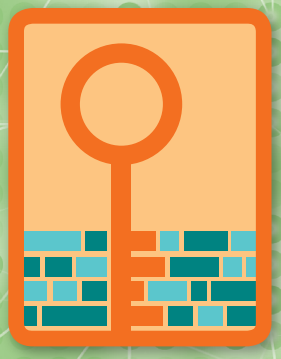


Badge 2: Cybersecurity Safeguards

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.

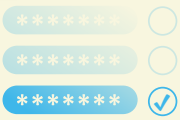
Some cell phones or apps are more secure than others. FaceTime, iMessage, WhatsApp, and Signal are examples of apps with **end-to-end encryption programs**, where your conversations and messages are encrypted throughout the entire transmission process. However, some of these programs only guarantee your 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.

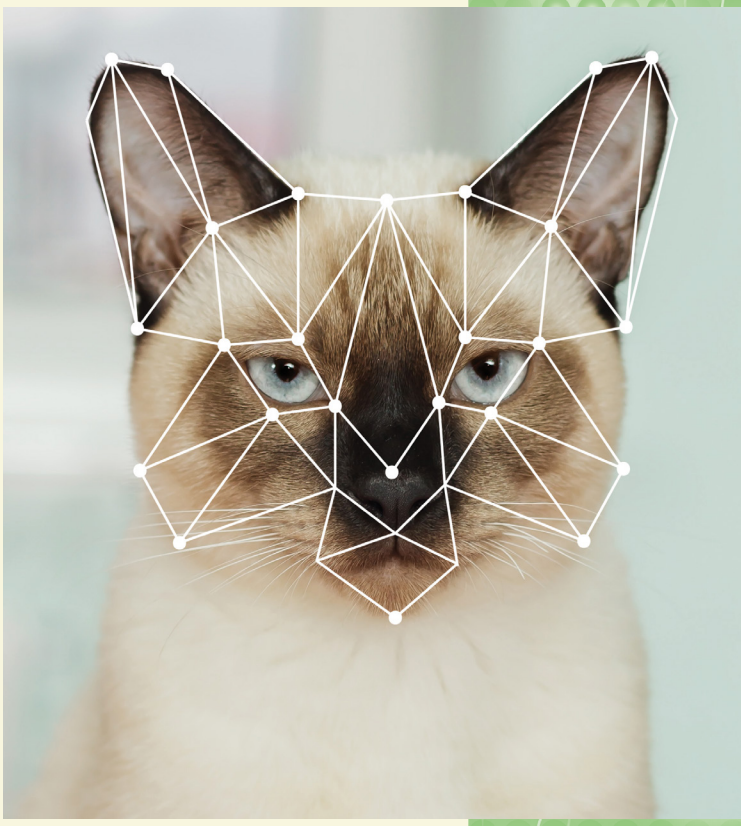
Smart speakers, like Alexa, are supposed to listen to your conversation so they know when you're asking them a question or giving a command. Sometimes, though, a smart speaker can misunderstand a conversation and record or transmit conversations that people meant to be private.

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: