Badge 2: Cybersecurity Safeguards

Who knows what you're up to? Your school keeps track of your grades and attendance, your doctor keeps track of your medicines and any illnesses you've had, and your parents probably keep track of who you spend your time with. That seems pretty normal.

But how would it feel if someone gathered information about you without your knowing? People interested in you or your data can find out a lot about you by looking at what you do online—your digital footprint. Learn how you create a digital footprint and how to guard your personal information from hackers.

Steps

1. **Guard your movements**
2. **Outsmart the online marketers**
3. **Plan your digital future**
4. **Take the rights steps to secure your data**
5. **Make cyberhygiene go viral**

Purpose

When I've earned this badge, I'll know how digital footprints track my online activities and steps I can take to protect my personal data.

STEP 1 Guard your movements

Who knows where you were yesterday? Probably your parents, teachers, coaches, and friends, right? But a hacker might know too. Everything you do online leaves a trail—a digital footprint. Just like a detective, a savvy hacker can piece together a lot of information about you by following your footprints. For example, posting on social media or using location services can give hackers enough information to figure out even more personal information like where you live or where you have a bank account.

Your personal data may be vulnerable to cyberattack if you aren't very careful about how you use digital devices like phones, tablets, and computers. Think about what you do every day and how your personal information might be vulnerable because of your actions.

What you do offline may impact your cybersecurity, too. Telling a friend your password, losing your driver's license, or throwing old boarding passes in the trash makes your personal information vulnerable.

How can you balance living in a digital world with safeguarding your privacy and personal information?

WORDS TO KNOW

Cookie a small data packet that websites can store on your device in order to collect information

Cyberhygiene the regular habits that computer users can take to improve their cybersecurity

Cyberstalking the use of the internet or other digital technology to stalk or harass an individual, group, or organization

Data vulnerability a weakness that leaves one's data open to a cyberattack

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

Identity theft a type of crime in which someone uses your personal information without your permission

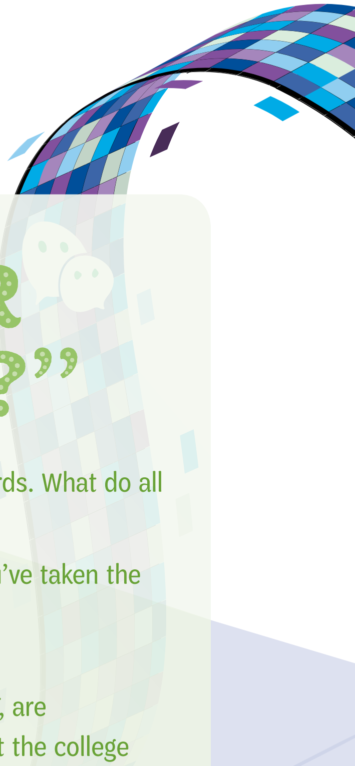
Personally identifiable information (PII) any information that can be used to identify, contact, or locate an individual, like your name, birthday, address, social security number, and email address or password. You should never share identifiable information with someone you don't know online

Social marketing influencing people to change their behaviors in order to benefit society

STEP 2 Outsmart the online marketers

Have you ever noticed that when you do an internet search for puppy videos that all of a sudden you're seeing ads for dog trainers, puppy chow, and dog-walking services? That's because online marketers use algorithms to track your online behaviors, so they know what to sell you.

Online marketers especially like to market to teenagers. They sometimes even disguise advertisements as games. How does knowing that advertisers are watching what you do online affect the decisions you make when using the internet?



WHO PROTECTS YOUR "PERMANENT RECORD?"

Test scores, vaccination records, home addresses, family members, phone numbers, and discipline records. What do all of these kinds of data have in common?

Schools, both K–12 and colleges and universities, collect and keep this information about students. If you've taken the PSAT or SAT, you've provided a lot of personal information along with your test answers.

- All educational institutions are at high risk for identity theft because they keep so much personal data about their students, and so many different kinds of people (students, parents, faculty, and vendors) use online portals to interact with the school.
- K–12 schools are being targeted by hackers with "ransomware," where they threaten to make data public unless schools pay a ransom.
- Academic services, like the SAT and ACT, are vulnerable to hacking. That could impact the college admissions process.
- Colleges and universities with hospitals and medical records are a favorite target of hackers. Those that do a lot of STEM research are also targets of foreign governments and businesses, to steal discoveries and innovations.

Cybersecurity is expensive, and many schools, both K-12 and higher education institutions, have tight budgets. Because of this, the field of education is very vulnerable to hacking.

STEP

3 Plan your digital future

Five or ten years from now, what do you imagine you'll be doing? Working? Going to college or graduate school? Starting your own company? It's exciting to think about what you might do in the future, but what you do on the internet today can impact your opportunities in the future.

It's not just hackers who look at digital footprints. Colleges, graduate schools, and employers will often do an internet search on a person before offering them a place at their school or a job. Even new friends may do a search. How could what you do online affect how people perceive you in the future?

The High Cost of Education?

College can be expensive, and many students receive scholarships or financial aid. Hackers go after money wherever they can find it, and college students are new targets.

The Department of Education has warned colleges and universities that hackers are sending phishing emails that pretend to be a bill from their school and tricking students into giving them access to their online student portals. Then, the hackers redirect deposits from financial aid providers to another account, stealing financial aid money that is supposed to go to the student!

The Department of Education has advised schools to make sure they use multi-factor identification strategies, like username and password, plus PIN or security questions, to make the portals more secure. They also encourage schools to warn students about phishing emails.

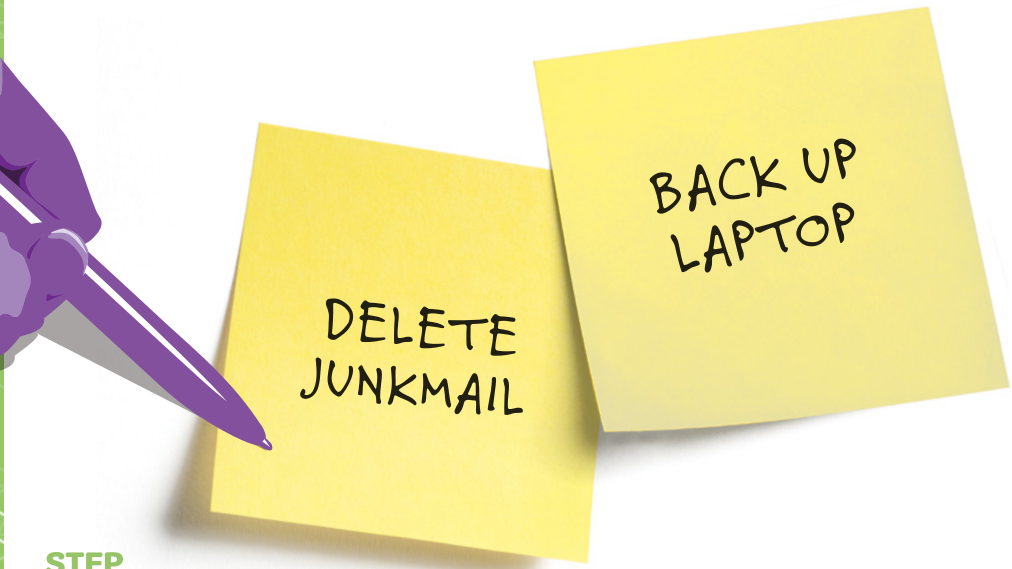
Do you know how to spot a phishing email?

STEP 4 Take the rights steps to secure your data

Keeping yourself healthy has many components. You need to get enough sleep, eat healthy food, and exercise. You also need to brush your teeth, have regular checkups, and wash your hands a lot. Don't forget to wear your seat belt and your bike helmet, too! All of these habits can be considered personal hygiene habits.

There are many different ways to safeguard your personal information online, too. **Cyberhygiene** includes regular steps you can take to protect your cybersecurity. Being thoughtful about how and what you post online is one way to protect your cybersecurity, but others are updating your software, backing up your data, and being wary of strange emails or friend requests from people you don't know.

What steps do you take regularly to protect your data? What steps do you need to add to your cyberhygiene routine?



STEP 5 Make cyberhygiene go viral

Launch your own Cyber Health Campaign! You've examined your own cyberhygiene habits. Now share what you've learned by creating a social marketing campaign to motivate others to do the same.

Just like the signs in restrooms that encourage everyone to wash their hands, raising awareness about safeguarding personal information benefits society by making it harder for hackers to steal information.

What creative ways can you motivate people to update their passwords, turn off their webcams, and use social media wisely? Which cyberhygiene habits do you find the most challenging? How can you encourage others to embrace them? What can you do to make cyberhygiene cool?

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

- Making a video to share my cyberhygiene campaign widely with others.
- Conducting a workshop at a community center to teach others how to keep data and personal information safe.
- Visiting a Cadette or Senior troop and teaching them about digital footprints.

I'm inspired to: