Badge 3: Cybersecurity Investigator

Cybersecurity investigators use their knowledge of technology, computer programming, and law enforcement techniques to solve all kinds of cybercrimes. Like police detectives, they look for clues to figure out how cybercrimes are committed and by whom. Every time they solve a crime, cyberinvestigators learn something useful to fight hackers in the future.

Steps

1. **Determine how the attack has affected the city**
2. **Identify suspects**
3. **Decide whether to pay the ransom**
4. **Figure out how the attack happened**
5. **Learn how to prevent future attacks**

Purpose

When I've earned this badge, I'll know how a city responds to a cyberattack and strategies it can use to prevent them.

STEP 1 Determine how a hack has affected the city

Many government services need computers to run effectively. If a hacker shut down a city's computer system, it could cause all kinds of problems.

- Stoplights could stop working
- Police and firefighter communication could be interrupted
- People could be unable to conduct city business, like paying parking tickets or taxes online
- City courts would have to use paper forms to process all trials and proceedings
- Computers that monitor water safety might stop working

CITIES THAT PROTECT YOUR DATA

Cities collect a lot of data about their residents. They have personal information about you if you pay taxes or have city-supported trash or recycling collection. If you use any of their online services to register for a class through the parks and recreation department or to check out e-books at the library, they have digital information about you, too.

Some cities are pioneers in restricting what happens to data and providing residents with more control over their data.

- Seattle has created a set of privacy principles and has privacy champions who are charged with implementing them. The principles require that the champions publish reports about how well they are doing at protecting people's privacy.
- New York City is focusing on the **Internet of things**, or the IoT. The IoT is the network of things or devices connected to the internet. Right now that means cell phones, tablets, and computers. It also includes coffee makers, thermostats, fitness trackers, or apps that let you turn on the lights in your house from your cell phone. This all can happen because the devices are sending messages through the internet via Wi-Fi. New York City wants to be the most tech-friendly city in the world, and that means creating strict privacy guidelines for the IoT.

STEP 2 Identify suspects

Hackers work in the shadows. They quietly look for ways to sneak in to computer systems or disguise themselves to trick people into giving them valuable information. So how do cybersecurity professionals figure out who the hackers are? They look for digital clues.

Every online action leaves a trail. Sometimes hackers work together to launch an attack. They may communicate with each other online with codes or using steganography. Use what you know about cybersecurity to identify suspects who may have hacked your city.

STEP 3 Decide whether to pay the ransom

When hackers break into systems and shut them down, they might ask for money to turn the computers back on. Whether or not to pay ransom to hackers is a difficult choice.

When a city or organization is hacked, leaders may ask themselves questions like:

- **Does paying ransom to a hacker encourage other hackers to do the same thing?**
- **If you don't pay the ransom, and can't figure out how to get your computer working again, what will the impact of that decision be? Who will suffer and who will benefit?**
- **Would it be worth it to just wait and try to catch the hacker?**

City officials have to take a lot of factors into account when handling a crisis like this. What do you think are the most important factors?

WORDS TO KNOW

Bitcoin an independent digital currency that is used and distributed electronically

Log file a security record of all the security-related events that occur within a given network system

Ransomware a type of malware that denies you access to your data until you pay a ransom

WILL YOUR VOTE COUNT?

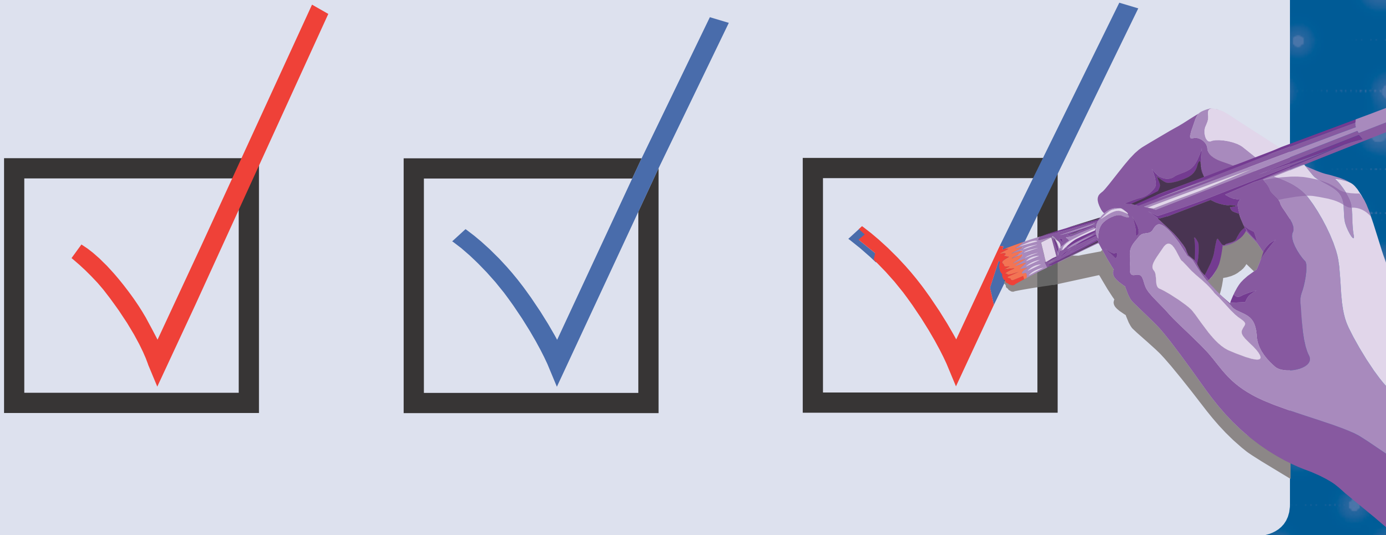
In some places in the world, people voting in elections mark a piece of paper and their votes are counted by hand. In other places, people vote on machines that may be mechanical or electronic. However, the internet has made protecting free and fair elections more complicated.

- Computer databases with voter registration data can be hacked by adding, deleting, or changing information.
- Fake social media accounts can try to influence people to vote in a particular way. For example, Russia created several fake social media accounts, posing as Americans, to try to influence the 2016 presidential election.
- Electronic voting machines can be hacked to break down or change the vote tally.
- Candidates' computers can be hacked and their information used by opponents or distributed to discredit them. Russian military officers were charged with breaking into the Democratic National Committees' computers and stealing information about the 2016 election.

To address these issues:

- Social media platforms, like Facebook, are working to identify and delete fake accounts.
- Computer security experts and professors from universities are working to create more secure electronic voting machines. These machines would create a paper trail. Each voter would get a paper receipt of their vote and the system would create a paper record that can be checked against the electronic results.

What kinds of cybersecurity safeguards and strategies could be used to make voting more secure?



DOES SOMETHING SEEM FISHY?

Phishing is a method hackers use to try to get you to give up personal information or accidently download malware or viruses. Hackers usually send out emails to lots and lots of people or embed bad links in apps hoping someone will “take the bait.”

Spear-phishing is when hackers try to get people to give them access to information or computer accounts, but they’re targeting just one specific person or a small group of people. For example, a hacker might email a specific company employee pretending to be the boss. The “boss” would ask the employee to transfer money to an account or send copies of company trade secrets. The employee thinks the email is real and does what is requested.

Catfishing is when someone creates a false identity on social media sites such as Facebook, Instagram, or dating sites. If you think someone’s page is too good to be true, it might be. Watch out for outrageous claims (I’m a supermodel!) or requests for money. If you’re suspicious, google their name or fact-check their bio. Reverse search their images to see if the same photo with someone else’s name comes up. You might be surprised what you find.

STEP 4 Figure out how the attack happened

To solve a crime, you have to look for clues. Fortunately, computers leave lots of clues because they document the time, location, and identity of everything a person does online. Every time you log in, send a message, or access a website, a record of your actions is created.

The tricky part is being able to find the actions of the hacker buried in the records of all the transactions that happened. The chances of finding these clues are slim unless you know what to look for. Cyberinvestigators and digital forensics experts know what a hacker's digital footprints look like and can follow them to track down the hacker.

STEP 5 Learn how to prevent future attacks

The best way to handle a cybersecurity crisis is to prevent it from happening in the first place. Cybersecurity professionals have identified many ways to protect digital devices and systems from attack, but some of them can be very expensive. Big companies might have a lot of money to spend on cybersecurity strategies, but local governments, smaller businesses, nonprofit organizations, and individuals will have to make tough choices about which security measures to use.

Which cybersecurity strategies do you think are the best ones? Which ones are the most affordable? What priorities should people use to choose their cybersecurity strategies?

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

- Organizing a mentoring event with female cybersecurity professionals sharing their experiences with my council.
- Creating a Bring-Your-Own-Device (BYOD) workshop in my school's computer lab to teach other students how to make their tech devices more secure.
- Interviewing local officials about my town's cybersecurity policies to share with others how cities work to protect their citizens' data.

I'm inspired to: