

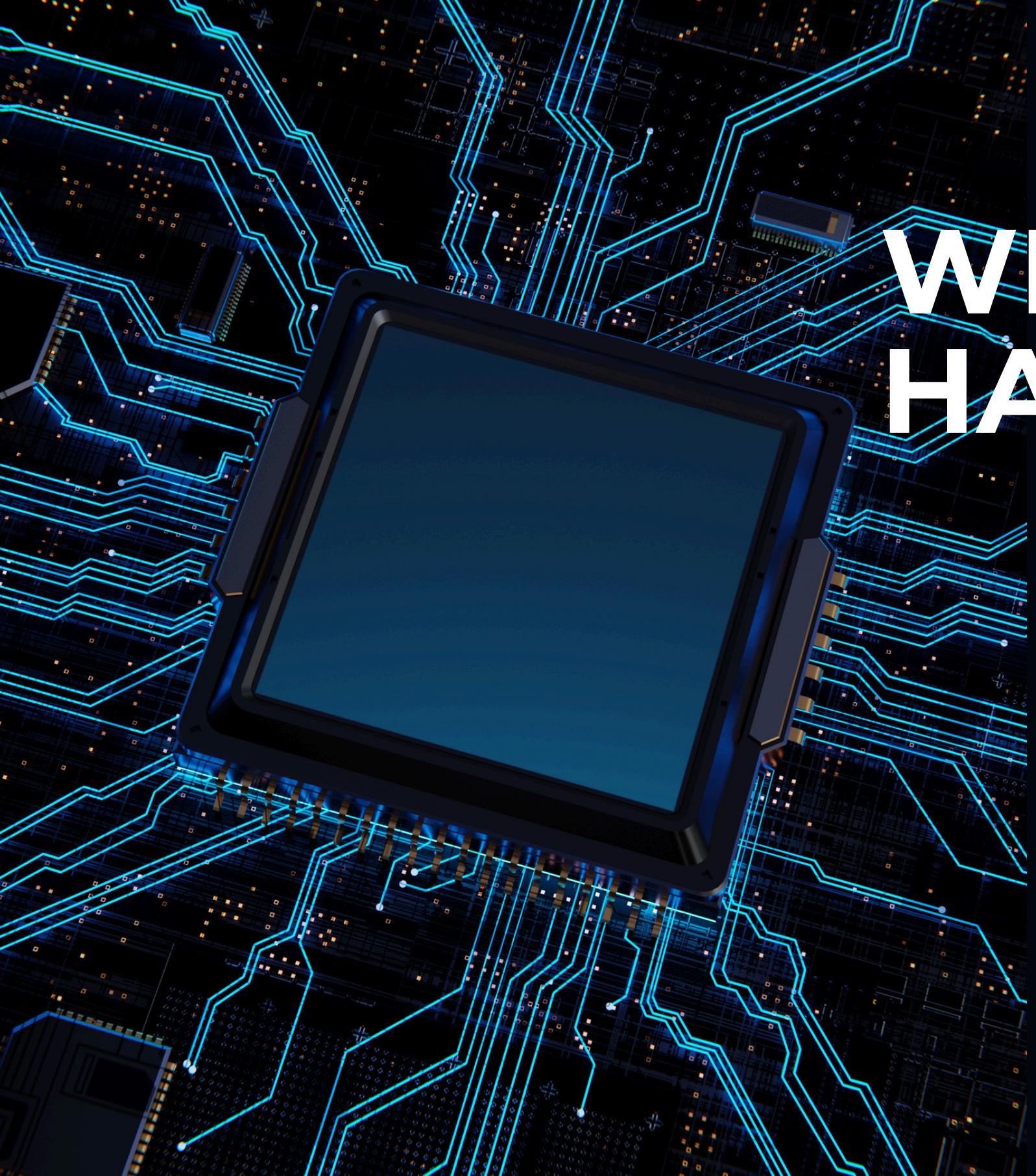
LESSON 6

Ethical Hacking & Careers

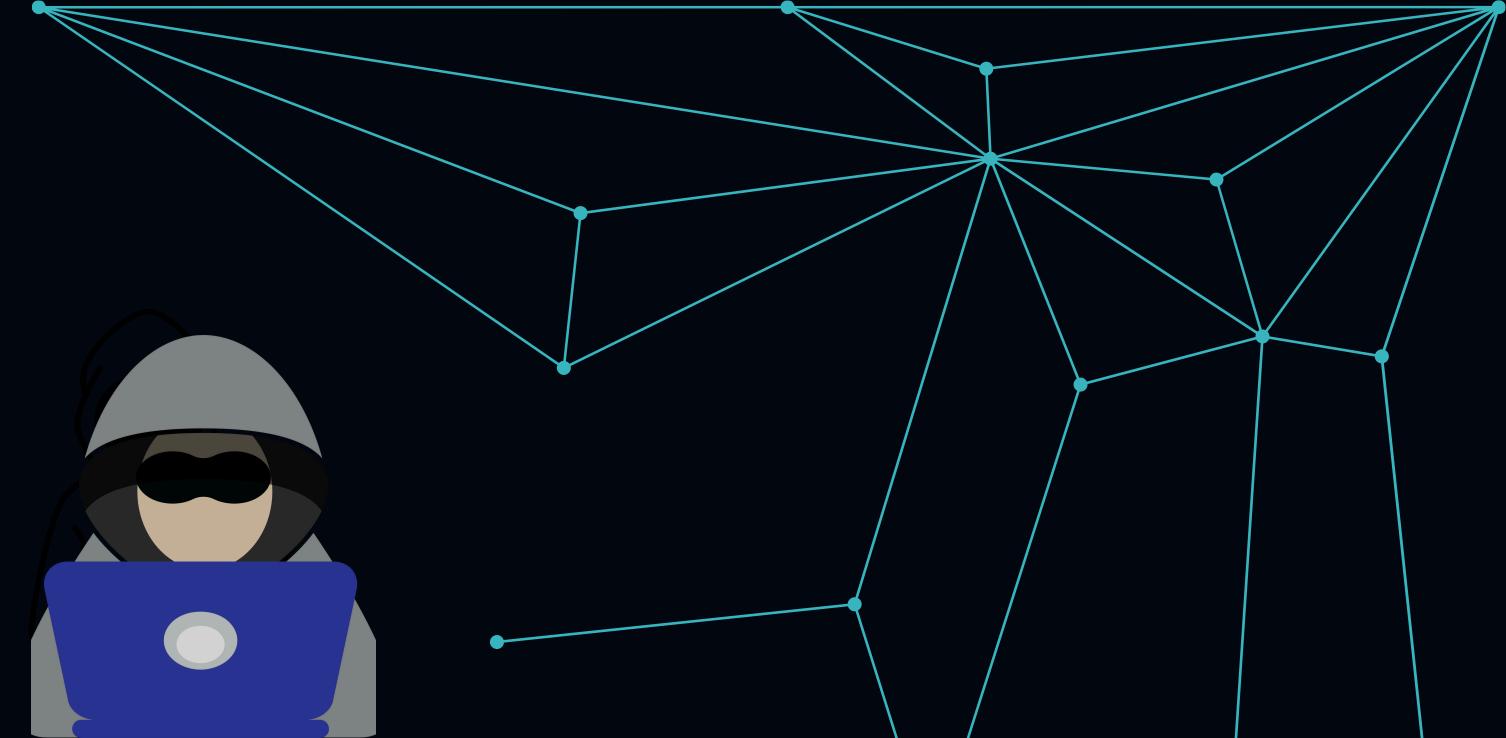
Objective:

Learn about ethical hackers, types of
hackers, bug bounties, and cool
cybersecurity careers!





WHO IS A HACKER?



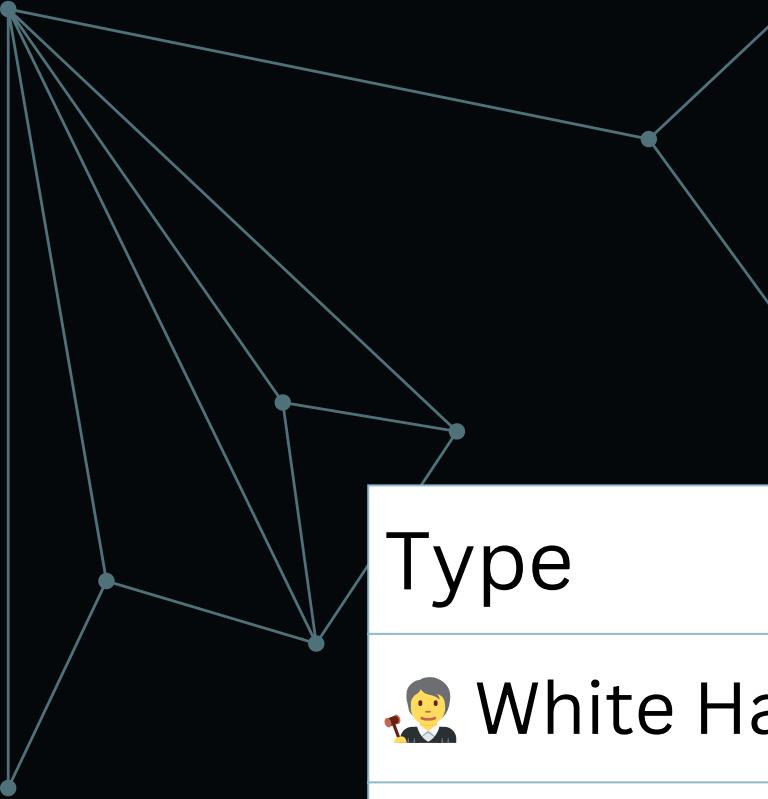
A hacker is someone who uses their tech skills to solve problems or find weaknesses in systems.

