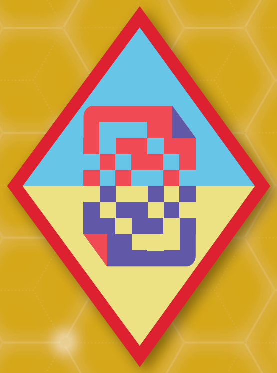


# Badge 1: Cybersecurity Basics

The internet lets people all over the world connect with each other and find information easily. That can make life easier, but also riskier. People store a lot of private information on their computers, phones, and tablets. Hackers are always trying new ways to collect our data, so learning how to keep your information safe is an important computer skill.

## Steps

1. **Crack a code**
2. **Hack a password**
3. **Explore two-factor authentication**
4. **Launch a Man-in-the-Middle attack**
5. **Explore social engineering**

## Purpose

**When I've earned this badge, I'll know how hackers steal information online and steps I can take to protect my data.**

## Is Someone Listening?

As hackers find more and more ways to listen in on phone calls or read texts, computer programmers are creating **end-to-end encryption** programs to keep your conversations and messages private. Some cell phone creators build encryption right into their phones. Apple's iPhones have encryption built into their FaceTime and iMessage programs, and even Apple can't access your information. Some communication apps like WhatsApp or Signal offer end-to-end encryption on calls and texts, but only if the person you're talking or texting with uses the program, too.

