# DIGITAL HEALTH BASICS

*A Beginner's Guide to Safe, Informed, and Balanced Digital Living*

Stephanie Garcia

# DIGITAL HEALTH BASICS

*A Beginner's Guide to Safe, Informed, and Balanced Digital Living*


---

## TABLE OF CONTENTS

1. Introduction: Why Digital Life Shapes Real Life
2. Technology in Everyday Living
3. Understanding Your Devices
4. What Is the Internet?
5. Websites, Web Addresses, Extensions, and Search Engines
6. Accounts, Passwords, Biometrics, and Device Recognition
7. Foundations of Digital Safety
8. Understanding Credit, Identity, and Why Protection Matters
9. Common Digital Harms
10. Online Spaces and Where Harms Occur
11. Digital Hygiene: Healthy Habits That Protect You
12. Reclaiming Balance: Why Disconnection Matters
13. Where to Get Help
14. Conclusion
15. APPENDIX A – REFERENCES
16. APPENDIX B – GLOSSARY OF DIGITAL TERMS

# INTRODUCTION — WHY DIGITAL LIFE SHAPES REAL LIFE

Technology now shapes nearly every part of modern life. We use it to communicate with family, work from anywhere, learn new skills, shop, manage money, navigate the world, and stay informed. These tools have made life easier and more connected—but they have also introduced new risks, new kinds of stress, and entirely new forms of harm.

For many people, the digital world grew faster than their understanding of it. Devices became more advanced, apps became more persuasive, and online interactions became more complex. As a result, many adults feel uncertain, overwhelmed, or left behind—not because they are incapable, but because technology has changed at a pace no one was prepared for.

You do not need any technical background to use this guide. It is written for beginners—people who may be using smartphones, apps, or the internet for the very first time. It can also be used as refresher training by users who have been using smart technology regularly.

---

## How to Use This Guide: Format That Builds Step by Step

To make learning simple and meaningful, each section of this guide follows the same structure, designed to support new learners and reduce confusion:

### *1. Key Terms First*

Before teaching any topic, the guide begins with a short list of definitions of new words or concepts. This ensures you never encounter unfamiliar terms without understanding them.

### *2. Clear Explanation of the Topic*

Each section then teaches the concept in a step-by-step manner, using real examples, simple analogies, and practical explanations.

### *3. Practical Everyday Application*

Instead of theory alone, the guide shows:

- Why the concept matters
- How it applies to real life
- What you need to do on your own device

### *4. Risks and Harms to Watch For*

When relevant, sections explain the risks connected to that part of digital life and how they appear in daily use.

### *5. What You Can Do to Stay Safe*

Actionable, simple steps for protecting your device, privacy, identity, and wellbeing.

### *6. Gentle Transitions Between Sections*

The guide is written in a way that one idea naturally prepares you for the next—building digital confidence brick by brick.

If you are interested in learning or refreshing your knowledge on specific topics in this guide, consult the Table of Contents as the sections can be stand-alone guides. Consult the Glossary for any unfamiliar terms.

---

## Why Digital Health Matters

Digital health is not only about cybersecurity. It includes:

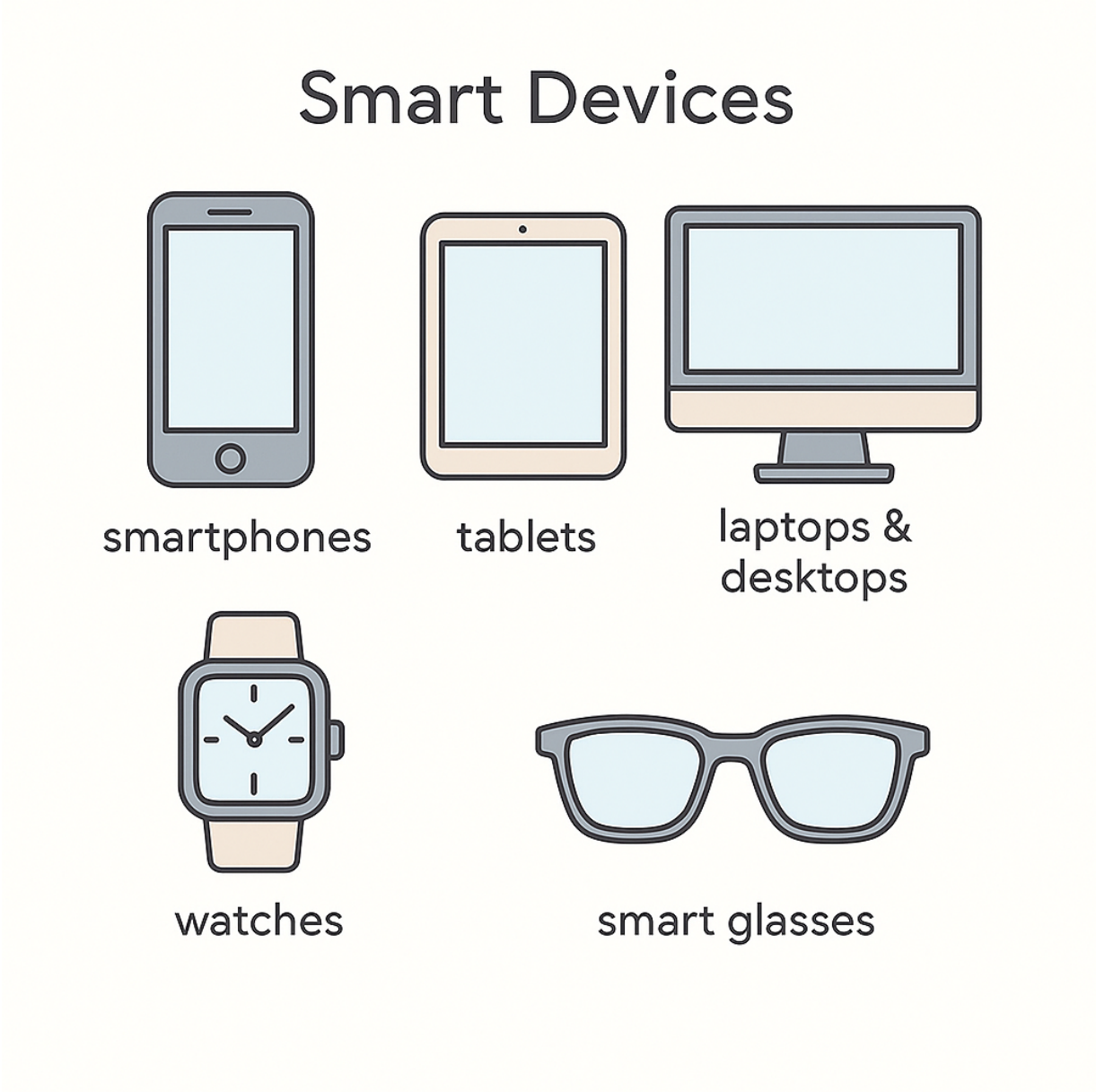
- protecting your identity
- managing your attention
- reducing stress
- recognizing harmful content
- preserving your mental and emotional wellbeing
- balancing screen time with real life
- understanding how technology influences your choices

With the right knowledge, anyone—at any age or skill level—can navigate digital life with confidence. This guide will show you how.

Before we can understand digital safety, we begin with the basic tools in our hands—the devices that connect us to the digital world.

# SECTION 2 — UNDERSTANDING YOUR DEVICES

*A clear foundation for everything else in digital life.*



## 🔷 Key Terms

**Device:** Any piece of technology you use to enter the digital world—such as a smartphone, tablet, laptop, or computer.

**Hardware:** The physical parts of a device (screen, buttons, camera, speakers).

**Software:** The programs and apps that make the device work.

**Operating System (OS):** The main software that controls everything on the device.
It manages apps, settings, files, security, and updates.

**Internet:** a giant, worldwide network connecting billions of computers and devices, allowing them to share information and talk to each other instantly

**Wi-Fi:** A wireless signal that connects your device to the internet.

**Mobile Data:** The internet connection provided by your phone company when you are not using Wi-Fi.

### Most Common Operating Systems:

- **iOS** — iPhones
- **iPadOS** — iPads
- **Android** — Samsung, Google Pixel, Motorola, and many other phones and tablets
- **Windows** — most laptops and desktop computers
- **macOS** — Apple Mac computers

### How They Differ:

- **iOS / iPadOS:** Clean design, fewer device models, strong privacy controls, easy for beginners.
- **Android:** Many kinds of devices, more customization, flexible storage options.
- **Windows:** Most widely used for school and work, supports many programs and printers.
- **macOS:** Strong security, stable performance, used a lot in creative fields.

**Website:** A collection of interconnected digital pages and content (text, images, videos) under a single domain name, accessible via the internet through a web browser, serving as an online presence for information, services, or entertainment.

**Browser:** An application used to visit websites (Chrome, Safari, Firefox, Edge).

**Bluetooth:** A short-range wireless connection for headphones, speakers, wearables, or cars.

**Storage:** The space on your device where apps, photos, videos, and files are saved.

**Settings:** Where you control how your device behaves — privacy, passwords, sound, brightness, updates.

**Update:** A software improvement that adds security fixes and new features.

**HTTP**: Hypertext Transfer Protocol is the basic system that allows your browser to load websites, but it does not encrypt your information, making it less secure.

**HTTPS:** Hypertext Transfer Protocol Secure is the secure version of HTTP that encrypts your information, protecting your data when you visit websites.

---

## 2.1 — Why Your Device Matters

Your device is the *gateway* to the digital world. Everything—from texting to shopping, from email to banking—begins with understanding the tool in your hand.

If you learn how your device works, every other part of this guide will make more sense.

---

## 2.2 — Types of Devices

**Smartphones:** Handheld devices used for calls, texts, internet, apps, photos, and maps. Examples: iPhone, Samsung Galaxy, Google Pixel.

**Tablets:** Larger touchscreens used for browsing, reading, watching videos, and creative apps. Examples: iPad, Lenovo Tablet.

**Laptops & Desktops:** More powerful computers used for writing, work, school, and file storage. Examples: Windows PC, MacBook.

**Wearables:** Small devices you wear that track health, display notifications, and pair with your phone. Examples: Apple Watch, Fitbit, Meta Smart Glasses.

**Smart TVs & Home Devices:** Televisions and smart speakers that connect to apps, streaming, and voice assistants.: Examples: Roku TV, Amazon Echo, Google Home.

---

## 2.3 — What an Operating System Does

Every device runs an operating system (OS), which is the main software that controls how your device works. Examples include iOS on iPhones, Android on most smartphones, and Windows on many computers. You can think of OS as the *brain* that tells the device how to behave.

The OS controls:

- how the screen looks
- how apps open and close
- how your device connects to Wi-Fi
- how notifications appear
- how your photos and files are organized
- how security works
- how updates are installed

If you understand your operating system, you can follow instructions more easily.

---

## 2.4 — Basic Device Functions

These are the core skills every beginner should know, because they appear everywhere in digital life.

**Connecting to Wi-Fi:** This lets your device go online without using cellular data.

**Installing Apps:** Apps are downloaded tools that let you check email, shop, navigate, message, or watch videos.

**Using the Browser:** A browser lets you visit websites, search for information, and enter web addresses.

**Managing Storage:** Every device has limited space. Deleting old apps, photos, or downloads helps your device run smoothly.

**Checking Settings:** The Settings menu controls:

- volume
- brightness
- passwords
- privacy
- Bluetooth
- notifications
- software updates

**Recognizing Security Alerts:** Your device may warn you about:

- outdated apps
- unsafe websites
- weak passwords
- untrusted connections

These alerts exist to protect you.

---

## 2.5 — Risks to Watch For (Device-Level Harms)

Even at the device level, certain risks can appear:

- **Outdated software** → makes your device easier to hack
- **Unknown apps** → may contain malware
- **Too many notifications** → increase stress and cause accidental clicks
- **Low storage** → makes the device slow or unstable
- **Ignoring security alerts** → compromises safety

These risks are small but important to notice.

---

## 2.6 — What You Can Do to Stay Safe

Simple protective habits:

- Keep your device updated automatically
- Only install apps from official stores
- Check your Settings monthly
- Delete apps you do not use
- Regularly restart your device
- Use a screen lock (Personal Identification Number [PIN], password, Face ID)
- Be cautious on public Wi-Fi

These habits form the foundation of digital safety.

## 2.7 — Why This Section Matters

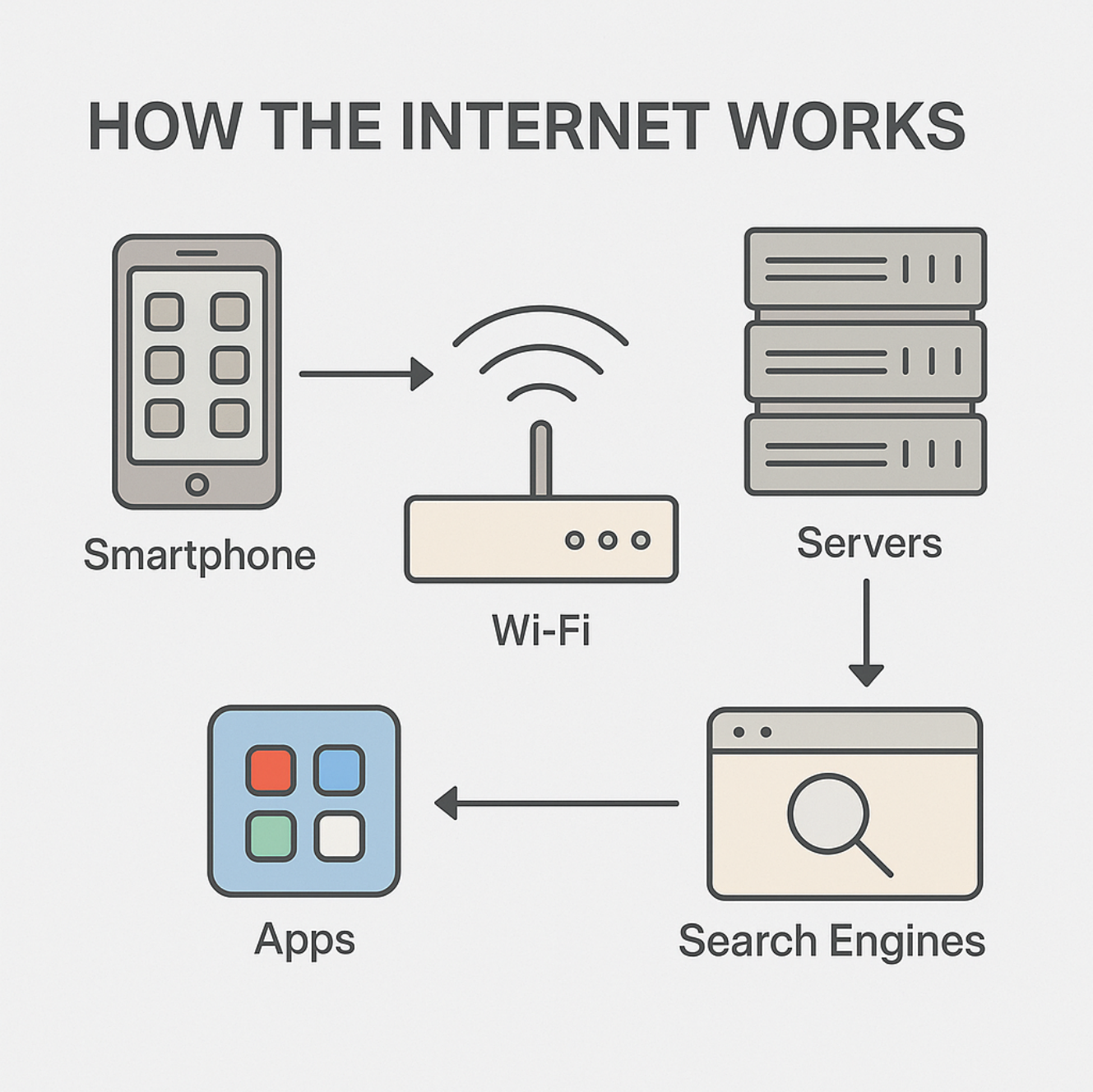
Before we talk about websites, platforms, scams, algorithms, or online harms, you need a strong understanding of the device itself. Once you know how your device works, everything else in the digital world becomes less confusing and much more manageable.

These devices are only as useful as the networks they rely on. Now that you understand how your device works, we can explore the larger system that connects everything—the internet itself.

---

# SECTION 3 — WHAT IS THE INTERNET?

*Understanding the invisible network that connects every device.*



## 🔷 Key Terms

**Internet**: A worldwide network that connects billions of devices so they can send and receive information.

**Network:** A group of connected devices that can communicate with each other.

**Wi-Fi:** A wireless signal that lets your device connect to the internet without cords.

**Mobile Data:** Internet provided by your phone company using cell towers.

**Router:** The device in your home that sends Wi-Fi to all your phones, TVs, and computers.

**Modem:** The device that brings the internet signal from your service provider into your home.

**ISP (Internet Service Provider):** The company you pay for home internet (Comcast, AT&T, Verizon, Spectrum).

**Server:** A powerful computer that stores websites, videos, apps, and online data that sends information to your device when you request it.

**Bandwidth:** How much information your internet connection can carry at once—like the width of a pipe.

**Browser:** An app (Chrome, Safari, Firefox, Edge) that lets you access websites.

**URL (Uniform Resource Locator, Web Address):** The text you type or click to reach a website (e.g., www.example.com).

**Public Wi-Fi:** Wi-Fi (Wireless Fidelity) in coffee shops, stores, hotels, or airports—often less secure.

**Cybercriminals:** people who use computers or the internet to steal information, money, or cause harm.

---

## 3.1 — What the Internet Actually Is

The internet is not one machine. It is a global system of connected devices—phones, computers, tablets, servers—speaking a common "language." Wi-Fi connects your device to your home router, which then connects to your internet provider. Mobile data connects through your phone company's cellular towers when Wi-Fi is not available. When you open an app, visit a website, send a message, or watch a video, your device sends a request through the network. A server somewhere else in the world responds by sending information back. You never see this process, but it happens every second you are online.

---

## 3.2 — How the Internet Works

1. **Your device connects to a network**
   - Either through **Wi-Fi** or **mobile data**.
2. **Your request travels to your ISP**
   This is the company providing your internet.
3. **The request goes to a server**
   Servers store websites, videos, maps, emails, and app data.
4. **The server sends information back**
   This might be:
   - A webpage
   - A video
   - A search result
   - A message
   - A photo
5. **Your device displays what you requested**
   All this happens in less than a second.

---

## 3.3 — Home Internet: What Each Device Does

**Modem:** Connects your home to the internet through your ISP.

**Router:**

- Sends the Wi-Fi signal around your home
- Controls who can connect
- Protects your devices with passwords and encryption

Many modern devices combine modem + router into one unit.

---

## 3.4 — Public Wi-Fi: What You Should Know

Public Wi-Fi is convenient but risky. Because it is shared by many strangers, it is easier for cybercriminals to:

- Intercept unprotected information
- Fake a Wi-Fi network that looks legitimate
- Access devices with weak security
- Capture passwords typed on unsafe websites

Use caution when using public Wi-Fi. If a website does not use HTTPS, anything you type—such as passwords or personal information—can potentially be seen by someone else on the network.

---

## 3.5 — Bandwidth

Bandwidth is like the width of a water pipe. The wider the pipe, the more water can flow through at once. If too many devices use the same connection, your internet may:

- Slow down
- Buffer videos (download in chunks)
- Drop calls
- Lag during games or meetings

---

## 3.6 — Risks to Watch For (Internet-Level Harms)

- Fake public Wi-Fi networks
- Weak router passwords
- Outdated modem/router equipment
- Unencrypted websites (no lock icon)
- Slow or overloaded connections
- Data theft on unsecured networks

These types of risks can affect your entire digital experience.

---

## 3.7 — What You Can Do to Stay Safe

- Use strong Wi-Fi passwords at home
- Update your router’s software when possible

- Avoid banking or entering personal information on public Wi-Fi
- Check for **HTTPS** and the lock icon on websites
- Forget networks you don't trust
- Restart your router occasionally
- Use your phone's mobile data if Wi-Fi feels unsafe

---

## 3.8 — Why This Section Matters

Everything in digital life—websites, apps, messages, shopping, social media—depends on the internet. Understanding how you connect and what risks exist helps you make safer decisions.

Now that you understand how the internet carries information, the next step is learning how to navigate it—starting with websites, web addresses, and search engines.

# SECTION 4 — WEBSITES, WEB ADDRESSES, EXTENSIONS & SEARCH ENGINES

*How to understand the places we visit online.*

## 🔷 Key Terms

**Website:** A collection of pages on the internet that provide information or services (ex: news sites, stores, government pages).

**Webpage:** A single page within a website, like a chapter in a book.

**Homepage:** The main page of a website—its front door.

**Browser:** The app you use to visit websites (Chrome, Safari, Edge, Firefox).

**URL (Web Address):** The text that tells your browser where to go, such as: **https://www.example.com**

**Domain:** The main name of a website (example.com).

**URL Extension:** The ending of the website address, which gives clues about what the site is:

- **.com** — commercial/business
- **.org** — nonprofit
- **.gov** — government
- **.edu** — education
- **.mil** — U.S. military
- **.net** — network or service provider
- **.ph / .uk / .ca / .jp** — country-specific domain

**HTTPS:** Secure version of HTTP. The "S" means "secure," showing the site protects your information.

**Lock Icon:** The small padlock next to a URL that shows your connection to the site is encrypted (safer).

**Search Engine:** A website used to search for information: Google, Bing, DuckDuckGo.

**Search Results Page:** The list of links a search engine shows after you type something in.

**Ad / Sponsored Link:** A paid result that appears at the top of search results; not always the best or safest option.

**About Us Page:** A webpage that explains who created the website or organization.

**Contact Page**: Where you can find phone numbers, emails, addresses, or support information.

**Privacy Policy:** A page explaining how the website collects, stores, or shares your information.

**Pop-up:** A small window that suddenly appears ("pops up") over the main webpage or application, usually to grab your attention for ads, newsletter sign-ups, discounts, or important alerts, often created by JavaScript to overlay content and drive user action like subscribing or claiming offers.

---

## 4.1 — What Is a Website?

A website is simply a place on the internet where information lives. It can be:

- a store
- a school or government office
- a news outlet
- a blog
- your bank
- a social media platform
- a video streaming service

Every website is made of **pages**, connected like rooms in a larger building.

---

## 4.2 — The Anatomy of a Website (Simple Breakdown)

Most websites contain:

- **Homepage** — the main starting point
- **Menu (Navigation Bar)** — links to important pages
- **About Page** — explains who runs the site
- **Contact Page** — phone numbers, emails, support forms
- **Footer** — small text at the bottom with legal info, terms, and links
- **Search Bar** — helps you find information inside the site

If a website hides contact information or seem secretive, it may not be trustworthy.

---

## 4.3 — How to Read a Web Address (URL)

Let's take an example:

**https://www.dolexample.gov/contact**

Breakdown:

- **https://** — secure connection
- **www** — part of the address format
- **dolexample** — website name
- **.gov** — government site
- **/contact** — the specific page you're visiting

This helps you verify whether a site is legitimate.

---

## 4.4 — URL Extensions and What They Tell You

### Common Extensions

- **.com** — companies and store websites
- **.org** — nonprofits or community organizations
- **.gov** — official government websites
- **.edu** — schools, universities, educational institutions
- **.mil** — U.S. military
- **.net** — networks, utilities, service providers

### International Extensions

These endings are called country-code top-level domains (ccTLDs). They show the website is associated with a specific country:

- **.ph** — Philippines
- **.uk** — United Kingdom
- **.ca** — Canada
- **.jp** — Japan
- **.au** — Australia

This is important when confirming which country's laws, prices, or services apply.

---

## 4.5 — What Makes a Website Legitimate?

Look for:

- **HTTPS** at the beginning
- **Lock icon**
- **Correct spelling** of the website
- **Clear About Us** page

- **Functional Contact page**
- **Professional layout**
- **No excessive pop-ups**
- **No strange or overly long URLs**

If any of these seem off, slow down and double-check.

---

## 4.6 — Search Engines: How They Work

Search engines scan billions of pages to help you find what you need. Most people use Google, but other search engines like Bing or DuckDuckGo may show different results. Google is good for broad searching, Bing works well with Microsoft devices, and DuckDuckGo focuses on privacy and tracks less of your activity.

When you type something like:

“symptoms of heat exhaustion”

Google shows:

- Relevant websites
- Videos
- News articles
- Health organizations
- Ads (usually at the top)

### Important to Know

Search engines show content by:

- popularity
- your past searches
- credibility
- advertising

This means:

- The top result is *not always the best*
- Ads are *not the same as trusted sources*

---

## 4.7 — Risks to Watch For (Website-Level Harms)

- **Fake websites** designed to look real
- **Typosquatting** (fake URLs like “bankofarnerica.com”)
- **Spoofed government websites**
- **Unsafe links hiding in ads**
- **Pop-ups that mimic warnings**
- **Unsecured HTTP sites**
- **Misleading information**
- **Fake stores offering impossible deals**

Websites can be manipulated easily, so knowing what to look for is important.

---

## 4.8 — What You Can Do to Stay Safe

- Always check the **URL**
- Look for **HTTPS** and the **lock icon**
- Use official search terms (“IRS”, “SSA”, “CDC”)
- Bookmark trusted websites
- Avoid clicking ads when searching for services
- Compare information across multiple credible sites
- Use caution with unfamiliar or flashy pages

When shopping online:

- Check reviews
- Verify seller legitimacy
- Examine return policies
- Look for secure checkout

A good rule to live by is that if it’s too good to be true, there is a high probability that it is not.

---

## 4.9 — Why This Section Matters

Once you can read a website address, recognize legitimate pages, and understand search results, the entire internet becomes safer and easier to navigate.

Every website we visit and every service we use asks us to create a digital identity. Knowing how accounts, passwords, and recognition systems work is essential for safety.

# SECTION 5 — ACCOUNTS, PASSWORDS, BIOMETRICS & DEVICE RECOGNITION

*How you prove who you are in the digital world.*

## 🔷 Key Terms

**Account:** A personal profile you create to use a website, platform, app, or service.

**Username:** The name you use to sign in or identify yourself on a platform (your email, or a chosen name).

**Password:** A secret combination of letters, numbers, and symbols that protects your account.

**Strong Password:** A password that is long (12+ characters) and difficult to guess.

**Password Manager:** A tool that stores and generates secure passwords for you.

**Multi-Factor Authentication (MFA):** A second step during login (a code, fingerprint, or app prompt) that proves the account belongs to you.

**Two-Step Verification:** Another name for MFA.

**Biometrics:** Ways of unlocking your device or account using your body — fingerprint, face scan, voice ID.

**Device Recognition:** When a system remembers a device you have logged in from before.

**Session:** A period of time you are logged into an account.

**Sign Out / Log Out:** Closing your session so no one else can access your account.

**Security Questions:** Backup questions used to verify your identity (often outdated and less secure).

**Authentication App:** A security tool that creates temporary 6-digit codes you use to confirm identity when logging into an account, making it much harder for anyone else to break in even if they have your password.

**Password Manager:** a secure app that creates, stores, and auto-fills strong, unique passwords for all your online accounts in one encrypted digital vault, requiring you to remember only a single "master password" to access them. It eliminates the need to reuse simple passwords, generating complex ones and protecting you from password reuse risks, and often includes features like compromise alerts and secure sharing.

## 5.1 — What an Account Is

In the digital world, an **account** is your identity. It tells a website or app:

- who you are
- what you like
- what services you use
- what information belongs to you

You use accounts for:

- email
- banking
- social media
- shopping
- streaming
- healthcare portals
- government services
- cloud storage

Each account holds personal and sometimes sensitive information.

---

## 5.2 — Why Passwords Matter

Passwords protect everything attached to an account — your messages, photos, money, documents, and identity.

A weak password allows:

- strangers to access your account
- scammers to lock you out
- criminals to impersonate you
- money or information to be stolen

Creating a strong password is one of the most important steps in digital safety.

---

## 5.3 — How to Create a Strong Password

A strong password is:

- **12 characters or more**

- Includes **upper- and lowercase letters**
- Includes **numbers and symbols**
- **Not** based on your name, birthday, or common words

Good pattern examples:

- Three random words + numbers
- A sentence with symbols
- A password generated by a password manager

Bad examples:

- “123456”
- “password”
- “iloveyou”
- “qwerty”

---

## 5.4 — Password Managers (Why They Matter)

Password managers:

- create strong passwords, avoid using names, birthdays, phone numbers, or common words like ‘password,’ ‘welcome,’ or ‘123456.’
- store them securely
- fill them in automatically
- prevent reusing the same password across sites
- reduce the stress of remembering dozens of logins

Examples:

- 1Password
- Bitwarden
- Dashlane
- LastPass (for experienced users)

Beginners benefit greatly from using a password manager.

---

## 5.5 — Multi-Factor Authentication (MFA)

MFA adds a second step when logging in, such as:

- a text message code

- an authentication app code
- a fingerprint
- a Face ID scan
- a backup code

Even if your password is stolen, MFA prevents unauthorized access.

**Best Option: Authentication app -** a second layer of security that asks you to prove it's really you by entering a 6-digit code, tapping an app, or using a fingerprint. Even if someone knows your password, they cannot get into your account without this second step.

In addition to passwords and codes, many devices use your physical features to help confirm your identity.

---

## 5.6 — Biometrics

Biometrics use the uniqueness of your body to unlock a device or verify identity.

Examples:

- Fingerprint scanners
- Facial recognition (Face ID)
- Voice recognition

Biometrics make logging in fast, easy, and secure.

---

## 5.7 — Device Recognition

Websites often ask:

"Do you want to trust this device?"

This means:

- the system will remember your phone, tablet, or computer
- future logins will be easier
- suspicious devices will be flagged

This is a convenience feature but should only be used on **your own** device.

---

## 5.8 — Sessions and Logging Out

Staying logged in is called a **session**. On shared or public devices, always **Sign Out** to protect your account.

On personal devices:

- It is safe to stay logged in with strong passwords and MFA
- Make sure you have biometrics or a lock screen enabled

---

## 5.9 — Risks to Watch For (Account-Level Harms)

- Weak passwords
- Reused passwords across multiple sites
- Text message-based MFA interception
- Password manager breaches (rare, but possible)
- Phishing attempts to steal login info
- Fake login pages
- Leaving accounts logged in on shared devices

---

## 5.10 — What You Can Do to Stay Safe

- Use long, strong passwords
- Never reuse passwords
- Use MFA for every important account
- Store passwords in a password manager
- Avoid clicking unknown login links
- Log out of accounts on shared or public computers
- Turn on security alerts and notifications
- Review active sessions periodically

---

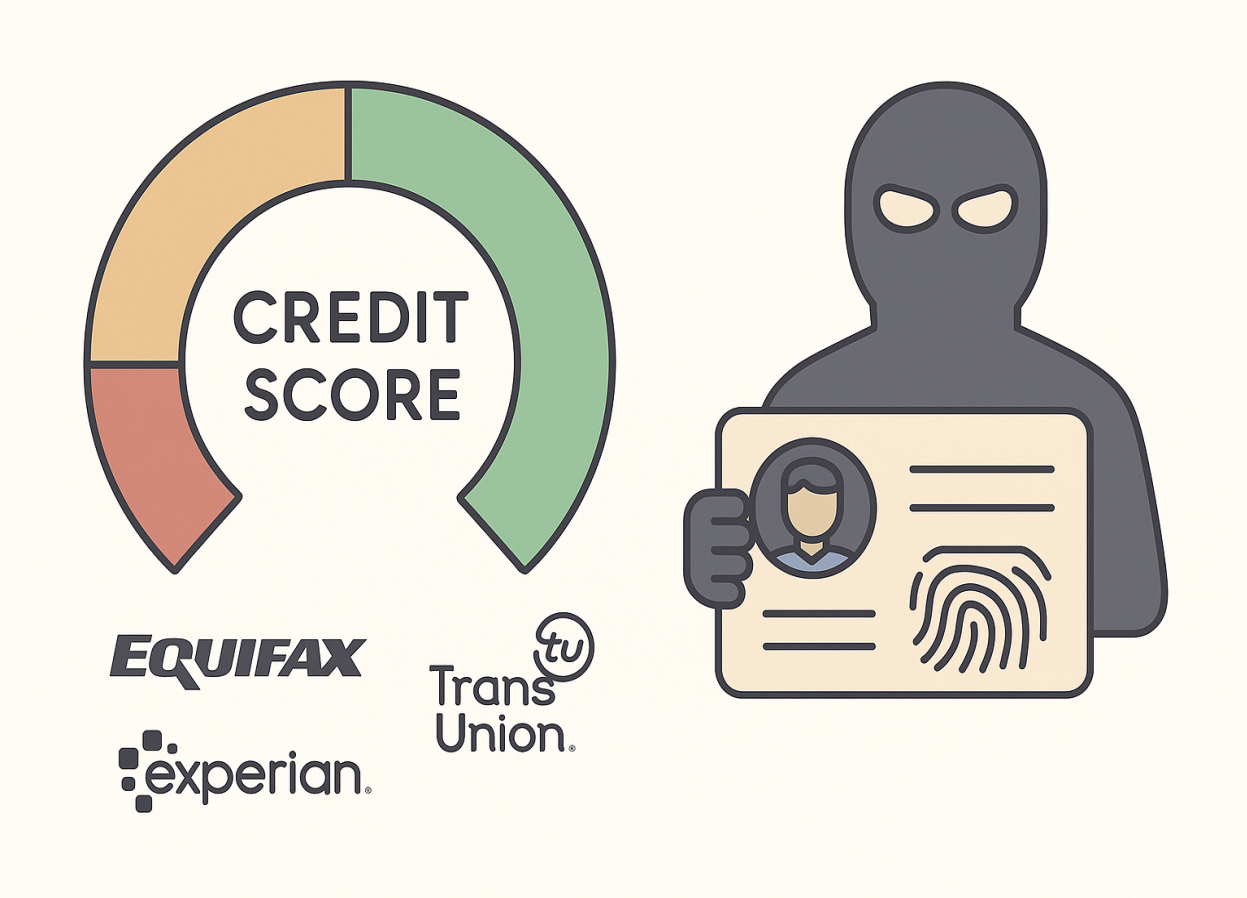
## 5.11 — Why This Section Matters

Your accounts are the foundation of your digital identity. If someone gains access to one email, bank account, or social platform, they can often access others. By understanding passwords, MFA, biometrics, and device recognition, you build strong defenses against identity theft and online fraud.

With the basics of identity and access in place, we can now learn the everyday habits that form the foundation of digital safety.

# SECTION 6 — CREDIT, IDENTITY & WHY PROTECTION MATTERS

*How your personal information becomes valuable—and vulnerable—online.*



## 🔷 Key Terms

**Identity:** The collection of information that describes who you are—your name, birthday, address, phone number, accounts, and personal details.

**Personal Information (PII):** Information that can identify you such as:

- full name
- date of birth
- address
- phone number
- Social Security Number
- email
- account numbers

**Identity Theft:** When someone steals your personal information and pretends to be you for financial gain or access to services.

**Fraud:** Dishonest behavior used to trick people into giving money or information.

**Credit:** Your **financial reputation** — a record that tells lenders how trustworthy you are with money.

**Credit Report:** A document showing your credit accounts, payment history, loans, and debts.

**Credit Score:** A number that represents your financial reliability (higher is better).

**Credit Bureaus:** These companies collect information about your financial history and create your credit report. The three major bureaus are:

- **Equifax**
- **Experian**
- **TransUnion**

**Credit Freeze:** A security measure that blocks new accounts from being opened in your name.

**Data Breach:** A security incident where personal information is exposed or stolen.

**Phishing:** A scam that tricks you into giving away personal or financial information.

**Malware:** Software designed to harm your device or steal information.

**Public Wi-Fi Attack:** When someone uses an unsecured public network to intercept your data.

**Hacking:** Hacking is the unauthorized access to computer systems, networks, or data, usually by exploiting security weaknesses to steal information, disrupt services, or cause damage.

---

## 6.1 — Why Your Identity Matters in Digital Life

Your identity is valuable. It includes your finances, personal details, online accounts, and your reputation.

Criminals target identity because it allows them to:

- open bank accounts in your name
- apply for loans
- file fraudulent taxes
- access your existing accounts
- impersonate you
- steal money or benefits

Protecting your identity is one of the most important parts of digital health.

---

## 6.2 — What Is Credit?

Credit describes **how well you handle money**. Lenders look at your credit to decide:

- whether to approve loans
- whether you can sign up for services
- what interest rate you get

Your credit report shows:

- loans or credit cards you have
- whether you've paid on time
- how much debt you owe

Your credit score is a three-digit summary of your credit health.

Identity theft often targets your credit, because criminals can profit from pretending to be you. For individuals who may not have credit or bank accounts, identity fraud may occur when a bad actor tries to open a cell phone plain in their name or apply for government benefits.

## 6.3 — How Identity Theft Happens

Common ways your identity gets stolen:

**Data Breaches:** When a company or service you use (store, bank, hospital) is hacked and your information leaks.

**Phishing Emails or Texts:** Messages pretending to be banks, delivery services, government agencies, or employers.

**Fake Banking Messages:** Texts or emails that ask you to "verify your account" or "fix a problem."

**Malware on Devices:** Apps or downloads that secretly collect your information.

**Stolen Mail:** Financial documents, credit card offers, and tax letters taken from your mailbox.

**Fake Online Stores:** Websites pretending to sell products but are actually collecting credit card numbers.

**Public Wi-Fi Attacks:** Criminals intercepting information sent across an unsecured network.

## 6.4 — Examples of Identity Theft

### Scenario A: New Credit Card You Never Applied For

A criminal uses your Social Security Number to open a credit card in your name.

### Scenario B: Someone Files Taxes Under Your Name

Your refund goes to a scammer before you even file.

### Scenario C: Unauthorized Purchases

Someone gains access to your Amazon, bank, or PayPal account and makes purchases.

### Scenario D: Loan Applications

You receive notices for loans you never applied for.

### Scenario E: Social Media Impersonation

Someone uses your photos and name to trick others into sending money.

---

## 6.5 — Risks to Watch For (Identity-Level Harms)

- receiving mail about accounts you don't recognize
- being locked out of your own account
- unexpected withdrawals or charges
- sudden drop in credit score
- messages asking for personal information
- unfamiliar devices logging into your accounts
- fake banking alerts
- websites asking for too much information

---

## 6.6 — What You Can Do to Stay Safe

### Check Your Credit Regularly

Use:

- **AnnualCreditReport.com** (free yearly checks)
- Credit monitoring from banks or services

**Freeze Your Credit:** This prevents new accounts from being opened in your name.

**Use Strong Passwords & MFA:** Protects your financial accounts from takeover.

### Limit Personal Information Online

Avoid posting:

- address
- birthday
- phone number
- school or workplace details

**Update Devices:** Protects against malware and security flaws.

**Verify Unexpected Messages:** Call the official number—not the one in the message.

**Avoid Financial Activity on Public Wi-Fi:** Switch to mobile data or wait until you're at home.

---

## 6.7 — Why This Section Matters

Identity theft can affect your finances for years. Once someone has your personal information, they can impersonate you across multiple services — banks, government, social media, or shopping platforms. By understanding how identity theft works and how to protect yourself, you take back control of your digital life and financial security.

Now that you understand how identity and credit can be exploited, the next step is learning the everyday habits that protect your information before harm occurs.

# SECTION 7 — FOUNDATIONS OF DIGITAL SAFETY

*The simple habits that protect you every day.*

## 🔷 Key Terms

**Safety Settings:** Tools on your device or apps that help protect your privacy and security.

**Notifications:** Alerts that pop up on your phone or computer. They can be helpful—but also overwhelming or manipulative.

**Secure Password:** A long, unique password that no one can guess.

**Verification:** Double-checking if a message, link, account, or website is real before interacting with it.

**URL (Web Address):** The link that tells your browser where to go.

**HTTPS:** A secure website connection that protects your data.

**Block:** To stop a user from contacting or seeing your profile.

**Report:** To notify the platform that harmful or suspicious behavior has occurred.

**Update:** A software improvement that adds security and fixes problems.

**Settings Menu:** The control center of your device, where you adjust privacy, security, and permissions.

**Permissions:** What an app is allowed to access (location, camera, microphone, photos, contacts, and more).

**Red Flags:** Warning signs that something online may be unsafe.

---

## 7.1 — What Digital Safety Actually Means

Digital safety does not require advanced technical knowledge. It is a set of **small, simple habits** that greatly reduce your risk of falling victim to scams, fraud, harassment, identity theft, or misinformation.

You can think of digital safety like locking your doors, washing your hands, or buckling your seatbelt—routine actions that protect you without requiring expertise.

---

## 7.2 — Core Principles of Everyday Digital Safety

These principles apply everywhere: websites, apps, email, texting, gaming, and social media.

### 1. Slow Down Before You Click

Most digital harm happens because someone feels rushed or pressured. Take a moment to check:

- the sender
- the link
- the request
- whether it makes sense

### 2. Verify the Source

Look for:

- correct spelling
- official website URLs
- known email addresses
- verified accounts
- legitimate phone numbers

If something feels off, stop and investigate.

**3. Use Strong, Unique Passwords:** Weak or repeated passwords make it easy for criminals to break into accounts.

**4. Turn On Multi-Factor Authentication (MFA):** This ensures someone cannot access your account even if they steal your password.

**5. Keep Devices Updated:** Updates patch security holes and improve protection.

**6. Limit Personal Information Online:** The less you share, the less can be used against you.

**7. Trust Your Instincts:** If a message feels urgent, emotional, or unusual, it may be a scam.

**8. Use Platform Tools (Block, Mute, Report):** These tools exist to protect you and others.

---

## 7.3 — Red Flags That Something May Be Unsafe

Look out for:

- emotional pressure ("URGENT!", "Don't tell anyone")
- spelling mistakes
- strange URLs
- unknown numbers
- requests for money
- requests for login codes
- threats or intimidation
- too-good-to-be-true offers
- messages claiming your account is in danger
- unexpected attachments
- deals that seem unrealistic

If one or more of these appear, pause and verify.

---

## 7.4 — Practical Everyday Safety Habits

**Check Before You Click:** Hover over links (or press and hold on mobile) to preview the real URL.

**Screen Messages:** Ignore messages from unknown people until verified.

**Use Official Apps:** Download apps only from your device's official store.

**Review App Permissions:** Turn off access for apps that don't need your camera, microphone, or location.

**Examine Website Features:** Look for https:// and a small lock icon next to the website name—this means the connection is encrypted.

**Sign Out on Shared Devices:** Especially in libraries, hotels, or workplaces.

**Avoid Public Wi-Fi for Sensitive Tasks:** Banking, emailing sensitive information, or entering passwords should be done on secure networks.

---

## 7.5 — Examples of Small Habits That Prevent Big Harm

### Example 1:

You receive a text from your "bank." Instead of tapping the link, you call the official number from the bank's website.
➡️ You avoid a phishing scam.

### Example 2:

Your device prompts an update. You allow it.
➡️ A security problem is fixed before someone can exploit it.

### Example 3:

A stranger sends a message asking for help. You ignore and report the account.
➡️ You avoid a grooming or extortion attempt.

### Example 4:

You check the website address before entering your login.
➡️ You avoid entering your password on a fake page.

---

## 7.6 — Risks to Watch For (General Digital Harms)

- fake websites
- emotional manipulation
- impersonation
- malware downloads
- identity theft
- clickbait links
- bogus contests or giveaways
- scare tactics ("Your account will be deleted!")
- romance scams
- fake tech support
- data leaks or breaches

Even beginners can learn to spot these patterns.

---

## 7.7 — What You Can Do to Stay Safe

- Enable MFA everywhere
- Keep your device updated
- Only connect to trusted Wi-Fi networks
- Review privacy settings monthly
- Block and report harmful interactions
- Use strong passwords
- Trust only official contact channels
- Delete apps you don’t use
- Use critical thinking when reading posts or news
- Compare information from multiple sources

These habits take only minutes but create a strong foundation of protection.

---

## 7.8 — Why This Section Matters

Digital safety is not a single skill—it is a mindset and a collection of simple, repeatable habits. Once these practices become part of your routine, you are far less likely to fall victim to scams, manipulation, or digital harm.

Harms take many shapes, but certain online spaces make them more likely to appear. Understanding each platform helps you navigate them with confidence.

# SECTION 8 — COMMON DIGITAL HARMS

*What can go wrong online — and how to recognize the warning signs.*

## 🔷 Key Terms

**Harm:** Anything online that can cause emotional, financial, physical, or privacy-related damage.

**Scam:** A dishonest attempt to steal money, information, or access.

**Fraud:** Using deception for financial gain, often by impersonating someone.

**Phishing:** Messages (email, text, or app) pretending to be legitimate to trick you into revealing personal or financial information.

**Smishing:** Phishing through **SMS text messages**.

**Vishing:** When phishing happens by phone call.

**Data Exposure:** When your personal information becomes visible or accessible to people who should not have it.

**Data Breach:** A security incident where large amounts of personal information are stolen from a company, website, or service.

**Malware:** Software that harms your device or steals information.

**Identity Theft:** When someone uses your personal information to pretend to be you.

**Bot Account:** A fake account controlled by software, not a real person.

**Predatory Messaging:** Messages designed to groom, exploit, manipulate, or pressure someone — especially minors.

**Grooming:** When someone builds trust with the intent to exploit or harm.

**Sextortion:** A form of blackmail involving private or intimate images.

**Misinformation:** False or misleading information that spreads online.

**Fake Seller:** A person or website pretending to sell goods but never delivering them or delivering counterfeit products.

**Fake Login Page:** Scammers often create fake login pages that look identical to real ones to steal your username and password. Always double-check the website address before typing anything.

**Public Wi-Fi Attack:** When someone uses an unsecured public network to intercept private information. For example, a scammer might create a fake “Airport_Free_WiFi” network to steal data

**Spoofing:** When a scammer makes a message or phone call look like it is coming from a trusted company or phone number.

---

## 8.1 — What Are Digital Harms?

Digital harms are negative experiences or attacks that happen online. They can affect:

- your money
- your identity
- your privacy
- your safety
- your mental health
- your relationships

Not all harms are obvious. Some appear slowly, quietly, or through everyday interactions.

This section explains each type of harm in simple terms with examples and prevention strategies.

---

## 8.2 — Harm Type: Data Breaches

**What It Is:** A **data breach** happens when a company you use gets hacked and your personal information is leaked.

### Examples

- A store or app announces that customer emails and passwords were exposed.
- A hospital accidentally leaks patient information.
- A bank reports unauthorized access to account details.

### Prevention

- Change passwords regularly.
- Use unique passwords for each account.
- Turn on MFA to protect access.
- Monitor your credit reports.

---

## 8.3 — Harm Type: Phishing Emails

**What It Is: Phishing** Emails pretend to be from a real company, designed to steal your information.

### Examples

- "Your package is delayed! Click here to fix your delivery."
- "Your bank account is locked. Sign in to restore access."
- Fake job offers or invoices.

### Prevention

- Do not click unknown links.
- Check the sender's email address.
- Delete suspicious messages.
- Contact the company using their official website or phone number.

## 8.4 — Harm Type: Fake Banking Messages

**What It Is:** Texts or emails that **pretend** to be from your bank to steal your login or card details.

### Examples

- Fake "fraud alerts" urging urgent action
- Requests to "verify your identity"
- Texts with fake login URLs

### Prevention

- Call your bank using the number on your card.
- Never reply to unexpected messages.
- Avoid clicking login links in texts.

---

## 8.5 — Harm Type: Malware

**What It Is:** Malware is **malicious software** that harms your device or steals information.

### Examples

- Fake apps disguised as cleaners or games

- Attachments in suspicious emails
- Downloads from untrusted websites

### Prevention

- Only download apps from official stores.
- Keep devices updated.
- Avoid clicking unknown attachments or downloads.

---

## 8.6 — Harm Type: Stolen Mail

**What It Is: Physical** or hard copy mail like credit card offers or bank statements taken from your mailbox.

### Examples

- Someone steals pre-approved credit offers.
- Tax documents disappear.
- Replacement debit cards are intercepted.

### Prevention

- Use a locked mailbox.
- Sign up for digital statements.
- Shred sensitive documents.

---

## 8.7 — Harm Type: Fake Online Stores

**What It Is: Fake** websites pretending to sell goods but stealing money or personal information.

### Examples

- Sites with extremely low prices
- New “brands” selling luxury goods cheaply
- Stores with no real reviews
- Fake order confirmations

### Prevention

- Look for HTTPS and the lock icon.

- Search for reviews outside the site.
- Avoid deals that seem too good to be true.

---

## 8.8 — Harm Type: Public Wi-Fi Attacks

**What It Is:** Criminals intercept data sent over unsecured **public** Wi-Fi.

### Examples

- Fake “Free Airport Wi-Fi” networks
- Intercepted passwords or banking info
- Man-in-the-middle attacks

### Prevention

- Avoid banking on public Wi-Fi.
- Use mobile data instead.
- “Forget” networks you don’t trust.

---

## 8.9 — Harm Type: Predatory Messaging

**What It Is:** Messages where someone tries to **manipulate, groom, or pressure** a person—especially children or teens.

### Examples

- Strangers asking personal questions
- Adults pretending to be teens
- Requests for photos
- “Secret friendship” behavior

### Prevention

- Block unknown contacts immediately.
- Report harmful messages.
- Keep accounts private.
- Teach minors to never share personal details.

---

## 8.10 — Harm Type: Scams and Digital Fraud

**What It Is: Scams** are attempts to steal money or trick users into giving up sensitive information.

### Examples

- Fake investments
- Lottery scams
- Romance scams
- Tech support scams
- Fake charity drives

### Prevention

- Never send money to strangers.
- Verify organizations directly.
- Avoid emotional or urgent requests.

---

## 8.11 — Harm Type: Misinformation & Rumors

**What It Is:** False or misleading information that spreads quickly online.

### Examples

- Fake health cures
- Doctored videos
- Misleading headlines
- Viral rumors on social media

### Prevention

- Check credible sources.
- Compare information across news outlets.
- Look for expert verification.

---

## 8.12 — Why This Section Matters

Understanding digital harms gives you the power to recognize them early—before damage occurs. These patterns repeat themselves across platforms. Once you learn to spot the signs, you cannot be fooled as easily, no matter where you are online.

These common harms show up differently depending on where you are online. To stay safe, it helps to understand how each major digital space works and what risks to expect.

# SECTION 9 — COMMON DIGITAL SPACES & WHERE HARMS OCCUR

*Understanding the online environments you use every day — and what risks to expect in each.*

## 🔷 Key Terms

**Platform:** A website, app, or service where people communicate, share, shop, or create content.

**Feed:** A scrolling list of posts, videos, or updates personalized for you.

**Algorithm:** A set of rules used by platforms to decide what you see first (posts, videos, ads). Algorithms show you more of what you engage with.

**Ad (Advertisement):** Sponsored content meant to sell products or influence you.

**Sponsored Post:** A paid post that looks like regular content.

**Reels / Shorts:** Short, vertical videos often recommended rapidly.

**Grooming:** When someone builds trust with harmful intentions, often toward minors.

**DM (Direct Message):** Private messages sent within an app.

**Group Chat / Forum Thread:** Spaces for group discussions.

**Creator / Influencer:** Someone who posts content to engage followers or earn money.

**Third-Party Seller:** An independent seller using platforms like Amazon, Temu, Wish, or Facebook Marketplace.

**Skin / Game Currency:** Digital items used in games; sometimes targeted in scams.

---

## 9.1 — What Are "Digital Spaces"?

Different digital spaces create different risks because of how people interact, share information, or communicate on each platform.

Each digital space has its own culture, communication style, and level of risk, so the same behavior can lead to very different outcomes depending on where you are online.

Digital spaces are online environments where people:

- post
- watch

- shop
- comment
- message
- play games
- join discussions

Each space is designed differently—and therefore has different risks.

Understanding the "personality" of each platform helps you know:

- who is there
- how information spreads
- what harms are common
- what to do when something goes wrong

With that foundation in mind, here's what you can expect across the most used digital spaces.

---

## 9.2 — TikTok

**What It Is:** A short-video platform where people watch, create, and share quick videos. TikTok relies heavily on recommendation algorithms that quickly learn your behavior and show you more of the same types of videos, which can influence what you see long-term.

### Common Harms

- Harmful or dangerous challenges
- Misinformation spreading quickly
- Predatory or inappropriate messaging
- Exposure to adult or violent content
- Overuse due to addictive design (infinite scrolling)

### If Something Goes Wrong

- Block the user
- Report the content or profile
- Turn on Restricted Mode
- Filter comments or messages
- Limit screen time using built-in tools

---

## 9.3 — Instagram & Facebook (Meta)

**What They Are:** Social networking platforms for posting photos, videos, messages, and joining groups. Used for communication, shopping, and following creators. These platforms blend personal communication with advertising, which can make it harder to distinguish between genuine posts and sponsored content.

### Common Harms

- Fake stores and purchase scams
- Account impersonation
- Unwanted messages
- Comparison pressure
- Data collection for targeted ads
- Manipulated “highlight reel” lifestyles
- Viral misinformation in groups

### If Something Goes Wrong

- Block and report profiles
- Adjust privacy settings to “Friends Only”
- Hide or unfollow harmful accounts
- Use two-factor authentication
- Review purchase history and seller reviews

---

## 9.4 — YouTube

**What It Is:** A video-sharing platform offering news, entertainment, tutorials, and educational content.

### Common Harms

- Radicalizing recommendations
- Misleading or edited videos
- Inappropriate children’s content
- Deceptive or overly persuasive advertising

### If Something Goes Wrong

- Block or restrict channels
- Turn on Restricted Mode
- Report misleading or harmful videos
- Disable autoplay to avoid problematic recommendations

## 9.5 — Snapchat

**What It Is:** A messaging app where photos and videos ("Snaps") disappear after being viewed. Popular with teens and young adults.

### Common Harms

- Bullying or harassment
- Sextortion
- Coercive or manipulative messages
- Location-based threats via Snap Map
- Misunderstanding that disappearing messages cannot be saved — they can be screenshotted, recorded, or saved by third-party apps.

### If Something Goes Wrong

- Disable Snap Map location sharing
- Block and report users
- Save evidence with screenshots if needed
- Turn off Quick Add for privacy
- Tell a trusted adult for safety concerns

---

## 9.6 — X (formerly Twitter)

**What It Is:** A platform for posting short text updates, news, and public conversations.

### Common Harms

- Harassment and hostile interactions
- Hate speech
- Bot accounts spreading misinformation
- Rapid spread of harmful rumors
- Fake "verified" accounts pretending to be real organizations

Recent changes to the verification system make it harder to confirm whether an account is official, increasing the risk of misinformation.

### If Something Goes Wrong

- Block or mute users
- Report harmful content

- Turn off public DMs
- Turn off “Who Can Message Me”
- Verify information with multiple sources
- Limit time spent on the feed

---

## 9.7 — Online Marketplaces (Amazon, Temu, Wish, Facebook Marketplace)

**What They Are:** Websites where users buy or sell goods, often through independent or overseas sellers.

### Common Harms

- Fake sellers
- Counterfeit or unsafe products
- Payment scams
- Delivery fraud
- Identity theft through fake checkout pages

Some scam stores mimic the exact layout and colors of well-known brands, making them appear legitimate at first glance.

### If Something Goes Wrong

- Contact platform support immediately
- Stop communication with the seller
- Request a refund through buyer protection
- Change saved payment information

---

## 9.8 — Online Forums & Gaming Platforms (Discord, Reddit, Roblox, Fortnite, Minecraft servers)

**What They Are:** Spaces for chatting, playing games, sharing opinions, and joining groups. Many are moderated by individuals rather than companies, meaning moderation can be inconsistent.

### Common Harms

- Bullying and harassment
- Grooming

- Pressure to share personal information
- Exposure to explicit language or content
- Digital item scams (skins, coins, credits)
- Pressure to join private voice chats where unsafe conversations occur

### If Something Goes Wrong

- Block or ban users
- Leave harmful servers or groups
- Report harassment or inappropriate behavior
- Turn off DMs from strangers
- Disable voice chat if needed
- Use parental controls for minors

---

## 9.9 — Why This Section Matters

Each digital space has its own strengths, risks, culture, and design features. Knowing what to expect in each space helps you:

- stay alert
- protect yourself
- guide children or older adults
- reduce exposure to harm
- make informed choices

Once you know the risks in each space, the next step is understanding what to do the moment something feels unsafe or harmful.

# SECTION 10 — WHAT TO DO WHEN HARM OCCURS

*Practical, step-by-step actions you can take on any platform.*

## 🔷 Key Terms

**Block:** Stops a person from contacting you, viewing your profile, or finding your account.

**Report:** Alerts the platform to harmful behavior so they can investigate or remove content.

**Mute:** Hides a person's content without notifying them.

**Screenshot:** A picture of your screen used to save evidence.

**Support/Help Center:** A platform's built-in resource for instructions, reporting, and safety tools.

**Appeal:** A request to the platform for review if action was taken on your account incorrectly.

**Trusted Contact:** A friend, family member, or advocate you notify when something goes wrong.

---

## 10.1 — First Steps: What To Do Immediately

Even with good habits, digital harm can still happen. What makes a difference is knowing exactly what to do, quickly and calmly, to protect yourself, your accounts, your identity, and your safety.

These steps apply to harassment, scams, threats, impersonation, fake purchases, grooming attempts, and nearly any other digital harm.

### Step 1 — Stop engaging

Stop responding immediately.  Do not argue, explain, or apologize — disengagement prevents escalation.

### Step 2 — Take screenshots

Capture:

- messages
- usernames
- profile photos
- dates and times
- URLs (if on a website)

If screenshots are not allowed or the content disappears, use a second device to take photos of the screen. This becomes evidence.

### Step 3 — Block the account

Blocking prevents further contact and does *not* notify the other person.

### Step 4 — Report the behavior to the platform

Platforms act faster when many people report harmful behavior.

### Step 5 — Tell a trusted person

Especially important for:

- minors
- older adults
- harassment
- threats
- financial scams

### Step 6 — Secure your accounts

Change passwords immediately if:

- someone tried to log in
- you clicked a suspicious link
- you shared personal info

### Step 7 — Update your device and apps

Harmful links sometimes rely on outdated software.

---

## 10.2 — When the Harm Involves Money

### If you sent money or payment info:

- Contact your bank card company immediately—they can stop payments or issue new cards
- Freeze your card or account
- Change your online banking password

- Check recent transactions
- Enable alerts for activity

### If you entered info on a fake website:

- Change your password
- Turn on MFA
- Monitor your bank
- Consider a **credit freeze**

### If someone used your card without permission:

- Dispute the charge
- Request a new card
- Review all automatic payments

If you are unsure whether you were scammed, your bank can help determine whether a charge or transaction is suspicious.

---

## 10.3 — When the Harm Involves Threats or Safety

If the message includes personal information about you or your location, treat it as a higher-risk situation and seek help immediately.

If you receive threats:

- Block the person
- Save all evidence
- Report to the platform
- Tell a trusted contact
- Consider contacting law enforcement if the threat is specific

If a child receives harmful content:

- Take screenshots
- Remove access temporarily
- Report immediately
- Consider parental controls
- Review chat logs if available

---

## 10.4 — When the Harm Involves Photos, Blackmail, or Sextortion

This requires calm and decisive action.

### Do:

- Save evidence
- Block the user
- Report the account
- Tell a trusted adult or friend
- Contact law enforcement if threatened

### Do NOT:

- Pay money- payment signals vulnerability and often leads to further demands
- Continue responding
- Try to negotiate

Criminals often demand more once payment begins.

---

## 10.5 — Platform Tools: How To Find Help on Any App

Every platform has a Help Center, usually located under:

• Settings
• Privacy
• Support
• Safety Center
• Report a Problem

Exact wording varies, but the functions are similar across apps.

### Where to find it (general instructions):

1. **Open the profile menu**
   Often shown as:
   - three lines
   - a gear icon
   - your profile photo
   - "Settings and Privacy"
2. **Select "Help," "Support," or "Report a Problem"**
   These may appear under:
   - Help Center

- Support
- Privacy & Safety
- Safety Center
- Report Abuse

3. **Type your issue into the search bar**
   Use simple terms like:
   - "harassment"
   - "scam"
   - "fake account"
   - "bullying"
   - "hacked account"

### Why this matters:

Platform support pages are updated constantly and will always reflect **the most accurate, current steps**—especially important for beginners.

---

## 10.6 — "If Something Goes Wrong" — Quick Guides for Each Platform

You already have full versions for Marketplaces and Gaming. Here are the remaining universal versions.

### TikTok — If Something Goes Wrong

- Block the user
- Report the video, message, or account
- Turn on Restricted Mode
- Hide offensive comments
- Adjust privacy settings to "Friends Only"
- Review active sessions for suspicious logins

### Instagram & Facebook — If Something Goes Wrong

- Block and report the profile
- Report fake stores or scam ads
- Set account to private
- Remove suspicious followers
- Enable MFA
- Review recent logins

### YouTube — If Something Goes Wrong

- Block the channel
- Report harmful videos
- Disable autoplay
- Clear your watch history to reset recommendations

### Snapchat — If Something Goes Wrong

- Block and report users
- Disable Snap Map location sharing
- Save evidence before messages disappear
- Turn off Quick Add
- Tell a trusted adult for safety concerns

### X (formerly Twitter) — If Something Goes Wrong

- Block or mute the account
- Report harassment or hate content
- Disable public DMs
- Limit who can reply to posts
- Review trusted sources before sharing news

### Online Forums & Gaming Platforms — If Something Goes Wrong

- Block or ban users
- Leave the server, channel, or group
- Turn off DMs from strangers
- Report the behavior to moderators
- Disable voice chat
- Use parental controls for minors

---

## 10.7 — Why This Section Matters

Knowing how to react during harm prevents:

- emotional panic
- financial loss
- account takeover
- escalation
- ongoing harassment
- trauma for minors
- identity theft
- manipulation

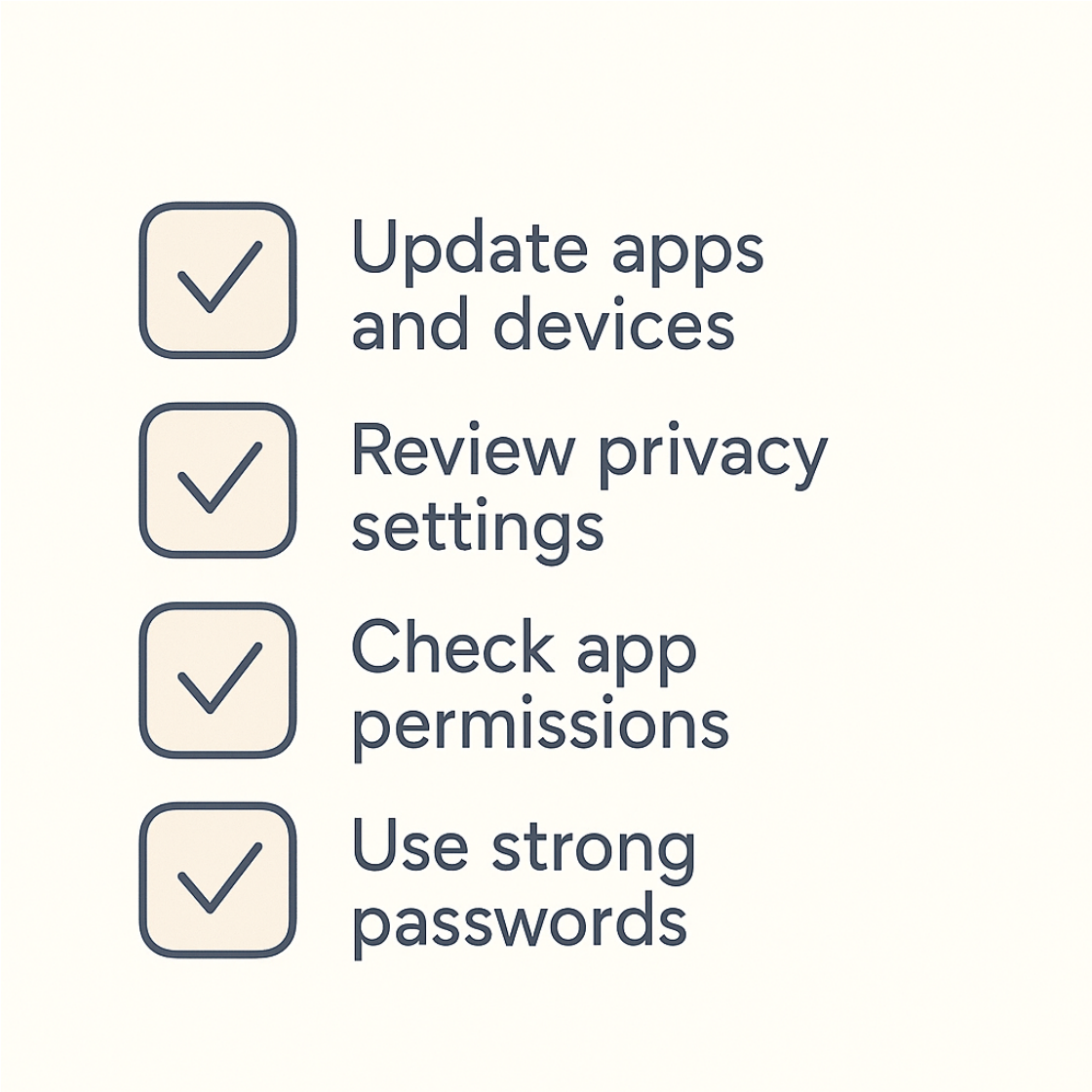
These steps apply across all digital platforms and can be adapted to any device.

With these response skills in place, you’re ready to strengthen the daily habits that prevent harm before it starts.

---

# SECTION 11 — DIGITAL HYGIENE: SIMPLE HABITS FOR SAFER DEVICES & HEALTHIER ONLINE LIFE

*Daily and weekly routines that protect your identity, your information, and your wellbeing.*



## 🔷 Key Terms

**Digital Hygiene:** The regular habits that keep your device and accounts clean, organized, updated, and secure.

**Update (Software Update):** An improvement to your device or app that fixes security issues and adds new features.

**App Permissions:** Settings that control what an app is allowed to access (camera, microphone, location, photos, contacts).

**Grayscale Mode:** A display setting that removes color from your screen to reduce overstimulation and addictive scrolling.

**Cache / Temporary Files:** Short-term files stored by apps or browsers to load things faster. These occasionally need clearing.

**Cloud Backup:** A saved copy of your device's important data (like iCloud or Google Drive) in case it is lost or damaged.

**Default Settings:** The automatic settings your device comes with — often not the safest or most private.

**Review Cycle:** A scheduled routine for checking settings, cleaning storage, and updating apps.

---

## 11.1 — What Is Digital Hygiene?

Digital hygiene is like brushing your teeth — a basic routine that protects you from bigger problems later. These small habits reduce your chances of experiencing:

- hacks
- identity theft
- device slowdowns
- intrusive ads
- overwhelming notifications
- distractions and stress
- privacy risks

It is not technical. It is practical.

---

## 11.2 — Core Digital Hygiene Habits (Beginners Can Do All of These)

### 1. Keep Devices and Apps Updated

Updates fix weaknesses criminals use to break into accounts. Regular updates are one of the simplest ways to prevent many common digital problems before they start.

**How to update (general instructions):**

- Open **Settings**
- Find **Software Update** or **System Update**
- Tap **Install**

**For apps:**

- Open your **App Store**
- Tap **Updates**
- Tap **Update All**

### 2. Review Privacy Settings

Most platforms allow you to control your settings. Every few months, check what information apps or websites can access.

**How to review privacy settings (general):**

- Open **Settings**
- Tap **Privacy** or **Privacy & Security**
- Review access to:
    - Location
    - Camera
    - Microphone
    - Photos
    - Contacts

Turn off anything that is not necessary.

### 3. Review App Permissions

Apps often request access they do not need. Review what information apps can access.

Examples:

- A calculator app should not need your location

- A flashlight app should not need your microphone
- A game should not need your contacts

**How to review app permissions:**

- Open **Settings**
- Tap **Apps** or **App Management**
- Choose an app
- Select **Permissions**
- Toggle off anything unnecessary

## 4. Organize and Clean Your Device

Digital clutter slows devices down.

Helpful habits:

- Delete unused apps
- Clear old downloads
- Organize photos into albums
- Empty trash folders
- Clear browser cache periodically

Clearing your cache removes temporary files that can slow things down or show outdated pages.

## 5. Turn Off Non-Essential Notifications

Many apps send constant alerts to keep you opening them. These interruptions can drain your time, attention, and mood. Turn off notifications for apps that are not essential, like shopping apps, games, or social media. Keep only what truly matters—messages, calls, and reminders.

**How to turn off notifications (general):**

- Open **Settings**
- Tap **Notifications**
- Choose an app
- Turn off **Allow Notifications**

Turn OFF notifications for:

- shopping apps
- games
- social media “likes”
- promotional messages

Turn ON notifications for:

- messages
- banking alerts
- two-factor authentication

## 6. Use Grayscale Mode When Needed

Grayscale makes your device less stimulating.

**How to turn on grayscale (general):**

- Open **Settings**
- Tap **Accessibility**
- Tap **Display & Text Size**
- Select **Color Filters**
- Choose **Grayscale**

This helps break addictive scrolling patterns.

## 7. Limit App Tracking

Apps track your behavior to show targeted ads.

**How to limit tracking:**

- Open **Settings**
- Go to **Privacy**
- Tap **Tracking**
- Turn off "Allow Apps to Request to Track"

## 8. Restart Your Device Weekly

This clears temporary files and resets slow functions. A simple restart fixes many issues.

## 9. Back Up Your Data

Protects you if your device breaks or is lost. Cloud backup means saving a copy of your important information to a secure online service so you can restore it later if needed.

Methods include:

- iCloud
- Google Drive
- OneDrive

---

## 11.3 — Weekly Digital Hygiene Checklist

Beginners can complete this simple routine in 10–15 minutes each week:

- update device software
- update apps
- review app permissions
- check storage
- delete unused apps
- clear old screenshots
- empty downloads folder
- review notifications
- restart device
- run a quick privacy check

---

## 11.4 — Monthly Digital Hygiene Checklist

Once a month:

- change one or two important passwords
- check financial accounts for unusual activity
- review device privacy settings
- update your password manager
- clear browser history and cookies
- review email filters
- delete outdated photos or files
- check who has access to shared documents

---

## 11.5 — Why Digital Hygiene Matters

Good digital hygiene protects your:

- personal information
- accounts
- money
- mental energy
- attention
- device performance

It prevents small issues from turning into major problems.

Digital hygiene keeps your accounts and devices safe, but safety also includes protecting your focus, time, and emotional well-being. That’s where healthy digital balance comes in.

# SECTION 12 — RECLAIMING BALANCE: WHY DISCONNECTION MATTERS

*How to stay connected without feeling overwhelmed, exhausted, or consumed by your devices.*

## 🔷 Key Terms

**Screen Time:** The amount of time you spend looking at a device each day.

**Scrolling:** Moving your finger up or down the screen to browse content.

**Doomscrolling:** Endlessly scrolling through negative news or upsetting content, even when it causes stress.

**Mindful Consumption:** Using your device with intention — choosing what you look at instead of letting the app decide for you.

**Addictive App:** An app designed to keep you engaged for long periods using notifications, infinite scrolling, and reward loops.

**Autoplay:** A feature that automatically loads the next video or post without your input.

**Focus Mode / Do Not Disturb:** Settings that silence notifications to help you concentrate or rest.

**Digital Boundaries:** Limits you set to protect your time, energy, and emotional health (e.g., no devices during meals or before bed).

**Wellbeing Tools:** Built-in settings that help monitor or reduce screen time.

---

## 12.1 — Why Balance Is Important

Technology keeps us connected, informed, and entertained. But constant use can also lead to:

- stress
- exhaustion
- distraction
- comparison pressure
- sleep problems
- reduced attention span
- social disconnection

Regaining balance does *not* mean giving up technology. It means being intentional — deciding how you use your device instead of letting your device use you.

---

## 12.2 — How Apps Are Designed to Capture Attention

Apps use bright colors, likes, alerts, and endless content to trigger dopamine, the brain's reward chemical. This makes it easy to lose track of time and hard to put the device down.

Apps keep you engaged with:

- endless scroll
- bright colors and reward effects
- notifications
- autoplay
- personalized recommendations
- "likes" and social feedback

Understanding this design helps you make conscious choices rather than reacting automatically.

---

## 12.3 — Recognizing Digital Fatigue

You may need a reset if you notice:

- difficulty focusing
- overwhelmed feelings
- checking your phone without purpose
- late-night scrolling
- constant distraction
- anxiety after using certain apps
- feeling pressured by social media

Digital fatigue is common — and fixable.

---

## 12.4 — How to Practice Mindful Digital Consumption

Mindful consumption means asking:

*"Why am I opening this app right now?"*
*"Is this helping me or draining me?"*

**Simple ways to practice:**

- Pause before opening an app
- Disable autoplay

- Hide apps you overuse
- Follow accounts that make you feel good
- Unfollow or mute accounts that cause stress
- Limit your news sources to a few trusted ones
- Spend more time creating and less time consuming

---

## 12.5 — How to Set Time Limits on Apps

All smartphones have screen-time tools.

### How to set limits (general):

1. Open **Settings**
2. Tap **Screen Time**, **Digital Wellbeing**, or **Wellness** (The exact name depends on your device)
3. Select **App Timers** or **App Limits**
4. Choose the app
5. Set a daily limit (15–60 minutes depending on the app)

Your device will remind you or block the app when you reach the limit.

---

## 12.6 — How to Use Focus Mode / Do Not Disturb

These features silence unimportant notifications so you can concentrate or rest.

### How to turn on Focus Mode:

1. Open **Settings**
2. Tap **Focus**, **Do Not Disturb**, or **Modes**
3. Choose a mode:
    - Work
    - Sleep
    - Personal
4. Customize which apps or people can reach you
5. Turn it on manually or schedule it daily

This reduces interruptions dramatically.

---

## 12.7 — How to Unfollow, Mute, or Remove Harmful Accounts

Many platforms allow you to control what you see without confronting anyone.

**General steps:**

1. Open the profile
2. Tap the three dots or menu
3. Select:
    - **Unfollow**
    - **Mute Posts/Stories**
    - **Hide**
    - **Block**

This is especially helpful for:

- comparison pressure
- anxiety
- triggering content
- misinformation

---

## 12.8 — How to Reduce Addictive Design Features

**Turn off autoplay:** Prevents endless video loops.

**Disable "endless scroll" triggers:** Decide to stop after the first natural break instead of continuing automatically.

**Remove color stimulation:** Using **grayscale mode** reduces cravings to keep scrolling.

**Turn off non-essential notifications:** Prevents apps from pulling your attention every few minutes.

**Delete or hide overused apps:** Out of sight = out of mind.

**Use widgets or folders:** Organize apps by purpose rather than impulse.

---

## 12.9 — Healthy Digital Boundaries

Simple boundaries can transform your mental energy.

### Examples:

- No phones during meals
- Place your phone in another room while sleeping
- Avoid screens for the first 30 minutes after waking
- “No scroll zones” (bathroom, bed, meetings, family time)
- News only from one reliable source per day
- Personal updates only after morning routine

These help you reconnect with offline life.

---

## 12.10 — Scheduled Digital Rest

Your brain needs rest the same way your body does.

### Ways to disconnect mindfully:

- Set **daily quiet hours** at night
- Schedule **weekend or evening breaks**
- Take a weekly “device-free hour”
- Do one activity daily with no screen present (walk, cook, meditate)
- Place your phone across the room instead of by your bed
- Put your phone out of reach during meals or conversations
- Use a physical alarm clock so you don’t start and end the day on your phone

You do *not* need to eliminate technology — just introduce healthier rhythms.

---

## 12.11 — Why This Section Matters

Digital life should support your wellbeing, not drain it.

By practicing mindful consumption and creating boundaries:

- stress decreases
- sleep improves

- focus sharpens
- relationships strengthen
- creativity increases
- you become less vulnerable to manipulation

Even with healthy habits, digital harm can still occur. Knowing where to turn for help, and which organizations protect you, is a key part of digital health.

# SECTION 13 — WHERE TO GET HELP

*Reliable support when you or someone you care about experiences digital harm, emotional distress, or identity issues.*

## 🔷 Key Terms

**Support Line:** A phone number or chat service where you can get professional help.

**Platform Support:** The help pages inside apps and websites that guide you through reporting, blocking, or securing your account.

**Cybercrime Unit:** A law enforcement group trained to handle online threats, scams, and identity theft.

**Identity Theft Protection Services:** Programs that help monitor your credit, secure your identity, and restore accounts after a breach.

**Crisis Support:** Immediate help for emotional distress, suicidal thoughts, or mental health emergencies.

**Hotline:** A phone number you can call anonymously for help.

---

## 13.1 — Why Knowing Where to Get Help Matters

Digital harm can be overwhelming and confusing. Whether it's:

- a scam
- harassment
- a hacked account
- sextortion
- identity theft
- exposure to harmful content
- emotional stress from online behavior

Most apps place their Help Center under your profile picture → Settings → Help or Support. No one should handle these situations alone. Help exists — and accessing it early prevents deeper harm.

The next section teaches you:

- where to go
- who to call
- what resources to use
- how to protect yourself and others

---

## 13.2 — Help for Identity Theft, Fraud & Financial Scams

### Federal Trade Commission (FTC)

**Website:** IdentityTheft.gov
Helps with:

- reporting identity theft
- creating recovery plans
- understanding scams

### Consumer Financial Protection Bureau (CFPB)

Helps if:

- banks refuse to reverse fraudulent charges
- credit bureaus do not respond
- financial companies act unfairly

### Credit Bureaus (Equifax, Experian, TransUnion)

Use for:

- credit freezes
- fraud alerts
- reviewing credit reports

### Your Bank or Credit Card Company

Contact immediately if:

- money was stolen
- accounts were accessed
- unauthorized purchases occurred

---

## 13.3 — Help for Online Harassment, Abuse & Threats

Contact your local police department if someone threatens your safety, demands money through blackmail, or tries to meet you in person after unwanted contact.

### Local Law Enforcement or Cybercrime Unit

Call if:

- threats include personal details
- harm feels imminent
- minors are involved
- blackmail or sextortion is present

### National Center for Missing & Exploited Children (NCMEC)

For threats or exploitation involving minors.

### Platforms' Safety Teams

Each app has a safety department (TikTok Safety, Meta Safety, YouTube Trust & Safety) that reviews reports.

---

## 13.4 — Help for Emotional Distress, Anxiety & Crisis Situations

Sometimes digital harm affects emotional health.

### 988 Suicide & Crisis Lifeline

Call or text **988** (U.S.) For:

- overwhelming stress
- emotional crises
- suicidal thoughts
- supporting someone in crisis

### Crisis Text Line

Text **HOME** to **741741** For:

- anxiety
- panic
- emotional distress
- needing someone to talk to

### Local community centers, counselors, or faith leaders

Many offer free or low-cost resources.

---

## 13.5 — Where to Find Help Inside Every Platform

Almost every app hides its **Support**, **Safety**, or **Help Center** inside similar menus.

### How to find help in any app:

1. Open the app
2. Tap your **Profile icon**
3. Look for **Settings**, **Privacy**, or **Support**
4. Select:
    - Help Center
    - Support
    - Report a Problem
    - Safety Center
5. Type your issue in the search bar

You will find step-by-step instructions for:

- blocking
- reporting
- recovering accounts
- securing passwords
- contacting support teams

---

## 13.6 — When You Should Seek Help With Law Enforcement Immediately

### Seek immediate help if:

- you are threatened
- someone knows your location
- a minor is involved
- intimate images are used for blackmail
- money or accounts were stolen
- your device was hacked
- you clicked a suspicious financial link
- you feel afraid or unsafe

- you feel emotionally overwhelmed

Support exists precisely for these situations.

---

## 13.7 — Additional Resources for Ongoing Protection

**Credit Monitoring Services:** Useful after data breaches or identity theft.

**Password Managers:** Reduce risk caused by weak or reused passwords.

**Parental Controls & Monitoring Tools:** Help protect minors from inappropriate contact or content.

**Fraud Alerts:** Notify you of suspicious financial activity.

---

## 13.8 — Why This Section Matters

Knowing where to turn for help:

- reduces panic
- speeds up recovery
- prevents financial or emotional escalation
- protects children and older adults
- helps law enforcement intervene
- empowers you to act confidently

Digital harm is never your fault. Support is available, and reaching out is a sign of strength.

# SECTION 14 — CONCLUSION: A SAFER, CALMER, MORE CONFIDENT DIGITAL LIFE

*Bringing everything together — and moving forward with clarity, control, and confidence.*

---

## 🔷 14.1 — What You Have Learned

By reaching the end of this guide, you now understand the **core foundations of digital life**:

- how devices work
- how the internet functions
- how websites and web addresses reveal trustworthiness
- how to build strong, secure accounts
- why identity and credit protection matter
- how to recognize the most common digital harms
- where harms appear across different platforms
- what to do when something goes wrong
- daily and weekly digital hygiene habits
- how to restore balance and protect your wellbeing
- where to get help when you need it

Congratulations! Many people use technology for decades without truly understanding these fundamentals. You now have the knowledge and resource to navigate digital life with clarity.

---

## 🔷 14.2 — Digital Safety Is a Skill, Not a Destination

The digital world evolves constantly. New platforms appear. Old platforms change their rules. Scams become more sophisticated. Apps introduce new features. Devices grow smarter — and more complex.

But the most important truth is this:

**Digital safety is not about memorizing every detail — it is about practicing core principles that apply everywhere.**

Those principles include:

- slowing down before clicking
- verifying sources
- protecting your accounts
- maintaining good digital hygiene
- disconnecting when needed
- trusting your instincts
- seeking help when something feels wrong

When these principles become habits, you are already ahead of most people online.

---

## 🔹 14.3 — You Are Not Alone

Everyone—from beginners to experts—struggles with technology at times.

It is normal to feel:

- confused
- overwhelmed
- anxious
- frustrated
- left behind

But help exists. Communities exist. Support lines exist. Platform tools exist. And knowledge makes all of it easier.

You never have to navigate digital challenges alone.

---

## 🔹 14.4 — A Calmer Digital Life Is Possible

With understanding comes control. With control comes calm. Your digital life can be:

- more secure
- less stressful
- better balanced
- more intentional
- more meaningful
- less overwhelming

Technology should serve you — not consume you. This guide has given you the language, tools, and awareness to make confident choices.

---

## 🔷 14.5 — Moving Forward: Small Steps, Big Impact

Here are simple next steps you can start today:

- Update your device
- Turn on multi-factor authentication
- Clean up your notifications
- Reduce your screen time by 10%
- Unfollow one account that drains you
- Set limits on addictive apps
- Review privacy settings this week
- Talk to a friend or family member about digital safety
- Bookmark this guide for future reference

Small steps add up. Each one reduces stress and increases your sense of control.

---

## 🔷 14.6 — Final Thoughts

Digital confidence grows with practice. You now have:

- foundational knowledge
- clear definitions
- step-by-step guidance
- practical habits
- an understanding of risks
- awareness of resources

Whether you're using technology for work, connection, entertainment, or everyday tasks, you now have the tools to do so safely.

Use this guide at your own pace, return to it whenever needed, and remember small steps build strong digital confidence. Feedback is always important – contact me if you have any questions or suggestions for improvement at scrylens00@gmail.com.

# APPENDIX A — REFERENCES

*Trusted organizations and resources that support digital safety, identity protection, mental wellbeing, and informed use of technology.*

## 🔷 A.1 — U.S. Government Resources for Digital Safety & Identity Protection

### Federal Trade Commission (FTC) — Identity Theft & Scams

**https://www.identitytheft.gov**
Official U.S. website for reporting identity theft, building a recovery plan, and learning how to avoid scams.

### Federal Trade Commission — Consumer Protection

**https://www.ftc.gov**
Guides on online shopping scams, privacy protection, and fraud prevention.

### Consumer Financial Protection Bureau (CFPB)

**https://www.consumerfinance.gov**
Information on financial scams, credit reporting errors, and disputes with lenders or credit bureaus.

### Cybersecurity & Infrastructure Security Agency (CISA)

**https://www.cisa.gov**
Federal cybersecurity guidance for individuals, families, and workplaces. CISA also provides easy-to-read alerts about new online threats, scams, and software vulnerabilities.

### USA.gov — Government Services & Digital Safety

**https://www.usa.gov/online-safety**
A central hub for federal information on privacy, safety, and avoiding online fraud.

---

## 🔷 A.2 — Credit & Financial Monitoring Resources

### AnnualCreditReport.com

**https://www.annualcreditreport.com**
The only government-authorized website for free yearly credit reports from Equifax, Experian, and TransUnion.

### Equifax

**https://www.equifax.com**
Provides credit reports, freezes, and fraud alerts.

### Experian

**https://www.experian.com**
Provides credit reports, freezes, identity protection tools, and fraud alerts.

### TransUnion

**https://www.transunion.com**
Provides credit monitoring, credit reports, and tools for detecting identity theft.

---

## 🔷 A.3 — Digital Wellbeing & Mental Health Resources

### 988 Suicide & Crisis Lifeline

**Call or text 988**
Immediate emotional support and crisis help available 24/7.

### Crisis Text Line

Text **HOME** to **741741**
Nonjudgmental support for anxiety, emotional overwhelm, or stressful digital interactions.

### National Alliance on Mental Illness (NAMI)

**https://www.nami.org**
Information, education, and local support groups.

These resources can support anyone experiencing digital fatigue, anxiety from online interactions, or emotional stress related to harmful digital content.

---

## 🔷 A.4 — Child & Teen Online Safety Resources

### National Center for Missing & Exploited Children (NCMEC)

**https://www.missingkids.org**
Resources for reporting online exploitation, sextortion, and harmful contact with minors.

### StopBullying.gov

**https://www.stopbullying.gov**
Guidance for kids, parents, and educators on cyberbullying prevention and intervention.

### Common Sense Media

**https://www.commonsensemedia.org**
Reviews of apps, games, and media to help families choose safe content.

These tools help families make safer choices and respond confidently when minors encounter harmful content or unsafe interactions online.

---

## 🔷 A.5 — General Digital Literacy & Learning

### Digital Literacy Resource Hub (U.S. Dept. of Education)

**https://digitalliteracy.gov**
Beginner-friendly tutorials for using computers, devices, and online tools.

### GCF Global — Free Technology Tutorials

**https://edu.gcfglobal.org/en/subjects/technology/**
Simple step-by-step lessons on basic computer and smartphone skills.

### Khan Academy — Technology Basics

**https://www.khanacademy.org**
Includes beginner-friendly lessons on internet basics, passwords, and online etiquette.

## 🔷 A.6 — Platform-Specific Safety Centers

Each platform updates these safety pages regularly, so they often provide the most accurate current instructions—especially helpful when the interface changes.

### TikTok Safety Center

https://www.tiktok.com/safety

### Meta (Facebook & Instagram) Safety Center

https://www.facebook.com/safety
https://about.instagram.com/community/safety

### YouTube Trust & Safety

https://support.google.com/youtube/answer/2802027

### Snapchat Safety Center

https://snap.com/en-US/safety/safety-center

### X (formerly Twitter) Safety

https://help.twitter.com/en/safety-and-security

### Discord Safety Center

https://discord.com/safety

### Reddit Safety & Security

https://www.redditinc.com/policies

### Roblox Safety

https://en.help.roblox.com/hc/en-us/categories/200213830-Safety

### Fortnite / Epic Games Safety

https://www.epicgames.com/site/en-US/parental-controls

## 🔷 A.7 — Cybercrime Reporting & Law Enforcement Contacts

### Internet Crime Complaint Center (IC3)

**https://www.ic3.gov**
For reporting online financial crimes, hacking, harassment, and fraud. Use IC3 for scams involving money, hacking, online extortion, fraud, or impersonation—not for minor disagreements or general harassment.

### Local Police or Sheriff

Contact when threats, extortion, impersonation, or stalking occur.

### State Attorney General's Office

Many AG offices offer scam alerts and consumer protection tools.

---

## 🔷 A.8 — Additional Tools for Privacy & Security

### Have I Been Pwned

https://haveibeenpwned.com
Check whether your email or password appeared in a data breach.

### Password Managers

- 1Password
- Bitwarden
- Dashlane
- Keeper
  Each provides tools for secure password storage and strong password generation.

### VPN Services (for advanced users)

Useful for privacy on public Wi-Fi; not necessary for beginners. VPNs can add privacy on public Wi-Fi, but they are optional and best suited for intermediate users. Beginners do not need them for everyday use.

# APPENDIX B — GLOSSARY OF DIGITAL TERMS

*Plain-language definitions for every major concept discussed in this guide.*

---

## 🔤 A

**Account:** A personal profile you create to use a website, app, or service.
**Ad / Advertisement:** Paid content meant to sell something or influence behavior.
**Addictive App:** An app designed to keep you engaged using notifications, endless scroll, or autoplay.
**Algorithm:** A set of rules apps use to decide what content you see first.
**App (Application):** A software program on your device, such as messaging apps, games, or banking apps.
**App Permissions:** Settings that control what information an app can access, like your camera, microphone, or location.
**Authentication App:** An app that creates temporary codes to verify your identity during login.
**Autoplay:** A feature that automatically plays the next video or post.

---

## 🔤 B

**Bandwidth:** How much data your internet connection can handle at once—like the width of a pipe.
**Biometrics:** Using your body (fingerprint, face scan, voice) to unlock a device or verify identity.
**Block:** A safety tool that prevents someone from contacting you or seeing your profile.
**Bluetooth:** A short-range wireless technology that connects devices like headphones or keyboards.
**Bot Account:** A fake or automated account not controlled by a real person.
**Browser:** An app used to visit websites (Chrome, Safari, Edge, Firefox).
**Buffering:** A pause or delay while a video loads due to slow internet.

---

## 🔤 C

**Cache:** Temporary files stored by apps or websites that help them load faster.
**Contact Page:** A webpage with phone numbers, emails, or support information.
**Credentials:** Your login details, usually your username and password.
**Credit:** Your financial reputation showing how you manage money and debt.
**Credit Freeze:** A tool that prevents new accounts from being opened in your name.
**Cyberbullying:** Bullying or harassment that happens online.
**Cybercriminals:** People who use computers or the internet to steal information, money, or access.

---

## 🔤 D

**Data Breach:** When a company, website, or service is hacked and personal information is leaked.
**Data Exposure:** When your information becomes visible to people who should not have access to it.
**Default Settings:** The automatic settings your device or apps come with—often not the safest.
**Device:** Any digital tool you use (phone, tablet, laptop, smartwatch, or computer).
**Device Recognition:** When a platform remembers a device you previously logged in on.
**Digital Hygiene:** The regular habits that keep your device, accounts, and data safe and organized.
**Direct Message (DM):** A private message sent inside an app.
**Display Settings:** Controls for brightness, color, text size, and accessibility features.
**Doomscrolling:** Endlessly scrolling through upsetting or negative content.
**Download:** Saving a file, image, app, or document to your device.

---

## 🔤 E

**Email:** Electronic mail sent through the internet.
**Encryption:** Technology that protects information so only the intended person can read it.
**Extension (URL Extension):** The ending of a web address (like .com or .gov) that identifies the type of site.

---

## 🔤 F

**Fake Seller:** Someone pretending to sell items online to steal money or information.
**Feed:** A scrolling list of videos, posts, or updates tailored to your interests.
**Firewall:** A security tool that blocks unsafe connections.
**Focus Mode / Do Not Disturb:** A tool that silences notifications to help you concentrate or rest.
**Fraud:** Tricking someone for financial gain.

---

## 🔤 G

**Gaming Currency / Skins:** Digital items used in games, often targeted in scams.
**Grayscale Mode:** A display mode that turns your screen black and white to reduce overstimulation.
**Grooming:** When someone builds trust with harmful intentions, often toward minors.

---

## 🔤 H

**Harassment:** Repeated or targeted harmful behavior online.
**Help Center:** A section within apps that provides safety tools and reporting instructions.
**Homepage:** The main page of a website.
**HTTP:** The basic system your browser uses to load websites, but without encryption.
**HTTPS:** A secure, encrypted version of HTTP that protects your information.

---

## 🔤 I

**Identity:** Information that describes who you are (name, birthday, address, accounts).
**Identity Theft:** When someone uses your personal information to pretend to be you.
**Incognito Mode:** A private browsing mode that doesn't save history or cookies.
**Internet:** The global network of connected devices that share information.
**ISP (Internet Service Provider):** The company you pay for internet service (Comcast, AT&T, Verizon).

---

## 🔤 K

**Keyboard Shortcuts:** Quick key combinations that perform tasks like copy/paste.

---

## 🔤 L

**Link:** Clickable text or an image that takes you to another webpage.
**Location Services:** Settings that let apps use your GPS location.
**Lock Screen:** The screen that appears before you unlock your device.

---

## 🔤 M

**Malware:** Harmful software used to damage or steal information.
**Memory (Storage):** The amount of space on your device for apps, files, and photos.
**MFA (Multi-Factor Authentication):** A second step during login, such as a code or fingerprint.
**Mindful Consumption:** Using your device intentionally instead of automatically.
**Modem:** A device that connects your home to the internet.
**Mute:** A tool that hides someone's content without blocking them.

---

## 🔤 N

**Notifications:** Alerts that apps send to get your attention.
**NSFW Content:** Material that is "Not Safe for Work"—explicit or inappropriate content.

---

## 🔤 O

**Operating System (OS):** The software that runs your device (iOS, Android, Windows, macOS).
**Operating System Examples:** Windows (PCs), macOS (Macs), iOS (iPhones), Android (many smartphones).
**Online Marketplace:** Websites where people buy or sell goods (Amazon, Temu, Facebook Marketplace).

---

## 🔤 P

**Password:** A secret combination used to log into accounts.
**Password Manager:** An app that creates and stores strong passwords.
**Personal Information (PII):** Any information that can identify you.
**Phishing:** Messages pretending to be legitimate to steal information.
**Platform:** Any website or app where people interact.
**Privacy Settings:** Controls that determine what others can see or access.
**Public Wi-Fi:** Open networks in places like cafes or airports—often less secure.

---

## 🔤 Q

**QR Code:** A square barcode you scan with your camera to open a link.

---

## 🔤 R

**Report:** Telling a platform that something harmful or suspicious happened.
**Reels / Shorts:** Short vertical videos recommended by algorithms.
**Router:** A device that sends Wi-Fi throughout your home.

---

## 🔤 S

**Scam:** A trick meant to steal money or information.
**Screenshot:** A picture of whatever is on your screen.
**Search Engine:** A tool that helps you find information online (Google, Bing).
**Session:** The time period when you're logged into an account.
**Settings:** Controls for privacy, security, notifications, and performance.
**Sextortion:** Blackmail involving private images.
**Spoofing:** Pretending to be a trusted phone number or website.
**Storage:** Space for apps, files, photos, and data on your device.

---

## 🔤 T

**Text Message (SMS):** A message sent through cellular networks.
**Tracking:** How apps follow your online behavior to show ads.
**Two-Step Verification:** Another term for MFA.

---

## 🔤 U

**Update:** A software fix or improvement.
**URL:** A website address you type or click.
**Username:** The name or email you use to sign in.

---

## 🔤 V

**Verification:** Checking if a message, account, or website is real before interacting.
**Vishing:** Phishing through phone calls.

---

## 🔤 W

**Webpage:** A single page on a website.
**Website:** A collection of connected pages on the internet.
**Wi-Fi:** A wireless internet connection.
**Wellbeing Tools:** Built-in settings that track or help reduce screen time.

---

## 🔤 X, Y, Z

**X (formerly Twitter):** A platform for posting short updates and news.
**YouTube:** A platform for watching and sharing videos.