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.

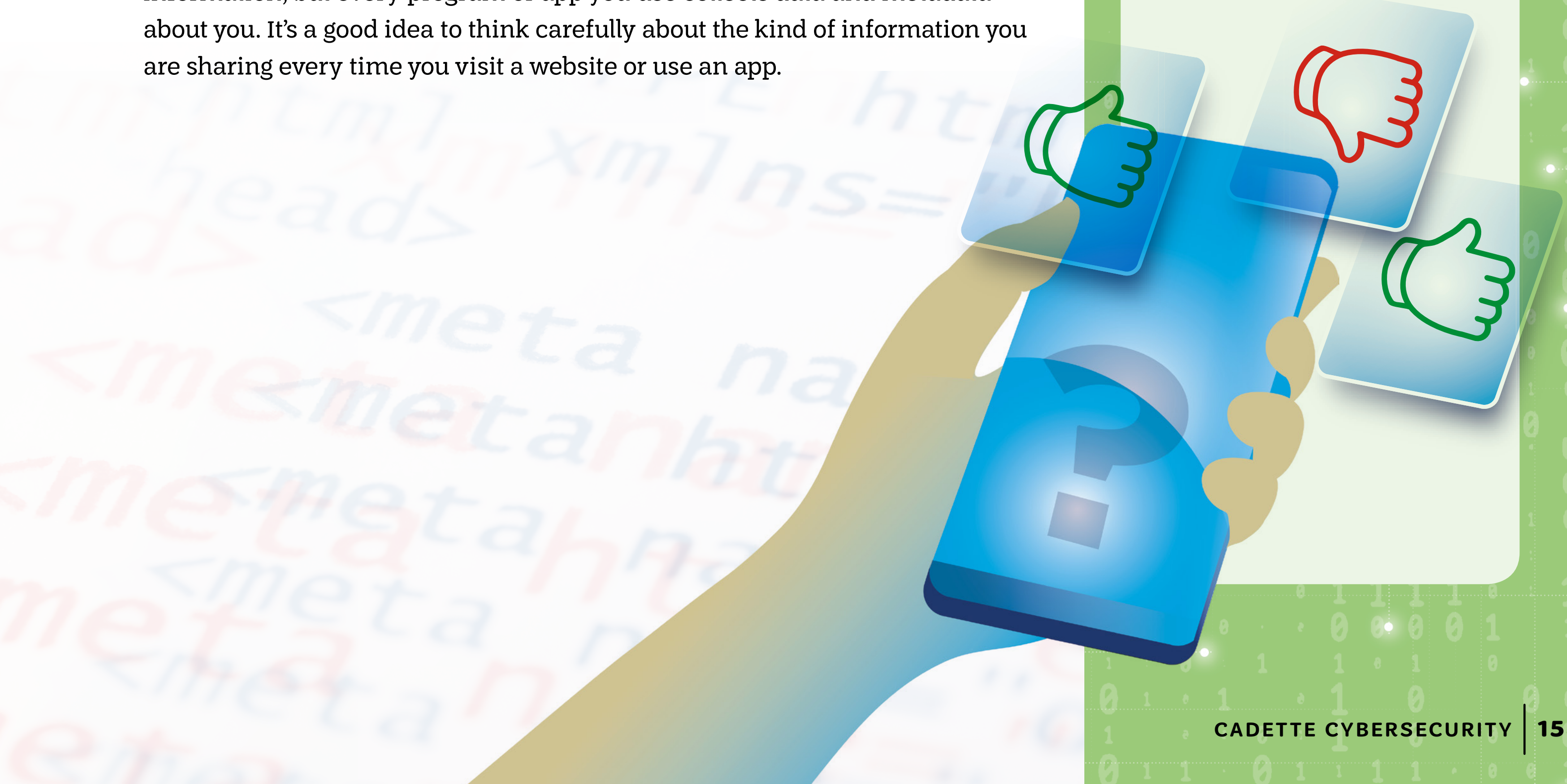
Unfriendly Apps

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: