Badge 3: Cybersecurity Investigator

Cybersecurity professionals crack codes, delete malware, and defend against hackers. You'll become a cybersecurity investigator by finding out how to protect your online identity, cracking codes, and figuring out the difference between real and fake information.

Steps

1. Create and crack a shift cipher code
2. Find out how device updates can help your security
3. Explore identity theft
4. Find out what to do if your identity is stolen
5. Investigate if a message is real or fake

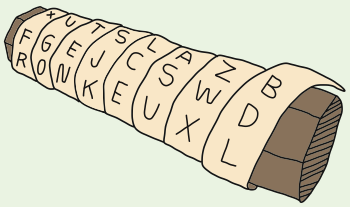
Purpose

When I've earned this badge, I'll know how computers use codes to communicate and how to spot cyber crime.

Ancient Cipher

People have been sending secret messages for hundreds of years. A scytale is an ancient coding tool from Greece. The Spartans used this tool to communicate secret messages during wartime. The tool is a cylinder made out of wood. Both the sender and the receiver of the message had to have the same size cylinder.

The sender would take a long narrow strip of leather or fabric and wind it around the scytale so that the coils of the fabric lined up. The sender wrote a message with one letter on each coil from left to right. The fabric was unwound from the scytale and scrunched up for transport. On its own, it just looked like a long strip of fabric. When the receiver got the fabric strip, she wrapped it around her scytale and lined up the coils to read the message.



STEP 1 Create and crack a shift cipher code

Computers use codes as their language. It's how computers communicate. And people who code computers, known as programmers, are always looking for ways to send coded information to protect private information, such as emails and bank accounts. It's called encryption.

Codes are a great way to change a message so it can't easily be understood. Another word for code is cipher. Codes replace letters with special numbers, letters, and symbols to make a message secret. When you crack the code, you decipher the message.

STEP 2 Find out how device updates can help your security

All digital devices have software that helps them run. That software gets updated regularly. Have you ever been on a digital device and had a window pop up telling you it's time to install a new update?

Software updates add new features and remove old features, but their most important job is making your device's security better.

Are You CYBER SAVVY?

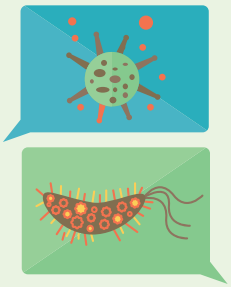
Take this quiz and see how cyber savvy you really are.

1. You just received an email from a rich person who wants your help. He has lots of money in another country but can't move it. He asks you to send him money. He says he will pay you back what you send him and then he will give you a bonus of extra money just for helping. What do you do?

   a. Send a note back saying you know this is a scam.
   b. Delete the email—tell an adult.
   c. Forward the email to your friends.
   d. Write back—it sounds cool!

2. You are shopping online and a window pops up saying that you have a virus. It says, "Click to resolve the issue." What do you do?

   a. Click and follow the directions.
   b. Close both the virus window and the shopping site window and don't return to the site.
   c. Hit the "back" button.
   d. Close the pop-up window.



3. How often should you back up your devices?

   a. Once a day
   b. Once a week
   c. Whenever you create new files
   d. When you think there may be a problem

4. You "meet" someone nice online. They tell you they are your age and ask what school you go to. They want to meet you in person. What do you do?

   a. Give your name and make a time to meet.
   b. Tell the person to stop bothering you.
   c. Tell your parents or another trusted adult. Show them the email.
   d. Give your name and school but don't meet.

Answers on page 23

Cybersecurity Calling

Do you like computers? How about solving puzzles, deciphering codes, and unraveling mysteries? If you said yes, a cybersecurity job could be in your future.

Tons of companies need people with strong computer skills to help protect information against cyber attacks.

From banks and hospitals to aerospace, pharmaceutical, military, and engineering organizations, any business that has classified or private information needs help keeping it safe.

With computers controlling more and more—from powering up cities, flying planes, and running machines that operate on people—there will be jobs in the future that we can't even imagine now.

STEP 3 Explore identity theft

Your identity includes private information, such as your name, address, birthday, and, when you get older, credit card information. Identity theft is a crime where cyber criminals steal your private information and pretend to be you online. They can buy items with your money, and then use your name if they get in trouble. It's one of the fastest growing crimes in the world.

STEP 4

Find out what to do if your identity is stolen

Criminals who steal personal and private information are called identity thieves. Once they get enough information, such as a name, an address, or a social security, bank account, passport, or credit card number, they pretend to be that person. They can use the information to buy expensive items or apply for credit cards.

If you or someone you know has their identity stolen, there are some actions you can take to help. You have to act fast. Report the theft to a trusted adult as soon as possible.

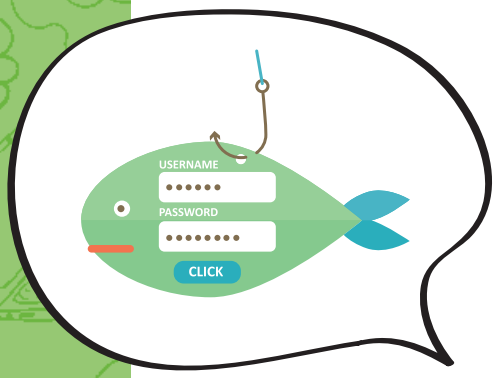
Make Your Device Safe

Protect your computer against viruses, spyware, worms, and other harmful malware. Keep software current so you have the most recent security updates and make sure you protect any devices (phones, tablets, laptops, desktops, and gaming systems) that connect to the internet by having good, strong passwords.

STEP

5 Investigate if a message is real or fake

When cyber criminals want to find out information, they will sometimes create online scams called phishing. Phishing is when a cyber criminal tries to get your information—such as your username, password, and credit card details, and sometimes even money—by pretending to be someone who is trustworthy. They send you a message via text, email, or social media and invite you to click on a fake webpage. If you do, you'll give them your private information without even realizing it! That's why it's important to only talk to people you already know and trust when you're online.



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

- Teaching my friends how to create a secret code or password.
- Making a poster about identity theft to hang at my school or library.
- Leading a workshop to teach others how to spot fake messages online.

I'm inspired to:

Answers : Page 19: 1. b 2. b 3. c 4. c