Junior Cybersecurity

Learn how computers work and how to stay safe and protected by earning these three badges!

Badge 1:
Cybersecurity Basics

Badge 2:
Cybersecurity Safeguards

Badge 3:
Cybersecurity Investigator

This Cybersecurity badge booklet for girls provides the badge requirements, background information, and fun facts about cybersecurity for all three Junior Cybersecurity badges. It does not include all the information needed to complete the badges. Volunteers may access the full meeting plans—including detailed activity instructions—on the Volunteer Toolkit (VTK) or by contacting their local council.

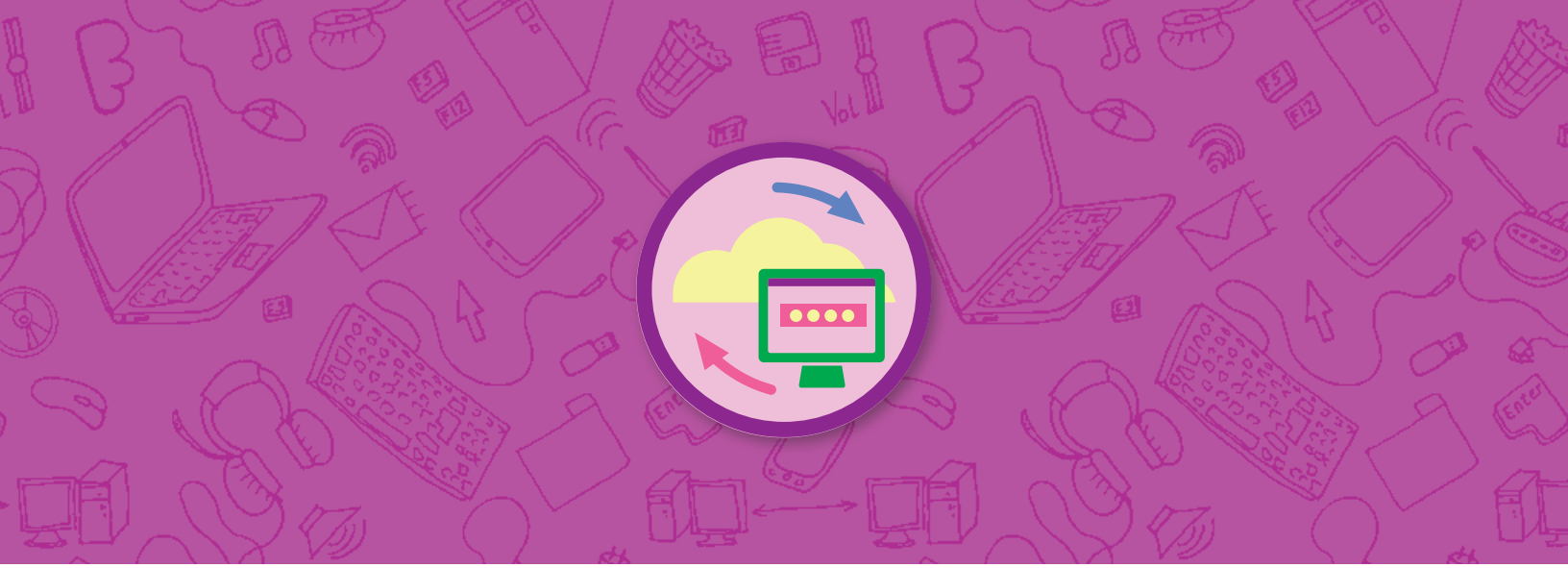
Welcome to the world of cybersecurity!

When you've earned these three badges, you'll know how to stay safe and keep information private when you're online. You'll also learn investigative skills that will help you spot problems and vulnerabilities in the cyber world.

Cybersecurity keeps the world safe. Every company that uses computers depends on people and software to protect them and the information they contain.

Do you love to solve puzzles and figure out mysteries and break codes? Then you'll love learning about cybersecurity—and how you can use your skills to keep people safe.

Volunteers, please see the Volunteer Toolkit (VTK) or contact your local council for the full meeting plans, including detailed activity instructions.



Badge 1: Cybersecurity Basics

More and more, computers run everything from city power grids, banks, and traffic lights to hospitals, schools, homes, cars, and phones. All those computers store information and data. It's important to keep that information safe—that's what cybersecurity is all about.

Steps

1. Find out how computers read information
2. Discover how networks work
3. Find out what protocols are and create one
4. Explore computer communication protocols
5. Find out what malware is

Purpose

When I've earned this badge, I'll know the basics of cybersecurity and how computers communicate.

Noticing Networks

Networks are groups that are connected in some way. For example, a group of people who all go to the same school is a network. Television stations that show the same programs can belong to a network. A Girl Scout troop is a network—and you belong to the network of Girl Scouts around the country and around the world! In the same way, computer networks are groups of computers that are connected to the internet.

Getting Connected

You probably have heard someone say they're "going on the internet" or "doing an online search."

All of those computers can talk to each other because of wires or cables on the ocean floor. There are 300 undersea cables that are responsible for almost all of the data traffic on the internet.

These cables connect continents and help get messages, photos, and video from one place to another in milliseconds.

STEP 1 Find out how computers read information

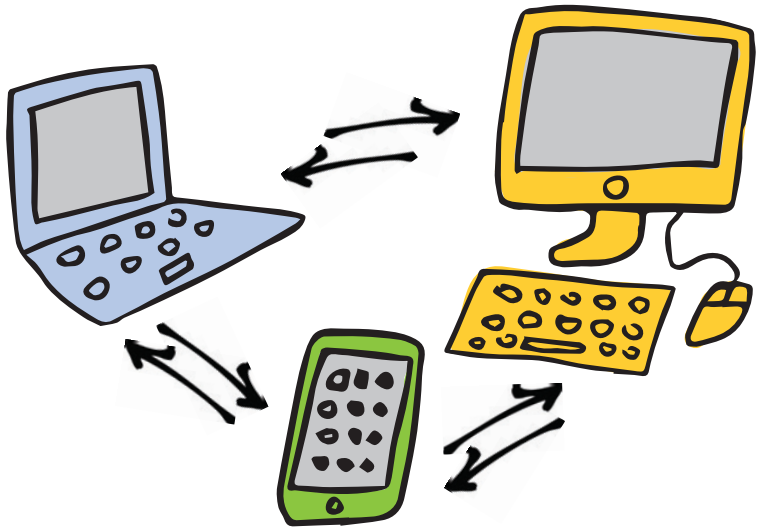
Computers have their own coded language to process information. This language uses the two numbers 0 and 1 in specific patterns to "speak" and share directions. It is called binary code. Any code that uses two elements is called a binary code.

When you go online or play a video game, binary code spells out what the computer should do.

STEP 2 Discover how networks work

Computers—and devices such as laptops, tablets, and smartphones—that are linked together are part of a network. Like tracks that connect train stations, computer networks are connected by the internet. Information such as photographs, emails, text messages, and files can be sent along the computer networks to reach different computers.

Every day you connect with a network of people. For example, you connect with your parents, your brother or sister your classmates, your teachers, your neighbor, your friends, and many others.



THREE SECRET CODES

One way of protecting a private message is to use a code. Here are three codes you can use with your friends. Give them a try—you'll learn how encryption works, which is an important way to keep information safe.

1. SECOND LETTER CODE

Read every second letter beginning with the first letter. When you finish, start with the second letter and skip every other letter.

WTEHLIISKOENCEOIDSEFSU!N

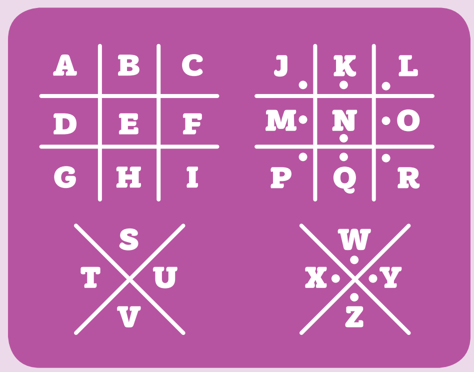
2. PIGPEN CODE

This one looks hard, but all it takes is the right key.

First, draw two tic-tac-toe grids. Below that, draw two Xs.

Then put dots in each box of the second tic-tac-toe box and the second X. Add the letters of the alphabet as shown in the diagram.

Each letter is represented by the lines (or the pigpen) that surround it. Now you can read pigpen!



3. MORSE CODE

Before phones, people communicated over huge distances using codes. Morse Code is one of those codes. It started as a series of indentations on paper in the 1830s, but it soon became a sound code. A pattern of long dashes and short dots represents the different letters.

