Privacy for the Everyday Person: A Guide To Staying Safer Online

By Astrid Floegel-Shetty

With generous support from the Rose Foundation for Communities and the Environment Privacy Rights Fund

OAKLAND PRIVACY

Editing support from J.P Massar and Yadi Younse

Table of Contents

Chapter 1 Introduction

VPN? Encryption? Tor Browser? Geo-location? Secure? Insecure? Data Breach?

What does it ALL MEAN?

If you've ever tried to understand how to protect your information online and felt completely overwhelmed—you're not alone. It feels like everyone's talking in code: VPNs, encryption, "end-to-end," cookies, firewalls…

You don't need to be a technology expert to protect your privacy online. You just need:

(1) an idea about why this privacy stuff actually matters to your everyday life,

(2) a few tools, and

(3) clear explanations.

What does it mean for me to have digital privacy?

Privacy means you get to decide who sees what about you. It's like having curtains in your home or apartment, because you just don't want strangers watching you eat cereal in your pajamas. Online, digital privacy means keeping your personal stuff—your searches, your messages, your health info, even your location—out of the hands of companies, hackers, and governments you didn't say "yes" to.

What's the point of trying to keep my online/digital life private?

Every little digital privacy change you do helps protect you from:

1) Your private information accidentally getting shared or stolen.
This includes your phone number, location, or even private photos being leaked online.
2) Someone pretending to be you online in order to open credit cards or steal money.*This is called* ***identity theft*** *. It can mess up your finances and take years to fix.*

3) Receiving junk messages or scam emails trying to trick you.
Scammers often send fake messages to your email or phone number in order to steal your information for identity theft by getting you to tell them information, like your credit card number.

4) Websites following everything you do online.
This is called ***tracking****. It's how online advertisements "follow you" around the internet after you search for something once. Say for instance you Googled "baby clothes" because your friend is hosting a baby shower. Now all the advertisements you see online are about babies and parenting.*

5) Companies creating a file about your online habits without asking you and selling that information.
When companies track what you do online, they gather personal information about you without permission—like what you search, buy, or watch. You may think, who cares? You should! Companies use this information to target you with ads, change what prices you see, and influence your choices without you even realizing it.

But more than all of that, digital privacy is about freedom to exist without surveillance. Privacy means you can explore, learn, talk, and live your life without being watched all the time in real life OR online.

This guide will walk you through simple steps you can take and tools you can use to begin your digital privacy journey. Unfortunately, no tool or setting can 100% guarantee complete digital privacy.

However, small steps (like using strong passwords, putting tape over your computer camera, keeping up with new software updates for your cell phone) can go a long way in keeping your digital life safer.

The goal is not perfection, but protection!

Read on to find out how you can implement digital privacy tools easily.

Chapter 2 Digital Privacy Tools

How do digital privacy tools work?

Think about digital privacy tools like this.

In a quiet neighborhood, there's often a long, straight stretch of road. What happens when there are no speed bumps? Most drivers naturally speed up, even if they don't mean to. And there are some people who take advantage of there being no speed bumps to drive really, really fast! But when there are speed bumps, those speed bumps reduce the chance that people will drive dangerously fast or drive down the street at all.

Or think about the locks on your front door, or even a security signs like "Protected by ADT" or "Beware of Dog." These security measures don't make your home completely safe from break-ins, but they make your home less appealing to someone looking for an easy target.

Privacy tools work the same way online.

When websites, apps, companies, governments, or even hackers know no one is watching—or your data is unprotected—they tend to speed towards stealing your data or see you as an easy target.

But when we add "speed bumps," "locks," and "security signs" to your digital life (like strong passwords, two-factor authentication (2FA), and privacy settings)—we slow them down! We send the message that this information is protected. Protected information is less accessible and appealing to websites, apps, companies, governments, and hackers.

These small steps (your digital speed bumps, locks, and signs) might not stop every threat, but they go a long way in making you a less appealing and much harder target.

You don't have to do everything.

But something is better than nothing!

Here are some some answers to questions you might have as you read this digital privacy guide.

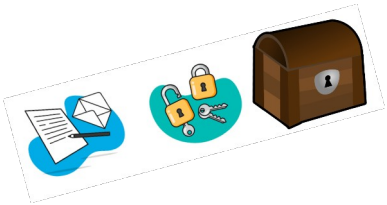
What does it mean when something is "secure" online?

"Secure" online means the site or app is doing things to keep your information safe. For example, a secure website (identified by the lock icon in your browser bar, shown in the pictures below) uses encryption, updates its systems and security protocols regularly, and doesn't ask for more data than it really needs.

It's like choosing a bank with a vault and security guards, instead of one with the back door wide open. Just be aware that "secure" does not mean you are perfectly protected––but that you have some form of protection.

What is encryption?

Imagine you're mailing a letter to a friend, but before you drop it in the mailbox, you put it inside a locked box—and only your friend (that you previously gave the key to) can open that box. That's basically what encryption does. It locks your messages, photos, and passwords in a way that makes them unreadable to anyone who doesn't have the key. So even if someone intercepts the box with the letter, that person won't be able to read your letter because he/she/they don't have the key to open the box!



Now that this has been explained, let's get into learning about specific digital privacy tools!

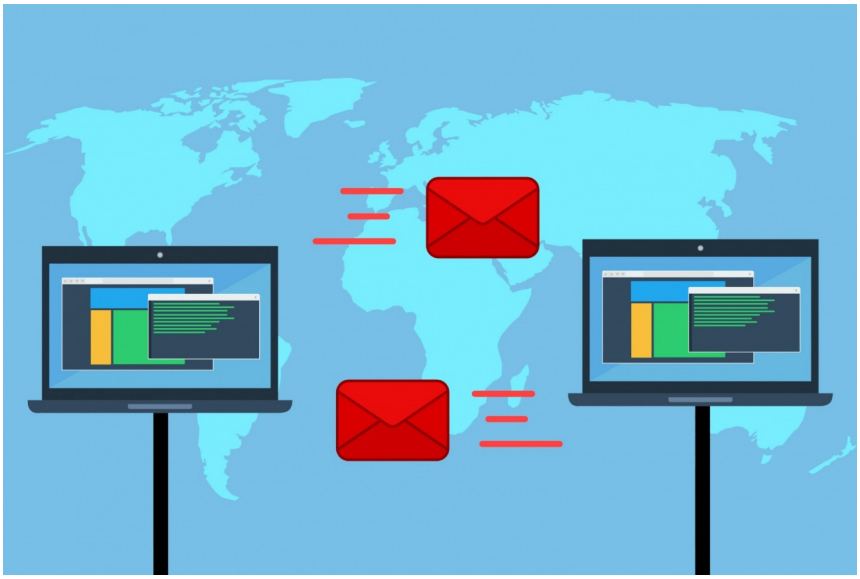
Just Remember: you don't have to do everything

But hopefully this guide helps you find easy things you can do!

Chapter 3 Email

Email is like a digital postcard: easy to send, easy to read—and easy to intercept.

Most people use email every day—for work, for online shopping, for communicating with friends, family, doctors, therapists, customer support, and for a lot more things…



But here's the reality: email is one of the least secure ways to communicate. Back in the early days of the internet and computers, people weren't thinking about hackers, surveillance, or scams. So email was not designed with a bunch of digital privacy features.

What Can Go Wrong with Email?

Spoofing & Phishing: Spoofing is the disguise. Phishing is the trick.

Spoofing is when someone pretends to be someone else by faking an email address, phone number, or website to look trustworthy. For example, this would include times when you've received a strange text message from someone claiming to be FedEx.

Phishing is the scam where the bad actors use that fake identity to send you an email asking for your password or credit card number. For example, the scammer pretending to be FedEx would say in an email that in order for your package to be delivered, you need to send your social security number. By spoofing the FedEx identity, the scammer is hoping to trick you into giving them your information, thereby making you a victim of a "phishing" attack.

