**Basics of Cyber Security: The Internet is Out to Get You (Unless You Read This)**

Meta Description: Everything you should have learned before clicking that link. A fun, suspiciously engaging beginner’s guide to not get wrecked online.



gpt-generated image (because why not)

*"I don’t need cybersecurity. I’m just a normal person." — Someone who’s about to lose $4,000 to a fake banking app (or an … scammer)*

If you use the internet, you are already in the game. You just didn’t read the rules. That’s where this article comes in to explain you why you should be well-informed.

This is the Basics of Cybersecurity module, and if done (read) right, it will be your favorite trauma-bonding experience with the internet. (its not that traumatising)

**What is Cyber Security (And Why Should You Give a Damn)?**



gpt-generated for cybersecurity?

Cyber security is the art of science of not getting pwned (hacked/rekt/destroyed/scammed).

It’s about protecting your:

* Data (your texts, files, memes)
* Devices (your phone, laptop, smart fridge)
* Identity (your precious login credentials “123456”)
* Sanity (Have you ever experienced/recovered from ransomware? No? Good. Let’s keep it that way. Wait a minute… Do you even know what ransomware is?)

***Pop Quiz Time?***

What does CIA stand for in cybersecurity?

* Central Intelligence Agency
* Confidentiality, Integrity, Availability

**Answer**: The first one is obviously wrong, it's the second one (and there it is, you have learned something so basic yet important)

**Who’s Out to Get You?**



gpt-generated for attackers

Cyber threats are like bad dates, they come in many forms and don't really care about your feelings.

Here’s the **hit list:**

* **Malware:**Viruses, worms, ransomware, spyware. Think of them as Evil Pokémon. I can’t imagine but assume like some round ball like thing approaches you and becomes a monster you never thought of.
* **Phishing:**Fake emails that look legit. **Spoiler**: They’re not.***Bonus Point*** if it’s from “Amazonn.com” (so amazon cant spell themselves right?)
* **Social Engineering:**You didn’t get hacked, you gave away your password to “*tech support*” (seriously if someone asks you you’re password, do you just give it away)
* **Ransomware**: “Pay us $300 in Bitcoin or your files will not see another day, get it.” (You lose alot of money or you just shutdown your pc hoping it goes away)
* **DDoS Attacks:** Basically, a flash mob on your website. But no music, just downtime. (your website will be down until the DDoS attack is completed)

***Engage?***

Think you could spot a phishing email?

Check your inbox right now maybe. Find one. Screenshot it and … well I didn't think we would get this far would we.

(Good News: We will cover email analysis as well in our publications)

**Cyber Hygiene: Your Digital Bathwater**



gpt-generated hygiene

Let’s be honest. You’ve probably done at least one of these crimes:

* Used the same password for everything
* Clicked “Remind me Later” on every software update
* Shared your Netflix login with someone named “B33n” (I dont even know whose B33n)
* Opened an email attachment titled *Invoice\_GUARANTEED\_PAYOUT.zip (if it was that guaranteed, it would be in your bank account lol)*

***Let’s fix that.***

Here is your **starter kit**:

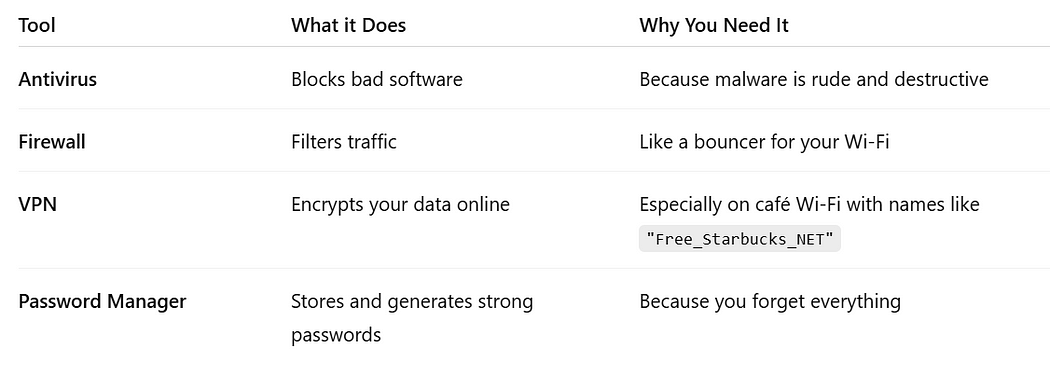
* Use unique, long passwords (14+ characters, no “1234”)
* Enable 2FA on literally everything
* Backup your stuff regularly
* Update your devices — yes, go ahead and restart it now
* Think before you click, if it sounds urgent (or too good to be true), it’s probably a scam

**Security Tools That Won’t Fry Your Brain**



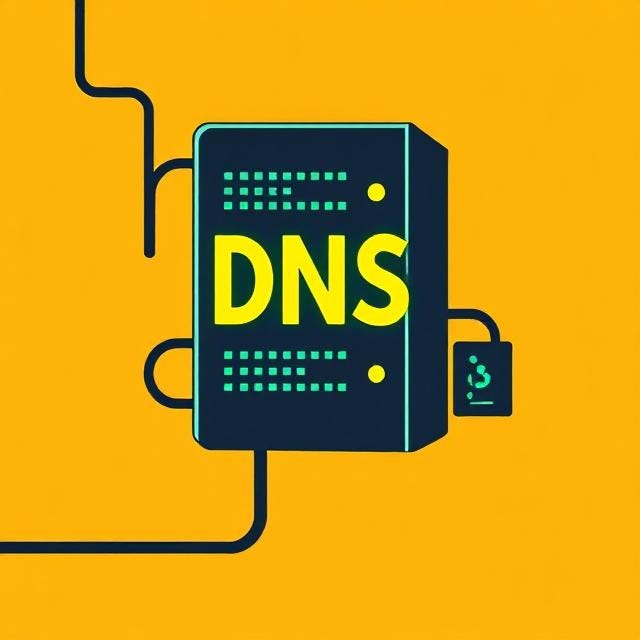
gpt-generated for tools

You don’t need to be a hacker. Just a little less reckless.



Your Basic Cyber Security Toolkit

**What Actually Happens When You Open a Website?**



gpt-generated DNS (I don't even know if this is a server — tried my best prompting)

Let’s break it down

1. You type *google.com*
2. Your browser asks **DNS**what that means
3. DNS says, “Here’s an IP Address”
4. Your Device connects to a server somewhere
5. The server sends data back
6. Website appears
7. Tracker cookies appear
8. Marketing appears
9. Existential crisis begins (Google existential crisis please, you will love it). Done? it’s just self reflection.

***Engage?***

Open Developer Tools in your Browser (F12 -> Network Tab)

Refresh a website

Marvel at the 243 (or some random number) files that loaded in 2 seconds

Realize you know nothing. And that’s okay, just move on. Not everything has to be known, even highly experienced Cybersecurity professionals do not know every single details in depth.

**Mobile Security 101: Your Pocket Spy Device**

If someone hacked your phone, they could:

* Read your messages
* Listen to your mic
* Track your GPS
* Access your photos (including *those*ones)

***Prevention Checklist:***

* Lock your screen (Doesn’t really help lol, another prevention would be throw away your phone, would you do it?)
* Don’t install sketchy apps (Seriously its below 1 star)
* Turn off Bluetooth & Wi-Fi when not in use
* Check app permissions — why does that flashlight need camera access?

**Don’t by a Cybercriminal (By Accident)**



gpt for clean cybersecurity specialist

It’s cool to learn. It’s not cool to be arrested.

*This module will lightly explain:*

* What’s legal hacking (white hat) vs illegal hacking (black hat)
* What happens when you DDoS your school “for fun” (expulsion, lawsuits, regrets)
* Why “testing a website’s login for vulnerabilities” without permission = felony

Remember:

*Learning = Good*

*Breaking Laws = Netflix documentary about you in 5 years (How a script kiddie got arrested for attempting to hack his own school to get the extra 5 grades)*

**So… Who works in Cyber Security Anyway?**

Cyber Security isn’t all hoodie-wearing hackers in basements.

Here’s the breakdown:

* **Red Team**: Break things legally
* **Blue Team:** Defend everything
* **GRC:** Governance, Risk, Compliance, basically spreadsheet and document ninjas
* **SOC analyst:**Watches alerts all days, questions life (at times)

***Curious?***

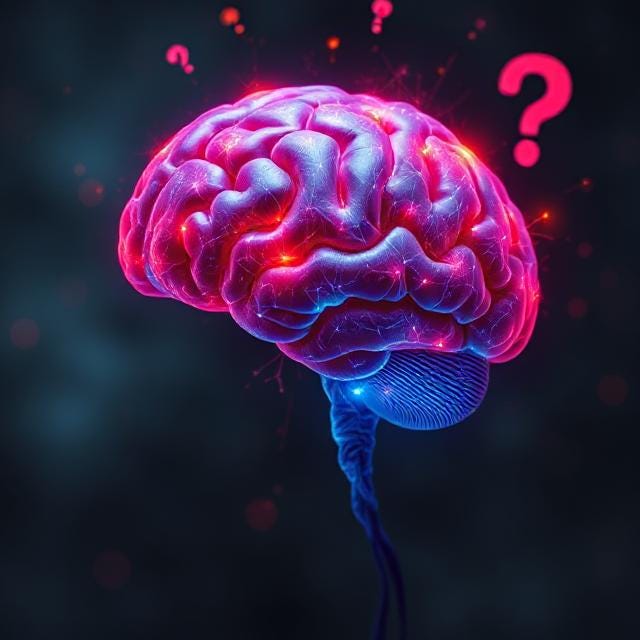
Google these roles. See which one makes you go “That’s me”

**TLDR: If you Remember Nothing Else:**

* You are a target. Even if you think you’re not
* Cybersecurity isn’t hard, just a habit
* Don’t be the weakest link. Be the suspicious one
* This is just the beginning

**Let’s Make it Interactive**

Hey, you made it this far- so let’s test if you were actually paying attention.



responsive-brain-cells

***Quick Quiz***

Which one is NOT a common phishing tactic?

1. “Your account has been locked! Click here to unlock.”
2. “You’ve inherited a million dollars from a prince.”
3. “Download this free antivirus from totally-legit-site.ru”
4. “We baked you cookies! Click to smell them.”

Drop your answer in the comments — I might personally not have cheated on this (personally).

***Mini Challenge***

Come up with the strongest password you can (without giving your actual one) — bonus points for creativity and humor.

* Tip: Make sure you can remember what you wrote too.

***Comment Prompt***

What’s the dumbest link you’ve ever clicked on?

(No judgement. Okay, maybe just a little)

***Quick Poll (Answer in Comments):***

Do you use 2FA (Two-Factor Authentication) on all your accounts?

A. Yes, like a true cyber warrior

B. On the important ones

C. What’s 2FA

**Conclusion**

If you survived this blog without clicking a shady link or reusing your pet’s name as a password. congrats, you’re officially less hackable.

**Enjoyed the read?**  
Smash the follow button, drop a comment, and share this with someone who still thinks “password” is a good password.