.... .- ...- .   ..-. ..- -.   -.. .   -.-. --- -.. .. -. --.

A .-
B -...
C -.-.
D -..
E .
F ..-.
G --.
H ....
I ..
J .---
K -.-
L .-..
M --
N -.
O ---
P .--.
Q --.-
R .-.
S ...
T -
U ..-
V ...-
W .--
X -..-
Y -.--
Z --..

Answers on page 9

WORDS TO KNOW

- **Anti-virus software:** Computer programs that scan your computer and keep it free of viruses.
- **Cipher:** A method of changing a message so as to conceal its meaning. For example, when you use special numbers, letters, and symbols in a code to send a secret message, you are using a cipher. When you figure out a code, you decipher it.
- **Code:** A system of symbols, such as letters or numbers, which are used to create a secret message. Code is also the language computers use. When you write code on a computer, you give it commands to tell it what to do.
- **Download:** Copying a file, such as a photo, video, app, or game, from one computer to another, usually over the internet.
- **Hacker:** Usually means a person who secretly gets access to a computer system to get information or cause damage. However, when it comes to hackers, there are good actors and bad actors (see page 14 to learn more).
- **Network:** A system of computers and other devices (such as printers) that are connected to each other.
- **Password:** A secret word or phrase usually made up of a string of characters—letters, numbers, and symbols—that allows you to get access to a computer or system.
- **Private information:** Facts about you that you don't want everyone to know. For example, your home address or the name of your school is private information. You don't want to share that with strangers.
- **Protocol:** A system of rules that explains the correct steps to follow.
- **Spam:** Unwanted emails—short for "Sending Particularly Annoying Messages."
- **Username:** A name, word, or characters you type so you can use a computer, cell phone, tablet, or website. Usernames are also called user IDs.

STEP 3 Find out what protocols are and how to create one

Protocols are important in everyday life. A protocol is a set of rules that says exactly how something should be done. We use protocols all the time.

For example, when a school bus stops and turns on its flashing red lights, drivers also stop. That helps keep children safe as they get off the bus. Before an airplane takes off, the pilot uses a checklist—a set of protocols—to make sure the equipment and instruments work properly.

When computers share data, they follow a set of rules or protocols that make it easier and safer to share information.

STEP 4 Explore computer communication protocols

If you want to communicate or speak with a friend, you might tap her on the shoulder, call her name, or wave to get her attention. Once she sees you and is ready, then you can talk. You make a connection first.

For a computer to pass along any information it must make a connection between the host and the server. In order to do this, the computer follows a three-step protocol called a handshake.

- **STEP 1** A request is sent out.
- **STEP 2** The request is received and understood.
- **STEP 3** The request and the acceptance of the request is then acknowledged by the sender. Now messages can be sent.

Handshake History

In ancient Greece, warriors would grasp each other's elbows to greet one another. It was a sign of peace. They did it to show they weren't holding any hidden weapons.

Even today, people often shake hands when they meet. It's a gesture of friendliness. It's also a communication protocol, just like a computer's handshake.

STEP

5 Find out what malware is

Combine the words "malicious" (meaning "harmful") and "software" and you get the word "malware." Malware is software that can attack computers, tablets, phones, and other digital devices and cause harm.

Computer viruses are one type of malware. Viruses can make their way into your computer or device when you download email attachments or content from someone else's flash drive. When you click on online ads or download programs from the internet, you also risk getting a virus. For this step, find out the ways that malware can enter your computer.

Malicious Malware

Take a look at the chart that shows the different kinds of malware and what they do.

They can be as nasty as they sound. Here are six common types of malware to avoid:

Viruses

A computer virus is a small program that sneaks into your computer on an email or a download. Then it copies itself and causes problems the same way that a cold virus does in your body. A virus might just slow down your device—or it might make you lose all your applications and documents!

Worms

Worms are programs designed to get into your computer, copy themselves, and quickly harm your device. A worm can infect your email account and then send a copy of itself to all of your email contacts!

Trojan horse

A Trojan horse seems to be a program that can be helpful. But when you download it, it attacks your device. The name comes from an old Greek story. The Greeks were battling the Trojans. They made a huge wooden horse, pushed it up to the city gates, and hid inside. The people of Troy thought it was a gift. They opened the gates and pulled it in. They had no idea there were soldiers inside waiting to attack.

Spyware

Spyware is sneaky software that installs itself onto devices. Once it's in your computer, it starts to steal passwords, email addresses, and other important information.

Adware

Adware uses clever advertisements to trick you into giving away your private information.

Ransomware

This software takes over a computer and kidnaps data. The attacker won't allow the user to access any information until a ransom is paid. Even then, they sometimes won't give you your data back.

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

- Creating a video about the most interesting thing I learned and sending it to my family members around the country.
- Talking to my parents about installing anti-virus software on our family computers.
- Putting together a workshop to help senior citizens protect their digital devices from malware.

I'm inspired to:

Answers: Page 5: 1. WE LIKE CODES! THIS ONE IS FUN, 2. X MARKS THE SPOT, 3. HAVE FUN DECODING

Badge 2: Cybersecurity Safeguards

Using computers and going online is fun and exciting, but there are certain rules that help you keep safe. Start by creating an online identity and protecting it. Then discover how to act responsibly, use devices safely, and figure out who is trustworthy online.

Steps

1. Create and protect a username
2. Create and protect a password
3. Discover how you share information and what to share
4. Find out that information posted online lasts forever
5. Find out how to figure out who you can trust online

Purpose

When I've earned this badge, I will know how to protect my online identity and stay safe online.

STEP

1 Create and protect a username

Your identity is who you are, but when you go online you need to keep your private information private. One way to do that is to create an online identity called a username or screen name. Usernames don't include your real name or any identifying information. We use usernames so we don't have to share our private information—our real names—with strangers.

Password Power

When you create a password, choose a phrase you can remember. It should be mysterious to other people, though. Mix uppercase letters with lowercase letters. Use numbers and symbols, too. Choose a combination that makes sense to you and then keep it to yourself.

WACKY PASSWORD GENERATOR

When you make a password, it should include words or phrases, numbers, and symbols. Here is a fun way to create silly passwords. Pick a letter from each group below. Write the word on the blanks at the bottom of the page.

1 The second letter of your first name:

A—Zippy
B—Flashy
C—Wizard
D—Doctor
E—Super
F—Mega
G—Wonder
H—Power
I—Amazing
J—Incredible
K—Ninja
L—Cyber
M—Professor
N—Agent
O—Silent
P—Thunder
Q—Sweet
R—Alpha
S—Warrior
T—Turbo
U—Star
V—Storm
W—Green
X—Champion
Y—Stealth
Z—Brilliant

2 The last letter of your middle name:

A—Spaghetti
B—Sleepy
C—Giggle
D—Hamster
E—Awesome
F—Jingle
G—Goofy
H—Candy
I—Electric
J—Potato
K—Happy
L—Golden
M—Muddy
N—Smartypants
O—Deep fried
P—Organic
Q—Sour
R—Undersea
S—Pony
T—Instant
U—Genius
V—Lightning
W—Pink
X—Fluffy
Y—Powerful
Z—Beyond

3 The month you were born:

January—Cupcake
February—Groundhog
March—Galaxy
April—Rainforest
May—Queenbee
June—Firefly
July—Fireworks
August—Shaggydog
September—Appletree
October—Ghost
November—Turkeytrot
December—Sparklylights

4 The number of people in your family

5 The number of letters in your favorite color

6 A symbol of your choice

My silly password:

_____ _____ _____

_____ _____ _____

STEP

2 Create and protect a password

When you go online, you need to protect your identity. Using a password is one way of doing this. Passwords are secret words and phrases that act as an online key to a locked door that keeps your private information safe.

PASSWORD CHECKLIST

Passwords are used to verify you are who you say you are. Explore what makes a good password.

- ☐ Don't use a short password. Make sure your password has at least 12 characters. Use at least one number, one uppercase letter, one lowercase letter, and one special symbol.
- ☐ Don't use words that can be found in the dictionary.
- ☐ Don't use names of your family, friends, or pets in your password.
- ☐ Don't use numbers that are personal, such as your home address or birthday.
- ☐ Don't use passwords that are easy to guess, such as your name, the word "password," or "12345."
- ☐ Don't create passwords that identify you or relate to anything about you, such as your name, school, or sports team. (Remember, a hacker can find out a lot about you from doing a search, like your name, where you were born, your age. That information can lead them to finding out your password.)
- ☐ Do make your password one of a kind and completely unpredictable. Create a pattern that is not obvious by adding numbers or symbols where you don't expect it.
- ☐ Do change your password every 10 weeks.
- ☐ Don't reuse a password you've used before.
- ☐ Don't share your password with anyone.

