

# Badge 3: Cybersecurity Investigator

**D**etectives 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

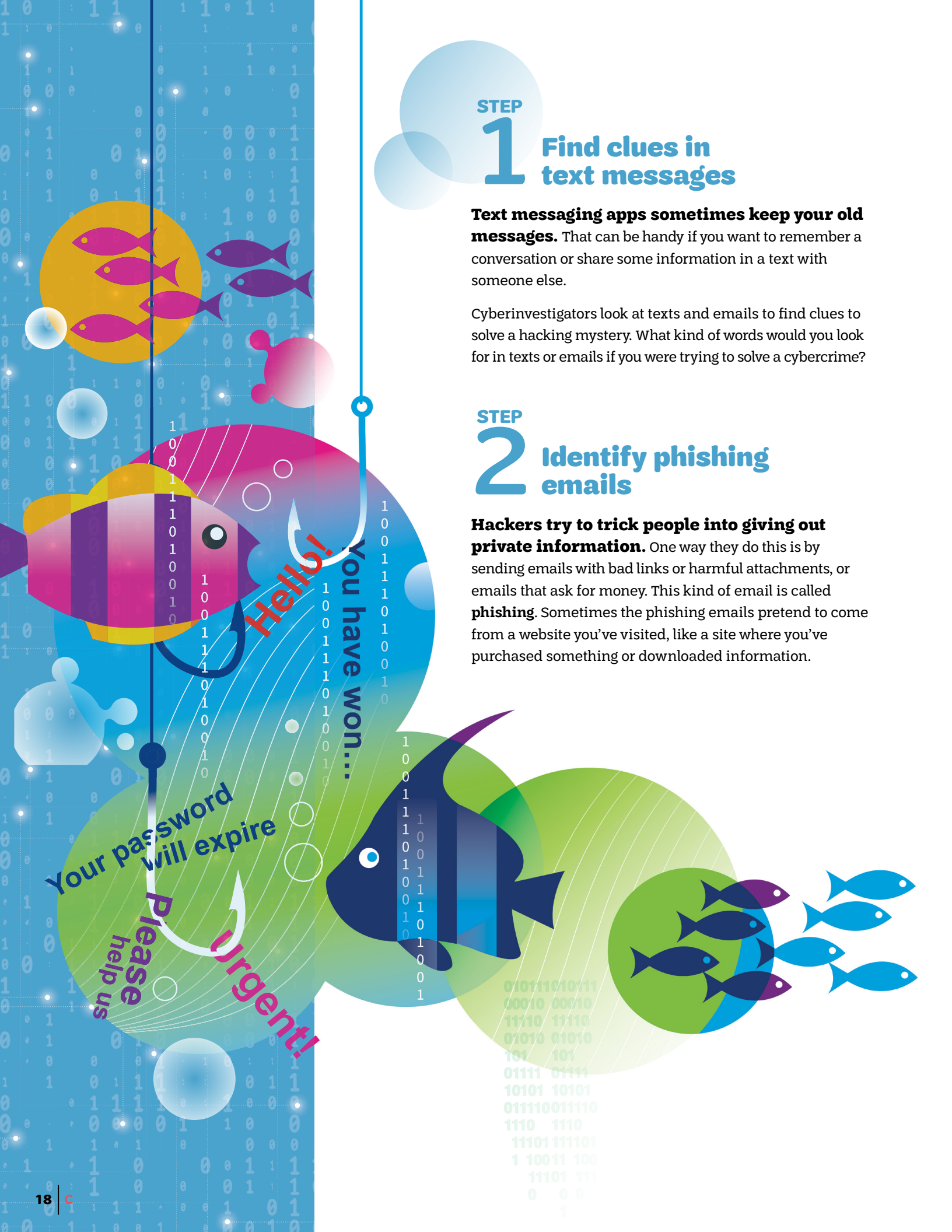
**Text messaging apps sometimes keep your old messages.** That can be handy if you want to remember a conversation or share some information in a text with someone else.

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

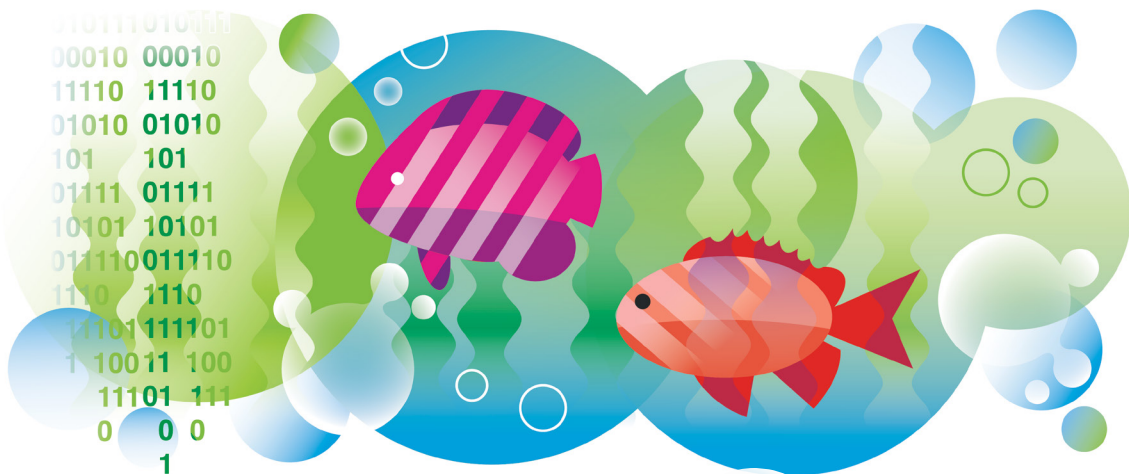
**Hackers try to trick people into giving out private information.** One way they do this is by sending emails with bad links or harmful attachments, or emails that ask for money. This kind of email is called **phishing**. Sometimes the phishing emails pretend to come from a website you've visited, like 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](https://www.girlscouts.org) is the correct web address. A hacker might change it to [girlsscouts.com](https://www.girlsscouts.com) or [girlscout.org](https://www.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.

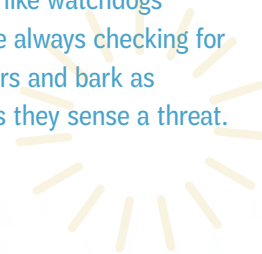
## **Penetration testers**

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:**