Senior Cybersecurity

Learn how to keep computers and information safe from hackers by earning these three badges!

Badge 1:
Cybersecurity Basics

Badge 2:
Cybersecurity Safeguards

Badge 3:
Cybersecurity Investigator

This booklet gives girls an overview of the badge requirements and badge steps for all three Senior Cybersecurity badges. It also includes interesting background information to spark girls' interest in cybersecurity. Volunteers can access the Volunteer Toolkit (VTK) to find complete meeting plans, including detailed activity instructions and handouts.

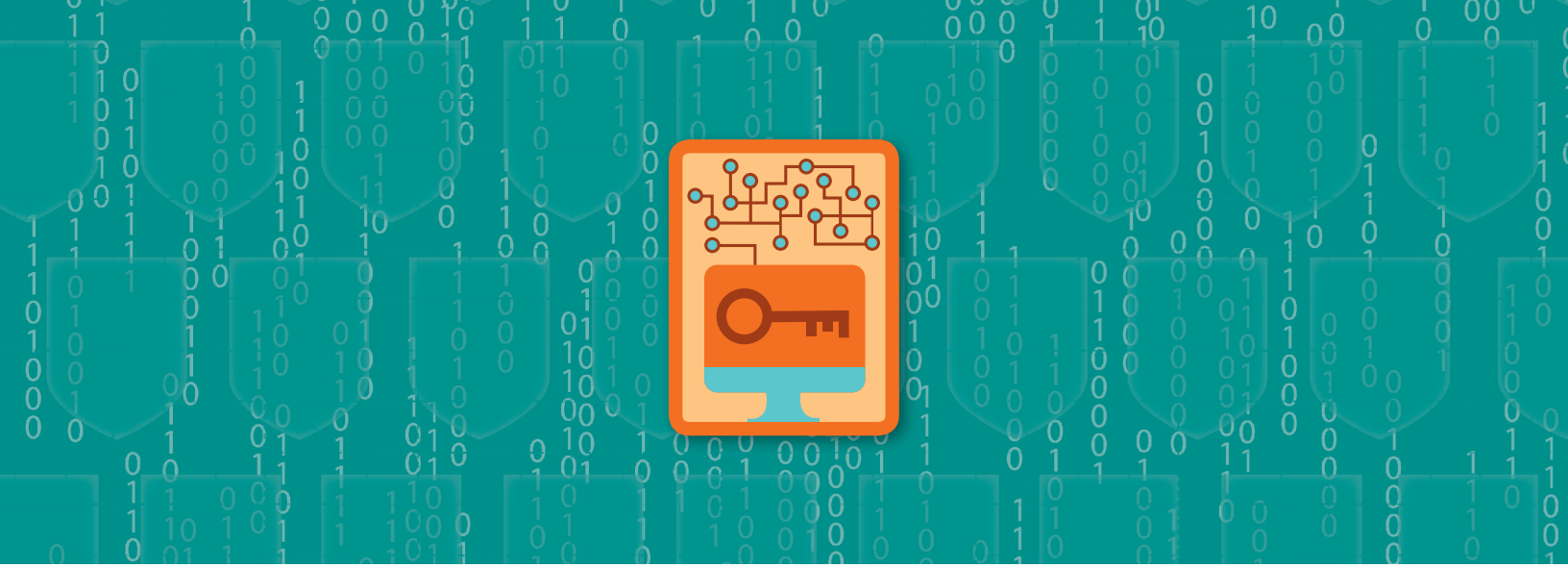
Welcome to the world of cybersecurity.

When you've earned these three badges, you'll know the 10 principles of cybersecurity and how to use them. You'll also know how to protect yourself and others from cyberattacks and how investigators solve cybercrimes.

Cybersecurity experts plan and build security systems for computers and companies to protect information and computer systems. You can apply the same concepts they use to protect your own electronic devices and information.

Cybersecurity experts also investigate cybercrimes, such as stealing private information or shutting down an organization's website or computer network. They combine law enforcement skills and cybersecurity knowledge to track down and catch hackers.

Volunteers can access the Volunteer Toolkit (VTK) to find complete meeting plans, including detailed activity instructions and handouts.



Badge 1: Cybersecurity Basics

If you want to stop hackers from stealing information or disrupting other people's computers, you need to know about how computers and computer programs work. Learn how computer programmers write code and set up systems to slow down or stop hackers.

Steps

1. **Find out how computers run multiple programs**
2. **Identify functions and privileges**
3. **Learn how computers hide information**
4. **Design a layered security system**
5. **Design a Rube Goldberg machine**

Purpose

When I've earned this badge, I'll know the principles of cybersecurity and how cybersecurity experts use them to protect computer networks and information.

STEP

1 Find out how computers run multiple programs

Imagine getting ready for school in the morning while you're talking to your mom, packing your lunch, and trying to find your cell phone. That's called multitasking.

The problem is that our brains aren't designed to multitask. You're more likely to make mistakes when you multitask.

Computers often have to multitask, too. When a computer multitasks, it creates an opportunity for hackers to break in. Every program you're running or website you're using provides a kind of entry point to your computer. Computer programmers have developed ways to help computers run multiple programs more efficiently and more safely.

- Each **process**, or program running, is separated into its own space in the computer's memory. You can see a form of this when you have multiple tabs open on your computer running different programs. This is called **process isolation**. Every program gets to work in its own space.
- **Domain separation** is another way programmers help computers multitask more efficiently. Domain separation helps prevent large data breaches by keeping different types of data separate, such as credit card numbers and social security numbers. Domain separation also restricts employees from having access to different kinds of data. For example, employees who work on the website may be restricted from accessing customer data, to prevent customer data from getting published on the website.

WORDS TO KNOW

Address space an area of the computer's memory that only one program can access

Bar code a black-and-white code that can contain a variety of different types of data and be read by a machine

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

Data packet a piece of a message (called a unit of data) that's transmitted through the internet

Digital object anything that is stored on a computer. This might be data, user information, software programs, etc.

Faraday cage a box or enclosure made of metal that conducts electricity and prevents electromagnetic charges from reaching whatever is inside it

Hops the number of routers that a packet passes through from its source to its destination

Hotspot a wireless access point, typically in a public location, that provides internet access to laptops, smartphones, or other devices

Insider threat a current or former employee, contractor, or other business partner who has access to an organization's data or network information. Because of this access, they could be involved in a cyberattack

IP address IP stands for internet protocol. It's a series of numbers unique to that device. Any device connected to a network has its own IP address

Privileges defining who can and cannot use an object

Process a program running on a computer

Security vulnerability a weakness in a device or program through which it can be hacked or exploited

Smart devices electronics that are connected to the internet, like phones, tablets, laptops, smart watches, smart TVs, smart thermostats, or home security systems

Stakeholder a person who is affected by an organization's actions and policies

Traceroute a list that shows the path data packets travel from one website or device to another

GenCyber's First Principles of Cybersecurity

Hackers constantly look for new ways to break into other people's computers. Cybersecurity experts have to make hacking as hard as possible. These ten principles of cybersecurity, created by the National Security Agency (NSA) and the National Science Foundation (NSF), cover different aspects of computing to make a computer system safer.

Abstraction removing any unnecessary information

Data hiding keeping information from being seen or accessed by certain users

Domain separation keeping things (like processes or user accounts) separate from each other

Layering using multiple strategies to protect yourself or your digital stuff

Least privilege giving as few people as necessary access to digital content

Minimization reducing the number of ways someone can hack a digital device or software

Modularity dividing software programs into small "modules," or components, so that you can edit them more easily

Process isolation running every computer program in its own area of a computer's memory

Resource encapsulation labeling a digital object, like a file or folder, based on who can use it and how it should be used

Simplicity making designs as simple, streamlined, and easy to understand as possible

DOES YOUR COMPUTER KNOW WHAT TIME IT IS?

GPS, or the Global Positioning System, is a group of satellites in space that work together to provide exact locations on earth. It's why the map app on your phone works, but is also really important in a lot of other ways.

For example, each satellite has a special clock in it, and they work together to give computers on earth the EXACT time down to the billionth of a second. Banks, airlines, fire stations, police departments, TV stations, and the military are just a few of the organizations that use computers or other technology that depend on the GPS clocks.

In 2016, a computer glitch caused some GPS satellites to transmit bad timing data. Computers on earth started shutting down. Cell phone towers stopped working. Radio stations lost their signals. Computers at all kinds of organizations—from businesses to government agencies—were affected.

The glitch was fixed in less than a day, but it brought a big problem into focus: much of the world's economy and services depends on the GPS clocks. If they fail, it impacts everything. Cybersecurity experts have warned that the all-important role GPS plays also makes it a prime target for hackers.

STEP 2 Identify functions and privileges

Would you wear swimming flippers to go ice skating? Would you try to frost a cake before you baked it? Of course not! You use ice skates for ice skating, not swimming flippers. And you need to bake a cake before you ice it.

These are examples of **resource encapsulation**. This cybersecurity idea labels parts of the program or data based on who can use it and how it's used. This protects the code or data from revealing any more about itself than it needs to run a program. Programmers bundle, or encapsulate, programming and data, and label it. All the contents of the bundle still work, but the user and the rest of the program don't have access to the details.

A related idea is **least privilege**. That means as few people as necessary should have access to digital "stuff." Identifying who can use computer hardware, programs, and data—and limiting how they can be used—limits the ways hackers make trouble.

STEP 3 Learn how computers hide information

Computer programmers use a similar idea called abstraction. The goal is to remove anything on the screen that can distract you or be used incorrectly.

For example, when you open a spreadsheet, you only see the columns and rows, numbers, and mathematical functions. You input your data and tell the spreadsheet to sum up columns or find averages. The program does the mathematical calculations for you, but you don't see how the math gets done. You just see the result of the calculation. When you create an account on a website, you don't see the code that stores your username and password so you can log in again later. You only see the login page.

Programmers want to provide the minimum information necessary to a user to accomplish a task. When you see a little hourglass or spinning circle on your computer screen, that means a part of the program you're using is running (like checking your username and password to log you in), but the programmer hasn't given you access to see it.

Another concept programmers use is called **data hiding**. That just means that programmers hide data from users who don't need access. For example, in banking, a teller will be able to see only data about your account needed to complete your transaction.

STEP

4 Design a layered security system

Trying to break into a computer security system is like trying to get out of an escape room, but in reverse. When you do an escape room activity, you solve a series of puzzles in a particular order to get out. When hackers want to break into a computer, they have to get through a series of security systems in a particular order to reach their goal.

Using multiple security strategies is called **layering**. Cybersecurity experts create a series of obstacles, such as firewalls and antivirus software, to protect the computer system. They also limit access through passwords, multi-factor authentication, and resource encapsulation. Layered security systems may have a time limit to ensure users really know the passwords and aren't just guessing. They may also lock users out after inputting the wrong password too many times.

Programmers also use **modularity** to make computers more secure. Programs are divided into smaller components, or "modules." If there's a problem, the programmer can edit or swap out the module instead of having to rewrite the whole program. Modularity applies to the parts of a computer, too. If your sound card fails, you can replace it. Modularity make computers and programs easier to fix and limits the damage a hacker can do.

STEP
5 Design a Rube Goldberg machine

Rube Goldberg's wacky machines may be great fun to build and play with, but you wouldn't want to be responsible for keeping one running smoothly. All those moving parts mean more for you to monitor and more places where the machine can break down.

In cybersecurity, less is more. That's another way of describing the principle of **simplicity**. The simpler, more streamlined, and easier to understand a program is, the better. When software is simple, it's easier to notice and fix problems. That makes the programs more secure.

Minimization is a cybersecurity concept that's similar to simplicity. It means reducing the number of ways that software can be attacked. When you work to make your programs simple and you limit access to data, you minimize the opportunities hackers have to break into your system.

SOLVE SIMPLE PROBLEMS IN COMPLEX WAYS

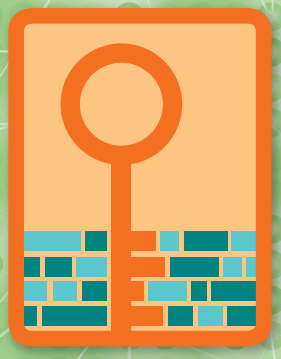
Reuben Goldberg was a famous cartoonist. He studied engineering in college and liked to invent things. He drew lots of different types of cartoons throughout his career, including political cartoons and ones about sports. He's most famous for his cartoon strip *The Inventions of Professor Lucifer Gorgonzola Butts*. Professor Butts invented crazy, ridiculously complicated machines to do simple tasks, such as opening an umbrella. The cartoons led to people describing needlessly complicated things as "Rube Goldberg machines."

Rube died in 1970, but people still hold contests to see who can build the best machine. Each contest has a task, such as assembling a hamburger, putting toothpaste on a toothbrush, or putting money in a piggy bank. Inventions are judged on creativity, silliness, and teamwork.

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

- Giving a classroom presentation about what I've learned.
- Partnering with a cybersecurity professional to create a video on the ten principles of cybersecurity.
- Developing a workshop for others showing them how to use concepts like least privilege and layering to improve their personal cybersecurity.

I'm inspired to:



Badge 2: Cybersecurity Safeguards

Mobile devices, such as your phone, tablet, or laptop, help you to stay connected no matter where you are. But when you're out and about, your digital information is more vulnerable. Learn how to keep your information and electronics safe when you're away from home.

Steps

1. **Protect your travel documents**
2. **Protect your Wi-Fi**
3. **Protect your conversations**
4. **Protect your electronics**
5. **Protect your environment**

Purpose

When I've earned this badge, I'll know how to keep myself and my data safe when I travel.

STEP 1

Protect your travel documents

When you travel, you often need an ID card or passport. Sometimes you need tickets or boarding passes. All these things contain personal information. Some of them even have bar codes that lead to data files with more information about you.

If someone has access to a bar code reader (they're available free online!), they can see what's in those personal data files. What should you do with your travel documents to keep your personal data safe?

STEP 2

Protect your Wi-Fi

Years ago, people had to connect to the internet by attaching a cable to their computers. In 1997, Wi-Fi was first made available to the public. It seemed like magic. Wi-Fi lets you connect to the internet using wireless transmitters and radio signals. No cables needed!

But there's a problem. If you don't use a secure Wi-Fi connection that encrypts your data, anyone can see what you're doing online and access your passwords and other private information.

How can you protect yourself? When you use public Wi-Fi in a coffee shop or library, look for servers that are secure. If you have to use a nonsecure server, remember that a hacker could intercept your information. Don't do any banking or shopping on a nonsecure server, or send emails with personal information like your birthday or address.

Remember these tips when you head out for an adventure.

Lock your devices.

Use your passcode or fingerprint to protect information on your smartphone or tablet.

Limit your location sharing.

Turn off location authorization on apps. Don't share photos or your location on social media while you're traveling.

Turn off your bluetooth.

If you use bluetooth to connect to a speaker at home, be sure it's turned off on your phone when you're traveling. Hackers may be able to locate your phone through bluetooth.

STEP

3 Protect your conversations

Cell phones have made communicating with people easy. Before cell phones, you had to find a pay phone or landline or send a letter in the mail. Now, you can call or send someone a message from nearly anywhere. However, that convenience comes with a price because cell phones don't guarantee your privacy.

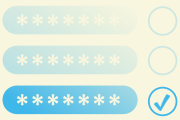
Some cell phones or apps are more secure than others. FaceTime, iMessage, WhatsApp, and Signal are examples of apps with **end-to-end encryption programs**, where your conversations and messages are encrypted throughout the entire transmission process. However, some of these programs only guarantee your conversation will be secure if the other person is also using the same app.

For a program to be effective, it has to be easy to use, easy to be encrypted and decrypted by the users, but hard to crack by hackers.

BE A SAVVY TRAVELLER!

Turn off Wi-Fi autoconnect.

If you've set your device to automatically connect to open Wi-Fi networks, turn that off. Make sure every Wi-Fi connection you use is secure.



Change your passwords.

Just in case someone figures out your password while you're traveling, it's a good idea to use a different one than you usually use at home. You can change it back when you get home.

Don't leave your digital devices out unattended.

If your hotel room has a safe, put your devices there when you aren't using them. If you must leave your devices in the car, lock them in the trunk.

Where Am I?

Did you know that your smartphone or tablet apps may be collecting and selling data about your location even when you aren't using them? This is called **location aggregation**. Businesses use this data to send ads and develop new products.

For example, a fast food restaurant chain may track where its customers go to see what other kinds of food they eat. Based on what they find, they may add more healthy options or start selling fancy coffee.

Hackers can also use that information to invade your privacy. By knowing where you go, they can figure out things like who your doctor is or which bank you use. Hackers can use this location information to try to access your personal information.

To protect yourself, read an app's terms of use or privacy policy before clicking "agree." You'll learn how your information could be used—and you may not agree to share it!

STEP 4

Protect your electronics

When a cell phone is on, it's always searching for a connection and sending out signals about where you are, even if it isn't making or receiving a call or text. Many smartphones can record conversations that could be transmitted to someone else later. To prevent other people from listening in on conversations or monitoring their location, people sometimes use a **Faraday cage.**

A Faraday cage is basically a metal box that prevents radio signals from getting to or from your phone or other digital device. It can also protect electronics from being damaged by a lightning strike or electromagnetic pulse.

Faraday bags are a type of Faraday cage made of a flexible metallic material.

STEP 5

Protect your environment

If you like spy movies, you're familiar with the scene where someone plants a "bug," or listening device, in an office, home, or hotel room. These tiny transmitters pick up noises, like conversations, and transmit them to someone listening or recording them. It sounds like movie stuff, but cybersecurity experts who work in government need to check for bugs in rooms where important meetings are taking place.

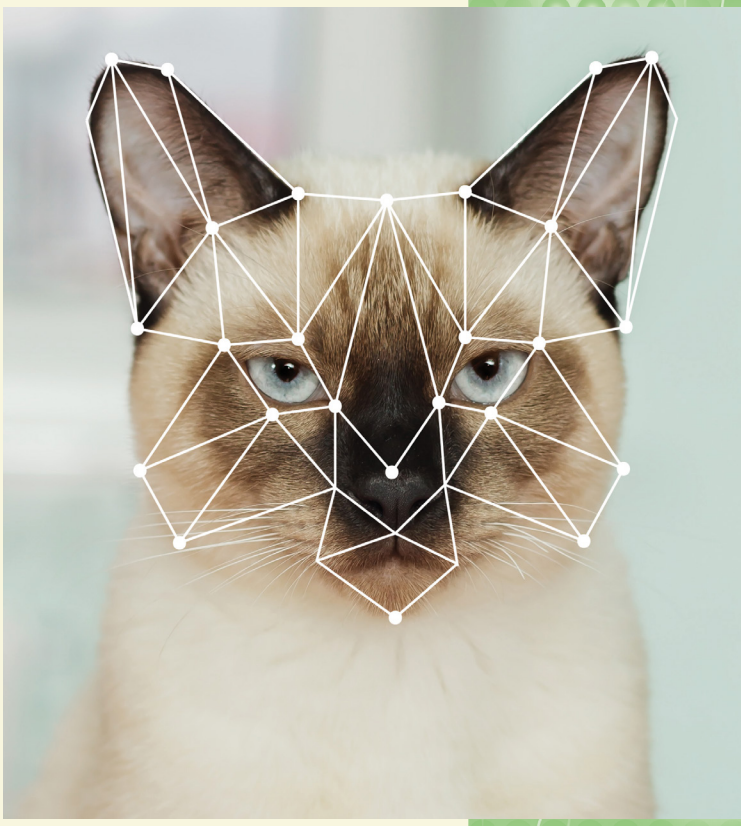
Smart speakers, like Alexa, are supposed to listen to your conversation so they know when you're asking them a question or giving a command. Sometimes, though, a smart speaker can misunderstand a conversation and record or transmit conversations that people meant to be private.

Being aware of your environment and devices that could threaten your privacy shows cybersecurity smarts.

FACE IT!

Facial recognition software can identify people by analyzing and comparing photographs. It uses algorithms to measure parts of a person's face, like the distance between their eyes. It can then make a "face print" or digital code of a face. Some software also analyzes people's skin texture and creates a unique "skin print." Those prints are then compared with photos of people in a database to look for a match. Software developers are even teaching facial recognition programs to understand how people look as they get older. That's called age progression.

In movies and TV shows, you see police trying to match a photo of a bad guy with photos in their database of known criminals. That's one use of facial recognition software, but there are many others:



- Social media sites use facial recognition to encourage you to tag people in pictures.
- Computers can use facial recognition to provide access to a specific computer. A computer using this software will only stay on if the correct user is in front of the screen. If that person moves away or someone else tries to use the computer, the computer shuts off.
- Airport security systems are working on a facial recognition system to speed up screening for frequent travelers.

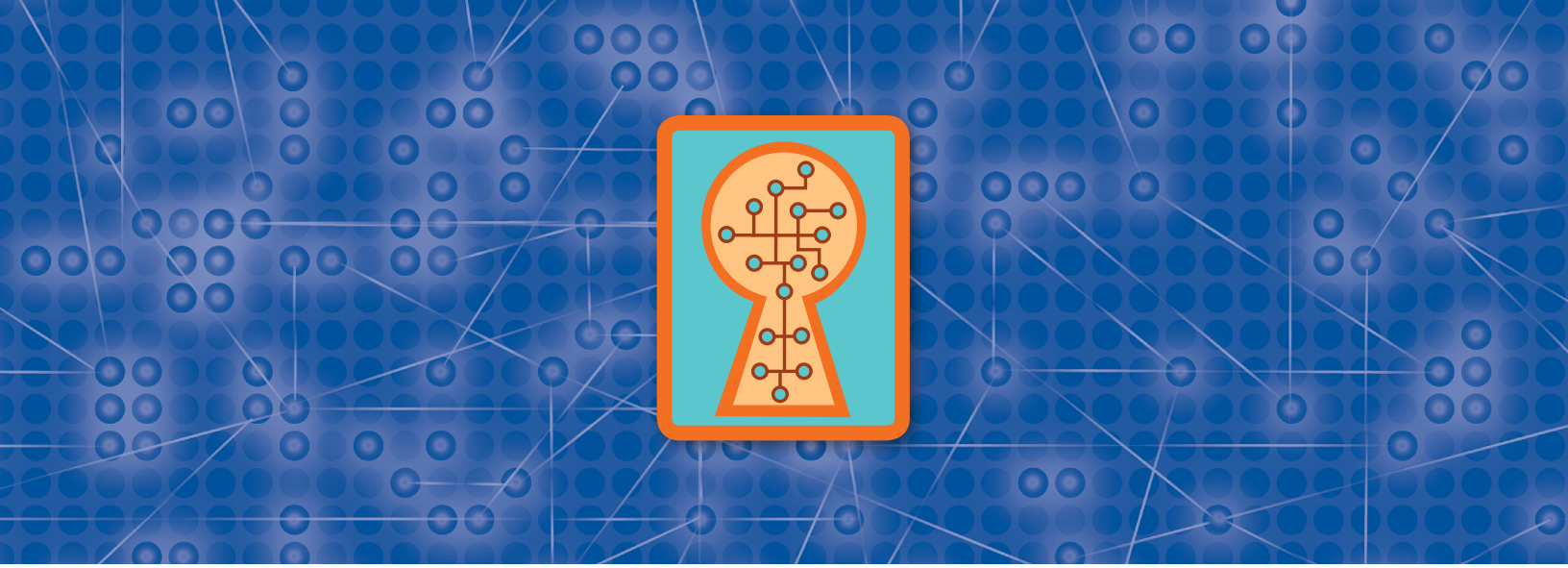
Facial recognition is a new technology that has raised a number of ethical questions. For example, sometimes a person gives permission for his or her photo to be taken—like a photo for an ID. In other cases, surveillance cameras take pictures of people without their knowledge.

How do you feel about your picture being taken without your knowing or giving permission?

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

- Developing a workshop for other teenagers about how to keep electronics and information safe when traveling.
- Giving a presentation about how phones, tablets, or smart home devices can accidentally record conversations.
- Helping friends and family members to update the software on their devices.

I'm inspired to:



Badge 3: Cybersecurity Investigator

Cybersecurity investigators are detectives who solve cybercrimes by using what they know about technology, cybersecurity, and traditional law enforcement techniques. That means they look for clues and piece together information to figure out how a crime was committed. They have to notice small details, but also understand how the different parts of computer systems and programs work together.

Steps

1. **Look for clues about a fictional hack**
2. **Learn how traceroutes work**
3. **Solve a cybercrime**
4. **Role-play how to handle the crisis**
5. **Play a life-sized version of Minesweeper**

Purpose

When I have earned this badge, I'll understand ways cybersecurity investigators solve crimes.

Don't Be Insecure

A regular http connection isn't secure. It sends your data over the internet in plain text, so anyone eavesdropping can see your information.

To protect people's information, programmers created HTTPS. That stands for "hypertext transfer protocol secure."

HTTPS connections are automatically encrypted and will notify you if a website you're visiting isn't secure. An HTTPS connection will have a lock icon and https:// in the web browser's address bar. If the https part is hidden, click inside the address bar; it will show the letters https before the site's URL.

Beware, though! Hackers constantly adapt to new security measures. They might add phony lock icons, create imposter sites, or send phishing emails to make their fake websites look like secure ones.

STEP 1

Look for clues about a fictional hack

The warning sign that you've been hacked might not even look like a cybersecurity problem at first. Maybe sales have plummeted on your company website, even though you usually have lots of customers. Maybe your family's credit card suddenly isn't being accepted at stores or restaurants. Maybe your house was broken into while you were on vacation.

Were you hacked—or are these problems caused by something else? It could be that no one is buying your products because they don't like them. It could be that the credit card doesn't work because the magnetic strip is worn out. It could be that a burglar was watching houses in your neighborhood and noticed that no one was in your house for a few days.

Or it could be that a hacker is behind each problem. Use what you've learned about digital security to solve this cybercrime.

STEP 2

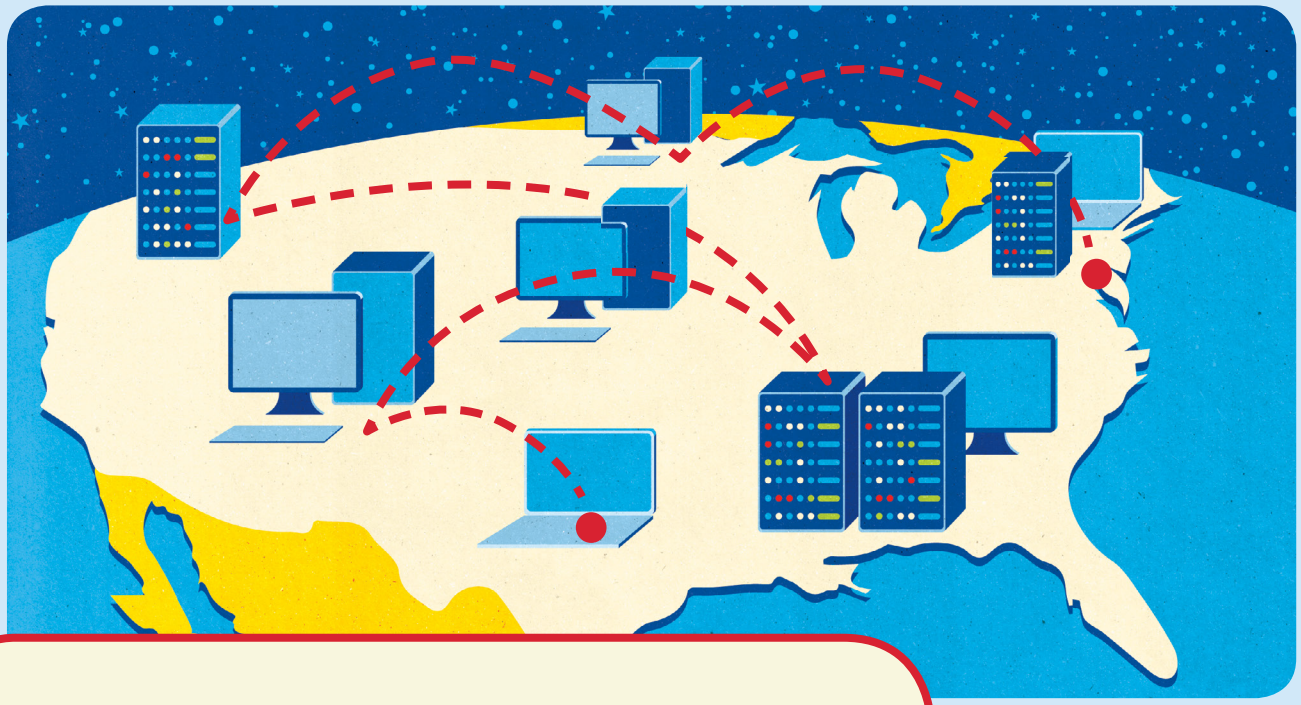
Learn how traceroutes work

When someone investigates a crime, they often recreate what happened. They look carefully at the crime scene and try to retrace the steps of the criminal. They look for footprints.

When information moves around the internet, it leaves footprints, too. Bits of information, called **data packets**, take a certain route to get from your computer to a website, for example. That route, or path, is called a **traceroute**. It lists all the stops your data packet makes along the path, like a trip itinerary. By studying traceroutes, cybersecurity investigators can see the path hackers' data packets took. Traceroutes can help investigators figure out where hackers are located or where they're sending or redirecting information.

Another good way to discern a fake website is by checking the spelling in the URL.

HOW TO READ A TRACEROUTE



```
Utility-MacBook-Pro-2:~ utility.terminal$ traceroute girlscouts.org traceroute
(209.66.73.87), 64 hops max, 52 byte packets
1  172.20.10.1 (172.20.10.1)  3.887 ms  3.807 ms  3.245 ms
2  145.sub-66-174-43.myvzw.com (66.174.43.145)  153.274 ms  49.206 ms  44.89
3  * * *
4  * * *
5  66.sub-69-83-106.myvzw.com (69.83.106.66)  42.031 ms  45.271 ms  28.852 ms
6  2.sub-69-83-107.myvzw.com (69.83.107.2)  41.095 ms  38.262 ms  40.946 ms
7  112.sub-69-83-96.myvzw.com (69.83.96.112)  47.276 ms  38.921 ms  34.988 ms
8  112.sub-69-83-96.myvzw.com (69.83.96.112)  48.028 ms  35.339 ms  42.050 ms
9  69.sub-69-83-96.myvzw.com (69.83.96.69)  30.932 ms  40.307 ms  39.802 ms
10  et-1-1-2.gw18.dfw9.alter.net (157.130.131.9)  43.054 ms  28.253 ms  29.0
11  0.ae1.br1.dfw13.alter.net (140.222.227.169)  42.743 ms  27.398 ms  28.95
12  xe-5-0-1.er2.dfw2.us.zip.zayo.com (64.125.13.25)  40.943 ms  42.475 ms
13  ae24.cs2.dfw2.us.zip.zayo.com (64.125.27.104)  93.879 ms  132.698 ms  11
14  ae5.cs2.iah1.us.eth.zayo.com  (64.125.28.102)  76.924 ms  86.856 ms  91.
15  ae3.cs2.dca2.us.eth.zayo.com  (64.125.29.44)  94.885 ms  85.481 ms  100.
16  ae4.cs2.lga5.us.eth.zayo.com  (64.125.29.30)  90.980 ms  107.770 ms  77.
17  ae12.er4.lga5.us.zip.zayo.com (64.125.27.197)  86.254 ms  89.839 ms  68.
18  209.66.94.14 (209.66.94.14)  80.432 ms  81.163 ms  79.936 ms
```

The website to which the user ran the traceroute.

The time it took to make the hop (e.g. 49.206 milliseconds).

Asterisks mean that either the identity of the "hop" is private or that the request timed out.

IP (internet protocol) address: any device connected to a network has its own IP address, a series of unique numbers.

Many traceroutes use codes that refer to locations around the globe (DFW = Dallas Fort Worth).

Each number represents one stop, or "hop," that the data packets make on their way.

LGA=LaGuardia (airport), New York City. The Girl Scouts website is hosted in New York City.

STEP 3 Solve a cybercrime

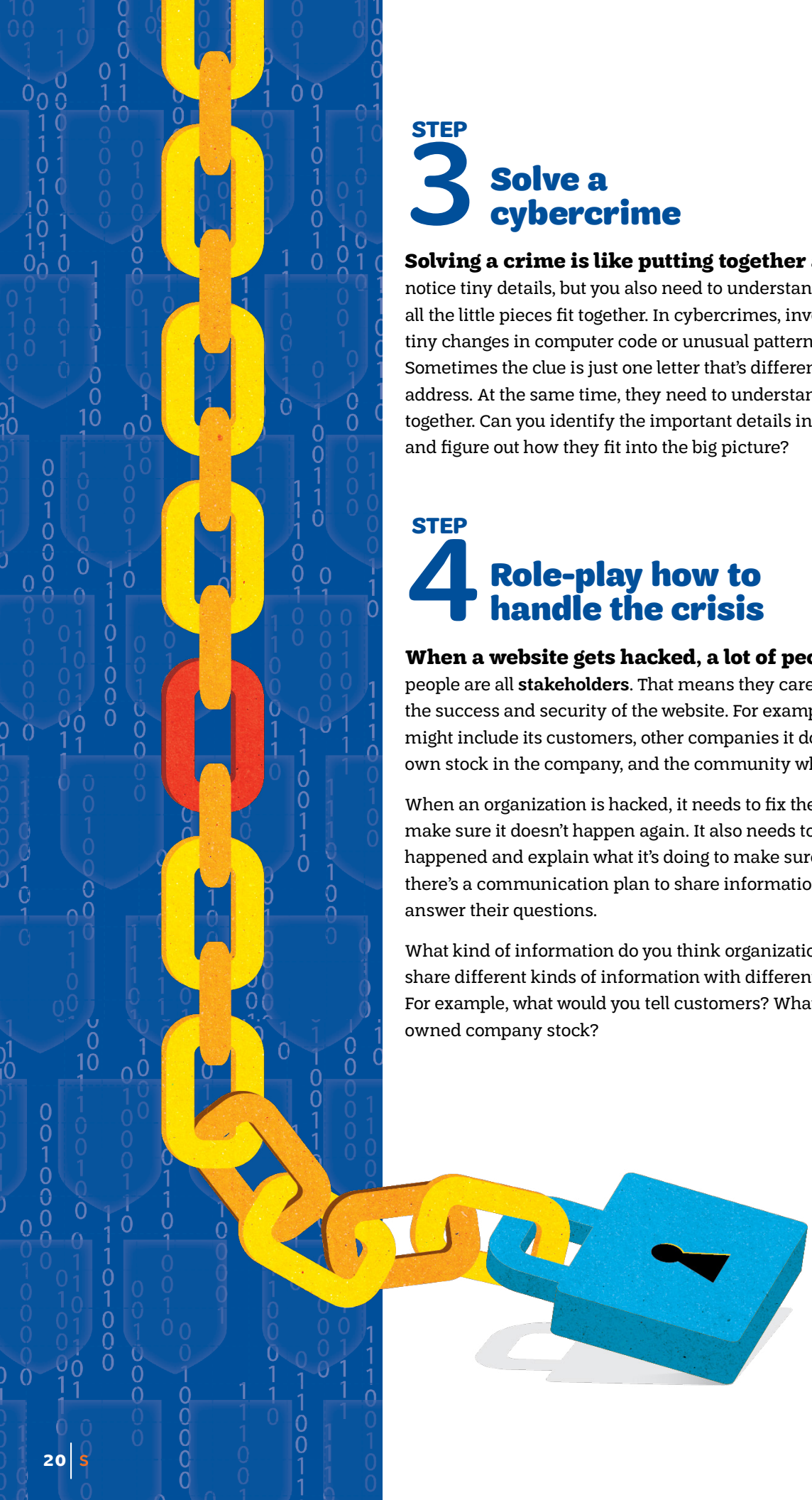
Solving a crime is like putting together a puzzle. You need to notice tiny details, but you also need to understand the bigger picture of how all the little pieces fit together. In cybercrimes, investigators need to notice tiny changes in computer code or unusual patterns in how sites are being used. Sometimes the clue is just one letter that's different in a code, email, or web address. At the same time, they need to understand how all the details work together. Can you identify the important details in code or traceroutes and figure out how they fit into the big picture?

STEP 4 Role-play how to handle the crisis

When a website gets hacked, a lot of people are affected. Those people are all **stakeholders**. That means they care about, or have "a stake in," the success and security of the website. For example, a business's stakeholders might include its customers, other companies it does business with, people who own stock in the company, and the community where it does business.

When an organization is hacked, it needs to fix the problem and take steps to make sure it doesn't happen again. It also needs to tell stakeholders about what happened and explain what it's doing to make sure the site is secure. Usually, there's a communication plan to share information with stakeholders and answer their questions.

What kind of information do you think organizations should share? Would you share different kinds of information with different groups of stakeholders? For example, what would you tell customers? What would you tell people who owned company stock?



SAVE MONEY WITH CYBERSECURITY

Cybercrime is expensive. When databases or websites get hacked, it costs the targeted organization a lot of money. Sometimes hackers steal trade secrets, such as information about how products are made (secret recipes!) or plans for new products in development.

The kinds of things that usually get stolen in a hack are:

- Personal information, such as addresses, dates of birth, or health information
- Credit card information
- Social Security numbers
- Trade secrets, corporate information, or software source code

When a shopping website gets hacked, it loses sales and customers, but the company also has to spend money to recover from the cybercrime. They need to:

- Research and fix the problem with their computers
- Notify customers, shareholders, and other stakeholders
- Create public relations campaigns to regain customers' trust
- Pay to have customers' credit cards reissued, repair stolen identities, or monitor their credit scores

Companies that experience a data breach can see their stock prices drop. The confidence in their brand name can also take a big hit for years after the event. That means that, even after the security problem is solved, customers may not return because they don't trust the company anymore.

Solving a cybercrime and recovering from it are very expensive. It's better to prevent these crimes from happening in the first place by having a strong cybersecurity system.

STEP

5 Play a life-sized version of Minesweeper

Protecting your organization from cybercrime is like playing Minesweeper. Your goal is to keep your computers and data safe so your organization can accomplish its goals.

You create "defenses" for your computer systems, such as training your employees about cybersecurity, backing up your data, and hiring white hat hackers to look for weakness. At the same time, black hat hackers are looking for the same weaknesses in your cybersecurity system, so they can break into your computers. They place "mines" like phishing or spoofing emails, or they take advantage of out-of-date software that can be more easily hacked.

If you can help your organization do its job without getting hacked by avoiding the hackers' "mines," you and your organization win!

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

- Creating an escape room to teach others how cybersecurity experts investigate hacks.
- Researching careers in cybersecurity investigation and sharing what I've learned with other students.
- Organizing a workshop to teach others how to run traceroutes.

I'm inspired to:

Made possible with a generous grant from Palo Alto Networks.

First published in 2019 by Girl Scouts of the United States of America

420 Fifth Avenue, New York, NY 10018-2798
www.girlscouts.org

UPC 64071

7 31955 64071 2