Does the Password Pass the Test?

Choose the most secure password in each group. Then put the letters connected to that password together to get a secret message. Write the letters in parentheses after that password in the blanks below. You will get a secret message!

1. **a.** BIGword$4me! (P-A-S)
   b. password (N-Q-D)
   c. 1234! (A-W-T)
2. **a.** 22222 (P-R-O)
   b. #$@^&& (N-Q-D)
   c. SIllyKItty8&8!! (S-W-O)
3. **a.** Myname12 (P-R-O)
   b. password000 (N-Q-D)
   c. DoGSrule2002! (R-D-P)
4. **a.** mypasswordisprivate (Z-Z-X)
   b. password (J-K-L)
   c. 2018ILOVEkale!! (O-W-E)
5. **a.** &haha (A-D-U)
   b. HAhaHAha:)77? (R-!-!)
   c. 98765$ (R-D-P)

ANSWER:

__-__-__-__-__-__-__-__-__-__-__-__-__

Answer on page 16

What Is a Hacker?

A hacker is a person who uses computer skills to solve a problem with technology. There are different kinds of hackers. Some are good actors and some are bad actors.

Good actors are people who tinker with computer systems to protect them. Companies sometimes hire these good actors to look for weaknesses and mistakes in their security systems so they can be fixed.

Bad actors are criminals who break into someone else's computer or a company's computer system and cause harm. Good actors can help keep bad actors from committing crimes.

STEP 3 Discover how you share information and what to share

Being online is like real life. There are people who you know and trust. You can share information with them.

There are also people you don't know, so you don't know if you can trust them.

In real life, you wouldn't give someone you don't know private information, such as where you live or where you go to school. You should follow that rule online too.

Just remember: if you wouldn't do it in real life, you shouldn't do it online either.

Eight Ways to Keep Your Family Computers Safe

You can help keep your family computers safe. Here's a checklist you and your family can go through together to be cyber savvy.

- Make sure you have anti-virus software in place.
- Turn on spam filters—this protects you from ads, scams, and unwanted emails that might carry viruses.
- Ask your parents to use computer settings to turn on parental controls. This will keep you from accidentally stumbling on to an unsafe website.
- Don't share any private information online.
- Cover or disconnect webcams from computers when you are not using them. If your webcam is part of your computer, you can cover it with a piece of tape or paper. If your webcam is separate from your computer, you can unplug it.
- Tell your parents about your favorite apps, websites, and videos. Let them know who you text or email. Your parents can help you make sure they're safe.
- If something on your computer bothers you—even if you're not quite sure why—tell an adult.

STEP 4 Find out that information posted online lasts forever

You can never really take back what you say or show online. If you send a message, post a photo, or share something online, it never really goes away. You may decide later that you want to delete it, but most information is stored on a server (sometimes called "the cloud"). That information stays in the cloud forever—which means someone can find it later, even if you try to get rid of it.

STEP 5 Find out how to figure out who you can trust online

It's easy for someone to pretend to be someone else online. Why? Because no one can see them.

For example, an imposter could send you an email that says you can win a prize if you click on a link.

This may sound like a good deal, but clicking on the link could help the imposter steal your private information.

Imposters aren't easy to spot, but keep these rules in mind:

- If you get an email from someone you don't know, don't open it. Show it to your parents or another trusted adult.
- If you get an email from someone you do know asking you to click on a link—don't! It might have been sent by a computer worm that takes over email accounts and sends copies of itself to all the contacts. Show the email to your parents or another trusted adult.
- Never chat with someone you meet online without checking with your parents.

What Is the Cloud?

When you hear someone talk about "the cloud," you might think it's up in the sky. When you're talking about computers, "the cloud" is just a network of large computers or servers that are all connected. All your online information is kept in the cloud.

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

- Telling my parents what I've learned about cybersecurity—the internet is always changing, so I may have learned something that will help them.
- Visiting a community center or senior center and helping people create more secure passwords.
- Doing a class presentation about how to be cybersecure and safe online.

I'm inspired to:

Answers: Page 13: PASSWORD POWER!!

Badge 3: Cybersecurity Investigator

Cybersecurity professionals crack codes, delete malware, and defend against hackers. You'll become a cybersecurity investigator by finding out how to protect your online identity, cracking codes, and figuring out the difference between real and fake information.

Steps

1. Create and crack a shift cipher code
2. Find out how device updates can help your security
3. Explore identity theft
4. Find out what to do if your identity is stolen
5. Investigate if a message is real or fake

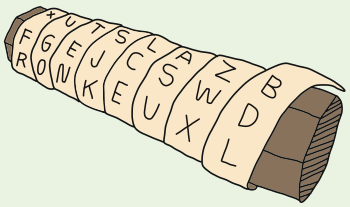
Purpose

When I've earned this badge, I'll know how computers use codes to communicate and how to spot cyber crime.

Ancient Cipher

People have been sending secret messages for hundreds of years. A scytale is an ancient coding tool from Greece. The Spartans used this tool to communicate secret messages during wartime. The tool is a cylinder made out of wood. Both the sender and the receiver of the message had to have the same size cylinder.

The sender would take a long narrow strip of leather or fabric and wind it around the scytale so that the coils of the fabric lined up. The sender wrote a message with one letter on each coil from left to right. The fabric was unwound from the scytale and scrunched up for transport. On its own, it just looked like a long strip of fabric. When the receiver got the fabric strip, she wrapped it around her scytale and lined up the coils to read the message.



STEP 1 Create and crack a shift cipher code

Computers use codes as their language. It's how computers communicate. And people who code computers, known as programmers, are always looking for ways to send coded information to protect private information, such as emails and bank accounts. It's called encryption.

Codes are a great way to change a message so it can't easily be understood. Another word for code is cipher. Codes replace letters with special numbers, letters, and symbols to make a message secret. When you crack the code, you decipher the message.

STEP 2 Find out how device updates can help your security

All digital devices have software that helps them run. That software gets updated regularly. Have you ever been on a digital device and had a window pop up telling you it's time to install a new update?

Software updates add new features and remove old features, but their most important job is making your device's security better.

Are You CYBER SAVVY?

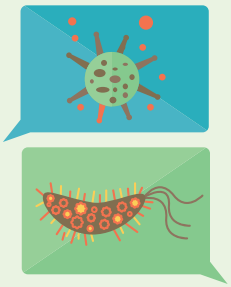
Take this quiz and see how cyber savvy you really are.

1. You just received an email from a rich person who wants your help. He has lots of money in another country but can't move it. He asks you to send him money. He says he will pay you back what you send him and then he will give you a bonus of extra money just for helping. What do you do?

   a. Send a note back saying you know this is a scam.
   b. Delete the email—tell an adult.
   c. Forward the email to your friends.
   d. Write back—it sounds cool!

2. You are shopping online and a window pops up saying that you have a virus. It says, "Click to resolve the issue." What do you do?

   a. Click and follow the directions.
   b. Close both the virus window and the shopping site window and don't return to the site.
   c. Hit the "back" button.
   d. Close the pop-up window.



3. How often should you back up your devices?

   a. Once a day
   b. Once a week
   c. Whenever you create new files
   d. When you think there may be a problem

4. You "meet" someone nice online. They tell you they are your age and ask what school you go to. They want to meet you in person. What do you do?

   a. Give your name and make a time to meet.
   b. Tell the person to stop bothering you.
   c. Tell your parents or another trusted adult. Show them the email.
   d. Give your name and school but don't meet.

Answers on page 23

Cybersecurity Calling

Do you like computers? How about solving puzzles, deciphering codes, and unraveling mysteries? If you said yes, a cybersecurity job could be in your future.

Tons of companies need people with strong computer skills to help protect information against cyber attacks.

From banks and hospitals to aerospace, pharmaceutical, military, and engineering organizations, any business that has classified or private information needs help keeping it safe.

With computers controlling more and more—from powering up cities, flying planes, and running machines that operate on people—there will be jobs in the future that we can't even imagine now.

STEP 3 Explore identity theft

Your identity includes private information, such as your name, address, birthday, and, when you get older, credit card information. Identity theft is a crime where cyber criminals steal your private information and pretend to be you online. They can buy items with your money, and then use your name if they get in trouble. It's one of the fastest growing crimes in the world.

STEP 4

Find out what to do if your identity is stolen

Criminals who steal personal and private information are called identity thieves. Once they get enough information, such as a name, an address, or a social security, bank account, passport, or credit card number, they pretend to be that person. They can use the information to buy expensive items or apply for credit cards.

If you or someone you know has their identity stolen, there are some actions you can take to help. You have to act fast. Report the theft to a trusted adult as soon as possible.

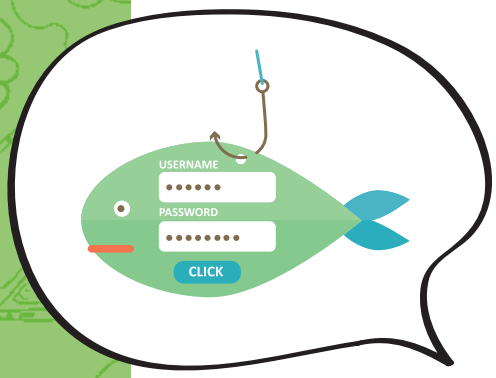
Make Your Device Safe

Protect your computer against viruses, spyware, worms, and other harmful malware. Keep software current so you have the most recent security updates and make sure you protect any devices (phones, tablets, laptops, desktops, and gaming systems) that connect to the internet by having good, strong passwords.

STEP

5 Investigate if a message is real or fake

When cyber criminals want to find out information, they will sometimes create online scams called phishing. Phishing is when a cyber criminal tries to get your information—such as your username, password, and credit card details, and sometimes even money—by pretending to be someone who is trustworthy. They send you a message via text, email, or social media and invite you to click on a fake webpage. If you do, you'll give them your private information without even realizing it! That's why it's important to only talk to people you already know and trust when you're online.

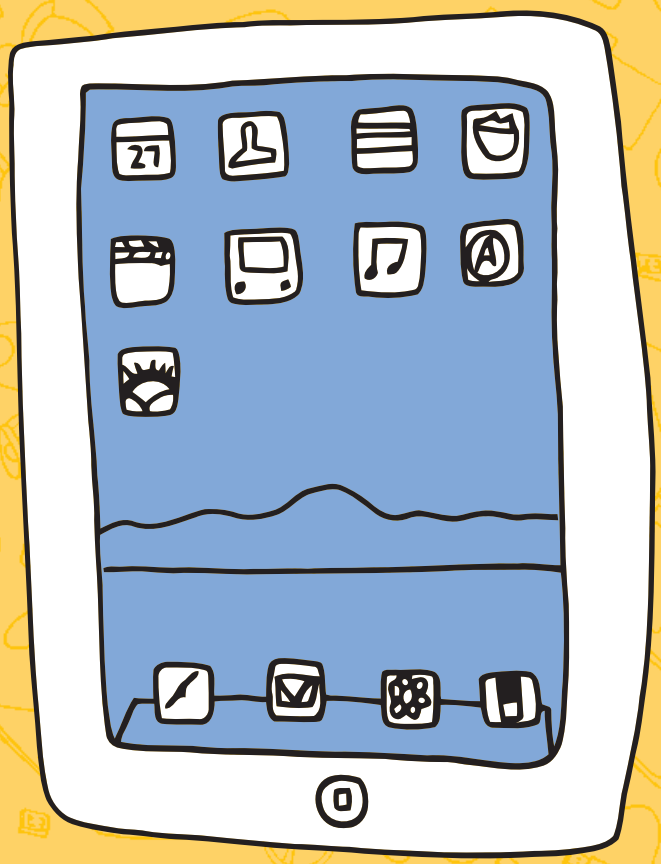


Now that I've earned this badge, I can give service by:

- Teaching my friends how to create a secret code or password.
- Making a poster about identity theft to hang at my school or library.
- Leading a workshop to teach others how to spot fake messages online.

I'm inspired to:

Answers : Page 19: 1. b 2. b 3. c 4. c



Made possible by a generous grant from Palo Alto Networks

First published in 2018 by Girl Scouts of the USA
420 Fifth Avenue, New York, NY 10018-2798
www.girlscouts.org

Printed in the United States

Stock images by: Adobe Stock

Special thanks to the Cybersecurity badge content partner, the Cyber Innovation Center.

UPC 64168

7 31955 64168 9