•

Using your email to reset your passwords

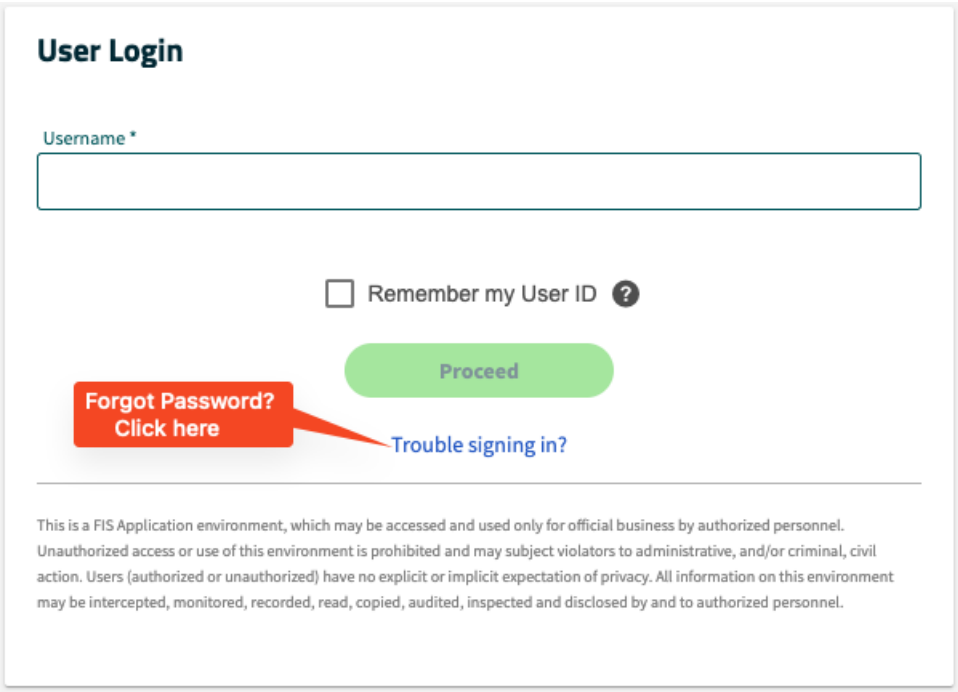
If someone breaks into your email, they can reset your passwords for other accounts (like your bank, shopping apps, or social media) because the password reset links that you get for those other accounts (usually after clicking "Forgot your Password?" or "Trouble Signing in?") go to your email. These hackers can ALSO read old messages, find personal info (like your address, contacts, or saved documents) and even send fake emails pretending to be you (like the spoofing we just learned about).

Government reading your emails

In many cases, law enforcement or intelligence agencies can request access to your emails from the company (like Google or Yahoo!) that stores them.

That's why protecting your email with a strong password and two-factor authentication (2FA) is one of the most important steps you can take for your overall privacy.

Read more about two factor authentication in Chapter 4.



So what can you do?

There's no one-size-fits-all answer. It depends on how you use email, what you're trying to protect, and who you're worried about.

Basic Email Safety Tips Everyone Should Know

1) Never email sensitive information like your SS#, banking info or passwords
Use an encrypted messaging app or call if you must send something personal.
See chapter 5 for more on recommended messaging apps.

2) Beware of clicking links in messages from people you don't know or even from people you do know, if the message seems strange.

Just report the strange email as "spam" and then delete the email.

If you're really not sure if the email is real, the next step is to (in a separate email! or a text message! or a phone call!) ask the person who sent you the original email if they actually sent that email to you.

3) Always log out of your email on shared computers, whether at home or the library.

4) Update the privacy settings of your email account.

Updating the Privacy Settings of Your Email Account

Make sure to turn on the privacy settings for your email. For example, Gmail lets you turn off targeted advertising, recording your YouTube and google maps history, and so much more.

Go to the settings for your email account and you will usually find a "Security" section that will allow you to make changes to protect your privacy. Find out more about the privacy settings for your: GMAIL; YAHOO / AOL ; MICROSOFT / OUTLOOK.

Also, create strong passwords for your email account and add two-factor authentication (2FA) if it's offered.

A strong password is one that's long, hard to guess, and not based on personal info like your name or birthday. The best passwords use a mix of letters (upper and lowercase), numbers, and symbols….something like **Purple$Guitar!Rain29**.

Even better? Use a **"passphrase"** made of random words, like **dog-tree-dance-honest**, especially if you're using a password manager to remember it for you.

Avoid anything short, simple, or reused across multiple accounts.

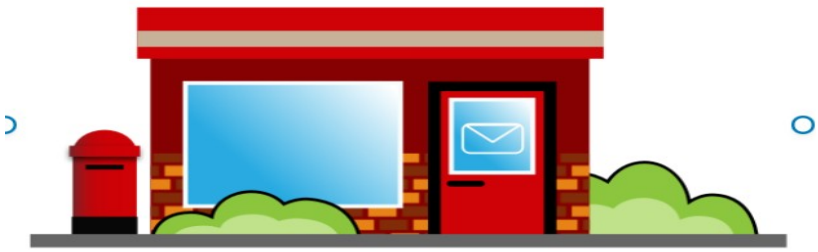
See Chapter 4 for more on password managers.

However, even if you have all the privacy settings turned on for your email, the company who hosts your email (Gmail, Yahoo, Outlook) can still see what's in your email.

Most email providers (like Gmail, Yahoo, or Outlook) store your messages on servers.

What does it mean when an email is "stored on a server"?

Let's say you write a letter to a friend. You don't hand it to them directly. Instead, you drop it off at the post office, and they hold onto it until your friend shows up to pick it up. The post officer is the "server."



That's basically what happens when you send or receive an email.

Instead of traveling directly from your phone or computer to someone else, your email first gets sent to a server, a powerful computer owned by a Big Tech company like Google (Gmail), Microsoft (Outlook), Yahoo, Apple, or another email provider.

That server stores a copy of your message, sometimes for years. That email may stay there even after you delete it from your inbox. The Big Tech company can access these emails whenever they want. Hackers might try to break into the server to steal messages. Governments or the police can gain access to your emails by using the law to force companies to open up the server.

So when people say "your email is stored on a server," they mean your email is sitting on someone else's computer, waiting to be read—and possibly copied, scanned, stolen, or leaked.

That's why choosing a more private email service, or learning to encrypt your own email, can give you more control of your email privacy.

Email Services to Consider

Here are some services that take extra steps to protect your messages:

Proton Mail

Based in Switzerland, where privacy laws are strong. Proton also offers a password manager, VPN, Drive, and calendar. Free & paid plans.

tuta

Based in Germany, another country with strong privacy protections. Includes encrypted calendar and contacts. Only uses renewable energy to power their service. Free & paid plans.

RISEUP

A nonprofit collective focused on secure communication for activists. Encrypts email on their own servers and avoids logging user activity. Free, but relies on donations to keep the service going.

These services won't stop all email risks, but they will do a better job than most email services (like Google, Yahoo, etc.) at keeping your emails private.

Want to Encrypt Your Own Emails? You Can—But It Can be A Bit Complicated.

There's a tool called PGP (Pretty Good Privacy) or its free version GPG (GNU Privacy Guard) that lets you encrypt your own email messages. It's like putting your message in a locked box so that only the person with the matching key can open.

Here's what it takes to set it up:

1. Download a program like PGP or GPG on your computer or phone.
2. Create two "keys"—one you can share with others (public), one that only you know (private). You give your public key to others. They use this public key to lock their messages to you. Only your private key can unlock those messages. (And you can lock your messages to others with the private key that they can open with the public key.)
3. You also need to use an email app that supports using these keys. Most people use Mozilla Thunderbird with an add-on called Enigmail to make an email that can use the public and private key system.

If this sounds a bit complicated, it is. But once you've set up the PGP or GPG system, it works reliably.

If you want to try this method out, the Electronic Frontier Foundation offers step-by-step instructions (with pictures):

- How to Use PGP on Windows: https://ssd.eff.org/en/module/how-use-pgp-windows
- How to Use PGP on Mac: https://ssd.eff.org/en/module/how-use-pgp-mac-os-x
- How to Use PGP on Linux: https://ssd.eff.org/en/module/how-use-pgp-linux

Email Plug-Ins

An email plug-in adds extra functions to your email. This includes Grammarly for Email, Boomerang for Gmail, SaneBox, or Mailtrack.

These plug-ins, and newer plug-ins using AI (artificial intelligence), do things like write emails for you, summarize long threads, schedule emails, check your grammar, or organize your messages.

While that sounds convenient, there's a catch: many plug-ins read and store your emails in order to work. That means your private messages could end up on someone else's server.

If you care about privacy, be picky about which email plug-ins you use, especially if they come from Big Tech companies or ask for full access to your inbox

So What's the Bottom Line When It Comes to Emails?

If you wouldn't write it on a postcard, don't send it in a plain old email.

Update the privacy settings in your email account, including 2FA.

Try using email services that have more secure servers.

Potentially set up your own email encryption.

Be careful about the add-ons you put in your email.

Chapter 4 Password Managers

What's a Password Manager and Why Should I Care?

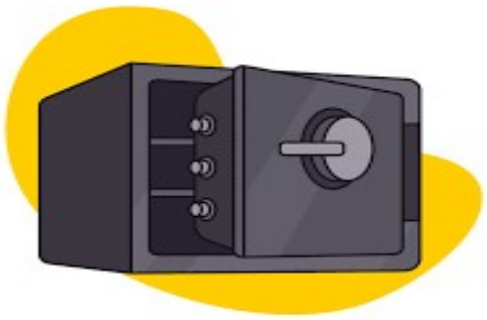
Ever forget a password and get stuck clicking "Reset my password" over and over? Or worse—do you use the same password for more than one site?

(No shame. Most people do.)

Here's the problem: if you use the same password on multiple websites and just one of those sites gets hacked, the thief now has the keys to your entire online life. Your email. Your bank. Even your streaming services like Netflix or HBO.

That's where password managers ("PMs") come in.

Think of a PM like a vault where all your precious things are stored inside. You only need to remember ONE "master password" (like a key or pin number for a vault) to unlock the vault. Inside the vault are all your other passwords.



The real benefits of a PM are the services they can offer.

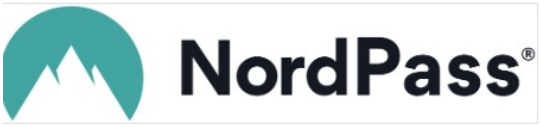
- Remember all your passwords for you. No sticky notes. No spreadsheets. No trying to remember if you used an upper or lowercase letter.
- Can automatically fill in passwords when you visit websites.
- Can generate new passwords for you that are long and weird (like gR%8K! z7fM$32) so the passwords are harder for hackers/thieves to figure out.
- Can alert you when your password has been discovered by hackers/thieves.
- Can allow you to easily and securely share passwords with friends and families.
- Allow you to remove access to your password when sharing it with friends or family members. Did you break up with your girlfriend, boyfriend, or partner? Take back your password that same night!
- Help your family manage their passwords–especially parents with kids or older adults with their elderly parents. No more mom calling you at 7 PM saying she doesn't remember the password for her email anymore.

There are different kinds of password managers:

Dashlane. A user-friendly password manager that also includes a password health checker and dark web alerts. Offers web and mobile apps.

Proton Pass. Proton also offers a VPN, encrypted email, and secure cloud storage.

Bitwarden. A free, open-source password manager that stores your passwords in a secure vault you can access on any device. You can host it yourself or use their cloud. It's one of the most trusted options in the privacy community.



NordPass. Nord also offers a VPN and secure cloud storage.

Should You Let Your Web Browser Or Device (like Chrome, Safari, Firefox, Apple Keychain) Save Your Passwords?

Most of us have seen the little pop-up: "Would you like to save this password in Chrome?"

Or Firefox. Or Safari. Or on an Apple iPhone. It's fast, easy, and it remembers your logins for you!

But is it actually safe to let your web browser or device store your passwords?

The short answer: It's better than nothing, but not the best option if you want more serious privacy protection.

The good?

Chrome, Firefox, and Safari all "**encrypt"** your saved passwords, meaning your passwords are saved in a scrambled form so that no one can read it. (So instead of saving your password as "applepie27" the password looks like "#4kkl3@*" to anyone other than you trying to access it online). Chrome, Firefox, and Safari will also warn you if a password shows up in a known data breach.

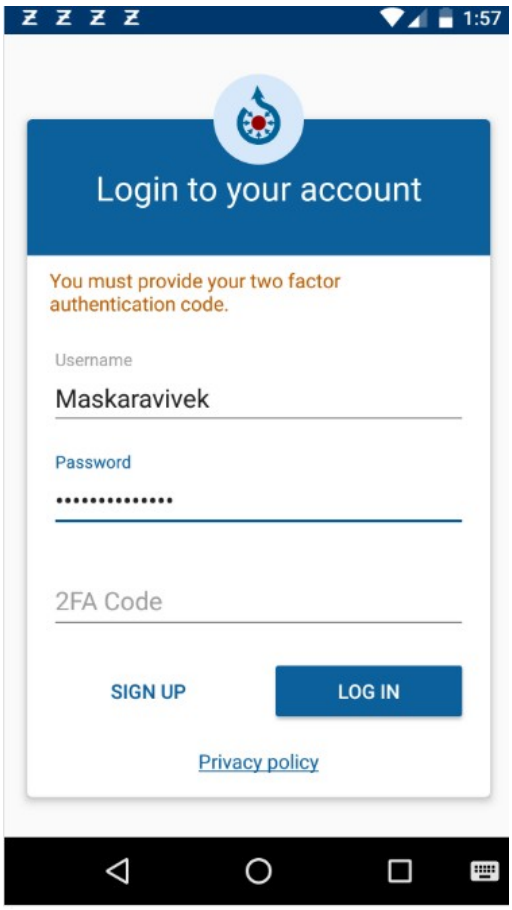
The bad?

- **Tied to Big Tech:** When you use a browser like Chrome, your passwords are stored with your Google account. That means one company may have access to your search history, location, emails, and passwords!
- **Limited Features**: Browser managers don't help you create strong passwords that are as good as the ones created by real password manager apps.
- **Risk of Device Theft**: If someone gets access to your unlocked device, they may be able to get your passwords right through the device or browser, especially if you're not using a master password to protect access to your password list stored in your browser.
- **No Two-Factor for the Vault**: Most browsers don't offer strong 2FA (two-factor authentication) for your browser password vault the way dedicated password managers do.

What Is Two-Factor Authentication (2FA), and Why Bother?

Maybe you've run into this before – you're trying to log into your Gmail or work email, and it sends a code to your phone or asks you to approve the sign-in on another app like "Duo Mobile," "Authy," "Microsoft Authenticator," "Google Authenticator," or "1Password."

Maybe your job required it. Or maybe your bank sent a warning email: “We’ve added extra protection to your account.”



You might’ve grumbled and thought, “Ugh, another step?”

So… what is Two-Factor Authentication (2FA)? Why does anyone use it? Doesn’t it just slow down logging into my accounts?

Two-Factor Authentication = Double Locks on Your Digital Door

Imagine your online account is like your front door. A password is your key. That’s one lock. But what if someone steals or copies your key? That’s where the second lock comes in.

Let's say someone steals your email password and they try to log into your email with that stolen password. If you've turned on 2FA, your email will require that this person provide a second key to verify their identity. Most hackers don't have that second key, so they give up.

That second key could be:

- A code texted to your phone
- A code emailed to your email account associated with the app you are trying to access
- A special app like Authy or Google Authenticator
- A physical key
- A fingerprint or face scan

When should you use 2FA?

Any time it's offered—especially for:

- Email accounts
- Banking and payment apps (Venmo, PayPal)
- Social media (Instagram, Facebook)
- Health records (Kaiser Permanente)
- Cloud storage (Google Drive, Dropbox)

Yes, it adds one extra step. But it blocks almost all the easy ways hackers break into your stuff. In fact, Microsoft said in 2024 that 99.9% of hacked accounts didn't have 2FA turned on. That's a huge number!

So the next time a website says "Add two-factor authentication?" just say yes. It's free, it's easy, and it can save you a massive headache down the line.

Is there a downside?

One downside of two-factor authentication is that some sites only give you one way to get the code, like sending the code to your phone or an email.

If you can't access that option, because you forgot your email password or your phone is lost/broken/ unavailable, you may not be able to log in at all.

2FA requires you to be careful that you have access to where the authentication code is sent!

So What's the Bottom Line When It Comes to Passwords?

(1) Password managers are a great way to create and keep track of strong passwords.

(2) Use 2FA whenever you can.

HERE is a YouTube video that covers Password Mangers.

Chapter 5 Private Texting

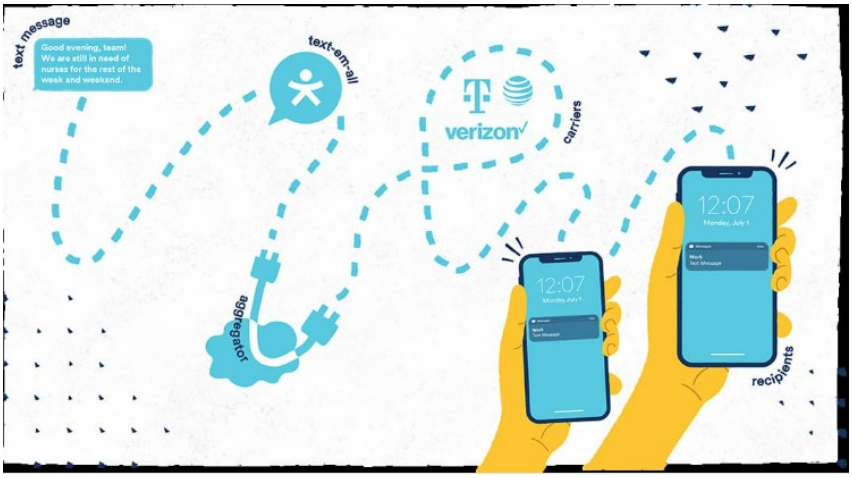
How to Send Messages Without Everyone Reading What You Wrote

Texting with a smartphone is how most of us talk: quick messages to friends, partners, coworkers, or family. But here's something many people don't realize—not all texts are private!

That message you sent last week ("Can you grab milk?") might not seem like a big deal. But what if it had been your new address? A bank link? A private photo? Or a conversation about your health, your kid, your job?

The truth is text messages can be read by your phone company, copied while the message is traveling from phone-to-phone, and even accessed in a data breach. Here's how that works:

1. You type a message on your phone: "Running late! Be there at 7"
2. Your phone sends that message to your phone company.
3. The phone company forwards that message to your friend's phone company.
4. Your friend's phone company sends that message to your friend's phone.



At no point in that communication chain is your text message digitally protected. Unless you're using what is called an "encrypted" texting app, the text message is visible to:

- Your phone company
- Hackers who may tap into weak parts of that text messaging system
- Anyone who gains access to the phone company's records
- Government agencies that request access to the phone company's records

That's where "encrypted messaging apps" come in! They are one of the easiest privacy upgrades you can make.

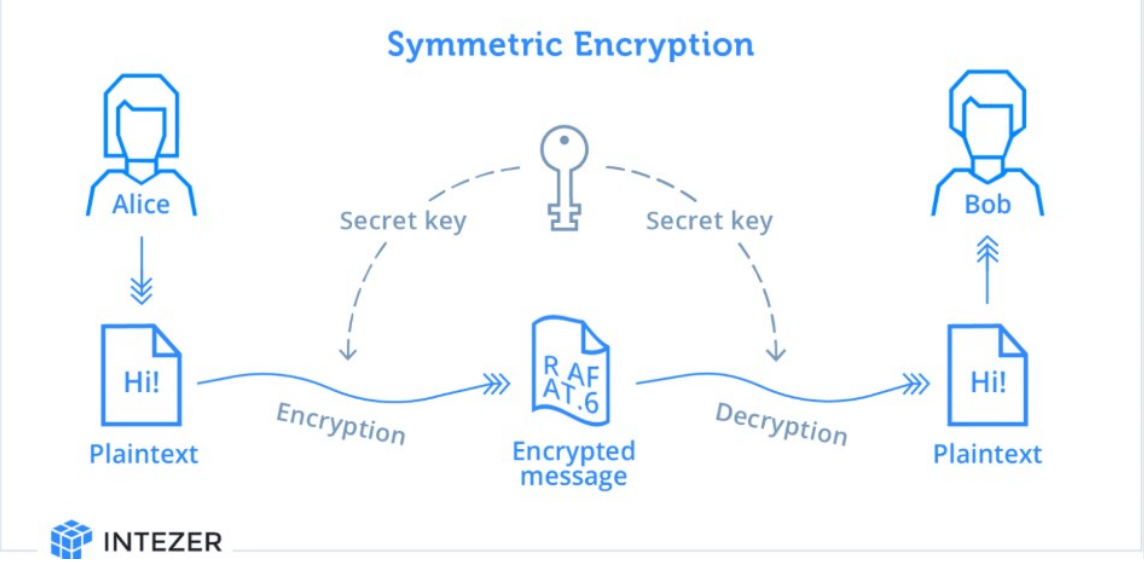
So what is Encrypted Messaging?

Encrypted texting is like putting your text message in a locked box, and only the person you're texting has the key to that locked box. Even if a hacker, a phone company, or even a government tries to grab the box with your text message, they can't read the text message inside because they don't have the key to that box!

I keep hearing about end-to-end encryption?

When someone says a service provides **end-to-end encryption**, they mean that only you and the person you're messaging can read the text messages because:

- The text message is locked ("encrypted") on your phone
- The text message stays locked while it travels to the other person's phone
- The text message is only unlocked when it arrives to the other person's phone because only the other person has the key to unlock ("decrypt") the message!



So, with end-to-end encryption, even if a hacker or company or government steals the text message as it travels from you to your friend, the hacker or company or government can't read the text message because they don't have the key to unlock the protection ("encryption") hiding your text!

Sometimes things are only "encrypted in transit." What does that mean? It means your message is protected while it's being sent, but the phone or tech company sending the message can still read or store it. This is like if the post office could read the contents of every letter you sent. In comparison, for end-to-end encryption, only the sender and the receiver can see what's inside your letter.

That's why end-to-end encryption is one of the most powerful tools for privacy today. It helps make sure that your text message are only read by you and the person you are sending the message to.

Okay, so how do I get this encrypted messaging you're taking about?

Let's go over the most common encrypted messaging services:

What is Signal? Signal is a texting program that provides mostly secure end-to-end encryption. Signal doesn't sell ads, and it doesn't collect your data. It runs entirely on donations and grants.

Sounds too good to be true? The catch is that both users have to have the program to enable the encryption, so you need to use Signal and you need to make your friends use Signal too.

Who owns Signal? The Signal Foundation, a non-profit organization focused on privacy.

What is Whatsapp? Whatsapp is heavily used outside America and was one of the first messaging services to use end-to-end encryption. However, even though your messages are encrypted, the company who owns WhatsApp (Meta, previously called Facebook) still collects metadata.

What does metadata mean? Let's say you send your friend a letter in the mail. The message is what you wrote inside the envelope. The metadata is what's on the outside of the envelope, which includes information like: Who the message is from; Who the message is going to; The date

What is Telegram? Telegram is a fairly new encrypted texting service. It offers self-destruct features similar to the program Snapchat. Regular chats on Telegram are not end-to-end encrypted unless you turn on "Secret Chat."

Who owns Telegram? Telegram was started by Pavel Durov, a Russian tech entrepreneur who left Russia and moved the company abroad. Telegram is now based in Dubai, and it's funded by private investors.

What is iMessage? When you send an iMessage (those blue bubble texts), Apple uses real end-to-end encryption. So, not even Apple can read what you wrote. But there's some drawbacks: this encryption only works if both people are using Apple devices, like iPhones. Apple collects some metadata, just like Meta for WhatsApp.

Also, if you back up your text messages to iCloud without turning on something called **Advanced Data Protection**, your messages are no longer fully private. This is because your messages will still be accessible to hackers and law enforcement if they get access to the iCloud.

So What's the Bottom Line When It Comes to Texting?

Use an encrypted messaging service whenever possible!

HERE is a video that discusses messaging apps.

Chapter 6 Browsers, Search Engines, and the Tools That Help You Stay Private Online

Every time you open your internet browser (whether it's Chrome, Safari, Firefox, or Edge) you're leaving little digital breadcrumbs behind. Those breadcrumbs tell companies what you search for, what websites you visit, how long you stay there, and sometimes even your location.

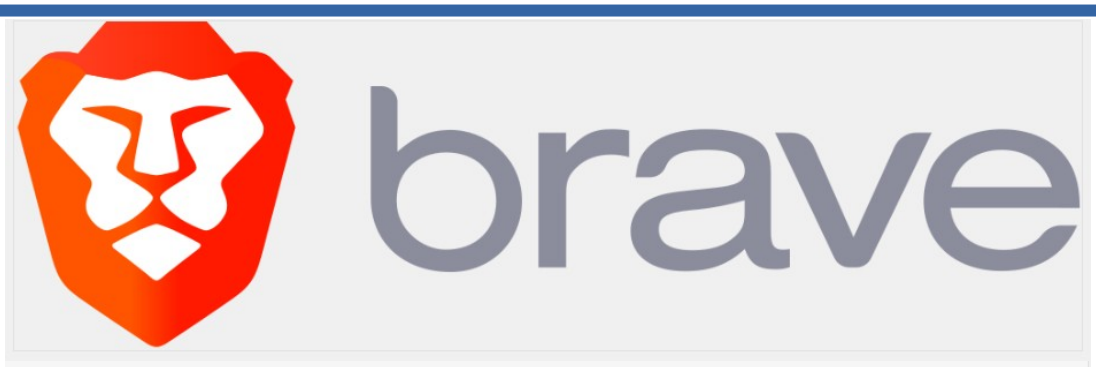
If that sounds creepy, you are not wrong!

There are tools that make it easier to browse online privately without needing to become a tech expert. Here we'll discuss some of them: privacy-enhancing browsers, ad-blocking software and Virtual Private Networks (VPNs).

Browsers and Search Engines: Pick the Right Door to the Internet

Most people use browsers like Chrome or Safari because they come pre-installed on devices. But these browsers often track what you do online. If you want a browser that gives you more control over your privacy, try Mozilla Firefox or Brave. They're free, work just like the other browsers, and don't spy on you as much.

For search engines, try switching from Google to Brave, Firefox, Startpage, or DuckDuckGo. These search engines don't keep a history of what you search for.


brave


mozilla
Firefox


LibreWolf


DuckDuckGo


Startpage

Stop the Trackers: Anti-Tracking Software

Every time you visit a website, "trackers" can start following you around the internet. These trackers watch what you click, what you search, and even how long you stay on a page.

And like a private detective, these trackers build a profile on you. This profile is used to target ads towards you or the profile is sold to other companies.

Anti-tracking tools block those trackers from spying on you. Here are a few good ones:

Ghostery blocks more than 1,800 tracking tools and shows you which sites are watching.

AdBlock Plus blocks pop-ups and ads.

uBlock is a free, open-source ad content blocker. Here is a blog post and video explaining how to install uBlock.

What's a VPN, and Do You Need One?

A VPN, or "Virtual Private Network", is a tool that hides what you do online from your internet provider, your school, your job, or anyone trying to spy on you—especially when you're using public Wi-Fi!

But not all VPNs are safe. Some track your activity and sell your data to advertisers, which completely defeats the purpose of using a VPN for privacy. That's why it's important to choose a VPN you can trust.

Safer choices include:

Mullvad is often called the best VPN for privacy. Mullvad doesn't record what websites you visit, when you connect, or how long you stay online.

You don't need to give your name, email, or any personal info. When you sign up, Mullvad gives you a random account number. You can even pay in cash by mailing Mullvad money in an envelope. That's how serious Mullvad is about privacy.

ProtonVPN

NordVPN

ExpressVPN

IPVanish

Want Even More Privacy? Try the Tor Browser

The Tor Browser is for people who want serious privacy. Tor hides your location, blocks trackers, and keeps your internet activity private. But there are trade-offs:

- Tor is slower than normal browsers.
- It can draw attention from government agencies, since they watch Tor traffic more closely.
- Some websites won't work properly on Tor.

Just a heads up, if you live in a small town and are the only one using Tor, your online activity might stand out.

What's the difference between VPN and Tor?

This gets a bit more technical, and it is not very necessary to understand if you plan on using a VPN and/or Tor. But if you're curious, read on!

A **VPN** creates a secure tunnel between your device and the internet. It hides your IP address (this is a number which identifies where you are, similar to a mailing address) and hides what you do online from your internet provider, workplace, school, etc. However, your VPN provider may keep a log of everything you do online, which is why it is so important to choose a trustworthy and privacy protecting VPN. For example, the ones identified above: Mullvad, ProtonVPN, NordVPN, etc. A VPN is good for everyday privacy, including using public Wi-Fi or online streaming.

Tor Browser sends your internet traffic through multiple random computers (called "nodes") before it reaches its final destination. This makes it very hard to trace anything back to you, even for governments or tech companies. This makes Tor Browser very good for maximum anonymity and high-risk situations (activism, journalism, sensitive research).

So What's the Bottom Line When It Comes to Browsers, Trackers, VPN, and Tor?

(1) There are browsers/search engines that do a better job protecting your digital privacy than Google.

(2) Use anti-tracking add-ons for extra protection online.

(3) A VPN and Tor are your best bets to hide your online activities.

HERE is a video about the privacy of browsers.

Chapter 7 Video Calls

Remember when video calls felt like something from the future? Now they're everywhere—school meetings, doctor visits, job interviews, check-ins with family, and even game nights. Whether you're using FaceTime, Zoom, Meetings, or WhatsApp, video conferencing is how a lot of us stay connected.

But just like with texting, not all video calls are private. Some video call companies watch what you do, store recordings, or track "metadata."

What is "metadata"?

We described this is the context of Chapter 5 on Private Texting. Metadata is information that describes or gives context to other data.

Think of it like a label on a package. The label tells you information about the package, just like metadata tells you information about the data. For example, for a photograph (the data), the metadata includes: the date and time the photo was taken, the camera model, the location (GPS coordinates), and perhaps the photographer's name.

Metadata for a video call can tell a company what kind of device you used (phone or computer, mac or windows), IP address (which shows your location), about when you called, who joined the call, and how long you stayed in the meeting.

Now let's go over your options for video calls:

FaceTime (Apple only): If you and the other person both use Apple devices (iPhones, iPads, or Macs), FaceTime is a pretty good option. Apple uses end-to-end encryption, which means your video call is locked down, and no one can watch or listen in (not even Apple).

But FaceTime only works with other Apple users. If one person's on Android, you're out of luck.

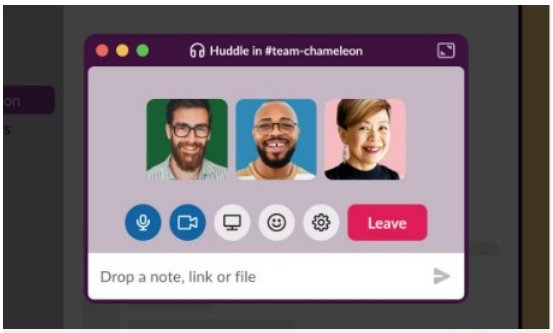
WhatsApp Video offers end-to-end encrypted video calls, so the video and audio are private. But WhatsApp is owned by Meta (the company behind Facebook), which collects lots of "metadata."

Zoom is used by schools, businesses, and families for everything from work meetings to birthday parties.

But here's what to know: Zoom does not use full end-to-end encryption by default. They do offer a feature called "end-to-end encryption", but you have to turn it on manually, and it has some limits (like you can't use all features when it's on). Also, all participants need to use the Zoom app—so yes, you'll need to download it. Zoom also collects some "metadata."

Google Meet is built into Gmail and Google Calendar. Google encrypts calls while they're are happening, but not with end-to-end encryption. That means Google could access the content of your video call if required. Google Meet also collects "metadata."

Jitsi Meet is a lesser-known but useful video service that focuses on privacy. Jitsi offers encrypted video conferencing through your browser. It doesn't collect "metadata," doesn't require registration, and you can use it on any device with a browser. You just go to the website, start a room, and send your friend or group the link.



Slack Huddle: Slack is a workplace messaging tool, and its Huddles feature lets people start quick voice or video chats. Huddles are encrypted while they happen between devices, but not with end-to-end encryption. Slack could technically access what was said or shown in the video. Slack also collects "metadata."

Microsoft Teams video calls are encrypted as they happen, but not with end-to-end encryption. The meeting organizer has to turn on end-to-end encryption before the meeting starts. Microsoft also collects "metadata."

AI (Artificial Intelligence) & Video Conferencing

More video conferencing apps (like Zoom, Microsoft Teams, and Google Meet) are now using AI to make calls smoother. AI can do things like:

- Turn speech into text (live captions or transcripts)
- Automatically summarize meetings
- Identify who's talking
- Filter out background noise

Just keep in mind: AI features often require recording or analyzing your voice, video, and what's said in meetings. That data might be stored, seen by people you didn't approve, or even used to train other AI models.

What can you do?

- Use privacy-respecting services when possible (like Jitsi Meet).
- Ask if meetings are being recorded and speak up if you're not comfortable.
- Turn off features you don't need, like auto-transcription or facial analysis.

So What's the Bottom Line When It Comes to Video Conferencing Services?

Video calls are convenient, but they're not always private! If you wouldn't say it in a room full of strangers, think twice before saying it on a video call.

Chapter 8 The Cloud

You've probably heard the phrase "the Cloud." But what does that really mean?

The Cloud is a way to store your files (like photos, documents, or backups) on someone else's computer that has much more memory than yours, most often some big company's computer (e.g. Amazon, Microsoft). You can then access your files on that other computer via the internet.

When something is in the Cloud, you can open it from anywhere. You don't need to carry a flash drive or worry about your computer crashing. All you need is an Internet connection. The Cloud is fast, easy, and used by billions of people every day.

But like anything online, the Cloud comes with privacy risks.

Common Cloud Providers You May Already Be Using

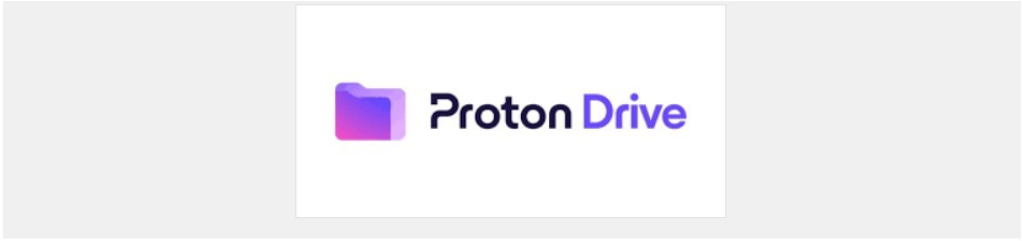
iCloud (Apple): If you have an iPhone, you're probably using iCloud. It automatically backs up your photos, texts, notes, and more. Apple says it **encrypts*** (see definition below) your data, but Apple holds the keys to your Cloud, which means they can still access your data in the Cloud if required by the police or the law. To prevent this, you have to turn on Advanced Data Protection.

Dropbox: Dropbox is a popular cloud storage service for sharing files and backing up work or personal documents. It's easy to use and works on any device. But Dropbox does not offer full end-to-end encryption* by default.

OneDrive: OneDrive is Microsoft's cloud storage system, built into most Windows computers. It backs up your documents, photos, and desktop folders online so you can reach them from anywhere. Microsoft holds the keys to your data, so they can read your files if needed. Files may be scanned for "policy violations," and your information could be shared with law enforcement or other third parties.

GoogleDrive: Your files are not end-to-end encrypted*, which means Google can access the contents if it wants to. Google can scan your files, link your activity to your personal profile, and hand over your data to authorities if asked.

What can I use?If you want more control over your data, there are cloud tools built specifically for privacy:



I need to delete a file on my computer. How can I make sure that it's really gone?

Most people don't realize that when you "delete" a file, it often isn't really gone from your computer. It just gets marked as "okay to overwrite." That means, until that memory space in your computer gets reused to save something else, someone could still recover the deleted file.

If you're using Windows, a free program called Eraser can actually shred files, making sure they're completely electronically erased and can't be recovered. Think of it like a digital paper shredder.

If you're using MacOs, you should enable FireVault or you can use the free program called Permanent Eraser.

So What's the Bottom Line When It Comes to Using the Cloud?

(1) Be careful about what you upload to the "Cloud."

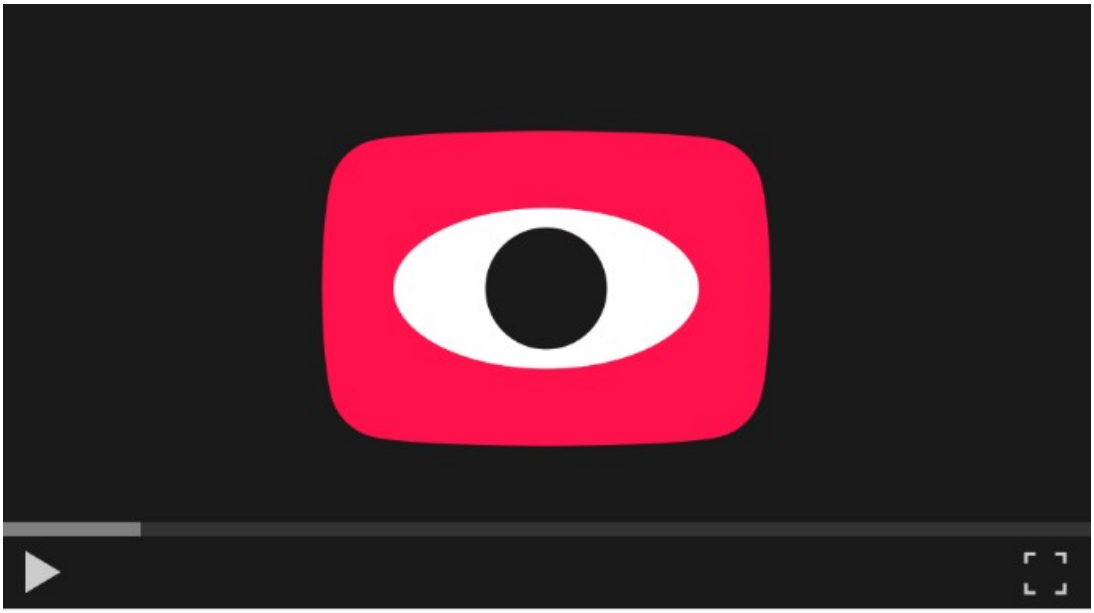
(2) Use a more secure "Cloud" whenever possible.

*Encryption explained in the "Introduction" chapter HERE

Chapter 9: Online Video Players

When you sit down to watch a video, the last thing you want is to be watched back! But that's exactly what happens when you use YouTube, streaming services, and smart TVs.

These tools are designed for convenience, but they also collect a lot of personal data. What you watch, how long you watch it, what you click on, what you pause on—they track it all. That information can be used to build a profile on you, show you targeted ads, or even shape your online experience.



Let's go a bit more into YouTube, which is free to use, but it's not free from tracking. Google (which owns YouTube) uses your video history, searches, and likes to:

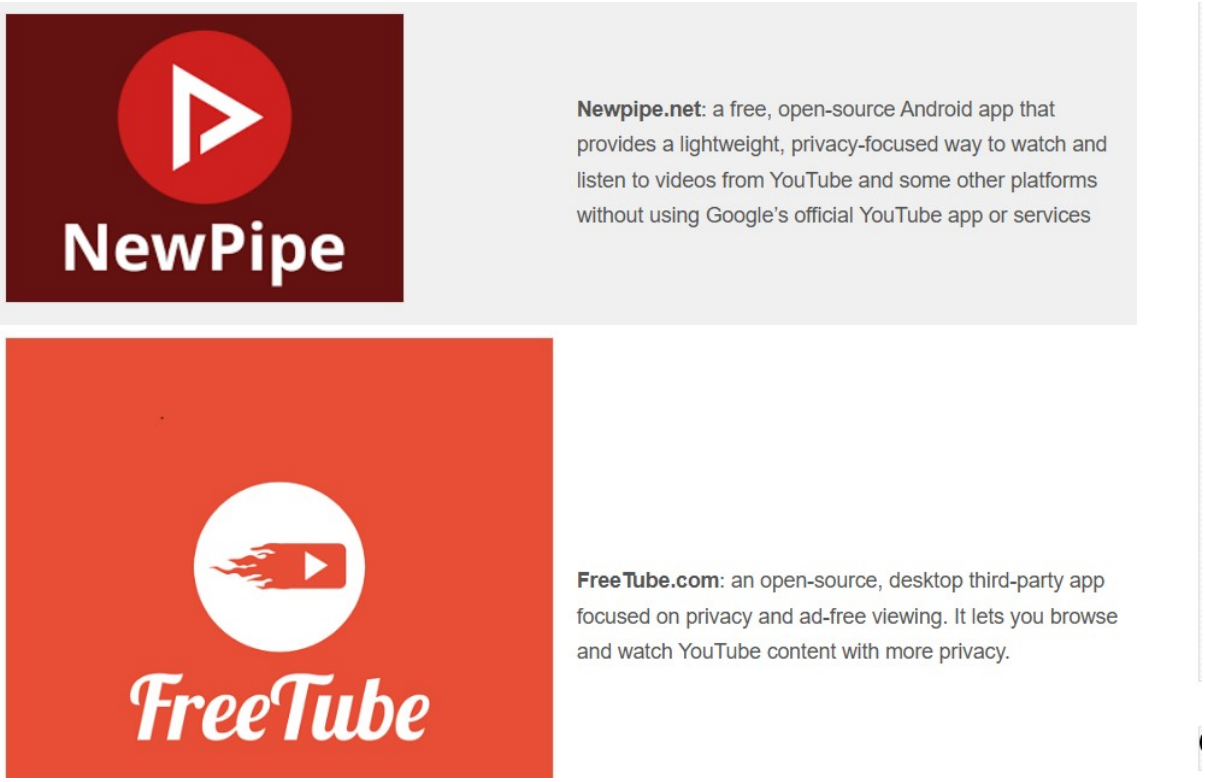
- Target you with ads
- Share data with advertisers and other partners

