Cyber
Ready
Balkans

Cyber Ready Balkans

A Guide for Youth into Cybersecurity

Resource

Ipsumus, L. R., & Dolor, S. A. (2021). Consequat Elit Sed Do Eiusmod: A Metaphysical Inquiry into Vitae Energetica. Loremia Academic Press.

About Us

We are a team of Chevening Cybersecurity Fellows from across the Balkans. The Fellows are professionals with diverse backgrounds in cybersecurity, from ethical hacking and digital forensics to risk management, governance, and cyber education.

This project, Cyber Ready Balkans, is funded by the UK Foreign, Commonwealth & Development Office (FCDO) through the Chevening Fellowship Programme. **It was born from a shared mission:** to connect the region, close the gap between education and opportunity, and introduce young people to the world of cybersecurity in a language they understand.

We've seen firsthand how many students in Kosovo, North Macedonia, and Montenegro have the talent and curiosity, but not the guidance or access to enter this field. Through this project, we aim to change that.

Table of Contents

What Cybersecurity Is

Where to Work in Cybersecurity in North Macedonia

What Cybersecurity Is?

Chapter 1: Why You Should Care

Chapter Goal:

Make you realize that cybersecurity isn't just for IT nerds; it's about you, your lives, and your future. It is designed to show you that you're already part of the cyber world, whether you like it or not.

1. A Wake-Up Call

Let's start with a story.

Arta had 12,000 followers on Instagram. She posted

photography, shared reels, built a small community. One day she clicked on a message offering a free camera lens giveaway. It looked legit. Within minutes, she was logged out. Her password didn't work. Her account was gone. Someone had taken over, changed the email, and started scamming her followers with crypto schemes.

No warning. No way back.

2. "But I'm Nobody..."

This is what most people think:

- "I'm not famous."
- "I don't have money."
- "Why would anyone hack me?"

Here's the truth: they don't care who you are.

Hackers cast wide nets. They want access: to your email, your phone, your followers, your files. Why?

- Your data = can be sold.
- Your device = can be used for attacks.
- Your account = can scam others.
- Your identity = can be copied.

You're not invisible. You're connected. And that's all it takes.

3. What's Actually at Risk?

Cybersecurity sounds abstract. So let's make it real.

Without it, you can lose:

- Your chats, DMs, and photos
- Your money and bank access
- Your reputation - through fake posts or leaked content
- Your future - college apps, job applications, all compromised
- Your ideas - stolen, copied, or erased

This isn't about "if." It's about "when."

4. It's Already Happening in Kosovo

This isn't just a Hollywood problem.

Right here in Kosovo:

- Students have been tricked with fake Erasmus links.
- Parents have clicked malware in WhatsApp groups.
- Government agencies have been hit with DDOS and malware.
- Phone scams and phishing emails are increasing every year.

Cybersecurity sounds abstract. So let's make it real.

5. Imagine Your Digital Life as a House

Let's simplify.

Think of your phone or laptop as your house.
Your messages = your private conversations.
Your photos = your personal memories.
Your emails = your work and future.

Now imagine leaving your front door wide open. Every day. With a note saying, "Help yourself."

Sounds crazy? That's how most people live online. Weak passwords. Clicking random links. No idea what's running in the background.

Cybersecurity is just this: closing the door. Locking it. Putting up an alarm.

6. This Isn't Just Today. It's Your Future.

You're not just online today.

You'll study, work, date, bank, buy, vote, and maybe even run a business online.

Everything is connected. And that means:

- A breach can hurt your reputation.
- A scam can drain your account.
- A hacked phone can ruin your job interview before it starts.

The digital you is just as real as the physical you.

If you don't protect it, someone else can control it.

7. Cybersecurity = Control, Power, Freedom

Forget the image of cybersecurity as boring, technical, or only for "hackers."

Here's what it really is:

- Control - You decide who sees your stuff.
- Power - You don't get fooled. You understand how things work.
- Freedom - You can move through the digital world safely.

Learning cybersecurity is not just smart, it's empowering. It makes you sharper, faster, more aware.

It's a skill that protects you, helps others, and opens career doors everywhere.

8. Are You at Risk? (Fast Self-Check)

Answer honestly:

- Do you reuse the same password everywhere?
- Have you ever clicked on a weird link from Instagram or WhatsApp?

- Do you use public Wi-Fi without a VPN?
- Do you know if your email has ever been leaked?

If you said "yes" to any of these... You're already exposed.

But don't worry. This guide is here to change that.

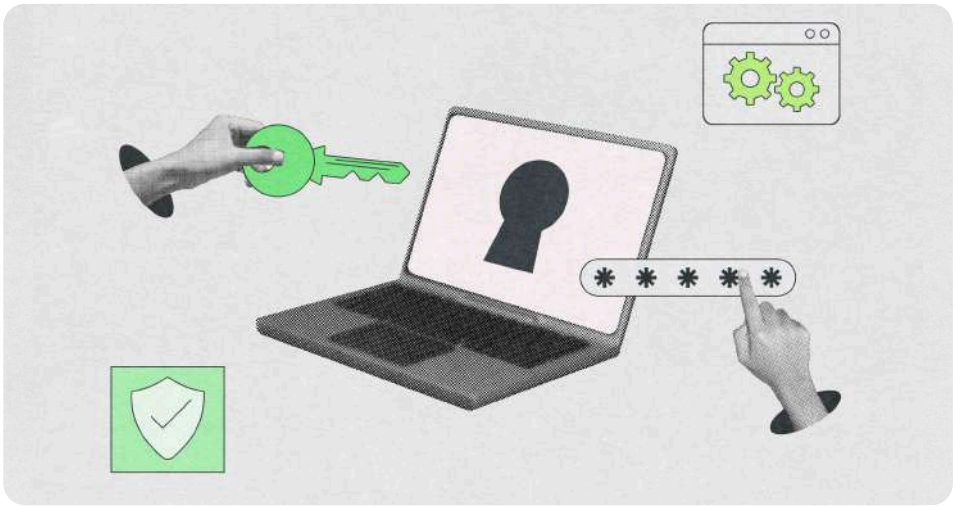
Final Word

You don't need to be scared. You need to be aware.

This is the start of learning how to protect yourself, and maybe one day, protect others too.

Let's move.

Chapter 2: What is Cybersecurity



It's not just about hacking.

It's about keeping your digital life safe, from the inside out.

1. Cybersecurity in One Sentence

Cybersecurity means **protecting computers, networks, devices, and data from being stolen, damaged, or misused.**

It's that simple.

2. What Needs Protecting?

Anything digital:

- Your phone
- Your laptop
- Your accounts
- Your photos, files, and messages
- School systems, bank servers, even water and energy infrastructure

If it's connected to the internet, it can be attacked. If it can be attacked, it needs security.

3. The Cybersecurity Triangle (CIA Triad)

This is the ABC of cybersecurity, used everywhere in the world.

- C - Confidentiality

  Keep it private. Only the right people should have access.
  Example: Your messages shouldn't be seen by strangers.

- I - Integrity

  Keep it accurate. No unauthorized changes.
  Example: Your school grades shouldn't be altered

by someone else.

- A - Availability

  Keep it accessible. You should be able to use it when you need it.
  Example: Your online banking should work when you log in.

Cybersecurity is about **balancing all three.**

4. What Cybersecurity Is Not

Let's clear up some confusion.

It's not just "hacking into systems."

It's not about sitting in a dark room typing code like in the movies.

It's not only for geniuses or IT people.

Yes, ethical hacking is part of it. But there's also:

- Risk analysis
- Policy writing
- Security awareness training
- Investigations
- System design

Cybersecurity is a team sport.

5. Who Works in Cybersecurity?

There are lots of different roles:

- **SOC Analyst** - Watches for threats 24/7
- **Penetration Tester** - Tries to hack systems (legally!)
- **Incident Responder** - Jumps in when something goes wrong
- **Security Engineer** - Builds secure systems
- **CISO (Chief Info Security Officer)** - Sets the big-picture strategy
- **Forensics Expert** - Investigates who did what

Some people code.
Some people write reports.
Some people train others.

There's a role for every type of brain.

6. You're Already Practicing Cybersecurity (Sort Of)

If you've ever:

- Set a strong password
- Used two-factor authentication (2FA)
- Reported a suspicious message
- Ignored a sketchy link

...congrats. You've already started.

Now it’s time to go deeper.

7. Why It Matters (More Than Ever)

- The more we live online, the more we need protection.
- Companies, hospitals, schools, and even governments can’t function without cybersecurity.
- Attacks are not rare. They happen every day.

Cybersecurity is no longer a niche. It’s a necessity.

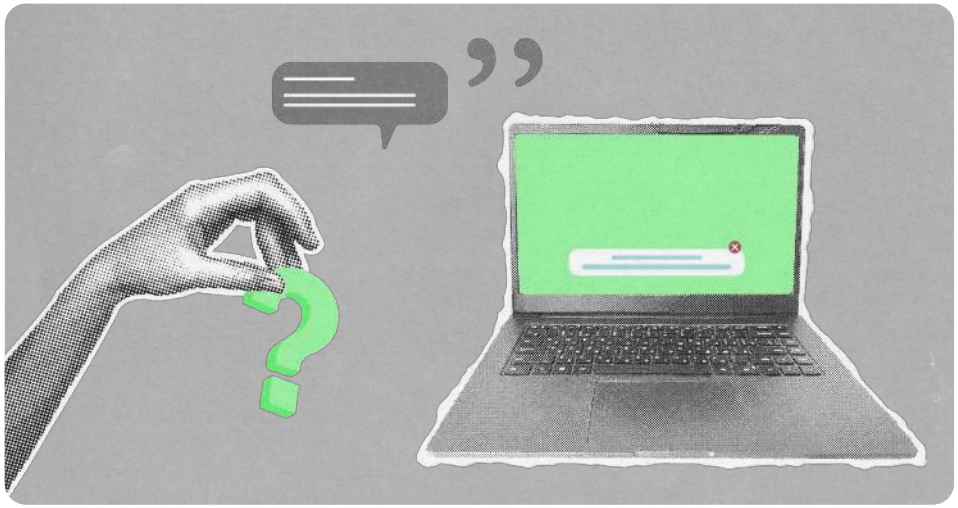
Summary

Cybersecurity is about **protecting people and systems in the digital world.**

It’s not one thing, it’s a universe of skills and roles.

And you don’t have to be an expert to start. You just need to be curious and alert.

CHAPTER 3: Who Are the Good and Bad Guys



In the world of cybersecurity, not all hackers wear hoodies.

Some protect you. Some steal from you. And some live in the grey.

1. Let’s Talk About Hackers

Say the word “hacker” and most people picture this:

> A guy in a hoodie, typing like crazy in a dark basement, with green code flying on the screen.

Yeah… no.

That's Hollywood. Here's reality:

> A hacker is anyone who understands how systems work, and how to break or improve them.

There are good hackers. Bad hackers. And ones who are a bit of both.

2. The Hat System

We sort hackers by "hat color" to show their intent:

- Black Hats: The Bad Guys

  They break into systems without permission.
  They steal, destroy, spy, scam, or hold data for ransom.

Why they hack:

- Money (stealing credit cards, selling data)
- Ego ("I did it because I could.")
- Revenge or chaos
- Government missions (aka **state-sponsored hackers**)

Example:

- Ransomware gangs locking up hospital systems until they're paid.
- A teen hacker selling Instagram logins.

- A foreign government spying on another country's elections.

- White Hats: The Good Guys

  They're cybersecurity professionals who help organizations stay safe.
  They test systems with permission, fix problems, teach users, and stop attacks.

What they do:

- Find vulnerabilities before bad guys do
- Respond to cyber incidents
- Build secure networks
- Train teams and raise awareness

They're the digital bodyguards.

- Gray Hats - The Blurry Middle

  They hack without permission, but not to hurt anyone.
  Sometimes they do it "for the greater good." But it's still risky.

Example:

- Someone finds a flaw in a government site, doesn't ask for permission, but reports it anyway.
- They might break a rule, but not with bad intentions.

Still… intent doesn't erase consequences. Gray hats walk a dangerous line.

3. The Criminal Types

Let's break down common black hats you might run into (or hear about):

- Script Kiddies
  - Use tools they don't fully understand
  - Download stuff online and "try it" on random targets
  - More annoying than dangerous, until they get lucky
- Organized Crime
  - Serious hackers-for-hire
  - Run like businesses
  - Use ransomware, steal data, and cash out via crypto
- Hacktivists
  - Mix of "hacker" and "activist"
  - Break into systems to protest or spread a political message
  - Example: Defacing websites or leaking documents
- State Actors
  - Work for governments

  - Target other countries, companies, or political groups
  - Highly trained, well-funded, and deadly serious

4. The Cyber Good Guys (White Hat Roles)

In the real world, white hats work as:

- **Penetration Testers (Pentesters)** - Paid to break in before the bad guys do.
- **SOC Analysts** - Watch systems 24/7 for suspicious activity.
- **Incident Responders** - The firefighters of cyber.
- **Forensics Experts** - Trace the who, what, when, and how of an attack.
- **Security Engineers** - Build defenses like firewalls, detection systems, and secure networks.

They are the ones keeping the lights on - and your data safe.

5. Why It's Not Just About "Right vs Wrong"

Sometimes, things get messy.

- A teenager hacks his school's system out of curiosity. Is he a black hat? Or just misguided?
- A whistleblower leaks government surveillance.

- Hero to some, criminal to others.

Cybersecurity isn't always clean-cut. But **your choices matter**. Intent matters. Permission matters.

6. So... What Kind of Hacker Do You Want to Be?

If you're curious... good.
If you like puzzles... great.
If you want to build, defend, and protect, welcome to the white hat path.

The world needs ethical hackers.

Not rebels without a cause, but warriors with purpose.

Summary

Hackers aren't one thing. They're people with skills, used for good, bad, or something in-between. The more you understand how hackers think, the better you can defend yourself... or join the defenders.

Next up: We'll explore how cyberattacks actually happen, step by step. Spoiler: It often starts with one click.

CHAPTER 4: How Cyberattacks Actually Happen

Hackers don't break in like in the movies.

They plan. They wait. They trick you. Let's break down how the attack really goes down.

1. One Click is All It Takes

Most cyberattacks don't start with fancy code. They start with you.

You clicking a link.
You opening a file.
You trusting the wrong thing.

The truth? Hackers don't "hack in." They "log in", because someone gave them access.

Let's see how that happens.

2. The Cyber Kill Chain (Simplified)

Here's the step-by-step strategy most attackers follow. Think of it like a playbook. It's called the Cyber Kill Chain - and no, it's not from Call of Duty.

You clicking a link.
You opening a file.
You trusting the wrong thing.

Step 1: Reconnaissance

Learn everything about the target.

- Google you
- Stalk your socials
- Check what software your school or company uses
- Scan your website
- Look for your email address or phone number

Why? So they can plan the perfect trick.

Step 2: Weaponization

- Create a fake website (looks just like your bank or school login)
- Build a PDF with hidden malware

- Write an email that sounds real, like it's from your boss, professor, or a company

Why? So the trap looks harmless.

Step 3: Delivery

Send the trap.

- Email
- Social media DMs
- Messaging apps
- Malicious ads or download links

Why? To get you to interact. That's the key.

Step 4: Exploitation

You open the file or click the link.

Now:

- Malware runs silently
- Your device starts sending info to the attacker
- You land on a fake page and enter your real password

Why? To gain control without you even noticing.

Step 5: Installation

Backdoors are set up.

- Malware installs itself permanently

- Attackers now have a secret way in
- You might still use your device like normal… but they're inside

Why? To stay inside undetected.

◆ Step 6: Command & Control

The attacker gives instructions remotely.

They might:

- Download more malware
- Use your device to attack others
- Steal passwords, files, or credit cards

Why? Your device becomes a tool.

◆ Step 7: Actions on Objectives

Time to finish the mission.

- Lock your files and demand ransom
- Steal your money or data
- Spy on your activity
- Wipe systems or damage them

Why? This is the goal. Everything else was preparation.

3. Real-World Example (Simplified)

Let's say you get this email:

"Hey! This is your school admin. There's a security update for your account. Please log in here: school-portal-login.site"

It looks right. You click. You type in your login.

Boom. You're in. But… So is the attacker.

They now:

- Log in as you
- Change your password
- Download private files
- Send phishing emails to your classmates using your name

And just like that, one click turned into a breach.

4. Bonus Trick: Pivoting

Once hackers get into one system, they look for ways to move deeper. This is called **pivoting**.

They hack your email → Then use it to access your cloud drive
They break into one school server → Then jump into the grading system
They hack one employee → Then reach the whole company

Cyberattacks grow like viruses. That's why early detection is key.

5. They Want You to Make It Easy

Most attackers don't want a challenge.

They look for:

- Weak passwords
- Old software with known flaws
- People who click without thinking
- Systems with no two-factor authentication

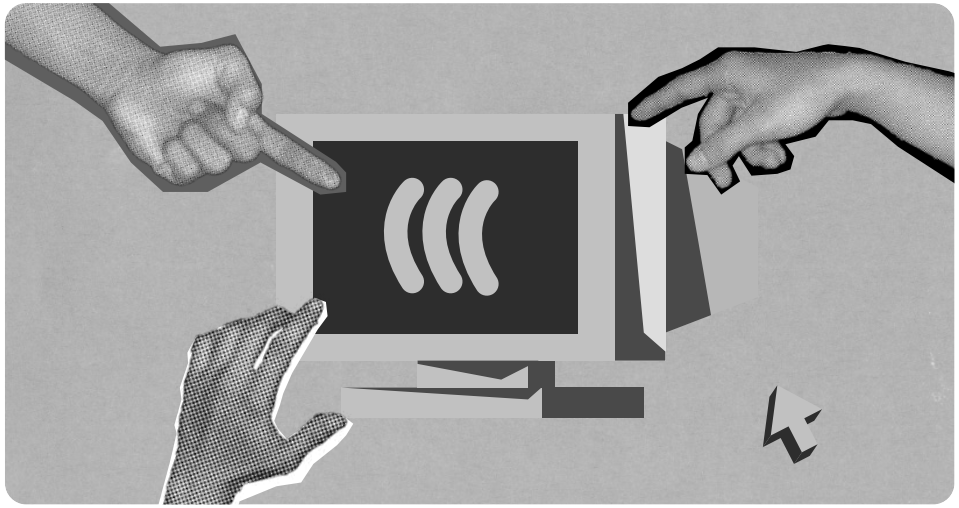
They want low effort, high reward. Don't give them that.

Summary: How Attacks Happen

1. They **watch** you.
2. They **trick** you.
3. They **get in.**
4. They **stay quiet.**
5. They **steal, break, or spy.**

Cyberattacks aren't magic. They're smart, sneaky, and patient.

CHAPTER 5: Types of Cyber Threats (That You'll Actually See)?



Forget the Hollywood hacks.

Let's talk about the real stuff that hits you: your phone, your accounts, your friends.

1. Phishing: The Fake Message Trap

What it is: A fake email, DM, or message trying to trick you into clicking a bad link, downloading malware, or giving away info.

How it looks:

- “Your package was delayed. Click here to track.”
- “Your school account will be suspended. Log in now.”
- “You’ve won a free iPhone!”

Why it works:

- It looks urgent.
- It looks legit.
- You click without thinking.

How to spot it:

- Check the sender’s email address - does it look weird?
- Hover over the link - does it lead to the real site?
- Bad grammar or unexpected pressure = red flag.

Rule: Don’t click links or download files unless you’re 100% sure.

2. Malware: The Silent Invader

What it is: Malicious software that infects your device.

How to spot it:

- **Spyware:** Watches you, records what you type.
- **Keyloggers:** Capture your passwords and messages.

- **Trojans:** Look like a normal file - but open the door to hackers.
- **Ransomware:** Locks your files and demands payment to unlock them.

How it gets in:

- Clicking shady links
- Downloading pirated games, movies, or cracked software
- Plugging in a random USB stick

Rule: If it’s free but shady… it’s probably a trap.

3. Password Attacks: Your Weakest Link

What it is: Hackers try to guess, steal, or crack your password.

Common methods:

- **Brute force:** Try thousands of combinations until they get in.
- **Credential stuffing**: Use passwords leaked from other sites you’ve used.
- **Phishing:** Trick you into typing your password into a fake page.

Signs you’ve been hit:

- You’re logged out and can’t get back in.

- You get password reset emails you didn't request.
- Your friends get weird messages from you.

Rule:

- Use strong, unique passwords.
- Turn on 2FA (two-factor authentication).
- Never reuse passwords.

4. Social Engineering: They Hack You, Not the Computer

What it is: Psychological tricks to make you give up information or access.

How it happens:

- We want to help.
- We don't want to look rude.
- We assume people are who they say they are.

Rule: Always double-check identities. Be polite but skeptical.

5. Public Wi-Fi Attacks: The Free Internet Trap

What it is: Open Wi-Fi in cafés, schools, airports can be fake, or insecure.

What can happen:

- Hackers can watch what you're doing.
- They can intercept passwords, messages, even payment info.
- They can pretend to be the Wi-Fi network you think is safe.

Rule:

- Avoid entering passwords or banking info on public Wi-Fi.
- Use a VPN if you have to connect.
- Ask: "Is this the official network?"

6. Account Hijacking: When You Lose Control

What it is: Someone takes over your email, Instagram, Snapchat, or bank account.

How they do it:

- Phishing
- Weak passwords
- Reused passwords from past breaches
- Sim-swapping (they take over your phone number)

Why it's dangerous:

- They can scam your followers.

- Leak your private messages.

Rule:

- Use 2FA.
- Monitor your logins.
- Act fast if something feels off.

7. Fake Apps, Downloads, and Tools: The Trojan Horse

What it is: Apps that pretend to be helpful, but are secretly malicious.

Common traps:

- "Download this app to see who viewed your profile!"
- Cracked versions of games or editing tools
- Fake antivirus or "cleaner" apps

They can:

- Steal data
- Spy on you
- Lock your device

Rule: Only download from official app stores. Check reviews. Avoid sketchy websites.

8. Disinformation: The Lies That Spread Like Fire

What it is: False or misleading content meant to trick, divide, or manipulate you.

Why it matters in cybersecurity:

- Hackers use fake news to cause chaos.
- Disinfo campaigns target elections, protests, or specific groups.
- You may unknowingly help spread it.

How to spot it:

- Check the source.
- Verify with a second (real) outlet.
- Be cautious with emotional headlines or viral posts.

Rule: Don't be a puppet. Think before you share.

Summary: The Threats You'll Actually See

You won't see lasers or explosions. You'll see:

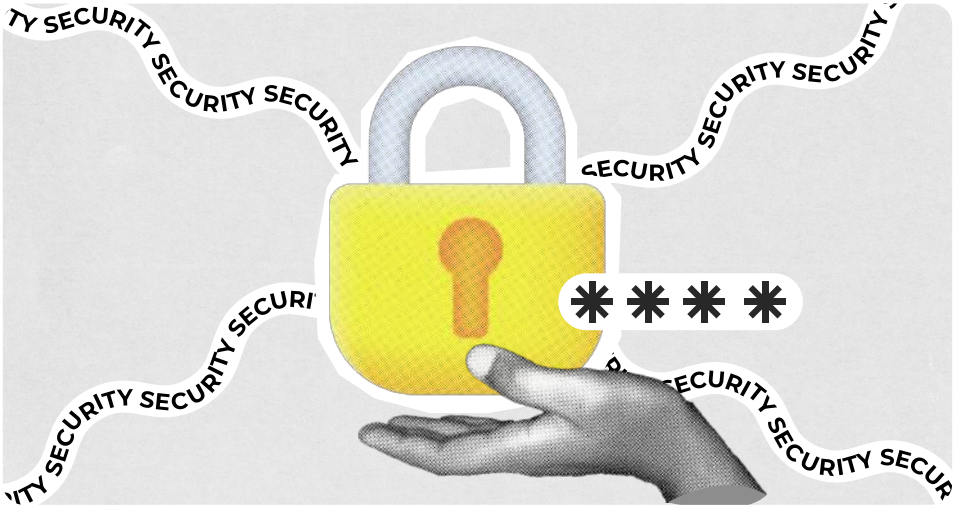
- A fake login page
- A suspicious email

- A “free” app
- A message that feels… off

But now, you’ll know what to look for.

Coming Up Next: We’ll zoom out and show where cybersecurity actually happens: your home, your school, your country. It’s not just your phone, it’s everywhere.

CHAPTER 6: Where Cybersecurity Happens



Cybersecurity isn’t just on your screen.

It’s in your school, your city, your country. It’s behind the scenes of everything you rely on.

1. It’s Bigger Than You Think

When people hear “cybersecurity,” they think:

- Hackers
- Phones
- Passwords

But it's much bigger.

Cybersecurity is the invisible shield protecting entire systems:

- Schools
- Hospitals
- Banks
- Airports
- Governments
- Even power plants and water systems

2. At Home: Your Personal Cyber Zone

Your home is a digital battlefield, whether you notice or not.

Devices at risk:

- Phones
- Laptops
- Smart TVs
- Wi-Fi routers
- Smart speakers (like Alexa or Google Home)

Common threats:

- Weak Wi-Fi passwords
- Fake apps
- Phishing messages
- Malware from pirated downloads

Good habits = good defense.
When your home is secure, you become harder to target.

Tip: Change your Wi-Fi password. Use unique passwords for all devices. Keep software updated.

3. At School: A Hacker's Playground

Schools use a ton of tech:

- Emails
- Online grade systems
- Student records
- Learning platforms (Google Classroom, Moodle)

Why schools are targeted:

- Easy access
- Tons of personal data
- Limited IT security in many places

What can go wrong:

- Grades changed
- Exams leaked
- Private data stolen

Tip: Don't share your login with friends. Report anything suspicious to your school IT team.

4. At Work: Even Part-Time Jobs

If you work at a coffee shop, bank, gym, or anywhere that handles:

- Credit cards
- Customer info
- Internal systems

...you're in the cyber game now.

What hackers want:

- Customer databases
- Card reader access
- Employee logins

Small businesses = big targets.
Why? They're often easier to hack.

Tip: Be careful what you access from work devices. Never open personal email or sketchy websites on them.

5. In Public: The Free Wi-Fi Trap

Anywhere that offers free Wi-Fi is a potential risk zone.

Think:

- Cafés
- Airports

- Libraries
- Hotels
- Shopping malls

Wha can happen:

- Hacker spy on your traffic
- Fake Wi-Fi networks trick you into connecting
- They can steal your logins in real time

Tip: Avoid logging into sensitive accounts on public Wi-Fi. Use a VPN if you must connect.

6. In Hospitals: Cyberattacks Can Kill

This is serious.

Hospitals are:

- Full of tech
- Connected to national systems
- Packed with critical data

Real danger:

- Ransomware attacks can shut down life-saving equipment
- Patient records can be stolen or tampered with
- Emergency rooms can be frozen mid-operation

This isn't just about data, it's about lives.

7. In Governments: The Cyber Cold War

Governments are always under attack.

What's targeted:

- National ID systems
- Border control
- Election infrastructure
- Classified info

Who's behind it:

- State-sponsored hackers from other countries
- Hacktivists
- Organized cybercrime groups

Why? Power, money, influence.

Kosovo, like every other country, is part of this cyber battlefield. That's why building local cyber talent with people like you is a national priority.

8. In Critical Infrastructure: Lights Out

Think about this:

- What if the power went out nationwide?
- What if water pumps stopped working?
- What if flights were grounded for days?

These systems rely on networks, and those networks can be attacked. **It's called Critical Infrastructure**, and defending it is top-level cybersecurity. Countries now treat cyber defense like national defense. This is where cybersecurity becomes a matter of national security.

9. Everywhere You Go

Cybersecurity isn't a place. It's a layer.

Every time you:

- Connect
- Log in
- Tap your card
- Share something
- Use smart tech

...you're part of a system that needs protection.

That's why cybersecurity professionals work across **every** sector: tech, law, finance, education, health, and more.

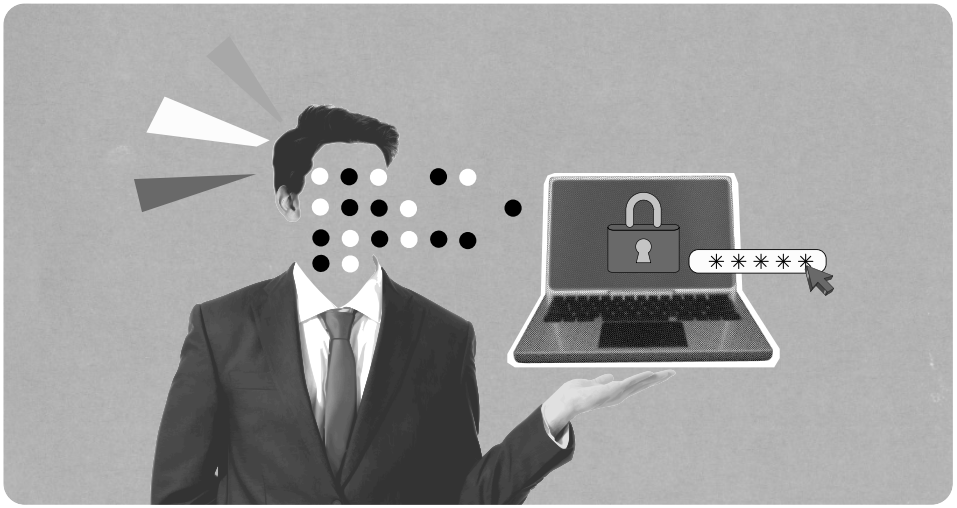
Summary: Cybersecurity Is Everywhere

- It's in your home, your school, your work.

- It protects businesses, hospitals, and entire countries.
- It's invisible, but vital.
- And now you know what's at stake.

Coming Up Next: Now let's look at what cybersecurity professionals actually do, and the different roles you could
play in this growing field.

CHAPTER 7: What Cybersecurity Professionals Actually Do



Not everyone in cybersecurity is a hacker.

Some watch. Some build. Some fix. Some lead. Let's meet the squad.

1. Cybersecurity Is a Team Sport

You've seen the threats. You've seen the battlefield.

Now meet the defenders: the people who keep systems, businesses, and even countries safe.

Cybersecurity isn't one job. It's a whole world of roles.

Different skills. Different brains. One mission. Let's break them down.

2. The Frontline Defenders

- SOC Analyst (Security Operations Center)

They're the security guards of the digital world.

What they do:

- Watch for alerts
- Spot unusual activity
- Respond to early signs of attacks

You'd like this if: You enjoy puzzles, spotting patterns, and working under pressure.

- Incident Responder

They jump in after something goes wrong.

What they do:

- Contain the breach
- Clean up the mess
- Find how it happened

Think of them as cyber firefighters.

You'd like this if: You stay calm in chaos, and love solving problems fast.

3. The Ethical Hackers

- Penetration Tester (Pentester)

Also called "ethical hackers." They try to break into systems, with permission.

What they do:

- Find weak spots before real attackers do
- Simulate attacks
- Write detailed reports about how they got in

You'd like this if: You love hacking games, CTFs (Capture the Flag), or thinking like a villain, for a good cause.

4. The Builders and Engineers

- Security Engineer

They build and maintain the tools that protect systems.

What they do:

- Configure firewalls
- Design secure networks
- Install security software
- Automate defenses

You'd like this if: You enjoy building things, writing scripts, and making systems work smoothly.

◆ Security Architect

They design entire security strategies.

What they do:

- Plan how to secure big systems
- Work with engineers and managers
- Think about both the tech and the business side

You'd like this if: You're a planner, a systems thinker, and like to design big-picture solutions.

5. The Investigators

◆ Digital Forensics Expert

They investigate after an incident, like digital detectives.

What they do:

- Examine logs and files
- Trace hacker activity
- Collect evidence for court cases

You'd like this if: You enjoy investigations, details, and tracking the truth.

◆ Threat Intelligence Analyst

They study hackers and threats around the world.

What they do:

- Track hacker groups
- Analyze global trends
- Warn companies about new attacks

You'd like this if: You're curious, strategic, and like to stay ahead of the game.

6. The Leaders and Communicators

◆ CISO (Chief Information Security Officer)

The boss of cybersecurity.

What they do:

- Lead the security team
- Make strategic decisions
- Manage budgets, risk, and people

You'd like this if: You want to lead, plan, and make an impact at the top level.

◆ Cybersecurity Consultant / Trainer

They work across different companies and help others understand cyber risks.

What they do:

- Write policies
- Train employees
- Advise teams on best practices

You'd like this if: You enjoy explaining things, working with people, and improving systems.

7. Wait: Do I Need to Be a Tech Genius?

Nope.

Some roles require technical skills (like coding or networking). Others need strong communication, analysis, or even law and psychology backgrounds.

In fact:

- Some of the best consultants used to be teachers.
- Some of the best analysts come from gaming or military backgrounds.
- Some amazing ethical hackers never went to university.

Cybersecurity is about mindset. Curious. Focused. Ethical. Problem-solver.

8. Where Do These Jobs Exist?

Everywhere.

- Tech companies
- Banks and telecoms
- Hospitals and schools
- Government and military

- NGOs and international organizations

And yes, **in Kosovo too.**

Summary: Find Your Role

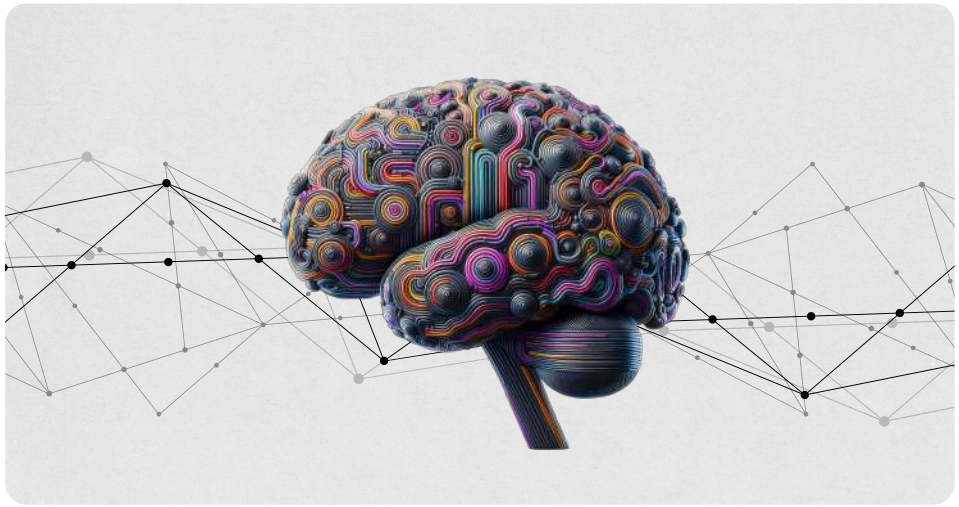
Here's the truth: You don't have to be a hacker to be in cybersecurity.

You can:

- Watch
- Build
- Investigate
- Advise
- Lead

Whatever your strength is, there's a role for you.

CHAPTER 8: Do You Need to Be a Genius or a Coder?



Short answer: No.

Long answer: Let's kill the myth.

1. The Myth That Stops People

When you hear "cybersecurity," what do you imagine?

- A guy in a hoodie typing 1,000 words per second?
- A genius who hacked NASA when they were 12?
- A programmer who speaks five coding languages fluently?

Here's the truth: **You don't need to be a genius. You don't need to be a programmer.**

What you do need:

- Curiosity
- Problem-solving
- A bit of patience
- Willingness to learn

That's it. The rest can be learned.

2. Many Roles Don't Require Coding

Let's be clear: There are cybersecurity jobs where coding helps (like penetration testing or malware analysis). But there are also jobs where you'll never touch a single line of code.

Examples:

- Security awareness trainer
- Policy advisor
- SOC analyst
- Risk assessor
- Digital forensics technician
- Threat intelligence analyst

Cybersecurity is part tech, part strategy, part communication, part psychology.

3. What Actually Matters More

- Critical Thinking

Can you break down a problem? Can you follow clues? You'd be surprised how many attacks get stopped just by asking smart questions.

- Curiosity

The best cyber professionals are curious. They dig. They test. They explore.

- Communication

You might know the risks, but can you explain them to others? Every org needs people who can teach, present, and guide.

- Ethics

You'll have access to systems, data, and trust. Ethics isn't optional; it's everything.

4. Real People, Real Backgrounds

Some of the best cybersecurity professionals:

- Never went to university
- Started in customer service or retail
- Came from military or police
- Switched from completely unrelated careers

You can enter this field from ANYWHERE.

5. What About Certifications?

Certs can be a great way to prove your skills, especially if you don't have a degree.

