Badge 1: Cybersecurity Basics

We use computers to help us with daily tasks like school, work, shopping, and getting directions to a restaurant. Businesses, governments, and organizations all use computers to accomplish their goals. Because computers play such a big role in our lives, they need to be protected from people who would use them to steal, manipulate, or cause trouble. Explore the basics of cybersecurity by learning about the different kinds of hackers, cyberwarfare, the ethics of hacking, and careers in cybersecurity.

Steps

1. **Learn about different kinds of hackers**
2. **Hide a message in plain sight**
3. **Debate the ethics of hacking**
4. **Learn cyberwarfare strategies**
5. **Explore careers in cybersecurity**

Purpose

When I've earned this badge, I'll know how hackers can hide dangerous code and how countries engage in cyberwarfare. I'll also understand the ethical questions raised by hacking and the possible career paths in cybersecurity.

“The Only Winning Move Is Not To Play”

In 1986, a movie called *WarGames* got the president thinking about cybersecurity. In the movie, a teenager accidentally almost starts World War III when he hacks into the computer that controls the U.S. government’s North American Aerospace Defense Command and monitors if anyone is sending missiles toward the United States.

President Reagan watched the movie and asked his advisors if it was really possible to hack into sensitive government computers. The answer was yes. In response, the president recommended some laws which created the Computer Fraud and Abuse Act. This was the first law to specifically focus on cybercrimes.

Because the world of computers changes so fast, the law has been revised many times and continues to need to be updated.

STEP 1 Learn about different kinds of hackers

Cybersecurity professionals hack, or break into, computer systems to find weaknesses before others can. They do that with the knowledge and permission of the company whose computers are being hacked. They’re hacking for good.

Criminal hackers break into computer systems without the knowledge or permission of the company being hacked. They aim to make money, build their reputation, discredit competitors, or cause chaos. They’re hacking for bad.

Then there are hackers who are in the middle. They hack into systems without permission, but don’t steal or exploit what they find. Instead, they might tell the company they hacked what they found and ask for money to fix it.

What do you think? Are these last kind of hackers black hat, white hat, or something in between?

WORDS TO KNOW

Black hat hacker someone who uses illegal or unethical means to break into computer systems for personal or financial gain

Cybersecurity the protection of digital devices, such as phones or computers, against attacks

Gray hat hacker a hacker whose motives and tactics fall somewhere in between black hat and white hat hackers. They generally have good intentions and do not plan to steal or exploit the security vulnerabilities they find. However, they may break into systems without the owner's knowledge or permission, and/or they may demand some kind of reward in return for their work

Internet of things the interconnection of everyday objects, such as microwaves, refrigerators, TVs, etc., that can send and receive data via the internet

Phishing a type of cyberattack in which a hacker sends an email that contains bad links, harmful attachments, or requests for money

Social engineering a cyberattack strategy that attempts to manipulate or deceive a user so that they give up their personal information

Steganography the practice of hiding secret information in otherwise non-secret media

White hat hacker an "ethical hacker" who uses his/her skills in legal ways to protect people and organizations

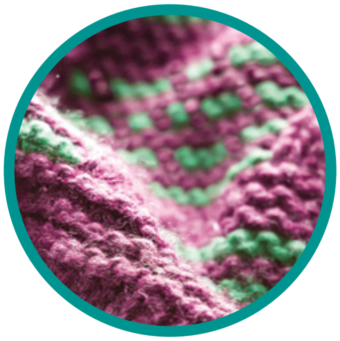
STEP 2 Hide a message in plain sight

Changing messages into a secret code, or encrypting them, is a way to hide messages from people. Another approach is to put the message right where people can see it, but in a way they don't notice it. This is called **steganography**. It's the practice of hiding secret messages in an otherwise non-secret medium.

Here are some non-digital examples of steganography.

Writing a message using special ink that is invisible except in special light.

Writing a message on an envelope and then covering it with a postage stamp.



Knitting a message in morse code into a sweater using different colors of yarn.

Embedding a message in a letter or article.

Hackers can use steganography too, to hide malware in regular computer code.

STEP 3 Debate the ethics of hacking

What does privacy mean? Do you have a right to keep all your information private? When should a company, like a phone or credit card company, keep your information private? When, if ever, should they share it with the government or other people or organizations? Should a library have to keep the record of the materials you've checked out secret? Who owns metadata? Is it ever acceptable to hack into a computer system or device without permission?

The ethics of cybersecurity are complicated. People working in the field struggle with these questions every day. As technology changes, more questions arise.

STEP 4 Learn cyberwarfare strategies

Spying in the 21st century goes beyond dead drops, safe houses, and secret meetings. Today, spying can mean monitoring or hacking into a target's computer systems. **Cyberwarfare** means launching a cyberattack against another country to disrupt or spy on their computer systems. What does it mean to engage in cyberwarfare? What are the risks and benefits?

STEP 5 Explore careers in cybersecurity

There are lots of careers in cybersecurity: digital forensics expert, cryptographer, cybercrime investigator, security architect, or ethical hacker. Each kind of job plays an important role in creating secure computer systems. Some of the jobs are more public, while others are behind the scenes. All of them require good problem-solving and people skills.

JOIN THE CYBERCRIME FIGHTING TEAM!

Cybersecurity needs people with different skills and specialties to stop hackers. Which job would you like best?

Chief Information Security Officer

oversees a company's entire program to protect their information and computers. If you were a CISO, people working in all the other positions listed here might work for you!

Cryptographer

writes algorithms to change readable data into encrypted code so it can travel securely from user to user.

Digital Forensics Expert

searches for digital traces and clues that help solve cybercrimes.

Ethical Hacker

hacks into a company's systems to find vulnerabilities that could be exploited. Ethical, or white hat hackers, have permission to attack a system for the purpose of making it more secure.

Security Architect

oversees a company's systems, tries to anticipate what hackers might do, and analyzes possible threats.

Security Software Developer

develops software to keep computer systems safe. This could be antivirus software; tools that look for malware, worms, or viruses; or user authentication programs.

Now that I’ve earned this badge, I can give service by:

- Hosting a steganography party. I can teach my friends how hackers hide dangerous code using steganography in phishing emails.
- Researching local cybersecurity firms (or businesses with a cybersecurity department) for a troop field trip.
- Researching privacy laws in my state and, if needed, advocating for stronger safeguards and personal control of data.

I’m inspired to: