LESSON 1 Understanding Online Safety

Introduce your students to the tools and techniques hackers employ to grab users' information, and then guide them to protect themselves against future attacks.

Objective
Students will analyze text, citing evidence and summarizing central ideas. They will make inferences to create their own cybersecurity protection plan.

Time
45 minutes

Materials
- Copies of *#CyberSmarts* student magazine
- Create Your Online Protection Plan activity sheet

Instructions
1 Ask students what they think cybersecurity might mean and involve. Collect student ideas on the board. Define cybersecurity as the practice of defending computers and servers, mobile devices, electronic systems, networks, and data from malicious attacks. Ask students why they think cybersecurity is important.

2 Prepare students to do a close reading of the article and job profiles in the student magazine by providing them with the following guiding questions:

- Why are cybersecurity professionals necessary in today's world?
- In what ways do people leave themselves vulnerable to being hacked?
- Why is it important to take steps to protect your identity while online?

3 Distribute copies of the student magazine and ask students to use the questions above to focus their reading.

4 Lead a class discussion about how hacking might affect students, asking them to use supporting details from the magazine and specific examples from their lives. Start with: Do you feel that your personal information is secure online?

5 Explain to students that the Children's Online Privacy Protection Act (COPPA) put restrictions in place to protect kids' personal information. Note that COPPA also rules that social media companies cannot allow children under the age of 13 to use their services.

6 Distribute the Create Your Online Protection Plan activity sheet and guide students to refer to the magazine as they complete their plans.

Level the Lesson

Grade 6 Since many sixth-graders may be under 13, use this as an opportunity to broach the subject of social media usage. Survey the class (possibly anonymously) about the apps and sites they use or want to use. Encourage them to have a conversation with their parent(s) or legal guardian(s) about which sites are appropriate to use and ways they can enjoy supervised access.

Name _____

Create Your Online Protection Plan

When it comes to online safety, it's best to think ahead. Use the boxes below to fill in the cyber threats you are most likely to encounter, when you encounter them, and how to protect yourself.

 **Cyber threat to watch for** *Ex: Pop-up ads*	 **I often see this when I'm...** *Ex: Checking text messages*	 **Strategy to protect myself** *Ex: Use antivirus software*

 **Cyber threat to watch for**	 **I often see this when I'm...**	 **Strategy to protect myself**

 **Cyber threat to watch for**	 **I often see this when I'm...**	 **Strategy to protect myself**

LESSON 2 Identifying Preventive Technologies

Inspire your students to explore the unique types of technology that cybersecurity pros use to combat threats and keep us safe.

Objective
Students will synthesize research information to convey technological processes using domain-specific language in an informational presentation.

Time
45 minutes, plus time to develop presentations

Materials
- Know Your Protection activity sheet available at **scholastic.com/cybersmarts**

Instructions
1 Explain what preventive technology is and how it's the first line of defense against cybersecurity threats. Give an example (e.g., antivirus software), then ask students to share others they know of.

2 Provide students with a list of preventive technologies built and used by cybersecurity pros (e.g., firewalls, ad blocker apps, antivirus software, voice recognition software, virtual private network). Explain that different technologies safeguard against different types of threats.

3 Divide students into small groups and assign each group a type of technology to learn more about (or have each group choose one). Download and distribute the Know Your Protection activity sheet. Give them the following research goals:

- Clearly and concisely describe what the technology is and how it works.
- Describe the specific threat(s) this technology protects against and situations when those threats are most likely to occur.
- Give user-oriented tips for how to activate the technology and ensure it's working.

4 Tell students they will present their research in a visual/interactive way. Provide these presentation options:

- **Option 1** Write and perform a skit, acting out a situation where personal data is at risk and how the assigned technology successfully protects the user.
- **Option 2** Write an interview/dialogue between a computer user and the assigned technology. Use role play to have the technology "come to life" and explain to the user how it works to keep people safe.

5 After the presentations, debrief by asking each group to share at least one thing they learned about a technology other than the one they researched.

Name _____

Know Your Protection

Learn the tools cybersecurity experts have developed to make sure you are not a target for hackers.

STEP 1: Choose one cybersecurity tool to research.

_____

_____

STEP 2: Compile research about the tool you selected.

- How does the technology work?

_____

_____

_____

- In what situations are these threats most likely to occur?

_____

_____

_____

- What tips should users follow to activate the technology and ensure it's working?

_____

_____

_____

ACT IT OUT

Bring your research to life by demonstrating how the technology you researched works.

Option 1
Perform a skit, acting out a situation where personal data is at risk and how the technology protects the user.

Option 2
Create an interview/dialogue between a computer user and the assigned technology. Use role-play to have the technology explain to the user how it protects their safety.

LESSON 3 Making Online Profiles More Secure

Inspire your students to explore the cybersecurity strategies that can help thwart threats and keep them safe.

Objective
Students will use analytical and reasoning skills to identify areas of vulnerability in an online profile and come up with strategies for how to make them more secure by applying information from a text.

Time
90 minutes (two class periods)

Materials
- Analyze Your Profile activity sheet
- Find the Security Holes! activity sheet

Instructions

1 Ask students to consider how they behave differently at home, in school, and around strangers. Have them explain why they may be more aware of/adjust their behavior depending on who they are with. Ask students to discuss in pairs why people are cautious around strangers. Have pairs share their discussions with the class.

2 Challenge students to compare being cautious around strangers to their habits on social media (Instagram, game chat, Snapchat, etc.). Ask them if they think their peers actively think about protecting their privacy online. If not, why do they think this is?

3 Ask a few volunteers to describe the purpose of an online profile. Emphasize that while a profile is meant to be public, people often forget that giving the outside world access to personal details can have negative and potentially dangerous consequences.

4 Prompt students to think about types of profile information that might make them vulnerable online. Co-create an anchor chart documenting student responses.

5 Explain that cybersecurity experts analyze how people use information online to identify security weaknesses and develop strategies to protect against potential threats.

6 Distribute the Analyze Your Profile activity sheet. Have students read the information and share what they found most surprising/interesting. Encourage them to use the sheet as a safety tool at home.

7 Distribute the Find the Security Holes! activity sheet. Once students have completed the sheets, review as a class. (Answers: Profile picture should not be a photo of the user—use an avatar or clip art; privacy settings should be "on"; do not use your real full name; birth date should not include year; do not share home or location; do not include school name or other personal details, like phone number.)

Extension

As a culminating project, instruct students to use what they learned to invent their own cybersecurity device. They should detail how it works, what it protects against, and how users can install it on their devices.

Name _____

Take This Home! Use this list to make sure all your profiles are safe.

Analyze Your Profile

Read the checklist below to make sure you aren't leaving yourself vulnerable to a cyberattack. Fill in any extra details you've learned in class or from additional research in the spaces below each set of tips.

STEP 1
These parts of your profile can give away too much private information:

- ☑ **Username** Avoid using any part of your first or last name.
- ☑ **Birthday** Don't post the year you were born—the whole Internet will know your age!
- ☑ **Location** Leave off your street address, town, and school name.
- ☑ **Phone number** Avoid listing your area code in particular; it can reveal your general location and leave you vulnerable to phone scams.
- ☑ _____

_____

STEP 2
Keep your personal information secure/protected from cyberthreats:

- ☑ Make sure your username and password meet maximum security standards.
- ☑ Don't publicly share your birthday.
- ☑ Don't use location tags in social media posts; avoid sharing your location publicly.
- ☑ Avoid saving your password for auto login; avoid staying logged in.
- ☑ _____

_____

STEP 3
Outsmart hackers on the hunt for vulnerable profiles:

- ☑ Check your privacy settings to make sure your profile info is restricted to who you want to view it (i.e., your close friends or family).
- ☑ Restrict access to your profile info, photos, posts, and other personal information.
- ☑ Never approve friend requests or add people you don't know in real life.
- ☑ Be careful about in-app purchases or clicking on pop-up links.
- ☑ Disable location sharing on social media apps so other users can't track you.
- ☑ _____

_____

Name _____

Find the Security Holes!

Attention, online gamers! Cyberthieves are looking for ways to steal your personal info—and even sell your account. Study the sample profile below and identify any red flags that could make it easy for your account to be hacked. Using the chart below, describe each issue you spot and write in a possible security fix.

Privacy Settings OFF

LEVEL: 2

Username: NickyBell2004

Birthday: September 29, 2004

Hometown: Berryville, VA

About me: I'm a student at Lincoln Middle School and I live to play Fortnite!

Starbright424: Hey, can you message me your number so we can talk stats? :)

Click here to leave a comment Comment

What raised a red flag?	Suggested security fix
1. _____	_____
2. _____	_____
3. _____	_____
4. _____	_____
5. _____	_____
6. _____	_____
7. _____	_____

Sponsored Educational Materials

SCHOLASTIC

#CyberSmarts

AKA: How not to get hacked online

\+ 3 cool crime-busting careers

Sponsored by Norton LifeLock

Photo JGI/Jamie Grill; Alyson Aliano; Hero Images; Eternity in an Instant

Hack-Proof Your Life!

Scammers all over the internet want to take over your video games, hijack your social media, and steal your money. Here's how they do it and how to keep your most personal info safe.

You've just finished a ton of homework and you're ready to kick back and play video games. You log in to your game account and immediately notice something's not right. For one thing, you have a bunch of new updates, which you definitely didn't buy. Not only that, but your screen name is different. You're totally shook when you realize what's up: You've been hacked.

Online scammers are everywhere. These cybercriminals may get into your bank account and steal your money, pretend to be you on social media, and even threaten to post personal stuff about you to scare you into giving them money. Gamers are especially vulnerable—after hackers log in and rack up purchases on kids' accounts, they can sell the souped-up user profiles for money.

One easy way to protect yourself: Do not reuse your password. According to Vinny Troia, CEO of Night Lion Security and a "certified ethical hacker" (he figures out hacks before they happen), "Once someone knows what your password is, they can go to other sites you're on and hack you over and over again."

How Hackers Get You

In movies, hackers are hoodie-wearing computer whizzes who command a computer screen, pounding at a keyboard to crack an enemy's code. But in the real world, hackers use "scripts," software that finds digital weaknesses. The scripts attempt to log in to thousands of computers at once using easy-to-guess usernames and passwords. Researchers at the University of Maryland found a pattern to the passwords that hackers try most. One of the most popular: a password that's either the same as your username or a close variation. Or one that's a username with a series of numbers tacked on, like 123. (Um, don't do this!)

Nearly 60 million Americans have been victims of identity theft —2018 online survey by the Harris Poll

Photos: Guerilla; Hero Images

Phishing Warning

Often, though, hackers *can* be super-sneaky individuals you meet online who will phish (pronounced "fish") for your login info. Last summer, Jake Bates, 13, was in a really intense battle with a gamer on Fortnite. The Mason, Ohio, teen had been chatting with his opponent for hours when the gamer said he could give Jake some cool new skins if he shared his username and password. What the gamer did next: He took over Jake's account and changed his password, recovery password, and phone number! The scam artist also accessed Jake's mom's credit card, and Jake's emails and everything in them. Lesson: Never give your account info to anyone—even a real-life friend.

> Every **39 seconds** there's a hacker attack
> —2017 Clark School, University of Maryland study

While teenagers might be easy targets, even adults (and schools) can be victims of phishing. One California teen sneakily got access to his school district's computer system by emailing teachers a link to a fake grade portal website that

MY COOL CYBER JOB

ROSHAN DANESHVARAN

CTO and co-founder of Syfer

What first sparked your interest in tech?

When I was a kid, I watched the original *Terminator* movie, and the idea of Skynet—an artificial intelligence system that could harm people—scared and intrigued me. I developed an interest in artificial intelligence and robotics and a fascination for what computers can do for us in the future.

So what do you do at your job?

I'm a cybersecurity professional. There are bad guys (cybercriminals) on the internet trying to steal money and information from people and companies. My job is to help people protect themselves against these criminals. I study networks and software, and ultimately I architect the cybersecurity safeguards to keep the bad guys away.

What do you love best about your job?

I defend what is good. I get to be a superhero, but in the cyber world. Cybersecurity is like playing chess, and methods evolve every day. I have to study and learn new techniques so that I can stay ahead of the criminals.

MY COOL CYBER JOB

HALEY DICKERSON

Marketing director for CyGlass

When did you first get interested in marketing?

I was always "marketing," even when I was 8 and wrote a strategy, in crayon, to promote my lemonade stand. In high school, I taught myself how to build a website, and I read books on different coding languages. From then on, I took every opportunity to work with my new skills: for local government campaigns, restaurants, friends and family.

How does what you studied in college relate to your job?

I unintentionally learned the pillars of marketing from behavioral neuropsychology: Why do people do what they do? And how can you manipulate this behavior? Taking information technology (IT) courses gave me the tools to be successful in digital marketing.

What would you say to kids thinking about getting into a field like cybersecurity?

As long as there is a way to store, send, and receive data from one device to another, there will be a high demand for talented cybersecurity professionals. With countless cyberattacks occurring across all industries and making daily news headlines, there is a major spotlight on cybersecurity right now that is here to stay.

Photos: kali9; Adam Crowley; Hero Images. Photo Courtesy of Haley Dickerson. Photo Courtesy of Roshan Daneshvaran

looked like the real one. Once teachers entered a username and password, the teen hacker used them to log in to the real portal. He changed his friends' grades to better ones and even lowered the grades of some students. Fortunately, the police caught him. When the phony email was traced back to the 16-year-old's computer, Secret Service agents broke down the door to his family's home and arrested him. He was charged with 14 felony crimes and was suspended from school.

40%
of Americans have had their password compromised
— 2017 Norton Cyber Security Insights Report

Staying Smart

Although you obviously can't control everything (like what happens at school), you can help keep your personal info protected. Be wary if someone you know is suddenly acting shady online, like sending you messages asking for money or to meet up somewhere alone. "Hackers trick people all the time into thinking that they are someone their victim knows and trusts," says Jordan McCarthy, infrastructure and security team lead at Tech Impact. If you get a weird message, talk to a trusted adult right away. For more tips on staying safe, check out the "Digital Dos and Don'ts" below.

DIGITAL DOS AND DON'TS

Be smart about online safety with these simple rules.

Don't use your name as a username or screen name. By doing a simple internet search, strangers can use your name to find out a ton of personal information about you. Don't pick a revealing number like your birth year, birthdate, or your jersey number, either.

Do use strong passwords! A strong password has eight characters or more (longer passwords are harder to crack), as well as a mixture of uppercase and lowercase letters, numbers, and special characters (like !, @, or #). It's best to use "nonsense" words that can't be found in a dictionary. Change your password regularly and don't share it with anyone, even friends. And always use different passwords for different sites.

Don't give out your name, number, or address to anyone online. Keep in mind that whoever is chatting over games or social media may not be who they say they are. And they could be trying to get your personal info.

Do keep your online presence clean. A good rule to remember: Would you say it in front of a teacher? Part of staying safe is keeping your digital footprint free of anything you might regret posting later.

Don't download apps from sources you don't know. There are fake apps that exist just so the bad guys can snag personal data off your phone. Get your apps from trusted stores like Google Play or the Apple App Store.

Do avoid public Wi-Fi if at all possible. Hackers love public Wi-Fi because they can easily get between you and the connection spot, and grab every single thing you're sending over the internet. To protect yourself, talk to your family about signing up for a VPN service if possible (VPN stands for virtual private network). A VPN uses "encryption" to change your internet activity into code—and make it unreadable to hackers.

MY COOL CYBER JOB

JORDAN MCCARTHY
Infrastructure and security team lead at Tech Impact

When did you get interested in computers?
When I was 13, I asked my aunt if I could have her broken computer to tinker with. I tore the machine apart and rebuilt it. I still remember the feeling of euphoria when I flipped the power switch–and the screen turned on! I was hooked, and I started a program at my school to collect dead computers, rebuild them, and distribute them to kids who didn't have computers at home.

What's your favorite part of your job?
I get alerted about several malicious hacking attacks every day, some of which are really clever. Whenever I hear about a new attack, I can usually shut down important parts of the systems the attackers are using within minutes—and prevent tens of thousands of people from information theft.

How much of cybersecurity work is what it seems like in the movies?
The stuff you see in hacker movies is obviously exaggerated, but my job does sometimes feel like that. There have been situations where I've been up against a hacker who is actively working in someone's systems, and I need to figure out how to kick them out before *they* figure out what I'm doing.

What's a cool way you solved a tech problem?
I helped my dad recover a bunch of critical data from a crashed computer by putting the hard drive in the freezer! It's a last-resort trick used to shrink "stuck" metal in the drive and get its parts spinning and working again.

Photo Courtesy of Jordan McCarthy