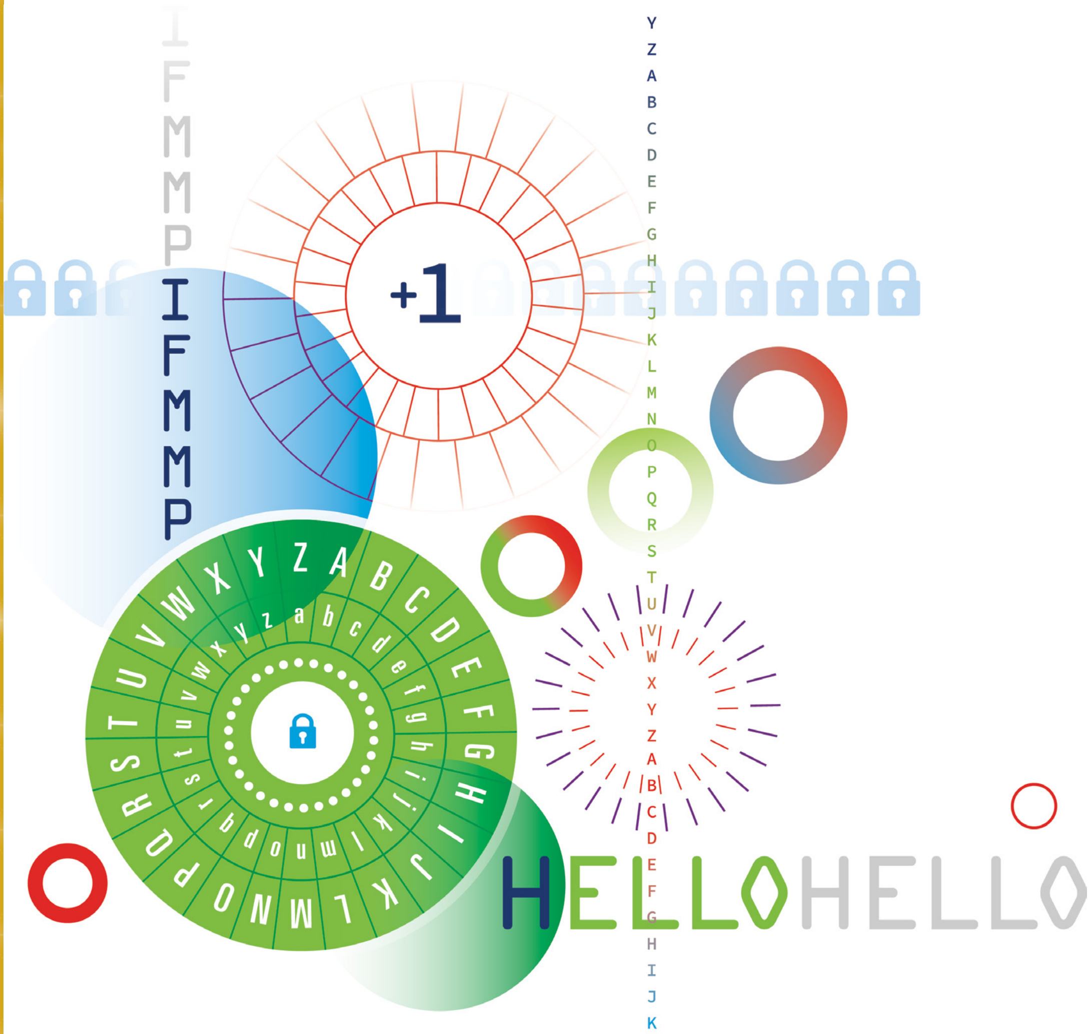
STEP 1

# Crack a code

**Wouldn't it be fun to have a secret language that only you and your friends knew?** You'd have to create your own secret code. **Cryptography** is the process of writing and solving codes.

When you take a message and turn it into a code, you **encrypt** it. When you turn the code back into a readable message, you **decrypt** it. It's easy to decrypt a message, if you have the encryption key that shows how the message was changed to make it unreadable. But if you don't have the key, you have to figure out the code on your own.

Decrypting a code without the key is called cracking a code. When you send a text or an email, your computer or phone automatically encrypts the message, and then the receiving computer or phone decrypts it.


IFMMP
IFMMP
+1
XYZABCDEFGHIJKLMNOPQRSTUVW
xyzabcdefghijklmnopqrstuvw
YZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJK
HELLOHELLO

# WORDS TO KNOW

**Brute force attack** when an attacker tries many different passwords in hopes of guessing correctly

**Computer network** a group of computers—or other digital devices—connected together in some way

**Cybersecurity** the protection of digital devices, such as phones or computers, against attacks

**Dictionary attack** when an attacker uses an existing list of words as potential passwords

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

**Encryption** the process of encoding a message or data so that people need a secret key or password to read it

**End-user license agreement (EULA)** a contract that gives a user the right to use software

**Malware** software that aims to cause damage to your computer or network

**Man-in-the-Middle** a type of cyberattack in which a hacker intercepts a message between two entities in order to spy on them or steal their information

**Metadata** data that describe or define another piece of data

**Nodes** as packets of data travel through a computer network, they stop at many different "nodes" along the way

**Packet** when you send a message, or submit information, through the internet, your message is broken up into smaller packets of data

**Personally identifiable information** any information that can be used to identify, contact, or locate an individual

**Phishing** a type of cyberattack in which a hacker sends an email that contains bad links, harmful attachments, or requests for money

**SMSing** a type of cyberattack in which a hacker sends a text message in order to try and steal your personal information

**Social engineering** a strategy that attempts to manipulate or deceive a user so that they give up their personal information

**Spoofing** a type of cyberattack in which a hacker pretends to be someone you know, or an organization you trust, in order to gain access to your information

**Spyware** software that secretly collects information about you

**Two-factor authentication** an extra layer of cybersecurity that requires two different types of validation (like a username/password AND a unique code sent to your phone) before allowing access

## STEP 2 Hack a password

**Every time you set up an account on your computer or phone, you have to create a password.** An account is just a way for the website or app you are using to know who you are. If you have email, keep or turn in school work online, or play online video games, you have created an account.

It can be hard to come up with a new password for every new account, so sometimes people use the same password for lots of their accounts. That's a bad idea. So is having a short password or one without numbers, upper and lowercase characters, or special characters. Why? Because a simple password is easier to guess. If someone wants to get into your account without your permission, you want it to be hard for them to guess your password.

### M1X !T / UP

To make a really strong password, you need to get creative. Here's why: Hackers have programs that can run through dictionaries with lightning speed. They can identify millions of passwords in minutes. Then they use another program to try all these passwords to hack into people's accounts. Hackers also have programs to search books, movie scripts, and song lyrics (like they do with dictionaries) to look for passwords, so don't use your a line from your favorite song or movie! They can even scan social media sites to get clues to people's passwords, like their birthdays or pet's name. So don't use your birthday or your pet's name as your password!

Because hackers expect people to follow grammar rules for capitalizing letters, the strongest passwords have numbers, special characters, and uppercase letters in unusual places.

- **The longer the password the better.** Some experts suggest 12 characters long. It takes a hacker's program longer to guess a long password than a short one.
- **Don't use numbers or symbols as obvious substitutions.** For example, !L0Vecat$ would be easy to crack because ! looks like I, 0 looks like o and $ looks like s.
- **You can use capital letters, numbers, and special characters in random ways to make a strong password.** If you wanted to use your troop number in your password, you could write grLsCttRP#2961 for Girl Scout Troop 2961.
- **Some experts suggest choosing four random, unusual words that make no sense together, like tunaFlipflopsnoreSHINY.** This is called a passphrase. Even though it doesn't have numbers or special characters, and the words are from the dictionary, the random combination of the words and the length of the password make it a strong password, and it may be easier to remember than one with random letters, numbers, and characters.

## STEP 3 Explore two-factor authentication

**Some computer security systems use something called two-factor authentication.** That means that the person wanting to get into the account must have two things to prove they should have access.

For example, if you've ever had to be picked up at school by a grown-up, you know about two-factor authentication. Most schools use two-factor authentication to make sure the grown-up is allowed to pick up the student. First, the grown-up has to show a photo ID, like a driver's license. The school checks to make sure the person matches the person on the ID. Then the school also checks the form that your parent or guardian completed at the beginning of the year listing who is allowed to pick you up. If that person isn't on the list, the school will call your parent to make sure it's ok. The photo ID and the list are the two factors.

In the computer world, sometimes you need both a password and a special number code that gets sent to your cell phone to get into a computer account. A special algorithm creates a new number code every time you log in. That code is a kind of number puzzle. If hackers want to get into an account with two-factor authentication, they have to figure out what the number code is, but it changes all the time. That's a tricky puzzle to solve.

### Better Safe Than Sorry

Because passwords can be easy to hack, cybersecurity specialists have added more layers to get into an account beyond your username and password. This is called multi-factor authentication. Some send a randomly generated code to your cell phone, some ask for a fingerprint or scan your eye, and some have an actual physical "key" that looks like a USB stick or flash drive.

# ARE YOU A GOOD HACKER OR A BAD HACKER?

Sometimes the word “hacker” makes people think “criminal.” But the term “computer hacking” doesn’t mean breaking the law or hurting people. It just means changing code.

- Schools and clubs hold **“hackathons”** where people get together and design or improve programs and apps. The hackathons are usually focused on meeting a need or solving a problem. Sometimes companies hire hackers to help them find weaknesses in their security measures. These people are **white hat hackers**. They hack for good.
- When people use their computer knowledge to break into private accounts and steal information or money, they are criminals. The computer world calls these people **black hat hackers.** (White hat hackers try to help others find weaknesses in their computer security systems before black hat hackers can.)
- There are even **gray hat hackers** who look for weaknesses in computer security systems without permission from the business or organization. When they find a weakness, they tell the organization about it. They also ask for money because they found the weakness before black hat hackers did. They are called gray hat hackers because hacking into someone’s account without their permission is illegal, but the hackers don’t use the information to steal from the organization.

## STEP 4 Launch a Man-in-the-Middle attack

**Have you ever played Keep Away or Monkey in the Middle?** It's a game where players try to throw a ball to each other while trying to keep one player from catching it. The player, or monkey, in the middle tries to intercept the ball as it's being thrown from one person to another.

Computer hackers try to do the same thing with information you send through the internet. They try to intercept your information as it travels from your computer or phone to its destination.

This kind of hacking is called a **Man-in-the-Middle attack**. The best way to keep a hacker from stealing your information while it's on the way to its destination is to be sure you're using a secure internet server. A secure server is one that isn't open to everyone. To use it, you have to have a password, and it limits what others can intercept when you are online.

## STEP 5 Explore social engineering

**Social engineering is a cyberattack strategy that attempts to manipulate or deceive a user so that they give up their personal information.** If it sounds too good to be true, it probably is!

No matter what your hobbies or interests are, scammers have developed many different techniques to get you to click on their link and/or send them money:

- Beware of any kind of prize if you must send money to claim it.
- Similarly, there are certain scams that take advantage of your creative talents and aspirations: for example, art and writing contests that require you to send money if you want your work to be published; modeling and acting agencies that promise to take headshots for you but never do.
- And if you're planning to attend college and searching for financial aid, be on the lookout for scholarship search sites that require you to pay a fee; most legitimate sites make this information available for free.

Before you click, do your homework. If an organization contacts you via email, phone, or online ads, research it before you do anything else. Find out if the organization is legitimate and whether what it is asking for is normal for that industry. The Better Business Bureau (BBB) is a good place to begin your research. And if you do fall victim to a scam, you can report it to the BBB as well.

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

- Holding a “Safe and Strong Passwords” workshop at a library or community center.
- Doing a school presentation about protecting personal data online.
- Creating a book display with a cybersecurity theme at my school or public library during October (National Cybersecurity Awareness Month).

## I’m inspired to: