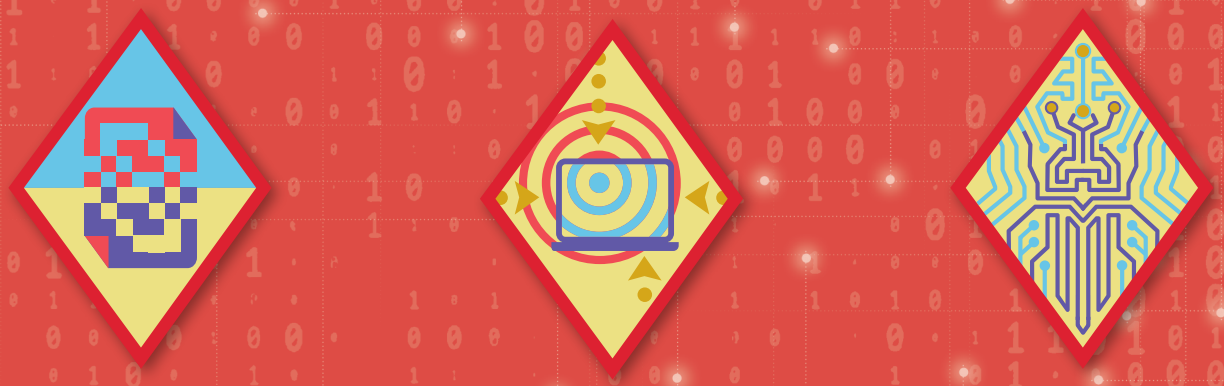


Cadette Cybersecurity

Learn ways to protect your data and how cybercrime is investigated and prevented.

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 Cadette 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.

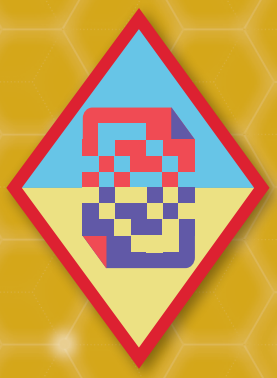
Welcome to the fast-paced world of cybersecurity.

"Cyber" means things related to computers, information technology, and virtual reality. "Security" means being free from danger or threat, so cybersecurity is all about keeping computers and their data safe.

People use computers in all areas of their lives—learning, shopping, banking, communication, entertainment, and more. Keeping all that information safe is what cybersecurity is all about.

When you've earned these three badges, you'll know how to keep your information safe online and how investigators track down hackers and fight cybercrime.

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



Badge 1: Cybersecurity Basics

The internet lets people all over the world connect with each other and find information easily. That can make life easier, but also riskier. People store a lot of private information on their computers, phones, and tablets. Hackers are always trying new ways to collect our data, so learning how to keep your information safe is an important computer skill.

Steps

1. **Crack a code**
2. **Hack a password**
3. **Explore two-factor authentication**
4. **Launch a Man-in-the-Middle attack**
5. **Explore social engineering**

Purpose

When I've earned this badge, I'll know how hackers steal information online and steps I can take to protect my data.

Is Someone Listening?

As hackers find more and more ways to listen in on phone calls or read texts, computer programmers are creating **end-to-end encryption** programs to keep your conversations and messages private. Some cell phone creators build encryption right into their phones. Apple's iPhones have encryption built into their FaceTime and iMessage programs, and even Apple can't access your information. Some communication apps like WhatsApp or Signal offer end-to-end encryption on calls and texts, but only if the person you're talking or texting with uses the program, too.

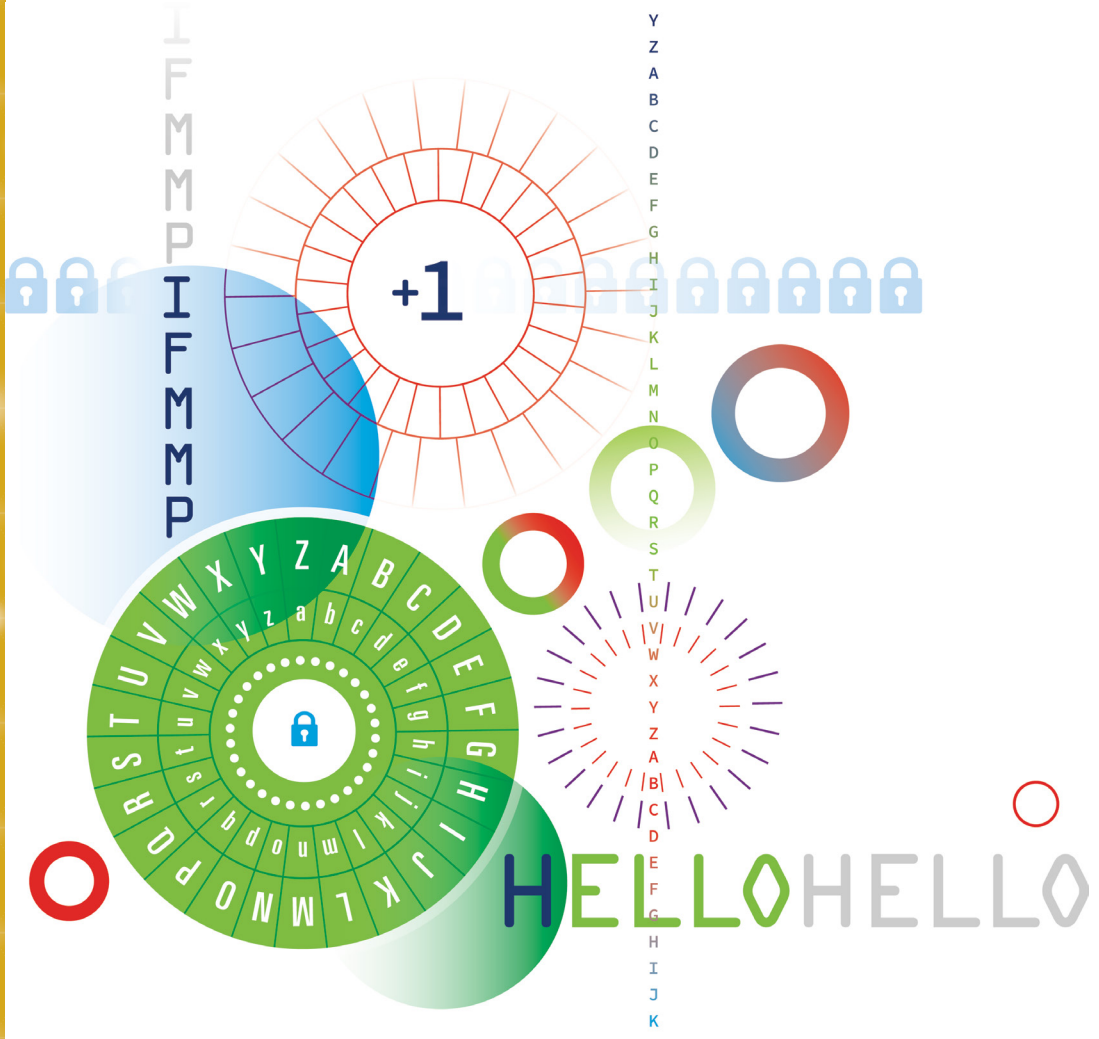
STEP 1

Crack a code

Wouldn't it be fun to have a secret language that only you and your friends knew? You'd have to create your own secret code. **Cryptography** is the process of writing and solving codes.

When you take a message and turn it into a code, you **encrypt** it. When you turn the code back into a readable message, you **decrypt** it. It's easy to decrypt a message, if you have the encryption key that shows how the message was changed to make it unreadable. But if you don't have the key, you have to figure out the code on your own.

Decrypting a code without the key is called cracking a code. When you send a text or an email, your computer or phone automatically encrypts the message, and then the receiving computer or phone decrypts it.



WORDS TO KNOW

Brute force attack when an attacker tries many different passwords in hopes of guessing correctly

Computer network a group of computers—or other digital devices—connected together in some way

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

Dictionary attack when an attacker uses an existing list of words as potential passwords

Digital footprint the information that exists about a person as a result of their online activity

Encryption the process of encoding a message or data so that people need a secret key or password to read it

End-user license agreement (EULA) a contract that gives a user the right to use software

Malware software that aims to cause damage to your computer or network

Man-in-the-Middle a type of cyberattack in which a hacker intercepts a message between two entities in order to spy on them or steal their information

Metadata data that describe or define another piece of data

Nodes as packets of data travel through a computer network, they stop at many different "nodes" along the way

Packet when you send a message, or submit information, through the internet, your message is broken up into smaller packets of data

Personally identifiable information any information that can be used to identify, contact, or locate an individual

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

SMSing a type of cyberattack in which a hacker sends a text message in order to try and steal your personal information

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

Spoofing a type of cyberattack in which a hacker pretends to be someone you know, or an organization you trust, in order to gain access to your information

Spyware software that secretly collects information about you

Two-factor authentication an extra layer of cybersecurity that requires two different types of validation (like a username/password AND a unique code sent to your phone) before allowing access

STEP
2 Hack a password

Every time you set up an account on your computer or phone, you have to create a password. An account is just a way for the website or app you are using to know who you are. If you have email, keep or turn in school work online, or play online video games, you have created an account.

It can be hard to come up with a new password for every new account, so sometimes people use the same password for lots of their accounts. That's a bad idea. So is having a short password or one without numbers, upper and lowercase characters, or special characters. Why? Because a simple password is easier to guess. If someone wants to get into your account without your permission, you want it to be hard for them to guess your password.

M1X !T / UP

To make a really strong password, you need to get creative. Here's why: Hackers have programs that can run through dictionaries with lightning speed. They can identify millions of passwords in minutes. Then they use another program to try all these passwords to hack into people's accounts. Hackers also have programs to search books, movie scripts, and song lyrics (like they do with dictionaries) to look for passwords, so don't use your a line from your favorite song or movie! They can even scan social media sites to get clues to people's passwords, like their birthdays or pet's name. So don't use your birthday or your pet's name as your password!

Because hackers expect people to follow grammar rules for capitalizing letters, the strongest passwords have numbers, special characters, and uppercase letters in unusual places.

- **The longer the password the better.** Some experts suggest 12 characters long. It takes a hacker's program longer to guess a long password than a short one.
- **Don't use numbers or symbols as obvious substitutions.** For example, !L0Vecat$ would be easy to crack because ! looks like I, 0 looks like o and $ looks like s.
- **You can use capital letters, numbers, and special characters in random ways to make a strong password.** If you wanted to use your troop number in your password, you could write grLsCttRP#2961 for Girl Scout Troop 2961.
- **Some experts suggest choosing four random, unusual words that make no sense together, like tunaFlipflopsnoreSHINY.** This is called a passphrase. Even though it doesn't have numbers or special characters, and the words are from the dictionary, the random combination of the words and the length of the password make it a strong password, and it may be easier to remember than one with random letters, numbers, and characters.

STEP
3 Explore two-factor authentication

Some computer security systems use something called two-factor authentication. That means that the person wanting to get into the account must have two things to prove they should have access.

For example, if you've ever had to be picked up at school by a grown-up, you know about two-factor authentication. Most schools use two-factor authentication to make sure the grown-up is allowed to pick up the student. First, the grown-up has to show a photo ID, like a driver's license. The school checks to make sure the person matches the person on the ID. Then the school also checks the form that your parent or guardian completed at the beginning of the year listing who is allowed to pick you up. If that person isn't on the list, the school will call your parent to make sure it's ok. The photo ID and the list are the two factors.

In the computer world, sometimes you need both a password and a special number code that gets sent to your cell phone to get into a computer account. A special algorithm creates a new number code every time you log in. That code is a kind of number puzzle. If hackers want to get into an account with two-factor authentication, they have to figure out what the number code is, but it changes all the time. That's a tricky puzzle to solve.

Better Safe Than Sorry

Because passwords can be easy to hack, cybersecurity specialists have added more layers to get into an account beyond your username and password. This is called multi-factor authentication. Some send a randomly generated code to your cell phone, some ask for a fingerprint or scan your eye, and some have an actual physical "key" that looks like a USB stick or flash drive.

ARE YOU A GOOD HACKER OR A BAD HACKER?

Sometimes the word "hacker" makes people think "criminal." But the term "computer hacking" doesn't mean breaking the law or hurting people. It just means changing code.

- Schools and clubs hold **"hackathons"** where people get together and design or improve programs and apps. The hackathons are usually focused on meeting a need or solving a problem. Sometimes companies hire hackers to help them find weaknesses in their security measures. These people are **white hat hackers**. They hack for good.
- When people use their computer knowledge to break into private accounts and steal information or money, they are criminals. The computer world calls these people **black hat hackers.** (White hat hackers try to help others find weaknesses in their computer security systems before black hat hackers can.)
- There are even **gray hat hackers** who look for weaknesses in computer security systems without permission from the business or organization. When they find a weakness, they tell the organization about it. They also ask for money because they found the weakness before black hat hackers did. They are called gray hat hackers because hacking into someone's account without their permission is illegal, but the hackers don't use the information to steal from the organization.

STEP 4

Launch a Man-in-the-Middle attack

Have you ever played Keep Away or Monkey in the Middle? It's a game where players try to throw a ball to each other while trying to keep one player from catching it. The player, or monkey, in the middle tries to intercept the ball as it's being thrown from one person to another.

Computer hackers try to do the same thing with information you send through the internet. They try to intercept your information as it travels from your computer or phone to its destination.

This kind of hacking is called a **Man-in-the-Middle attack**. The best way to keep a hacker from stealing your information while it's on the way to its destination is to be sure you're using a secure internet server. A secure server is one that isn't open to everyone. To use it, you have to have a password, and it limits what others can intercept when you are online.

STEP 5

Explore social engineering

Social engineering is a cyberattack strategy that attempts to manipulate or deceive a user so that they give up their personal information. If it sounds too good to be true, it probably is!

No matter what your hobbies or interests are, scammers have developed many different techniques to get you to click on their link and/or send them money:

- **Beware of any kind of prize if you must send money to claim it.**
- **Similarly, there are certain scams that take advantage of your creative talents and aspirations: for example, art and writing contests that require you to send money if you want your work to be published; modeling and acting agencies that promise to take headshots for you but never do.**
- **And if you're planning to attend college and searching for financial aid, be on the lookout for scholarship search sites that require you to pay a fee; most legitimate sites make this information available for free.**

Before you click, do your homework. If an organization contacts you via email, phone, or online ads, research it before you do anything else. Find out if the organization is legitimate and whether what it is asking for is normal for that industry. The Better Business Bureau (BBB) is a good place to begin your research. And if you do fall victim to a scam, you can report it to the BBB as well.

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

- Holding a "Safe and Strong Passwords" workshop at a library or community center.
- Doing a school presentation about protecting personal data online.
- Creating a book display with a cybersecurity theme at my school or public library during October (National Cybersecurity Awareness Month).

I'm inspired to:

Badge 2: Cybersecurity Safeguards

Every time you do something on a computer or other digital device, that device—and the app, website, or social media program you're using—collects and keeps information about you and what you're doing. It's important to keep that information private because hackers can use it to steal your identity. Learn how computers and programs collect information about you and how to protect it.

Steps

1. **Guard your identity**
2. **Create a profile based on your interests**
3. **Learn about metadata**
4. **Shop for apps in a life-sized app store**
5. **Inventory your digital presence**

Purpose

When I've earned this badge, I'll understand how computers and apps gather data about me and how I can control and protect that data.

STEP

1 Guard your identity

Your personally identifiable information (PII) includes any information that can be used to identify, contact, or locate you—like your name, birthday, address, social security number, and email address or password. You should never share identifiable information with someone you don't know online.

However, even if you only share non-identifying information, all of the things you share can sometimes be combined to identify you! In order to keep your identity private online, you need to be careful about both WHAT you share and HOW MUCH you share.

SEEING IS BELIEVING... OR IS IT?

When is a photograph not a photograph? Photos and videos on computers and other digital devices are bits of data that can be altered. Sometimes you change the photo yourself, adding a filter or changing the lighting. Sometimes your phone changes it for you, without your knowing.

When you take a selfie or a picture of someone else on your phone, you think it's just that: one picture. In fact, some photo apps take many pictures, blend them together, and touch them up to create the final picture you see. It's not actually one photo you took, but a processed image created by a computer program. In some cases, you have to turn on "beauty mode" in your photo app. In other cases, the algorithm to synthesize and touch up your photos is the default setting on the phone's photo app.

Changing what people see isn't limited to photos. Some folks use artificial intelligence programs to alter real video footage. They make it look like people have been filmed doing or saying things they haven't done or said. These videos are called **"deepfakes."** Some of them are just silly, like replacing one actor's face with another in a movie clip. Some have been used to create fake news, though, like video clips of leaders saying things they've never really said.

STEP

2 Create a profile based on your interests

Pretend that you've just met someone new at school. You're asking each other questions to learn more about each other. Here are some questions you might ask:

- How old are you?
- Where do you live?
- Where do you go to school?
- Do you have brothers or sisters? How many? How old are they?
- Who is your favorite musician or author?
- What is your favorite TV show or movie?
- Do you play sports or an instrument?
- Do you take ballet or act in school plays?
- Where have you traveled?

All your answers add up to a description of who you are. It makes sense that a friend would know these things about you, but what about a stranger? That might not be as safe.

Strangers can find out all kinds of information about you online. Everything you do, from internet searches to online shopping to social media posts, leaves a trail of information. That trail is your **digital footprint**.

Companies that want you to buy their products will track the websites you visit, so they can send you ads. Hackers can learn about you, too, and use that information to trick you. For example, they may send you an email that looks like it came from your favorite shopping website. They'll tell you about a great sale and ask you to click on a button. But, when you do, the hackers might send a virus to your computer.

STEP

3 Learn about metadata

Every time you send an email, text a friend, create a document, or take a photo, your digital device collects data about what you've done. This includes information that identifies your smartphone or tablet and when and where you were when you emailed, texted, or took a photo of your dog.

All that information is called **metadata**. It's information about your information. If you know what to look for, you can find out a lot about someone by examining their metadata. Hackers know that—but you can stop them from knowing all about you by protecting your data.

HOW TO READ A USER AGREEMENT

A user agreement tells you what rights you have and what rights you are giving up when you use an app.

- **Look at the printer-friendly version.** The type will be a little bigger on your screen. That makes it easier to read than the regular version that makes you scroll and scroll and scroll to get to the end.
- **Look for section headings in bold.** This lets you find the important sections, like the ones on privacy.
- **Look for sections in ALL CAPS.** They will have important information.
- **Use a search function on your computer to look for specific words in the document.**
  - "Privacy" and "data" are good words to search for.
  - "Arbitration" will tell you what kinds of rights you have if you have a disagreement with the app company.
  - "Waivers and releases" will talk about what rights you're giving up, like possibly the right to sue the app company.
  - "Opt out" will tell you if you have the option to opt out of any of their requirements. That means you might be able to tell them you don't want them to share your data or have access to your contacts or photos.
  - "Content" will talk about what the app can do with your content, like posts on social media, and what your rights to your content are.
- **Look up words you don't understand.** User agreements use difficult words on purpose. Your dictionary is your friend!

STEP 4

Shop for apps in a life-sized app store

How do you choose an app to download? Do you ask friends what they like? Do you read ads for them in social media? Do you browse through Google Play Store?

No matter what app you choose, you usually have to click a box that says you have agreed to the **"terms of use"** or "user agreement." These user agreements tell you what the app company can do with your data and the rules you have to follow when you use the app. If you want to use an app, you have to click a box that says you agree with everything the user agreement says.

Most people just click the box without reading the user agreement. User agreements tend to be very long and hard to read. But guess what—by clicking "I agree," you're actually signing a contract! For example, you may be giving an app permission to access your contacts, location, photos, and more.

What would you do to make user agreements better or easier to understand?

STEP 5

Inventory your digital presence

The internet is a powerful tool! You can chat with friends, research school projects, play games, watch videos, or listen to music. The downside is that you leave information about yourself with every screen tap and click of the mouse. Some programs, like social media, allow you to share personal information, but every program or app you use collects data and metadata about you. It's a good idea to think carefully about the kind of information you are sharing every time you visit a website or use an app.

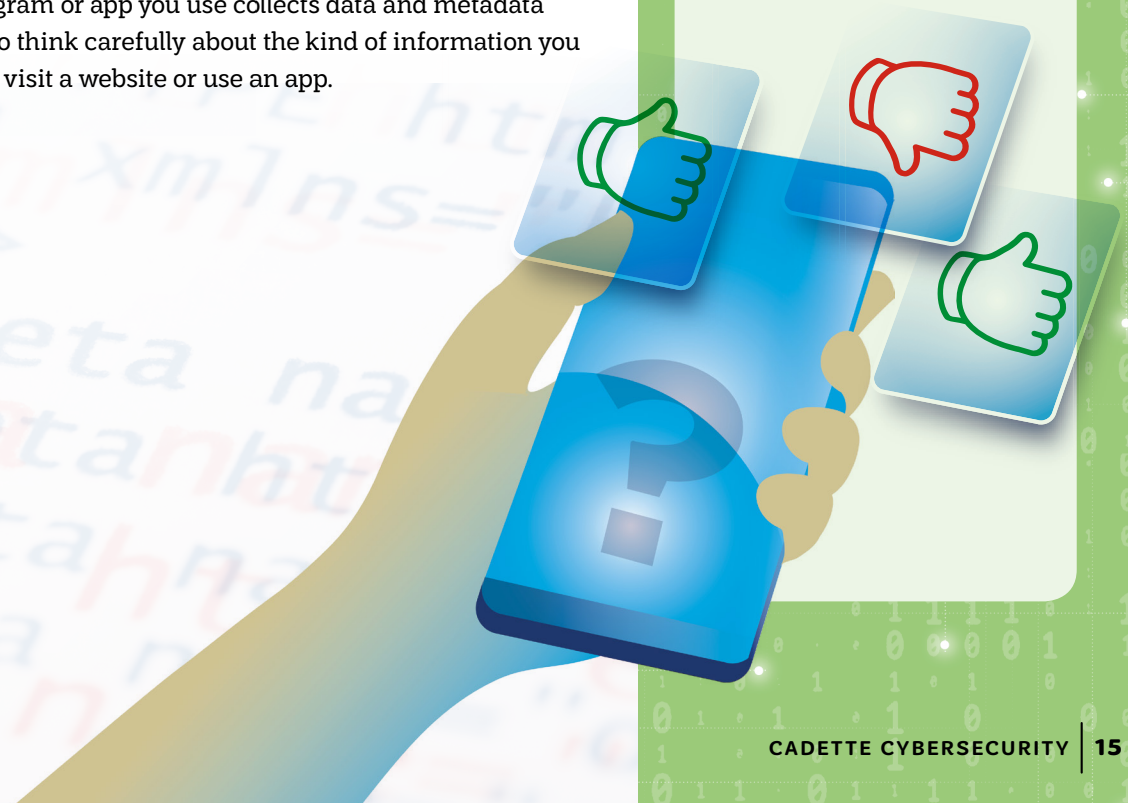
Unfriendly Apps

Have you ever wondered why some apps are free and others aren't?

Think about it: if an app is free, how does the business that made the app make money?

In some cases, the business sell ads to other companies. Those ads pop up while you're using the app. In other cases, the business collects and sells your data to other companies. They use it to figure out if you might want to buy their product.

Cybersecurity experts have noticed that some free apps encourage kids to click links or download games—and that click or download could help hackers break into their devices.



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

- Helping friends to turn off metadata and location services on their devices.
- Rewriting a EULA for a popular app in plain language so others can understand what could happen with their data.
- Teaching others about their digital footprint and how to keep their personal information safe.

I'm inspired to:

Badge 3: Cybersecurity Investigator

Detectives use clues to solve crimes. Cyberinvestigators also use clues to solve cybercrimes, such as stealing people's credit card information or making websites crash. If you know what to look for, you can find clues about hackers and what they are up to. Use what you've learned about cybersecurity to solve some cybercrimes!

Steps

1. **Find clues in text messages**
2. **Identify phishing emails**
3. **Learn how hackers use social media**
4. **Analyze log files**
5. **Protect your identity from hackers**

Purpose

When I've earned this badge, I'll know about skills cyberinvestigators use and ways to prevent cybercrimes from happening.

STEP 1

Find clues in text messages

Text messaging apps sometimes keep your old messages. That can be handy if you want to remember a conversation or share some information in a text with someone else.

Cyberinvestigators look at texts and emails to find clues to solve a hacking mystery. What kind of words would you look for in texts or emails if you were trying to solve a cybercrime?

STEP 2

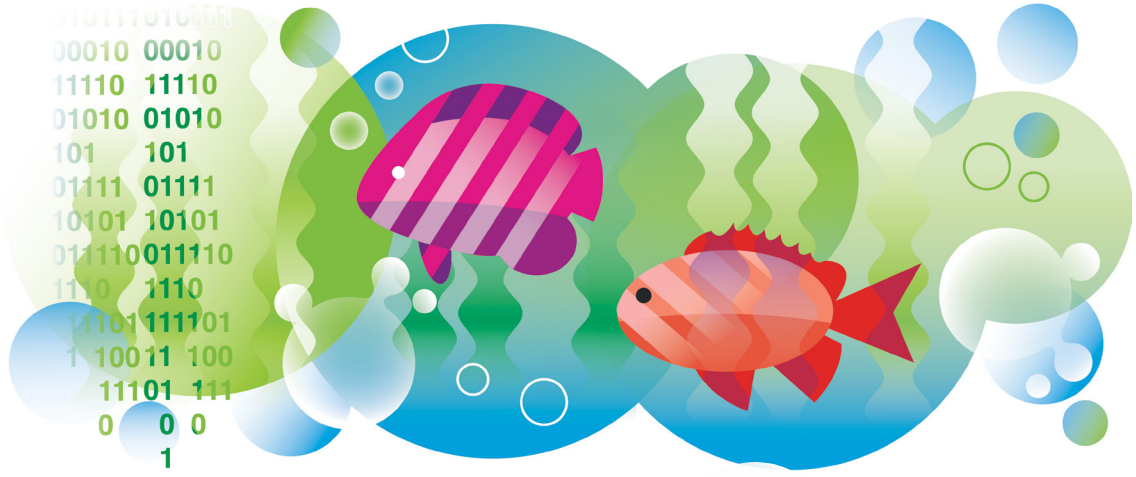
Identify phishing emails

Hackers try to trick people into giving out private information. One way they do this is by sending emails with bad links or harmful attachments, or emails that ask for money. This kind of email is called **phishing**. Sometimes the phishing emails pretend to come from a website you've visited, like a site where you've purchased something or downloaded information.

SOMETHING PHISHY

In 1996, hackers stole passwords and accounts from America Online with fake emails asking for information. Hackers called the scam phishing because it was kind of like fishing. They lured people with the fake email, and some of them "took the bait," like a fish does. This was the one of the times people used the term "phishing." Learn how to spot "phishy" emails and avoid them! Here are common ways hackers phish for information:

- **Sending you an email from a website you use, asking you to confirm your personal information, like your login and password.** The real website or business wouldn't ask you for this information. Take a look at the sender's email address. It's probably just a little bit different from the company's official email address.
- **Changing the web address—just a little bit—of a website you know and trust.** For example, girlscouts.org is the correct web address. A hacker might change it to girlsscouts.com or girlscout.org. If you are suspicious of a link, you can hover your cursor over it, but don't click. It will show you the URL or web address where you would go if you clicked. Look at it carefully. It's probably a fake.
- **Emails with poor spelling and grammar.** A real email from a website you use wouldn't have lots of spelling or grammar mistakes. It's also likely that they wouldn't just say "Dear Customer."
- **Emails written to make you think there's an emergency or that you can get free money.** If the email says "URGENT Action Required" or threatens to close your account if you don't respond, it's probably a scam. So are any emails that ask you for money or information, but promise you'll get lots of money in return.



STEP
3 Learn how hackers use social media

When you post updates on social media, you share information about where you are and what you like to do. You might mention your birthday. Some people make a big mistake—they list where they go to school or where they live! Hackers can piece together all this information and use it to steal your identity.

Think carefully about what you post on social media and who you accept as friends. Don't accept friend requests from people you don't know. They may be hackers trying to gather your personal information. Remember when you are posting on social media that hackers may be watching, so don't post personal information that could help them steal your identity or figure out your passwords.

JOIN THE CYBERCRIME-FIGHTING TEAM!

Cyberinvestigators combine law enforcement and tech knowledge to solve crimes. They may work with **forensic experts,** who piece together data from computers and networks to find the criminals.

Cryptographers write the encryption programs companies use to protect their data.

Penetration testers and **ethical hackers** try to break into secure computer programs and sites to find weaknesses. Penetration testers typically work directly for the company. Ethical hackers tend to work for consulting companies who provide cybersecurity services to lots of businesses and organizations.

Security architects design cybersecurity systems. They test a company's security plan to look for weaknesses. Then they create a plan to make the computer systems more secure.

Threat hunters do the same thing as penetration testers and ethical hackers, but they look for threats happening in real time. They monitor a company's computer systems to watch for signs that someone is trying to hack in. They are kind of like watchdogs that are always checking for intruders and bark as soon as they sense a threat.

Where's My Phone?

Geolocation is the process cell phone companies use to know the location of your devices.

Telecom companies need to know where you are to connect your call. Your phone is always sending out a signal to find the nearest cell towers. When the phone finds a tower, it sends a signal through that tower to the phone company. Then when you get a call or text, the cell phone provider knows where to send it.

But other companies can buy that information, and sometimes your location is sold to companies that use it without your permission. They might use it to send you location-related ads you don't want to see or hackers may use the information to know when your house is empty so it is easier to rob.

STEP 4

Analyze log files

Computers collect metadata. Those are details about what you do online or on a specific computer.

Cyberinvestigators look at metadata called computer **log files** to help them track down cybercriminals. Log files contain information about all the tasks or operations a computer does. They keep track of what operations were done on which computer, when, and by whom. Places with lots of computers, like libraries, schools, or businesses, have very long log files, because they track everything that happens on every computer.

STEP 5

Protect your identity from hackers

Hackers make trouble in lots of ways.

- **They crack people's passwords and steal credit card numbers.**
- **They send phishy emails that get you to give them personal information or to download malware.**
- **They get personal information about people from emails, texts, and social media posts.**
- **They secretly install software on computers to spy on people or damage their computers.**

What can you do to defend yourself from cyberattacks? The first step is to think carefully about what you do online and who you share information with, both online and off.

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

- Making a video for my school or library computer labs with tips for how to spot phishing emails.
- Creating a presentation about how to stay safe on social media.
- Teaching others how to keep their accounts secure.

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 64067
7 31955 64067 5