Hackers can be protectors or attackers

→ Not all hackers are bad!

Teacher Notes:

Ask students: What comes to mind when you hear “hacker”? Let them answer, then guide them into understanding the broader definition.



TYPES OF HACKERS



Type	Description
White Hat	Ethical hackers who protect systems & people
Black Hat	Hackers who break into systems for personal gain
Grey Hat	Hackers who break into systems without permission but don't mean harm
Script Kiddies	Beginners who use tools they didn't create
Hacktivists	Hackers who promote a political or social cause
State-sponsored	Hackers hired by governments for spying or cyberwar
Organized Crime	Criminal groups that hack for money and fraud

Teacher Notes:

Use real-world analogies (e.g., White Hat = digital police). Discuss how motivation and legality make the difference between types.

COMPARE THE HATS

ACTIVITY SLIDE



- White Hat: “I help fix security flaws.”
- Black Hat: “I steal data and cause harm.”
- Grey Hat: “I hack for fun, but I tell people what I find.”
- Script Kiddie: “I copy and paste code I don’t understand.”
- Hacktivist: “I hack to fight for a cause.”
- State-Sponsored: “I work for my government.”

Teacher Notes:

Let students guess which “hat” each voice belongs to.
Optional: assign roles for a mini-drama/skit or class read-aloud.

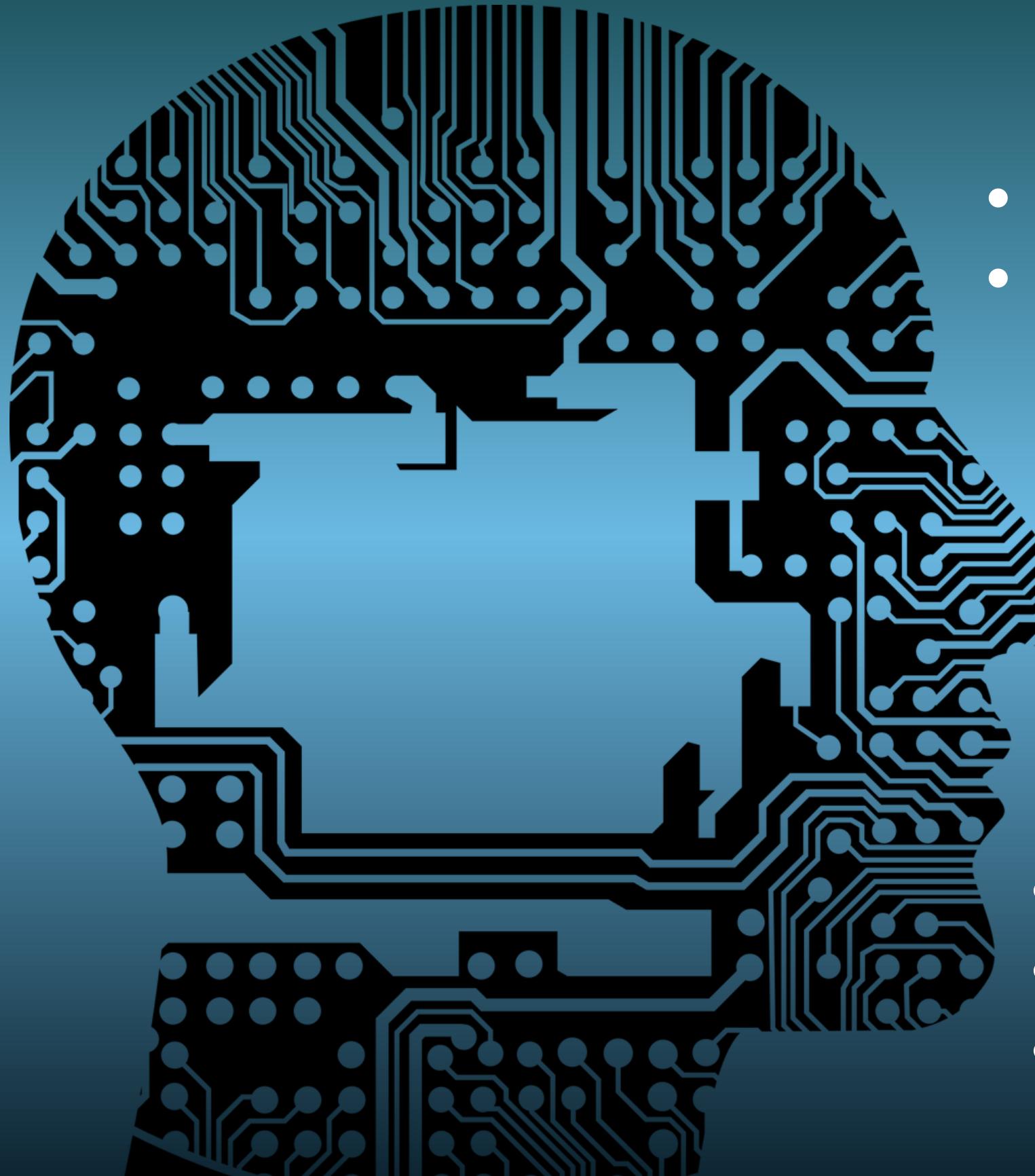
WHAT IS ETHICAL HACKING?

Ethical hacking is using hacking skills for good.

- ✓ Find weaknesses
- ✓ Help fix them
- ✓ Get paid for it — legally!



Defender vs Attacker



WHITE HAT:

- prioritizes Integrity; Transparency; Responsibility
- Objective, Factual and Analytical

BLACK HAT:

- Associated with Malicious intent
- Exploits vulnerabilities for personal gain or harm
- critical; cautious and risk-aware

BUG BOUNTIES

GET PAID TO HACK!

Some companies pay hackers to find security bugs

This is called a bug bounty

You get paid legally to make the internet safer!

Companies like Google, Apple, and Facebook pay people to find bugs in their systems.

💸 Report the bug → Get rewarded!

Real-Life Example:
Santiago Lopez (Argentina) made \$1 million in bug bounties at age 19.



CYBERSECURITY CAREER PATHS



- Penetration Tester
Tries to break into systems (legally!) to help make them safer.
- Digital Forensics Analyst
Investigates cybercrimes and finds out what happened.
- Security Analyst
Monitors networks and systems to stop hackers.
- And many more!
Ethical hackers work in banks, tech companies, government, and even video games!

Teacher Notes:

You can use visuals or icons here. Ask students which career they find most exciting and why.

HACKER ETHICS & RULES



- Always get permission before hacking
- Never hack a real system without approval
- Use legal tools and platforms only
- Do no harm — ethical hackers protect, not destroy

Teacher Notes:

Reinforce that ethics are the backbone of cybersecurity careers. Real hackers face prison time if they break laws.



QUICK ACTIVITY



Would you rather...

- Hack into a game to fix a bug
- Help a company stop a scam
- Investigate a hacker's tracks
- Why? Tell a friend!

Teacher's Notes:

Encourage students to choose an answer and explain their reasoning. Use it as a fun, interactive way to spark discussion about ethical decisions in cybersecurity.

WRAP-UP – WHY IT MATTERS

- Hacking isn't always bad
- You can be a hero in tech
- Start learning today with safe platforms
- There's a future in cybersecurity for YOU!



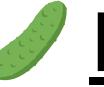
Teacher Notes:
End with motivation. If students are interested, suggest exploring more on cyberstartamerica.org or local tech programs.

Ready to Explore?

 TryHackMe Beginner Rooms:

 [Introduction to Cyber Security](#)

 [Mr. Robot](#)

 [Pickle Rick](#)

 Additional Sites to Explore:

[Hacker101](#)

[Hack The Box](#)

[Bugcrowd](#)

Teacher Notes:

If devices are available, let them explore in pairs or assign this as homework.

Case Study 1: The Bank That Almost Blew Up

Scenario:

In 2016, ethical hacker Leigh-Anne Galloway discovered a flaw in a major UK bank's app that let attackers drain accounts without passwords.

Action:

- Reported via the bank's bug bounty program.
- Worked with developers to patch the flaw in 48 hours.

Impact:

- Prevented \$2M+ in potential thefts.
- Strengthened global app security standards.

Discussion Q:

"Why might banks pay hackers instead of hiring more security staff?"

Mini Quiz

1. What's a White Hat hacker?
2. What's a bug bounty?
3. Name two types of hackers.
4. True or False: Script Kiddies are professional hackers.
5. Name one cybersecurity career.

Teacher Notes:

Use this as a quick review. You can turn it into a game with teams or offer small rewards.