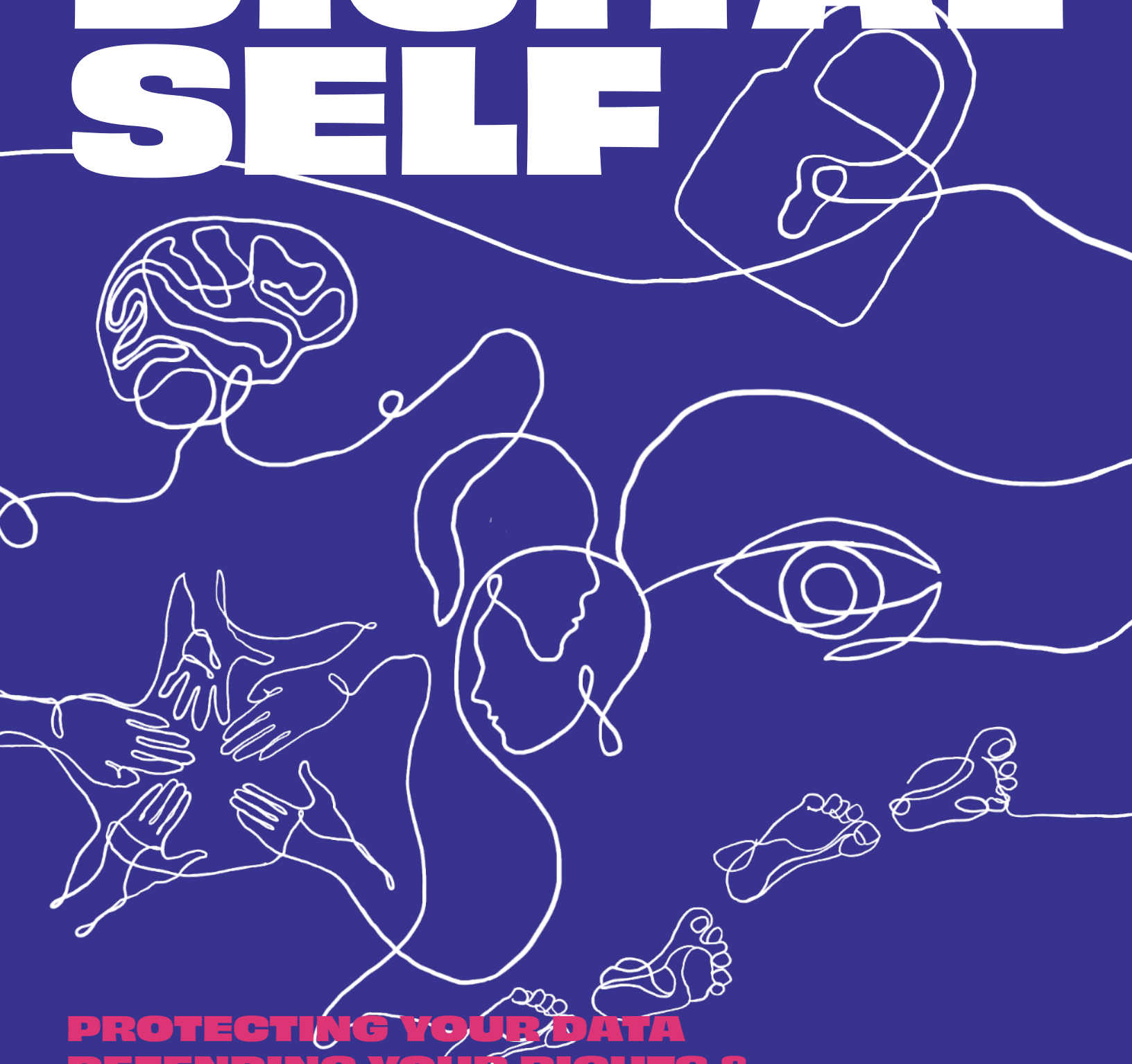
# UNDERSTANDING YOUR DIGITAL SELF



**PROTECTING YOUR DATA
DEFENDING YOUR RIGHTS &
BUILDING BETTER FUTURES ONLINE.**

## DEVELOPED & COORDINATED BY:

Avery Crower - Graduate Student at Parsons School of Design | MS Design and Urban Ecologies Program



## ACKNOWLEDGMENTS:

Community Tech Lab NY - Luis Munive &
Oscar Comunidad


This toolkit is divided into 5 sections, each focused on a key system of your digital self. Use them together or individually, whatever best supports your needs.

Protect your digital self by keeping these 5 systems safe, strong, and secure.

# DIGITAL

# PREFACE

In today's world, navigating digital spaces is as important as navigating physical ones. Our devices, accounts, and online behaviors form an invisible extension of ourselves, which we call our digital self, or our digital body. Protecting this digital self is essential for preserving your privacy, autonomy, and safety.

This toolkit is a guide for anyone who wants to better understand how technology shapes their lives and how to take back some control.

## HOW THIS TOOLKIT WORKS:

Your Digital Self is designed to be modular. Each section stands on its own, focusing on a different part of your digital self — starting with the core foundations of knowledge (Digital Literacy), to what you leave behind (Digital Footprint), to who's watching (Digital Surveillance), to how you appear online (Digital Presence), and how you can advocate for better systems (Digital Advocacy).

You can move through the toolkit in order or jump to the sections most relevant to you. Every topic offers practical tools, reflection exercises, and actionable steps to strengthen your digital health.

The toolkit uses the metaphor of a body scan,  treating your digital self with the same care you give your physical self. Each section protects a different "vital system."

## WHO IS THIS FOR:

This resource is for:

- Individuals who want to strengthen their digital privacy
- Community organizers and educators
- Youth groups, mutual aid networks, and advocacy organizations
- Anyone running workshops or conversations around digital rights, security, or inclusion

Whether you're just beginning your privacy journey or looking to sharpen your knowledge, this toolkit is made to be accessible and adaptable.

## HOW TO USE IT:

**Independently:** Treat this toolkit like a guidebook. Choose a section to dive into, complete the reflection activities, and apply the practices to your everyday tech use.

**In Shared Spaces:** This toolkit is also workshop-friendly. Use the sections as modules for discussions, community trainings, or even casual group conversations. Reflection prompts, checklists, and activities are designed to be printable, shareable, and remixable.

**In Workshops:** Each section can be the foundation for a workshop session, classroom lesson, or community meeting. Start with a short discussion of the concepts, invite personal reflection, then move into practical activities or demonstrations.

You can explore, share, and adapt the materials to fit the needs of your space.

## USING THIS TOOLKIT IN WORKSHOPS

This toolkit is built to support a variety of group learning environments—from classroom settings and community centers to informal living room gatherings. Each section can serve as a standalone session or be integrated into a multi-part workshop series. The modular format makes it easy to tailor discussions to different audiences based on age, digital literacy levels, or community needs. Here are ways to bring it to life in workshops:

- **Start with a Check-In:** Open with a prompt related to the section (e.g., "When was the last time you checked your privacy settings?" or "What do you think happens to your data after you close an app?").
- **Use the Reflection Activities:** Each section includes prompts that can spark personal insights and group discussions. Encourage journaling or small group sharing.
- **Facilitate Hands-On Demos:** Walk participants through privacy settings, data tracking tools, or encrypted messaging apps. Make it interactive—bring devices if possible.
- **Print and Remix Tools:** Use the checklists and exercises as printouts, handouts, or projected slides. Let participants annotate or personalize them.
- **Host Role-Plays or Scenarios:** Act out real-life tech situations (e.g., responding to a phishing scam or deciding whether to use a public Wi-Fi network) and talk through choices.
- **Build Together:** Use the Advocacy section to co-create privacy pledges, group norms for safe tech use, or strategies to support others.
- **End with a Takeaway:** Encourage participants to name one practice they'll try, one thing they'll share, or one tool they'll explore further.

## NAVIGATING YOUR DIGITAL SELF TOOLKIT:

The toolkit is structured like a digital body map:

- Digital Literacy (The Brain): Core knowledge and awareness
- Digital Footprint (Your Feet & Trail): What you leave behind
- Digital Surveillance (The Eyes Watching You): Who sees you and how
- Digital Presence (Your Outer Layer): How you appear online
- Digital Advocacy (Your Armor and Voice): How you defend and strengthen your digital rights

Each part connects to the next,  building a fuller picture of your digital self and how to be digitally private.

02

# DIGITAL FOOTPRINT

# WHAT IS A DIGITAL FOOTPRINT?

Your digital footprint is the trail of data you leave behind whenever you use the internet; both the information you actively share (like posts and internet searches) and the data collected passively (like cookies, IP addresses, and location data).

This footprint includes all traces, content, and data points connected to your online activity, shaping how people, companies, and institutions perceive and treat you.

**It can have lasting impacts on your privacy, security, reputation, and even your access to opportunities in areas like employment and education.**

# KEY TERMS

**Understanding your digital footprint starts with knowing the key terms behind how data is created, tracked, and used.**

**VOLUNTARY DATA:** The information you intentionally and knowingly provide while using digital platforms, such as an Instagram post or a subscription sign-up.

**INVOLUNTARY DATA:** The information collected about you without your explicit input or awareness. It's often gathered automatically in the background as you browse or interact with digital tools. Even if you didn't click "share," it's most likely shared anyway.

**METADATA:** Data about your data. It's secondary information embedded within digital files or communications, describing when, where, and how something was created. Metadata can reveal details like the time, location, device used, or sender and recipient, offering hidden insights into behavior, movement, and routines.

**THIRD-PARTY PLUGIN:** A third-party plugin is a tool or feature embedded into a website by an external company, rather than the owner of the site. These plugins, such as embedded videos, comment sections, or social media buttons, often collect user data for the third-party, even if the user does not engage with the tool directly.

**API:** An Application Programming Interface (API) is a set of protocols that allows different software systems to communicate and exchange data. While APIs enable convenient integration between platforms, such as connecting a map to a ride-share app, they also serve as channels through which user data is transferred, sometimes without clear user awareness or consent.

**DATA BROKER:** A data broker is a company that collects, aggregates, and sells personal information about individuals, often without their direct knowledge. This data is sourced from public records, digital interactions, commercial transactions, and app usage. Brokers compile detailed profiles used for marketing, insurance, credit scoring, or surveillance purposes.

**INFERENCE ALGORITHM:** Using patterns in digital behavior, systems can infer details like age, political views, income, and mental health, even if never directly shared. Built into platforms and ad systems, these predictive models use incomplete data to create detailed user profiles, shaping what content, services, or opportunities people see, or are excluded from, without their consent.

**DIGITAL FINGERPRINTING:** A tracking method that identifies and monitors users based on the unique configuration of their device and browser, such as what browser you use, your screen size, installed fonts and plugins ,and language. Unlike cookies, digital fingerprints can't be easily deleted or turned off, which makes them a powerful and hard-to-detect tracking method.

# VOLUNTARY & INVOLUNTARY DATA COLLECTION

## WHAT ARE YOU GIVING VS. WHATS BEING TAKEN?

### VOLUNTARY

You choose to share, even if you don't always realize what you're giving up long-

**Examples:**

- Signing up for a newsletter
- Posting a photo publicly
- Filling out a form with your name and email
- Accepting cookies (even if you don't read them)
- Adding a location to your Instagram photo
- Uploading a video to TikTok
- Using your face to unlock your phone
- Joining a loyalty program or rewards app
- Agreeing to app permissions for convenience (like a weather app using your location)
- Taking online personality quizzes
- Commenting or liking posts on public forums or pages

### INVOLUNTARY

Data collected about you, even if you never actively shared it.

**Examples:**

- Location tracking is running silently in the background on apps
- Bluetooth and Wi-Fi track your device as you move through stores, airports, or cities.
- Data brokers will buy and sell your personal information without consent.
- Smart TVs track what you watch and reporting it back to advertisers
- Facial recognition scanning you in public without your knowledge.
- Predictive text algorithms analyze your messages and emails.
- Keyword scanning by email providers for ad targeting, like Gmail scanning emails for product ads.

**Not all data is voluntary. Some is taken without asking.**

# HOW IS YOUR DATA COLLECTED, STORED, & SOLD?

## COLLECTION

It starts with your clicks, swipes, searches, and shares.

- Websites you visit
- Apps you download
- What you type, watch, buy, or like
- Cookies, device sensors, and location tracking
- Voice assistants listening for commands
- Even if you don't submit a form, just being online creates data trails.

## STORAGE

Your data doesn't disappear, it gets saved.

- Stored in massive databases or cloud servers
- Linked to identifiers like your IP, email, or device ID
- Analyzed to build profiles about your habits, interests, and behavior.

## SALE

Your digital self becomes a product. Data brokers, advertisers, and third-party companies may:

- Buy and sell your data to target you with ads.
- Share your behavior with other platforms
- Use it to influence your decisions, limit your options, or predict your actions. You rarely see it, but your information becomes someone else's profit.

**You are not the customer, you are the product.**
**Knowing how your data moves is the first step to protecting it.**

# HOW IS YOUR DIGITAL FOOTPRINT BUILT?

Every click, search, and scroll adds to the file on you


# DATA DETOX CHECKLIST

TOOL: De-clutter your digital trail and take back control of what you leave behind

## REVIEW YOUR *VOLUNTARY* FOOTPRINT

*Everything you’ve intentionally posted, shared, or signed up for.*

- ☐ Google yourself - What shows up?
- ☐ Check your public social media profiles - What can strangers see?
- ☐ Delete or hide old accounts you no longer use (you can use tools like JustDelete.me)
- ☐ Unsubscribe from email lists you don’t need
- ☐ Clear out your public comment history on blogs, forums, Reddit, etc.
- ☐ Update or remove outdated bios, photos, or contact info that you no longer want out there
- ☐ Create a “burner” email for apps, contests, or one-time downloads
- ☐ Delete apps you no longer use.

## QUICK SCAVENGER HUNT

Pick one file topic from the left and find a real example on your phone!

- **Voluntary Data:** Delete an old post you don’t want to be public.
- **Plug-Ins:** Spot a hidden “Like” button or embedded map.
- **Inference Algorithms:** Think about a creepy targeted ad you saw.
- **Metadata:** Check a photo for hidden location info.

## REDUCE YOUR IN*VOLUNTARY* FOOTPRINT

*The stuff collected passively, without your full awareness.*

- ☐ Turn off location services for apps that don’t need it

  *Settings > Privacy & Security > Location Services > Disable location for all apps, or Individually based on your preference.*

- ☐ Disable auto-fill and saved passwords in browsers you don’t trust

  *Do this in the settings of your chosen browser app*

- ☐ Use Privacy-first browsers like Brave, Tor, or DuckDuckGo.
- ☐ Clear cookies and site data regularly (or auto-delete when browser closes)

  *Settings > Privacy & Security > Clear Browsing Data*

- ☐ Add extensions like uBlock Origin or Privacy Badger to block trackers

  *These extensions block ads, trackers, and known malicious scripts, making your page load faster and preventing it from tracking you.*

**Small actions add up.**

**FIND IT. FIX IT. PROTECT YOUR FOOTPRINT**

# APP PERMISSIONS MAP

When you download an app, it often asks for access to different parts of your phone, like your location, contacts, microphone, camera, or even your calendar and health data. Some of these permissions are necessary for the app to function, but many are turned on by default or requested in ways that make it feel easier to say yes than to ask questions.

The truth is, by granting access, you're often giving away more than just functionality; you're giving apps insight into your daily life, your habits, and even your identity. This map breaks down the most common types of permissions apps request and why they matter.

The good news? You have the power to change most of these settings in your phone's privacy menu, but you have to know they're there first.

## CONTACTS

**What they get:** Names, Numbers, email addresses, and social connections.
**Why it matters:** Apps can map your relationships, sync them to third parties, or use them for growth tactics ("invite your friends!"). You're not just giving up your privacy - you're giving up theirs too.

## LOCATION

**What they get:** Your real-time location, past locations, travel routes, nearby Wi-Fi networks, where you've been, how often, and when.
**Why it matters:** Apps like ride shares need your location to work, but many keep tracking you in the background, even when you're not using them. Over time, that data can reveal patterns about your home, work, habits, routines.

## CAMERA

**What they get:** Access to your photos and videos.
**Why it matters:** Some apps can activate your camera without clear consent or might continue to access it even when not in use. Apps don't need your camera unless you're actively using features like video or scanning, and even then, you can turn it on just when needed.

## MICROPHONE

**What they get:** Audio input - potentially ambient conversation, background noise, and voice commands.
**Why it matters:** Some apps may be passively listening. Even if not recording, data like sound patterns can be used to guess context (like if you're in a busy place, with music, or around other voices).

## CALENDAR

**What they get:** Events, times, locations, and attendees
**Why it matters:** Apps can analyze how busy you are, where you're going, who you meet with, and even what kinds of events you attend, which can be used for profiling or ad targeting.

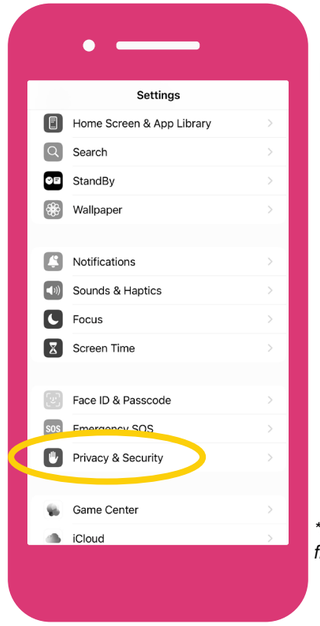
# HOW TO:
# MANAGE YOUR APP PERMISSIONS

## IPHONE APP PERMISSIONS:

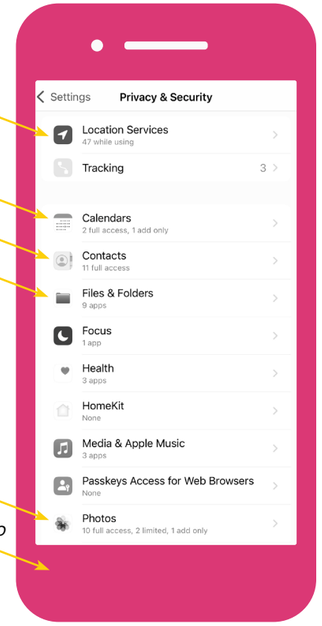
1. Go to your Settings App

2. Scroll to find Privacy & Security

3. Adjust what personal information your apps have access to




Location Services
Calendar
Contacts
Files
Photos
*Scroll down on this page to find Microphone*

