Core Concepts & Definitions

Internet Street Smarts™

CYBER COLLECTIVE

Table of Contents

This document provides key terms and definitions essential for navigating the online world safely. Each concept is explained with clear, real-life examples and analogies to help you understand how they apply to your digital life.

We've included three important sections for each concept:

1. **How to Explain This to an Elder**: Simple, relatable explanations to help you teach the older adults in your life how to stay safe online.
2. **How to Explain This to a Kid**: Easy-to-understand descriptions for teaching younger children or teens about online safety.
3. **Social Justice Lens**: Where relevant, this lens highlights how these issues affect marginalized communities, ensuring the broader social impact of digital safety is understood.

By learning these core concepts, you'll not only protect yourself but also help spread digital literacy within your community, making the internet a safer place for everyone.

Core Concepts

Algorithmic Bias

- **Definition:** Algorithmic bias is when a computer program makes decisions that are unfair because of the data it learned from or how it was built. It means the system may treat some people differently without intending to.
- **Example:** Imagine teaching a robot to recognize fruit, but you only show it red apples. Later, when it sees a green apple, it might not recognize it as an apple at all. The robot isn't trying to be unfair—it just didn't learn enough variety.
- **Social Justice Lens:** Algorithmic bias can affect everyday things like job applications, loans, or even what shows up in your search results. It's important because these systems can unintentionally repeat unfair patterns from the real world.
- **How to Explain This to an Elder:** "It's like if a scale was made a little uneven. Even if you put the same weight on both sides, it might tip unfairly. Computers can be like that too—they sometimes lean in one direction because of how they were set up."
- **How to Explain This to a Kid:** "It's like if your game always makes one player slower than the other, even if both are playing the same way. That wouldn't be fair. Algorithmic bias is when a computer makes choices that aren't fair like that."

Cyber Threats

- **Definition:** Online risks like hacking, identity theft, scams, and malware.
- **Example:** Just as you wouldn't leave your front door unlocked, you need to protect your online accounts and devices to prevent break-ins.
- **Social Justice Lens:** Vulnerable communities are often more at risk because they may not have access to cybersecurity education or tools, leaving them exposed to scams or identity theft.
- **How to Explain This to an Elder:** "Think of your online accounts like your house. You wouldn't leave the front door unlocked at night because someone could break in. The same thing applies online—if you don't secure your accounts, someone could break in and steal your information."
- **How to Explain This to a Kid:** "Imagine if you left your bedroom door wide open, and someone came in and took your toys. That's what happens when you don't protect your online accounts—someone could break in and steal your personal stuff."

Data Privacy

- **Definition:** The protection of personal information from unauthorized access or misuse. It's about knowing what data is collected, how it's used, and who has access to it.
- **Example:** Think of your house as your personal data. If you leave the door unlocked, anyone can walk in. Data privacy is about locking that door and only letting in trusted people.
- **Social Justice Lens:** Data privacy is a universal right, but marginalized communities often face greater risks because their data is more likely to be exploited without consent, perpetuating inequalities.
- **How to Explain This to an Elder:** "It's like keeping your home secure. If you don't lock the door, anyone can walk in. Online, protecting your personal information works the same way—you need to lock your 'digital door' so only trusted people have access."
- **How to Explain This to a Kid:** "It's like making sure no one reads your diary unless you say it's okay. Just like you keep your secrets safe, data privacy helps you keep your personal information safe from others."

Digital Surveillance

- **Definition:** The monitoring of online activity by third parties, including governments and corporations, often without the user's knowledge or consent.
- **Example:** It's like being followed by a camera everywhere you go—even in your own home. Every click, search, and message is watched.
- **Social Justice Lens:** Surveillance disproportionately impacts marginalized communities, reinforcing power imbalances and leading to unjust profiling.
- **How to Explain This to an Elder:** "It's like having someone watch everything you do, even inside your own home. Online, many companies and governments track what you do without you knowing, which can feel like someone is always watching."
- **How to Explain This to a Kid:** "Imagine if someone was following you around the playground and writing down everything you do. That's what happens with online surveillance—someone watches what you do on the

internet, even if you don’t know it."

Digital Wellness

- **Definition:** Maintaining a healthy balance of online activity and ensuring mental, emotional, and physical well-being when using technology.
- **Example:** Just like you take breaks during the day to stay energized, digital wellness means taking breaks from screens to avoid burnout.
- **Social Justice Lens:** Marginalized communities often face higher stress online, whether from harassment or overexposure to harmful content, making digital wellness crucial for mental health.
- **How to Explain This to an Elder:** "Just like you take breaks during the day to rest, you need to take breaks from your phone or computer. Spending too much time online can make you feel overwhelmed, and digital wellness helps you stay balanced."
- **How to Explain This to a Kid:** "You know how your eyes get tired when you play video games too long? Digital wellness is about taking breaks so your brain doesn’t get tired from being online all the time."

Basic Terminology

Ad Blockers

- **Definition:** Software that prevents online advertisements from displaying, which also helps to prevent tracking by advertisers.
- **Example/Analogy:** Using an ad blocker is like putting a “No Soliciting” sign on your door—it keeps unwanted ads and data tracking out.
- **Social Justice Lens:** Targeted ads often exploit racial stereotypes or manipulate vulnerable populations. By using ad blockers, marginalized individuals can avoid harmful advertising and reduce their exposure to manipulative marketing practices.
- **How to Explain This to an Elder:** "It’s like putting a sign on your front door that says ‘No Salespeople.’ An ad blocker keeps unwanted ads from popping up and tracking what you do online."
- **How to Explain This to a Kid:** "Imagine if you kept getting interrupted while playing a game by people trying to sell you stuff. An ad blocker stops those interruptions and keeps you from being tracked."

Cookies

- **Definition**: Small files stored on a user’s computer by websites to track browsing activity and preferences.
- **Example/Analogy**: Cookies are like breadcrumbs—each one tells a story about where you’ve been online, allowing websites to remember your preferences.
- **Social Justice Lens**: The tracking and use of cookies can lead to discriminatory practices, such as price manipulation or targeted ads based on race, income, or location, further entrenching economic and social disparities.
- **How to Explain This to an Elder**: "Cookies are like little notes websites leave on your computer to remember where you’ve been online. They help websites remember your preferences but can also track your movements."
- **How to Explain This to a Kid**: "It’s like leaving a trail of breadcrumbs while walking through the woods. Cookies are little pieces of information that show where you’ve been online."

Deepfakes

- **Definition:** AI-generated fake media, such as videos or audio recordings, designed to deceive or manipulate.
- **Example/Analogy:** A deepfake is like a counterfeit painting—it looks real, but it's a fake created to fool others.
- **Social Justice Lens:** Deepfakes can be weaponized to target marginalized individuals or groups, spreading false information that reinforces harmful stereotypes or leads to real-world consequences, such as defamation or violence.
- **How to Explain This to an Elder:** "It's like a fake video of someone doing something they didn't actually do. These fake videos can be used to trick or manipulate people."
- **How to Explain This to a Kid:** "It's like someone editing a video to make it look like you did something you didn't do. It's a trick to make people believe something that's not true."

Multi-Factor Authentication (MFA)

- **Definition**: A security measure that requires users to verify their identity in more than one way (e.g., password + fingerprint) before accessing an account.
- **Example/Analogy**: MFA is like having two locks on your door—you need both keys to get in, making it much harder for someone to break in.
- **Social Justice Lens**: Providing marginalized communities with easy-to-use MFA tools can empower them to protect their data and online identities, helping to bridge the digital safety gap.
- **How to Explain This to an Elder**: "It's like having two locks on your door. Even if someone can get through one lock, the second one makes it much harder for them to break in."
- **How to Explain This to a Kid**: "It's like having two secret codes to get into your game. Even if someone guesses the first code, they can't get in without the second one."

Password Manager

- **Definition**: A tool that stores and generates strong passwords, keeping them secure for different accounts.
- **Example/Analogy**: Think of a password manager like a safe—it holds all your keys (passwords) in one place, and only you have the combination to open it.
- **Social Justice Lens**: Accessible password managers help protect marginalized communities from common risks like weak or reused passwords, which are often exploited by cybercriminals to gain unauthorized access to personal accounts.
- **How to Explain This to an Elder**: "It's like having a safe where you store all your keys. Instead of remembering every password, you only need to remember the combination to open the safe."
- **How to Explain This to a Kid**: "It's like having a treasure chest where you store all your secret codes. You only need one key to unlock it, and it keeps everything safe."

Personal Identifiable Information (PII)

- **Definition**: Any data that can be used to identify an individual, such as name, address, Social Security number, or email.
- **Example/Analogy**: Just like your fingerprint uniquely identifies you, PII is any information that could single you out in a crowd of data.
- **Social Justice Lens**: PII is often used without consent, and marginalized groups may have their data sold or exploited for surveillance, marketing, or discriminatory practices.
- **How to Explain This to an Elder**: "Think of PII like your ID card—it's information that tells people who you are. If someone gets that information without permission, they could misuse it."
- **How to Explain This to a Kid**: "It's like your name tag at school—it shows who you are. You wouldn't want someone you don't trust to have that information, right?"

Phishing

- **Definition**: A type of scam designed to trick individuals into providing personal information like login credentials or credit card numbers through fake communications (emails, texts, etc.).
- **Example/Analogy**: Phishing is like a fake lottery ticket—someone pretends to offer you something exciting, but really they're just trying to steal your information.
- **Social Justice Lens**: Phishing schemes disproportionately target vulnerable populations, especially those who may not have access to cybersecurity education or tools to protect themselves. This often results in financial loss or identity theft, which can have lasting impacts on their economic security.
- **How to Explain This to an Elder**: "It's like getting a call from someone pretending to be your bank, asking for your account details. Phishing is when someone tries to trick you into giving away personal information."
- **How to Explain This to a Kid**: "Imagine someone pretending to be your friend to get your lunch money. Phishing is when someone online pretends to be someone they're not to trick you into giving them your private information."

Ransomware

- **Definition**: A type of malicious software that encrypts a victim's data and demands payment to restore access.
- **Example/Analogy**: Ransomware is like a thief breaking into your house, locking all your valuables in a safe, and demanding money for the combination to unlock it.
- **Social Justice Lens**: Ransomware attacks often target institutions that serve marginalized communities, such as schools or hospitals, where a breach can disproportionately impact those who are already vulnerable.
- **How to Explain This to an Elder**: "It's like someone breaking into your home, locking all your important belongings in a safe, and demanding money to give you the key to open it."
- **How to Explain This to a Kid**: "Imagine a thief locking all your toys in a

box and telling you that you have to pay them to get the key to open it."

Social Engineering

- **Definition**: A tactic that uses psychological manipulation to trick people into revealing confidential information.
- **Example/Analogy**: Social engineering is like a con artist convincing someone to hand over their bank account information by pretending to be a trusted friend or authority figure.
- **Social Justice Lens**: Social engineering scams often target marginalized communities, exploiting their lack of access to security tools or digital literacy. These attacks can lead to devastating financial and personal consequences.
- **How to Explain This to an Elder**: "It's like someone pretending to be a trusted friend and convincing you to give them your personal information, like your bank account number."
- **How to Explain This to a Kid**: "Imagine someone pretending to be your teacher to get your personal information. Social engineering tricks people into giving away things they wouldn't normally share."

VPN (Virtual Private Network)

- **Definition**: A tool that masks a user's IP address, making their online activities more private and secure.
- **Example/Analogy**: A VPN is like wearing a disguise when you go out—no one knows who you are or where you've been.
- **Social Justice Lens**: VPNs can protect activists, journalists, and marginalized individuals from surveillance, censorship, and exploitation by providing anonymity and security online.
- **How to Explain This to an Elder**: "It's like wearing a disguise when you're out in public. A VPN hides your online identity and keeps your activities private."
- **How to Explain This to a Kid**: "It's like wearing a mask so no one knows who you are. A VPN keeps your online activity private."

Common Scams

Crypto Scams

Promises of high returns in cryptocurrency investments that turn out to be fraudulent.

Deepfake Scams

AI-generated videos or audio recordings that mimic real people to deceive victims.

Fake Job Scams

Scammers post fake job listings to steal personal information or money.

- **Example:** A job post on LinkedIn offers a too-good-to-be-true salary but provides no real company info.

IRS/Government Impersonation Scams

Scammers pretending to be government officials, threatening fines or arrest unless you pay immediately.

Payment App Scams

Scammers trick people into sending money through apps like Venmo or CashApp.

- **Example**: Someone sends you money "by mistake" and asks you to return it. Don’t fall for it—it’s often a scam.

Phishing

Trickery through emails, texts, or messages that impersonate trusted sources to steal sensitive information.

- **Example:** Getting a message from a "friend" on Facebook asking, "Is this you in this video?" Be careful—this is a common tactic to hack your account.

QR Code Scams

Malicious QR codes that lead to harmful websites or malware downloads.

Ransomware

A type of malware that locks your files and demands payment to unlock them.

Romance Scams

Scammers build fake relationships online to manipulate victims into giving them money or personal information.

Social Engineering

Psychological manipulation used to trick people into revealing confidential information.

- **Example:** Getting a fake phone call from someone posing as a government official, asking for money to clear a "debt."

Tech Support Scams

Fraudsters pose as tech support agents to gain access to your computer or install malware.