•Link your activity to your Google account

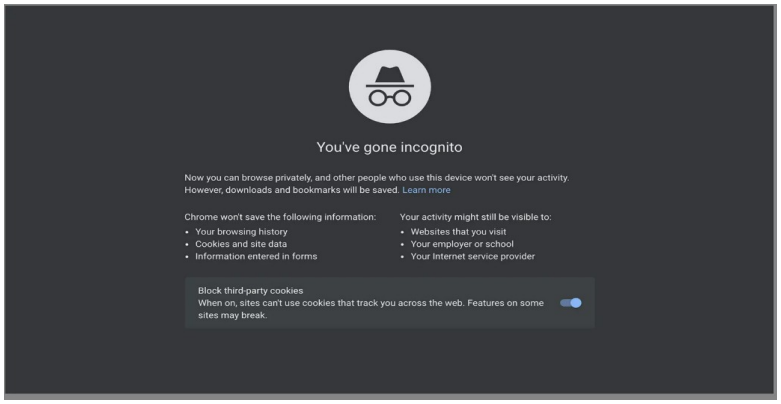
If you're signed into your Gmail account, the tracking gets even more personal information from you. Your YouTube behavior is connected to your Gmail, location, and search history.

Private Alternatives to YouTube

If you like watching YouTube videos but don't want to be tracked, try these two tools:



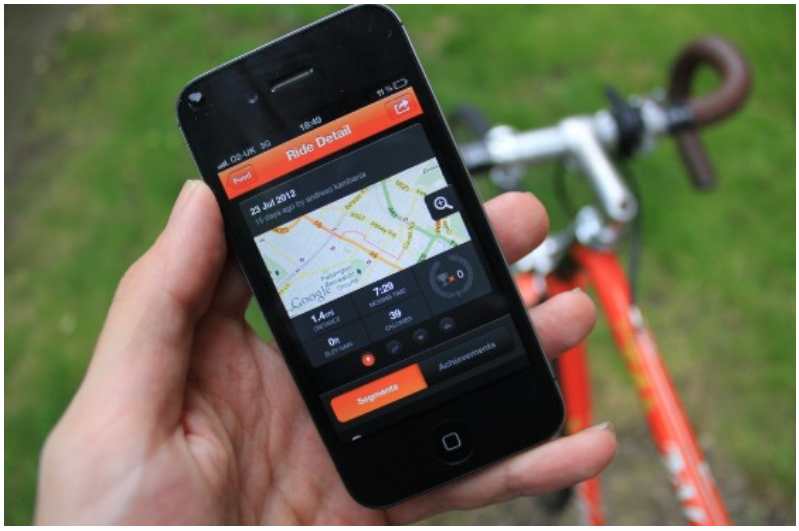
You can also watch YouTube videos in Incognito mode on your browser or using a VPN.



(We talked about VPNs and how they can be used to hide what you do on the Internet previously HERE.)

Chapter 10: Health Trackers

Health apps can help you track your steps, workouts, heart rate, sleep, or even your menstrual cycle. They're built into many phones (like Apple Health, Samsung Health, and Google Fit) or downloaded separately (like Strava and Flo). These apps are super convenient, but they also collect some of the most private and sensitive information about you!



And here's the thing: not all health data is protected, especially if you're using a regular app instead of visiting a doctor. That means your information (like how often you run, when you ovulate, or how much you sleep) can be stored, shared, or even sold by the company who owns the app.

HERE is a review of the privacy of common reproductive health apps (for periods, pregnancy, fertility, etc.)

What You Can Do to Protect Your Health Data

- Turn off cloud backups for health and fitness apps if you don't want your data stored online.
- Use a strong phone pass-code and/or password for the app if the option is offered.

- Review app permissions (Does your step counter really need access to your microphone or contacts? Probably not. Click HERE for how to change iPhone settings. HERE for Android.)
- Avoid logging very sensitive health data in the apps.

Chapter 11: Smart Assistants and Privacy (Why You Might Want to Skip Saying “Hey Alexa”)

Smart assistants like Amazon Alexa, Google Assistant, and Apple Siri can be handy. You can ask them to play music, set a timer, or check the weather, all by just talking. But the way they work comes with real privacy risks.

These devices are always listening for their "wake word" (like "Hey Siri" or "Alexa"). That means they're constantly monitoring sound in your home, waiting to be activated. Sometimes, they start recording by accident, like when you say something that sounds like their name.

Companies say these recordings are safe, but in many cases:

- The recordings are stored and can be reviewed by employees
- Some voice clips are kept unless you delete them manually
- The data may be shared with other companies or law enforcement

Our Advice: Don't Use Speech-Activated Smart Assistants

Devices that are always listening are not great for privacy. You don't need to give up smart tools altogether, but we recommend skipping voice-activated assistants and using apps or devices that put you in control!

Chapter 12: Data Breach (Before Your Personal Information Ends Up Stolen)

A "data breach" happens when a company or organization that holds your personal information gets hacked or leaks information by mistake. This can include things like:

- Your name, address, phone number
- Email and passwords
- Social Security number
- Credit card or bank account details
- Health or insurance records

Once this information is out there, it can be used (sometimes months or even years later) for identity theft or credit fraud.

What to Do If You Hear About a Data Breach

You might get an email or news alert saying your data was part of a breach. Even if it's just your email and password, it's smart to take the alert seriously. Two of the most important steps are:

(1) Freeze Your Credit

Freezing your credit means no one can open new accounts in your name (not even you) until you unfreeze it. It's free to do, and you can turn it on and off anytime.

Freezing your credit does NOT affect your current credit cards or loans. It protects you from someone taking out a credit card, loan, or apartment lease using your identity.

You need to freeze your credit with each of the three major credit bureaus: Equifax, Experian, TransUnion.

This is one of the strongest steps you can take to stop identity theft before it happens.

(2) Obtain Your Free Weekly Credit Report from These Three Credit Bureaus

AnnualCreditReport.com is the official site established by the 3 major credit bureaus (Equifax, Experian, TransUnion) to comply with the federal law requiting them to offer at least 1 free credit report annually. These 3 credit bureaus now voluntarily offer weekly credit reports. You just have to register!

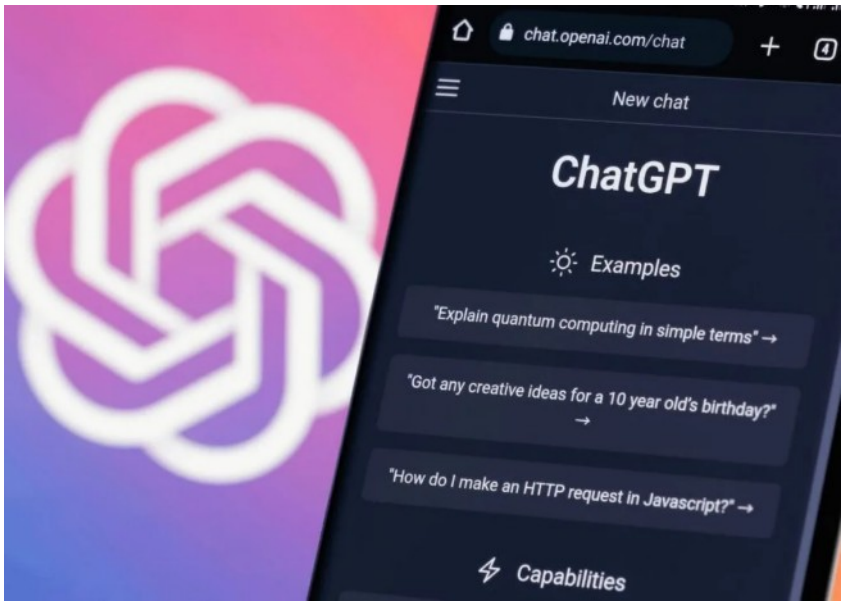
Do I Also Need to Pay a Company to Monitor If My Personal Information is Online?