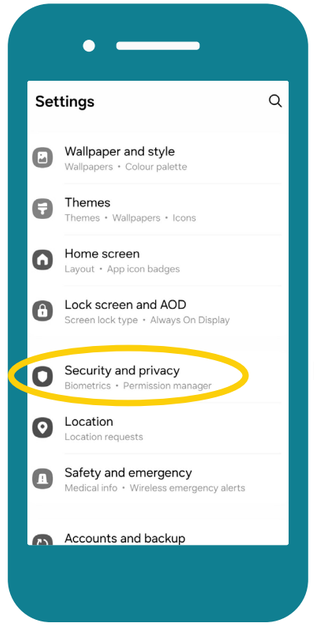



## ANDROID APP PERMISSIONS:

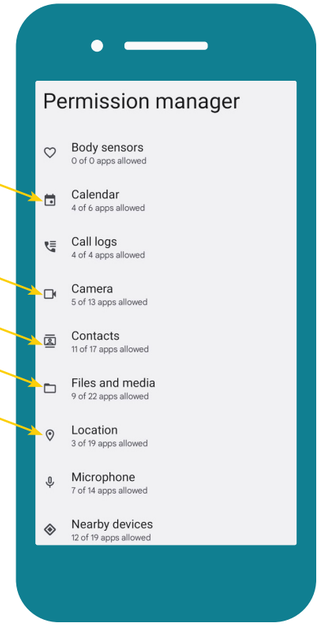
1. Go to your Settings App

2. Scroll to find Privacy & Security

3. Adjust what personal information your apps have access to




Calendar
Camera
Contacts
Files
Location Services



# PROTECT YOUR ACCOUNTS

## PASSWORDS, 2FA, & PASSWORD MANAGERS

Your accounts are the keys to your digital life. Strong passwords and two-factor authentication (2FA) keep your digital footprint safe from breaches, hacks, and impersonation.

### CREATE STRONG, UNIQUE PASSWORDS

- Use long passwords - at least 12-16 characters
- Avoid using obvious information as your password (birthdays, pets, nicknames)
- Never use the same password across multiple sites

### USE A PASSWORD MANAGER

Password managers create, store, and autofill strong, unique passwords for your accounts, so you don't have to remember them all.

***How they work:***

- You set one strong master password to unlock the manager
- The manager encrypts all your saved passwords, keeping them secure.
- When you log in to a website or app, the manager can autofill your password safely
- Some password managers also suggest strong passwords when you're creating new accounts

The passwords stay encrypted until you unlock them with your master password, meaning even the company that makes the manager can't see them.

Reusing passwords across accounts is risky. Password managers help you stay safe without having to memorize dozens of complex passwords.

*Recommended Password Manager: Bitwarden*

### TWO-FACTOR AUTHENTICATION (2FA)

Two-factor authentication (2FA) adds an extra layer of security to your accounts.

Even if someone steals your password, they can't get in without a second code

**How to Turn on 2FA:**

***1. Open the app or website settings.***

Look for Settings → Security → Two-Factor Authentication or Login Security.

***2. Choose your authentication method.***

- Authentication App (Duo Mobile, Aegis Authenticator, 2FAS): recommended method
- Text Message (SMS): less secure, but better than nothing
- Security Key or Hardware Token — a physical device for even stronger protection.

***3. Follow the setup instructions.***

- If using an app, scan the QR code or enter a setup key.

If using SMS, confirm your phone number.

***4. Save your backup codes!***

Backup codes help you get back into your account if you lose access to your phone.

**The more doors you lock, the harder it is to break in.**

# WHAT IS ENCRYPTION?

Encryption transforms readable data (like a message or file) into scrambled code that looks like gibberish unless you have the right cryptographic key to unlock it.

### HOW IT WORKS:

**Plain Text** → **[Encryption Key]** → **Encrypted Data**

**Encrypted Data** → **[Decryption Key]** → **Plain Text Again**

### WHERE ENCRYPTION HAPPENS:

- Secure Websites (https)
- Messaging Apps
- Password Managers
- Email Services
- Cloud Backups
- VPNs

### WHY ENCRYPTION MATTERS:

- Protects your privacy
- Secures your identity, passwords, and messages.
- Blocks hackers and unauthorized access
- Builds trust in digital communication
- Often required by law for sensitive info (healthcare, banking)

### TYPES OF ENCRYPTION:

**Basic Encryption:** Your data is encrypted, but the service (like Google or Facebook) might still have access to the key

**End-to-End Encryption (E2EE):** Only the sender and recipient have the keys. No one else, not even the app, can read it.

### TIPS FOR EVERYDAY PROTECTION:

- Use messaging apps with E2EE (Signal is the best option)
- Avoid syncing encrypted content to cloud services without checking settings
- Use password managers and encrypted storage.
- Keep software up to date (encryption breaks if the system is weak!)

**Encryption is the foundation of digital privacy, but not all encryption protects you equally.**