services you use. Because your data is encrypted locally on your devices and is then decrypted only once it reaches your VPN's servers, using a VPN also means shifting trust from your ISP to the VPN provider. You'll want to find a VPN that you can really trust.

Not all VPN services are created equal. Things you might want to check when looking for the VPN that's right for you are their privacy policy, the country in which they are incorporated and the country from which they operate (which will help you determine how much you can trust them based on the kind of laws and policies that they have to comply with), who is operating the service, and the technology and security protocols they use to protect your information.
Free VPNs are usually not recommended as many of them profit off of selling the very same data people wanted them to protect.

A VPN provider I feel comfortable mentioning here is ProtonVPN (built by the same folks behind ProtonMail). ProtonVPN uses the well-regarded OpenVPN protocol, has some very interesting security features, and has recently received a pretty strong endorsement by Mozilla. Here's VPNpro's review of their product: ProtonVPN Review

If what you're looking for is an anonymity tool, then you might be better off with the Tor Browser rather than just a VPN.

In some countries using tools like a VPN may be against the law. You should research the laws regarding encryption software and VPNs in the country where you live or travel to before signing up.

PS: VPNs Are Absolutely a Solution to a Policy Problem / Mo Bitar

17. Webcam security

Webcams are a piece of hardware that is generally easy and very cheap to hack. Consider putting some tape (or a very cool sticker) over yours.

This will not make you surveillance-proof, and there's probably plenty of other cameras around you at all times over which you have less or no control over, not to mention microphones (which are much more difficult to cover or disable)… But hey! At least you're doing something, and while you're hopefully feeling good about it, you're also subtly telling other people that you do care about security and privacy (which is important, and cool).

18. Data backup

A good step you can take to try to prevent losing your data to ransomware, or to an Hard Disk Drive or Solid State Drive failure (which will happen at some point) is backups.
You can back your files up to another drive (using tools such as SyncBackFree) or you can back them up to a cloud storage service (such as OneDrive, Google Drive, Dropbox, or Sync if you prefer a zero-knowledge offering). Or you can do both.

While choosing the option (or combination of options) that best fits your needs take into account the sensitivity of the data in question, and the trust you're willing to place in the cloud storage provider.

19. Personal security assessment

A good way to go about implementing the chapters of this list is defining your threat model.
• What are you trying to protect?
What is it you consider personal/sensitive enough that you're willing to take extra steps in order to avoid it falling into the wrong hands, or going public?
• From whom are you trying to protect it from?
Are you worried about police surveillance, corporate surveillance, surveillance from your parents, threats from people with physical access to your devices and systems such as spouses, roommates, and employers, or what you're interested about is adopting general security measures to avoid losing your information to hackers?
• If that person or entity were to come after what you're trying to protect, how would they do it?
Would they just need to grab your device? Would they need to guess a PIN? Would they need to gain remote access to your devices using malware? Would they need to guess the password you keep reusing? Would they be willing to force you into unlocking your data for them?
• If they were to succede, how bad would the consequences be?
What could be the worst case scenario? How would you handle such a situation, if you were confronted with it?
• How likely is it that someone will come after what you're trying to protect?
How valuable do you think your information is for the person or entity in question?
• What resources such as time (and maybe money) are you willing to invest to secure what you're trying to protect?

While going through this keep in mind that figuring out who and what you trust, as well as realizing the fact that if there is someone targeting you their capabilities will likely grow over time can be very important.

Here's a good resource from the Electronic Frontier Foundation that dives a little deeper into the topic: Assessing Your Risks (EFF).

20. Conclusion

What we've seen so far are actions you can take to better protect your data and the data other people might be sharing with you. Here's the thing, though: Digital security is only as strong as its weakest link.

Once you start thinking about your personal information security as a team sport (and you should) you can ask yourself: Do the people I share personal, private, and/or sensitive information with protect their data (and the data I share with them) as well ?
Would it make sense for me to suggest, ask, or even demand they follow good practices similar to the ones highlighted on this page?

Personal security and privacy is fun, and important. It should be something we talk about, because it's something that touches most of us every day.

As Edward Snowden so brilliantly put it:
"Privacy isn't about something to hide. Privacy is about something to protect. That's who you are. That's what you believe in, that's who you want to become. Privacy is the right to the self. Privacy is what gives you the ability to share with the world who you are, on your own terms, for them to understand what you're trying to be. And to protect for yourself the parts of you that you're not sure about, that you're still experimenting with. If we don't have privacy, what we're losing is the ability to make mistakes. We're losing the ability to be ourselves. Privacy is the fountainhead of all other rights. Freedom of speech doesn't have a lot of meaning if you can't have a quiet space… to decide what it is that you actually wanna say. Freedom of religion doesn't mean that if you can't figure out what you actually believe without being influenced by the criticisms and sort of outside direction and peer pressure of others. And it goes on and on and on. But privacy is baked into our language, our core concepts of government and self in every way… without privacy, you won't have anything for yourself. So when people say that to me, I say back arguing that you don't have privacy because you have nothing to hide is like arguing that you don't care about free speech because you have nothing to say."

Take care

Page last updated: 9 January 2019

•

Download page as PDF