Probably not. Most people can stay safe without paying for an identity or credit monitoring service, as long as they take a few basic steps to secure their digital security and privacy, including:

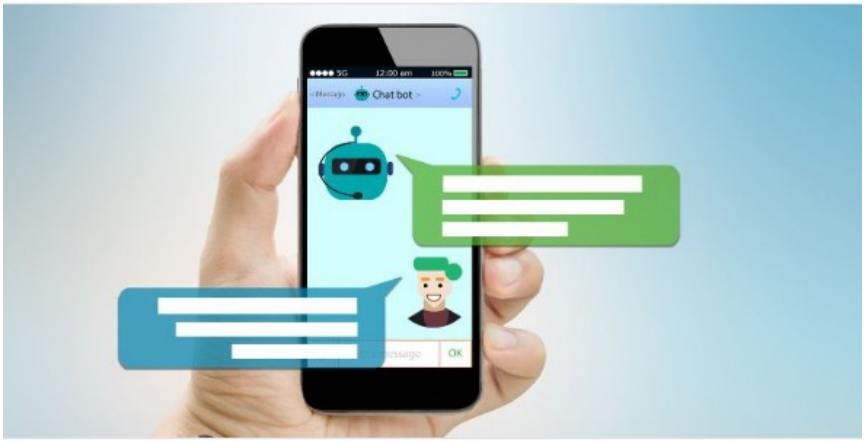
- freezing their credit
- checking their credit reports from AnnualCreditReport.com
- setting up alerts on their bank and credit cards to receive texts when there is suspicious activity
- using strong passwords and Two-Factor Authorization (2FA), especially for email, bank, or shopping accounts.

Chapter 13: Generative AI (What to Know Before You "ChatGPT")

You've probably heard a lot about AI tools lately, like ChatGPT, Gemini, or Perplexity. Maybe you've seen a friend use them or even tried them yourself to do everything from finding the best Chinese restaurant in your neighborhood to figuring out creative ideas for your 10 year old's birthday!



These AI tools are like super-powered versions of Google that you can have a conversation with, almost like a real person who can answer almost any question you can think of.



However, there is a catch: when you use these AI tools, you aren't just searching for a quick answer. You are giving information to a digital program that remembers *everything* you tell it. Because of this, you should be careful about what you share!

There are three big issues with using these AI tools:

1. The "Memory" Risk

Most AI tools are set to "remember" whatever you tell them. If you tell an AI your private medical symptoms or a secret about your job, that that information is now stored with the company providing the AI Assistant.

2. The “Stranger” Risk

Sometimes, real people (employees at the AI tool company) read through chats to make sure the AI isn’t being rude or broken. You should assume that anything you type could eventually be seen by a human eyes.

3. The “Confused” Risk

AI tools are great, but they aren’t always right. They can “hallucinate,” which is a fancy way of saying they can sound very confident while saying something that is completely untrue. Never use AI tools for important (medical, legal, financial) advice without double-checking whether that information is correct.

Here are general tips to stay safe:

- **Don’t share personal or sensitive data:** Don’t share your full name, your kids’ names, your home address, or your specific health/financial information.
- **Keep it General:** Instead of saying, “Why does my elbow hurt after hitting it on my door at 123 Main St?” just ask, “Why would an elbow hurt after hitting a door?”
- **Check the Settings:** Most of these apps have a “Privacy” or “Data” section in the settings. Look for a switch that says “Don’t use my data for training” and turn it on! (Or, why not, ask the AI Assistant how to do it!)

HERE is a longer video about the privacy of AI tools.

Chapter 14:CALIFORNIA – Deleting Your Data Online

In California, there is a powerful new law called the Delete Act (and a tool it creates called DROP). If you live in California, this is a game-changer for your privacy.

What is the "Delete Act"?

Right now, there are hundreds of companies called "Data Brokers." These are companies you've likely never heard of, but their entire job is to collect your personal info (like your income, your hobbies, or your political party) and sell it to others.

Even if you are careful with what you post on social media, Data Brokers are still "vacuuming up" info about you from public records and other apps, from what you buy to where you visit to whom you are related to!

Before this law, if you wanted your data deleted, you had to find every single one of those hundreds of companies and ask them one by one, an almost impossible task!

The Delete Act changes that. It creates a "one-stop-shop" where you can tell every registered data broker ALL AT ONCE to delete your information.

What is "DROP"?

DROP stands for the **D**elete **R**equest and **O**pt-out **P**latform.

Think of it like the "Do Not Call" registry, but for your personal data. Starting in January 2026, you will be able to go to a single website and click one button, which will send a "Delete Me" notice to every Data Broker in California.

Why Should You Care?

- **Stops the Profiling:** A DROP notice stops companies from building a secret file on you to decide what ads you see or whether to approve you for certain services.
- **Ongoing Protection:** Once you make the request through DROP, data brokers have to keep deleting your info every 45 days. They can't just delete it once and then start collecting it again the next week.

•**Stiff Penalties:** If a company doesn't follow your request, the state can fine them $200 per day, per request. This financial punishment makes companies take your privacy very seriously.

What Should You Do?

Use the DROP Button, starting Jan 2026

The official platform (DROP), built by the California Privacy Protection Agency, is HERE.

You might see companies today offering to "clean up your data" for a monthly fee. While some are helpful, remember that the California DROP platform will be FREE. You won't have to pay a private company to do what the state is making available for everyone.

ADDITIONAL RESOURCES

HERE is a more in-depth explanation of the DELETE Act and the DROP tool it creates.

HERE is a more in-depth video about Data Brokers.

Chapter 15: Resources

Surveillance Self Defense	A guide from the Electronic Frontier Foundation that teaches you how to protect your privacy online. It covers tools, strategies, and step-by-step tutorials for defending yourself from government and corporate surveillance.	Attending a Protest How to: Get to Know iPhone Privacy and Security Settings Privacy for Students
Defend Our Movements	A toolkit for activists, organizers, and marginalized communities to strengthen digital security.	Using Facebook in an Era of Mass Deportation Anti-Doxxing Guide for Activists Facing Attacks from the Alt-Right
Tech Activist	A resource hub focused on tech education and privacy rights for Black and brown communities. Offers workshops and training to empower digital freedom and resist surveillance.	Ongoing Virtual Classes – Offline and Online Security Tips for Protesters and Organizers
Electronic Privacy Information Center (EPIC)	EPIC is a public interest research center in Washington, DC. EPIC routinely files amicus briefs in federal courts, pursues open government cases, defends consumer privacy, organizes conferences for NGOs, and speaks before Congress and judicial organizations about emerging privacy and civil liberties issues.	Guide to Practical Privacy Tools
Civil Liberties Defense Center	Provides legal support and	Digital Security Program

	education for activists and movements. Focuses on defending civil rights in court and offering "know your rights" resources.	
Equality Labs	Equality Labs is a coalition of artists, advocates, healers, technologists and organizers working on intractable systems of oppression through a collaborative solution-making model for movements.	Digital Security
Privacy Rights Clearinghouse	Privacy Rights Clearinghouse is a 501(c)(3) non-profit organization committed to advancing data privacy for all by expanding access to information, increasing participation in policy discussions, and advocating for stronger rights.	Law Overview Mobile Health and Fitness apps
Wizcase Online Privacy Guide	A great introduction to Virtual Private Networks with pictures and practical advice!	
Privacy Guides	Privacy Guides is a socially motivated website that provides information for protecting your data security and privacy. We are a non-profit project with a mission to inform the public about the value of digital privacy, and about global government initiatives which aim to monitor your online activity. Our website is free of advertisements and not affiliated with any of the listed providers. Privacy Guides is built by volunteers and staff members around the world. All changes to our recommendations and resources are reviewed by at least two trusted individuals, and we work diligently to ensure our content is updated as quickly as possible to adapt to the ever-changing cybersecurity threat landscape.	Recommended Privacy Tools
Digital Privacy YouTube Videos	NBTV is a project of the Ludlow Institute, a research and media institute dedicated to helping you reclaim control of your digital life. Created and hosted by Naomi Brockwell.	Find videos HERE!