Beginner-friendly ones include:

- **CompTIA Security+** - broad intro to cybersecurity concepts
- **Cisco CyberOps** - good for SOC roles
- **Google Cybersecurity Certificate** - great for self-paced learners
- **TryHackMe / Hack The Box** - hands-on platforms to practice skills

You can start small. Some certs take just weeks to prepare for.

6. What About Age?

Too young? Too old? Doesn't matter.

- Teenagers can start with online labs and YouTube.
- 20-somethings can pivot from other fields.
- 30+? 40+? You bring maturity and life experience, huge advantages in leadership, consulting, or training.

There is no fixed path. There's just your path.

7. How to Get Started Without Coding

Here's a roadmap:

- Learn the basics from books, videos, or courses
- Practice safe habits (passwords, phishing awareness)
- Try free tools like Wireshark, VirusTotal, Shodan
- Watch YouTube breakdowns of real-world hacks
- Follow cybersecurity people on social media
- Explore free platforms like TryHackMe or Blue Team Labs
- Attend local workshops, tech meetups, or CTFs

You'll be amazed how far you can go without writing a single line of code.

8. Should You Learn Coding Eventually?

Maybe. Maybe not.

If you want to go deeper (like into hacking, scripting, or building tools), learning coding will help. But even then, you can learn it later. You don't need it to start. Most people in cyber learned things on the job, piece by piece. Don't let "not knowing code" stop you.

Summary: No, You Don't Need to Be a Genius or a Coder

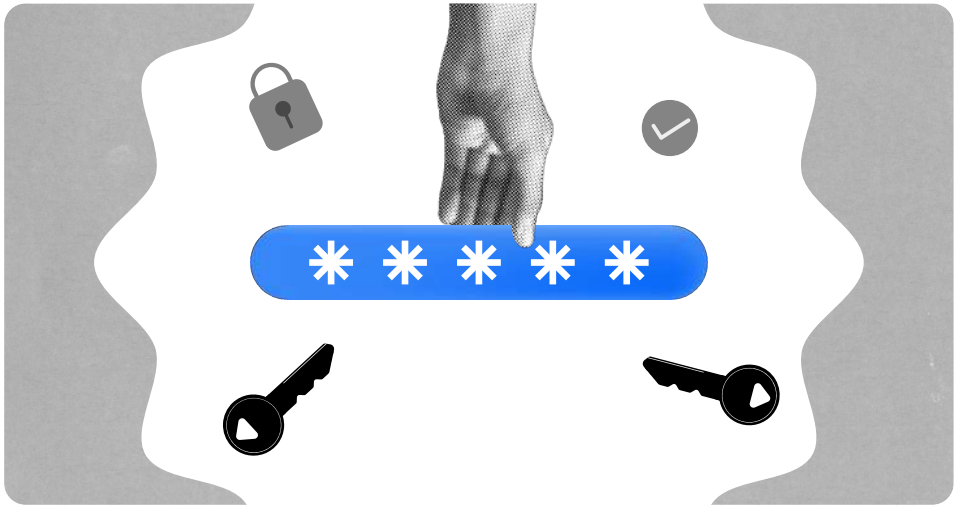
You need:

- Curiosity
- A sharp mind
- A strong sense of right and wrong
- A drive to learn and protect others

That's what makes a cybersecurity professional.

Coming Up Next: Let's talk about why this matters beyond money or tech: because cybersecurity gives you power, control, and freedom.

CHAPTER 9: Cybersecurity = Power, Control, and Freedom



This isn't just about tech.

It's about taking back control of your life, your identity, your future.

1. Cybersecurity Is Not Just Protection

When people hear "cybersecurity" they think: "It's about stopping hackers." That's part of it.

But at its core, cybersecurity is about something deeper:

- **Control**
- **Power**
- **Freedom**

Let's break that down.

2. CONTROL: You Own Your Digital Life

The internet is chaotic. Everyone wants your attention, your data, your time.

Hackers. Advertisers. Scammers. Apps. Algorithms.

Cybersecurity gives you the tools to take back control:

- You decide who sees your stuff.
- You know when something's shady.
- You set the rules for your own privacy.

Most people don't control their digital lives. They drift. Cybersecurity wakes you up. It turns you from a passive user into an active guardian.

3. POWER: You Understand What Others Don't

Let's be real: most people don't know what's going on online.

You will.

You will.

- You'll know how attacks happen.
- You'll know what data is being collected.
- You'll know how to protect yourself and others.
- You'll know how to break things ethically, and fix them better.

In a world full of digital threats, knowledge is power. **Cybersecurity turns you into someone others depend on**. You don't get lost. You lead.

4. FREEDOM: You Move Without Fear

Cyber attacks create fear.
Fear of being watched.
Fear of being hacked.
Fear of losing everything.

But when you know how to defend yourself, that fear disappears.

- You don't fall for scams.
- You don't panic over fake emails.
- You don't live paranoid, you live prepared.

That's real freedom. **Cybersecurity lets you live online with confidence.**

5. Bonus: You Can Help Others Too

What you learn isn't just for you.

You can help:

- Your parents avoid scams
- Your school protect student data
- Your workplace stay secure
- Your country grow its digital resilience

You're not just protecting yourself. You're part of a movement, of ethical, smart, capable people who make the internet safer. That's real influence. That's real leadership.

6. This Is Bigger Than a Job

Cybersecurity isn't just something you "do." It's something you are.

It's a way of thinking:

- Spot the hidden risk.
- Think like the attacker.
- Protect people.
- Be smarter than the threat.

Whether you become a pentester, a trainer, a consultant, or just someone who knows how to stay safe, you'll walk through the world sharper.

That's what this is really about.

Summary: This Is Your Superpower

Cybersecurity gives you:

- Control over your own data and life
- Power to understand and outsmart threats
- Freedom to explore the digital world without fear

And once you have it?

Nobody can take it from you.

Coming Up Next: So how do you actually get started? What can you do today to begin your journey? Let's talk about that.

CHAPTER 10: How to Start Thinking Like a Hacker (Ethically)

To beat a hacker, you have to think like one.

But to be great at cybersecurity, you have to do it **ethically.**

1. Good Hackers Think Differently

Hackers see the world in terms of:

- How things work
- Where they can break
- And how to fix them (or exploit them)

It's not about chaos. It's about curiosity.

The best defenders are creative. They see the holes others don't.

The mindset is this:

> "What if I press here? What if someone forgot to lock this part? What happens if I change this input?"

This is how hackers think. And now... so can you.

2. The Hacker Mindset = Curiosity + Skepticism

Let's break it down:

- How things work
- Where they can break
- And how to fix them (or exploit them)

◆ Curiosity

- You want to understand systems, not just use them.
- You explore settings, dig into how things work.
- You ask, "What happens if...?"

◆ Skepticism

- You don't trust links blindly.
- You question every login page.
- You notice weird patterns others ignore.

Together, that makes you powerful. You stop being just a "user." You become a hunter.

3. Start Small: Analyze What You Use Every Day

Try this exercise:

Look at your favorite app or website and ask:

- What happens when I click "Forgot password"?
- What if someone guessed my security question?
- Can I open this in multiple tabs and confuse it?
- Does the URL change when I log in? What does it show?

You're not breaking anything. You're learning. This is the beginning of **reconnaissance**: a key skill for ethical hackers.

4. Practice "Digital Awareness" Daily

Just like martial artists stay alert in the street, cyber professionals stay alert online.

Examples:

- You spot a fake link in a friend's message.
- You notice that a login page looks slightly off.
- You see a USB stick lying around, and don't plug it in.

These small decisions = the hacker mindset in action. You're training your eye.

5. Use the Same Tools as Real Hackers

Yes, seriously. Cybersecurity students use real tools that hackers use, but in labs, not on live targets.

You can try:

- **TryHackMe** (free gamified hacking challenges)
- **Shodan.io** (search engine for exposed devices)
- **VirusTotal** (scan links and files for malware)
- **Burp Suite** (for web testing; start with the free version)
- **Wireshark** (see what's happening on a network)

Important: Only test systems you own or have permission to use. That's what makes you ethical.

6. Learn to Break Things So You Can Fix Them

Let's be honest: breaking things is fun. But what makes you a white hat (the good kind of hacker) is your purpose.

You break things to:

- Understand them

- Improve them
- Help others stay safe

That's what companies pay for. That's what schools, hospitals, and governments need.

7. Hack the Right Way (Ethical Boundaries)

Yes:

- Join legal Capture The Flag (CTF) competitions
- Hack test environments like TryHackMe or Hack The Box
- Learn from ethical hacker YouTube channels
- Research vulnerabilities in safe, permission-based systems

No:

- Don't test websites or apps without permission
- Don't access accounts that aren't yours
- Don't share private data or "leaks" you come across
- Don't think "just looking" means no harm

Being ethical isn't about rules, it's about responsibility.

8. Think Like a Hacker. Act Like a Protector.

A great ethical hacker doesn't just know the tricks.

They know:

- How real attackers operate
- How systems can fail
- How people get fooled

But they also:

- Know when to stop
- Respect boundaries
- Work for the good side

It's like being a lockpicker who helps improve door designs.

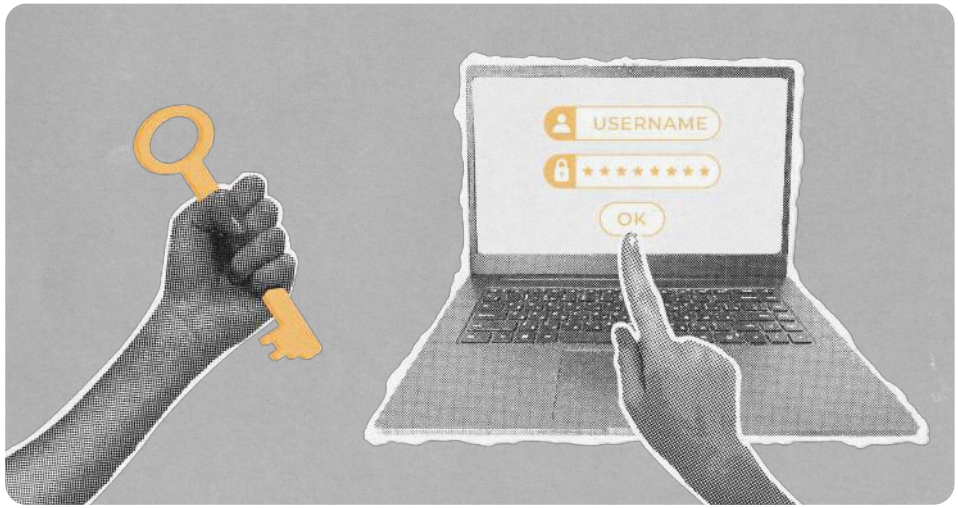
Summary: Train Your Mind Like a Hacker

To start thinking like a hacker:

- Stay curious
- Question everything
- Explore how things work
- Practice safely
- And always act ethically

Coming Up Next : Before we wrap up, let's talk about basic cyber hygiene, small habits that protect you right now, even before your career begins.

CHAPTER 11: Cyber Hygiene You Can Do Today



You don't need to be an expert to stay safe online.

A few simple habits go a long way Let's make them part of your daily life..

1. What Is Cyber Hygiene?

Cyber hygiene is just like personal hygiene.

- You brush your teeth daily to prevent cavities.
- You shower so you don't smell like a gym bag.

- You cut your nails, clean your ears, and wash your hands.

But they also:

Cyber hygiene = small digital habits that prevent bigger problems. You don't need advanced tools. Just consistency and awareness.

2. Use Strong, Unique Passwords

If you reuse the same password everywhere, it's like using one key for your house, your car, your locker, and your bike. If someone steals it once, they own your entire life.

How to fix it:

- Use different passwords for each site.
- Make them long (at least 12 characters).
- Avoid names, dates, or easy guesses.

Pro tip: Use a password manager (like Bitwarden or 1Password).

It remembers everything so you don't have to.

3. Turn On Two-Factor Authentication (2FA)

This is one of the most powerful defenses you can use.

How it works:

- You log in with your password.
- Then, you confirm it's really you with a code from your phone or app.

Even if someone steals your password, they still can't get in.

Where to use it:

- Email
- Social media
- Banking
- Anything important

Turn it on. Today.

4. Don't Click Random Links

If something feels off, it probably is.

Examples of sketchy links:

- "Click here to claim your prize!"
- "Your account is suspended, log in now!"
- Shortened links (bit.ly, tinyurl) from strangers

What to do instead:

- Go to the site directly (don't click; type it)
- Hover over the link to preview where it really goes

- Ask: Would this company really contact me this way?

If unsure, don't click. Ever.

5. Keep Your Software Updated

Yes, updates are annoying. Yes, they matter.
Most hackers use **old vulnerabilities**, things that updates already fixed.

What to update:

- Your phone
- Your apps
- Your laptop
- Your browser
- Your router (yes, even that)

Make it a habit. Updates = patches = protection.

6. Avoid Public Wi-Fi (Unless You Know What You're Doing)

Public Wi-Fi is like shouting your passwords across a crowded room.

Safer options:

- Use your mobile data if possible.
- If you have to use public Wi-Fi:

- Don't log into sensitive accounts.
- Use a VPN (virtual private network) to encrypt your connection.

7. Think Before You Share

That funny post, cute selfie, or angry tweet might be harmless.

Or... it might:

- Give away your location
- Expose personal info
- Be used to impersonate you later

Ask yourself:

- Would I be okay if this got screenshotted and sent to strangers?
- Am I giving away more than I realize?

Digital footprints are permanent. Walk wisely.

8. Use Antivirus (Even a Free One)

Antivirus isn't perfect. But it helps catch basic malware before it spreads.

Good free options:

- Windows Defender (built-in on Windows)

- Bitdefender Free
- Avast or AVG (with caution; avoid bloatware)

Just don't rely on it as your only defense. Think of it like wearing a seatbelt—not crashing is still better.

9. Backup Your Stuff

If ransomware hits, or your laptop dies, or your files get wiped… You'll wish you had a backup.

What to back up:

- Photos
- School projects
- Documents
- Anything you care about

Where to back it up:

- An external drive
- A cloud service (Google Drive, Dropbox, iCloud)

Do it regularly. Your future self will thank you.

10. Talk About It

Cyber hygiene gets stronger when it's shared.

Help your:

- Parents update their devices

- Siblings avoid sketchy downloads
- Friends stop reusing "123456" as a password

You don't need to preach. Just be the smart one in the group. Security spreads.

Summary: Small Habits, Big Protection

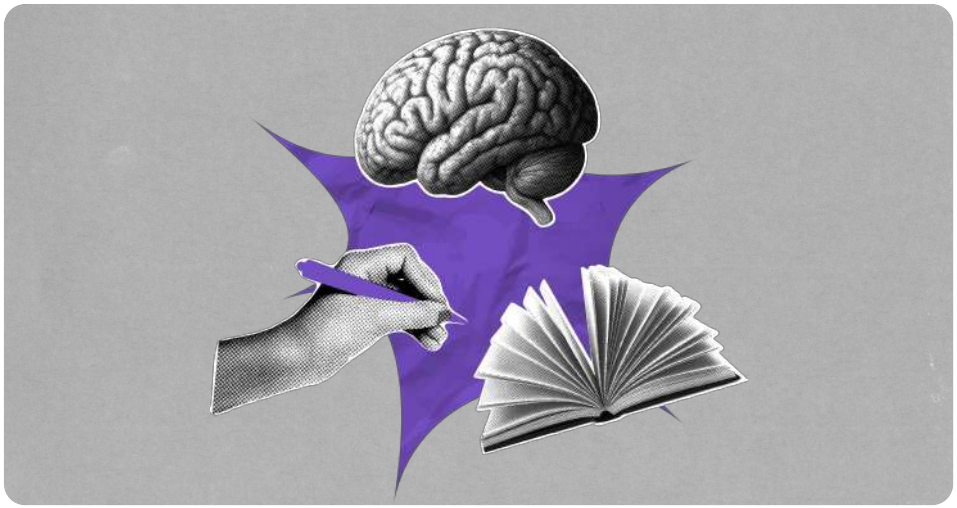
Start here. Start now.

- Unique passwords
- 2FA everywhere
- Don't click shady links
- Update everything
- Backup your stuff
- Stay sharp and aware

You don't need to do it all at once. But the sooner you start, the safer you'll be.

Coming Up Next: Let's wrap up this journey with your next steps: how to keep learning, how to explore cyber careers in Kosovo, and how to take this seriously, without losing the fun.

How to Get an Education in Cybersecurity in North Macedonia



CHAPTER 1: Why This Matters

Chapter Goal: To show you that if you want to enter the cyber world, North Macedonia already offers educational pathways—both academic and professional—that can take you there. You do not have to go abroad to start your cyber journey In North Macedonia, there are universities, higher education institutions, and training centers that offer programs related to cybersecurity,

ICT, and digital security. You have options:

- a university degree
- practical training
- or a combination of both

CHAPTER 2: Universities – the Academic Path

In North Macedonia, there is still no standalone academic degree officially titled "Cybersecurity," but several universities offer study programs and courses that provide a strong foundation for a career in the cyber sector. These programs cover knowledge areas such as:

- computer science
- informatics and information security
- networks and telecommunications
- digital infrastructure and systems

Students are often involved in:

- competitions and CTF activities
- research and practical projects
- conferences and workshops

Elective courses related to cyber topics

◆ Ss. Cyril and Methodius University in Skopje

Faculty of Computer Science and Engineering (FINKI) – Skopje

FINKI is the faculty with the strongest technical foundation in the country and offers the most direct preparation for a technical cybersecurity career. Cybersecurity is studied through courses and topics such as:

- computer network security
- information security
- cryptography
- system and network administration

The faculty has an active student community, including:

- CTF competitions
- hackathons
- research groups

➡️ Most suitable for students who want deep technical knowledge, programming and networking skills, and a later entry into SOC, penetration testing, or engineering roles.

◆ St. Clement of Ohrid University – Bitola

Faculty of Information and Communication Technologies (FICT) – Bitola

FICT offers studies in information and communication technologies with a solid ICT foundation. Programs and fields include:

- information and communication technologies
- computer science
- internet and software technologies

The focus is on:

- computer networks and systems
- information and digital security
- practical work and laboratory exercises

FICT delivers:

- undergraduate studies
- postgraduate (master's) studies
- doctoral studies

Although the programs are not formally labeled as "Cybersecurity," some of the courses and research cover information protection, network security, and ICT-related risks.

➡️ Suitable for students who want a combination of ICT and hands-on practice, with the possibility of cyber specialization at the master's level.

Faculty of Security – Skopje

The Faculty of Security is a public faculty focused on security sciences rather than classical technical IT education.

Cyber-related topics are studied within:

- information security
- cybercrime and digital threats
- critical infrastructure protection
- national and international security

The focus is on:

- cyber risk analysis
- legal and institutional aspects
- policies, strategies, and security governance

➡️ Most suitable for students interested in cybersecurity from the perspective of policy, law, criminology, and institutional security, rather than technical hacking.

South East European University (SEEU) – Tetovo

SEEU offers study programs in computer science and ICT, with a strong emphasis on applied knowledge.

Programs in:

- computer science
- information and communication technologies

Focus areas include:

- practical skills
- digital security
- alignment with European standards

SEEU frequently collaborates on international and European projects, enabling students to gain:

- exposure to real-life cases
- experience working in a multicultural environment

➡️ A good choice for students who want a practical IT foundation with a European perspective.

Goce Delchev University – Štip

Faculty of Informatics – UGD Štip

The Faculty of Informatics in Štip is the main technical ICT faculty in the eastern region of the country. It offers programs in:

- computer science
- computer engineering and technologies
- information technologies

The focus is on:

- practical ICT skills
- software and systems development

- technical courses that form the foundation for cybersecurity (networks, systems, application logic)

Within the study programs, topics include:

- information security
- digital infrastructure
- data protection

➡️ Suitable for students who want a solid technical IT foundation as a basis for a future cybersecurity career.

◆ Military Academy “General Mihajlo Apostolski” / MAGMA

UGD Štip / Skopje

The Military Academy does not offer a classical civilian degree titled “Cybersecurity,” but cybersecurity is a key component of education and training in the defense context.

Within officer studies and specialized programs, the following are covered:

- information systems and communications
- information security
- defense ICT systems
- protection of C2 / C3I systems

Through MAGMA, the Academy delivers:

- trainings and workshops
- research and analyses
- tabletop exercises (TTX)
- cooperation with state and international partners

➡️ Most suitable for those interested in cybersecurity in a defense, strategic, and state-security context, rather than commercial IT.

Key Message of the Academic Path

In North Macedonia:

- the academic path provides the foundation
- cybersecurity specialization comes through elective courses, internships, projects, and additional trainings

➡️ **University is a starting point, not a final destination**

CHAPTER 3: Beyond Universities – Professional Schools and Trainings

Not everyone has to spend 3–4 years at a university. In North Macedonia, there are practical and faster pathways into the cyber field

- SEMOS Education

Practical IT and cybersecurity trainings. Focus areas:

- cybersecurity and networks
- system administration
- cloud technologies and data protection

Offers internationally recognized programs and certifications (Microsoft, EC-Council, Cisco, CompTIA, and others). With long-standing links to the IT industry and experienced professional instructors.

➡️ A good choice for practical skills, certification, and fast entry into the IT/cyber sector.

- Seavus Education & Development Center (SEDC Academy)

Practical IT and cybersecurity trainings. Focus on:

- system security
- networks
- cloud and data protection

Strong links with the IT industry.

- Brainster

Intensive programs (lasting several months). Topics related to:

- IT security
- QA and systems analysis
- digital risks

Designed for rapid employability.

- Brainster

Intensive programs (lasting several months). Topics related to:

- IT security
- QA and systems analysis
- digital risks

Designed for rapid employability.

- Creative Hub

IT and digital programs. Introductory trainings in

- technical literacy

- digital security

A good starting point for a career switch.

◆ Ministry of Defense of the Republic of North Macedonia /Army of the Republic of North Macedonia

Specialized state-led training. Topics include:

- cyber defense
- incident management
- protection of critical infrastructure

Focus on national security.

CHAPTER 4: Online Platforms and Labs (Used Also in North Macedonia)

These platforms are used by students, professionals, and institutions:

- TryHackMe
- Hack The Box
- Blue Team Labs
- Coursera / edX (including courses with European and NATO partner institutions)

➡️ Excellent for hands-on practice without risk, alongside studies or work.

CHAPTER 5: How to Choose Your Path

Ask yourself:

- Do I want a degree (3–4 years, academic foundation)?
- Do I want fast, practical skills (a few months)?
- Or a combination: university + certifications?

The good news: North Macedonia offers all three options.

Summary: Your Options in North Macedonia

You do not have to leave the country to study cybersecurity.

Universities:

- Ss. Cyril and Methodius University (UKIM) / FINKI

- St. Clement of Ohrid University (UKLO) – FICT and Faculty of Security
- Goce Delchev University – Štip / MAGMA
- South East European University (SEEU)

Professional schools and trainings:

- SEMOS Education
- SEDC
- Brainster
- Creative Hub

State and institutional centers:

- Ministry of Defense
- Army of the Republic of North Macedonia
- MKD-CIRT
- Ministry of Interior – Cybercrime and Internet Fraud Unit

Online platforms:

- TryHackMe
- Hack The Box
- Blue Team Labs

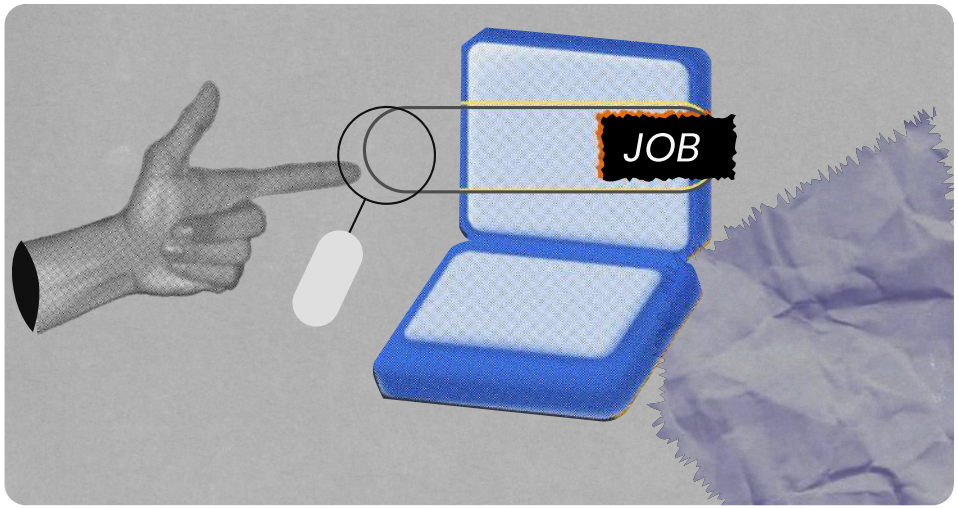
Your choice depends on:

- how deep you want to go

- how fast you want to get there
- and which role you see yourself in

But one thing is clear: the opportunities are already here – in North Macedonia.

Where to Work in Cybersecurity in North Macedonia



CHAPTER 1: Why Jobs in Cybersecurity Are Everywhere

Chapter Goal: To show you that cybersecurity is not "one profession," but hundreds of different roles spread across the public sector, banks, telecommunications, IT companies, NGOs, and even hospitals, airports, and energy systems.

Cybersecurity in North Macedonia is growing rapidly. Every institution or company that uses:

- computers
- networks
- data

...must have protection. This means that jobs are opening:

- in public institutions
- in banks and financial institutions
- in the telecom and IT sector
- in critical infrastructure

If you have the skills, the demand already exists.

CHAPTER 2: Careers in the Public Sector

Working in the public sector means:

- protecting the state, institutions, and citizens.

1. **Ministry of Digital Transformation**

The leading institution for digitalization and cybersecurity policies.

Responsible for:

- digital public services
- coordination of cybersecurity
- alignment with EU and NIS directive

Job roles include:

- cybersecurity policy experts
- digital risk analysts
- national strategy coordinators

If you want, I can continue translating the next institutions and roles in the public sector (CERTs, ministries, regulators, police, etc.) or help structure this as a career guide for students and young professionals.

2. MARNet (MARNET)

The national academic and research network. Host of the national CERT for the academic sector. Responsible for monitoring, detecting, and responding to cyber incidents in the education sector.

Job roles:

- SOC analysts
- network engineers
- incident responders

➡️ **A good entry point for young professionals.**

3. Agency for Electronic Communications (AEC)

The national telecommunications regulator. Involved in:

- cyber incidents in telecommunications
- coordination with telecom operators
- alignment with European standards

Job roles:

- cyber analysts
- regulatory and security experts
- technical inspectors

4. National and Sectoral CSIRT Teams

MKD-CIRT (National Computer Incident Response Team)

The national institution responsible for the prevention, detection, and response to cyber incidents in North Macedonia.

Coordinates responses to:

- cyberattacks
- malware
- phishing and other digital threats

Provides:

- alerts and notifications
- technical support and guidance

- cooperation with institutions, operators, and international CERT/CSIRT networks

➡️ A key role in national cybersecurity and an important hub for professionals interested in incident response, coordination, and protection of critical systems.

In North Macedonia, in line with European practices, critical sectors develop their own CSIRT or cyber-security functions, especially in:

- energy
- healthcare
- transport
- telecommunications

Job roles include:

- sectoral cyber analysts
- system security engineers
- incident handlers

5. Critical Public Operators

Every operator of essential services must have a designated cybersecurity officer or team, including:

- electricity distribution
- water supply
- public transport
- airports

Job roles include:

- security engineers
- cyber resilience officers
- IT security coordinators

CHAPTER 3: Careers in the Financial Sector

Banks are among the most frequent targets of cyberattacks. That is why they are also among the largest employers of cybersecurity professionals.

National Bank of the Republic of North Macedonia (NBRNM)

Sets the regulatory framework for cybersecurity in the financial sector. Supervises banks and financial institutions.

Job roles:

- cyber risk experts
- compliance analysts
- IT supervisory specialists

Commercial Banks (Examples in North Macedonia)

- Komercijalna Banka
- Stopanska Banka

- Halkbank
- NLB Banka
- ProCredit Bank

Typical roles:

- CISO (Chief Information Security Officer)
- IT Security Manager
- SOC Analyst
- Digital Forensics Officer
- Risk & Compliance Specialist

Microfinance Institutions and FinTech

Even smaller institutions are highly digitalized:

- savings institutions
- fintech startups
- mobile and online banking platforms

Job roles:

- cybersecurity officers
- data protection experts
- cloud and application security specialists

Summary: Where the Jobs Are in North Macedonia

Cybersecurity in North Macedonia is not “the future.” It is the present. Job opportunities exist in:

- the public sector
- banking and finance
- telecommunications
- critical infrastructure
- the IT and startup ecosystem

Whether you:

- want to protect the state
- want a stable career in banking
- or want a dynamic role in the IT sector

➡️ Cybersecurity has a place for you.

Below is the same structure and logic, fully adapted to North Macedonia, with real companies, consulting firms, and NGOs. The text is prepared to be inserted directly as Chapters 4 and 5 in the guide.

CHAPTER 4: Private Sector and Consulting

The private sector is the most diverse field for a career in cybersecurity. From large telecom operators to startups and consulting firms—every company that works with sensitive data needs cybersecurity experts.

Telecommunications Companies

Telecom operators manage massive networks and millions of users, making them part of critical infrastructure.

- aA1 Macedonia
- Macedonian Telecom

Typical roles:

- Network Security Engineer
- SOC Analyst
- Incident Responder
- Penetration Tester (internal or external)

➡️ An excellent environment for learning network security, monitoring, and incident response.

Cybersecurity and IT Consulting Companies

These companies work with banks, public institutions,

and international clients.

- **Nextsense** – IT and cyber consulting, security solutions
- **Netcetera** – software and security for the financial sector
- **Endava** – cloud, DevSecOps, application security
- **Seavus** – enterprise systems, QA, and security
- **CodeWell** – IT and security services
- **Inscale** – cloud, infrastructure, and security
- **TESSA SEC DOO** – cybersecurity, penetration testing, incident response, and consulting
- **Tessa Tech (Tessa Group)** – IT services and security infrastructure solutions

Typical roles:

- Cybersecurity Consultant
- Penetration Tester
- Risk & Compliance Specialist
- Cloud Security Engineer
- Junior SOC Analyst (a common entry-level position)

Software and Technology Companies

In tech companies, cybersecurity often overlaps with development, QA, and cloud.

- ITgma
- Semos Cloud

- **Synami**
- **Quantix**
- **Pabau**

Roles that often require cybersecurity skills:

- Application Security Engineer
- DevSecOps Engineer
- QA Security Tester
- Cloud Security Specialist

➡️ If you like coding + security, this is an ideal sector.

Why This Matters

In the private sector:

- cybersecurity is directly linked to business outcomes
- salaries and career progression are often faster
- you can work for international clients while based in North Macedonia

CHAPTER 5: NGOs and Civil Society

Not all cybersecurity careers are corporate. In North Macedonia, NGOs and civil society organizations actively work on cybersecurity, digital rights, privacy, and research.

Organizations and Initiatives

- **IMPETUS – Center for Internet, Development and Good Governance** – cybersecurity, digital rights, public policies, education
- **Women4Cyber Macedonia** – part of the European network for empowering women in cybersecurity
- **IGF MKD** – digital rights, privacy, media literacy

Typical Roles in the NGO Sector

- Cybersecurity Trainer / Educator
- Policy & Research Analyst
- Digital Rights Advocate
- Campaign & Awareness Specialist
- Project Coordinator (cyber & digital projects)

➡️ **These roles are ideal if you want:**

- social impact
- work with young people, institutions, and media
- a combination of cybersecurity knowledge and public policy

Summary: Private Sector and NGOs in North Macedonia

In North Macedonia, cybersecurity careers exist in:

- telecommunications
- IT and consulting companies
- software and cloud firms
- NGOs and research centers

Whether you want:

- a corporate career
- startup dynamics
- or work with a social mission

➡️ Cybersecurity has space for you too.

CHAPTER 6: Critical Infrastructure

Critical infrastructure = the backbone of the state.
Its protection is not just an IT issue, but a matter of national security. Everything that, if it stops, brings the state to a halt belongs here.

Energy Sector

- **AD ESM** – electricity generation
- **MEPSO** – electricity transmission
- **EVN Macedonia** – distribution and supply

➡️ **High risk:** SCADA/ICS systems, remote control, industrial networks.

Transport

- **Skopje International Airport**
- **Public Enterprise Railways of the Republic of North Macedonia**
- **Public Enterprise for State Ro**

➡️ **Focus:** security of traffic systems, logistics, navigation, and control.

Healthcare

- **University Clinics – Skopje**

- Institute of Public Health
- Private hospitals and clinics (information systems, patient data)

➡️ Risks: ransomware, theft of medical data, service disruption.

Water and Sewage Systems

- **Public Utility "Water Supply and Sewerage" – Skopje**
- **Regional and municipal public enterprises**
- **Water supply and wastewater systems**

➡️ Critical: industrial control systems and remote operations.

Digital Infrastructure and Telecommunications

- **Macedonian Telecom**
- **A1 Macedonia**

➡️ The backbone of the internet, mobile communications, and digital services.

Public Administration

- Ministries
- Municipalities
- Assembly of the Republic of North Macedonia

➡️ Targets of attacks: data, electoral processes, and

citizen services.

Food Production and Distribution

- Large food production facilities
- Cold chains, warehouses, and distribution centers

➡️ Risks: manipulation of logistics, disruption of supply chains

Typical Cyber Roles in Critical Infrastructure

Jobs in these sectors most often involve:

- protection of SCADA / ICS systems
- network and anomaly monitoring
- incident response in vital services
- risk management and resilience
- coordination with state institutions

➡️ Less "hacking," more "stability, security, and responsibility."

CHAPTER 7: Your Cyber Career Map (North Macedonia)

Here is the big picture—where you can work:

- **Government and institutions** – defending the state
- **Banks and finance** – protecting money and trust

- **Private companies** – building and securing technology
- **NGOs and research centers** – educating, analyzing, influencing
- **Critical infrastructure** – keeping society functioning

If you want, I can also:

- turn this into a **visual career map,**
- adapt it for **high-school students, or**
- align roles with **NICE / EU cyber skills frameworks**

Key Message

Cybersecurity is not a single pathway. It is an ecosystem.

And North Macedonia is already building that ecosystem—across institutions, companies, academia, and critical sectors.

➡️ The question is not whether there is a place for you

➡️ The question is where you want to be within it.

📊 CYBER CAREER MAP

Sector → Roles → Required Skills

🧭 How to use this table

- Choose the sector that attracts you
- Look at the roles that feel natural to you
- Focus on the skills — that is your career roadmap

Sector	Typical Roles	Required Skills
🏛️ **Public Sector:** Government Ministries, regulators, MKD-CIRT, defense	• Cyber Analyst • Incident Responder • CSIRT Officer • Policy & Strategy Expert	• Cyber Incident Analysis • Risk Management • Institutional Processes • Report and Policy Writing • Coordination and Communication
🏦 Financial Sector Banks, fintech, insurance	• SOC Analyst • IT Security Manager • Digital Forensics Officer • Risk & Compliance Specialist • CISO (Chief Information Security Officer)	• Log Analysis and Monitoring • Identity & Access • Management (IAM) • Regulations and Compliance • Incident Response • Working Under Pressure
🏢 Private IT / Cyber Consulting IT companies, MSSPs, startups	• Cybersecurity • Consultant • Penetration Tester • Cloud Security Engineer • DevSecOps Engineer • Junior SOC Analyst	• Networks and Systems • Cloud Technologies • Application Security • Security Tools (SIEM, Wireshark, Burp Suite) • Problem-Solving

Sector	Typical Roles	Required Skills
🛰️ Critical Infrastructure Energy, transport, healthcare, water, telecom	• ICS/SCADA Security Engineer • Network Monitoring Analyst • Incident Handler (Vital Services) • Cyber Resilience Officer	• Industrial Systems (ICS/SCADA) • Network Security • Risk Management • Crisis Management • Institutional Coordination
🧠 NGOs / Research / Think Tanks	• Cybersecurity Trainer • Policy Researcher • Digital Rights Advocate • Awareness Campaign Designer	• Cybersecurity Fundamentals • Research and Analysis • Public Communication • Education and Presentations • Advocacy and Writing
🎓 Academia / Education	• Researcher / Teaching • Assistant University • LecturerCyber Trainer	• Theoretical Foundations • Research Methodologies • Academic Writing • Mentoring and Training