# Cadette Cybersecurity Basics

**Pillar:** STEAM
**Outcomes:** Positive Values, Community Problem Solving

**Cadettes will earn their badge by learning how hackers steal information online and steps they can take to protect their data. The internet lets people all over the world connect with other people and find information easily. That can make life easier, but also riskier. People store a lot of private information on their phones, computers, 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.** Note: This is the first of three sequential Cybersecurity badges and this is all about learning some basics. The other badges help put these concepts into practice.

1. Crack a code. Wouldn't it be fun to have a secret language that only you and your friends knew? You would 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 is easy to decrypt a message if you have the encryption key. But if you do not have the key, you must figure it out on your own. Decrypting a code without a key is called cracking a code. Phones automatically do all these steps every time you send a message.
    a. Learn how **end to end encryption** works – these are programs to keep your conversations private.
    b. Learn more about the following words here: brute force attack, dictionary attack, packet, phishing, social engineering, spoofing, spyware, man-in-the-middle, malware, digital footprint, metadata.

2. Hack a password. Every time you set up an account on your computer or phone, you must create a password. This helps the website or app know who you are. 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 accounts. That is a bad idea! So are simple passwords because they are easier to guess.
    a. Make a strong and creative password. Hackers have programs that can identify millions of passwords in minutes. They can scan social media to find out more about you like pet names, birthdays, even favorite movies! Learn more about strong **passwords** and **passphrases**.

3. Explore **two-factor authentication**. This means that the person wanting to get into the account must have two things to prove they should have access. This is similar in your schools. If an adult other than your parent wants to pick you up, they might have to show an ID like a driver's license and then they compare that with the list your parents gave the school for approved adults. The ID and the list are the two factors. In the computer world, sometimes you need a password AND a special number code that is sent to your cell phone to get into your computer account. This makes it more difficult for hackers to figure out both, since the special code changes all the time.
    a. Not all hackers are bad. Sometimes people think all hackers are criminals. Hacking just means changing code and it can be helpful sometimes. Learn about the difference between **white hat** and **black hat hackers** here.

4. Launch a Man-in-the-Middle attack. Man-in-the-Middle is like the game of Keep Away, where people try to throw a ball to each other while one person in the middle tries to grab it. Computer hackers do the same thing with information you send through the internet. They try to intercept your information as it travels to

its destination. The best way to keep a hacker from stealing your information is to be sure you are using a **secure internet server** – not one that's open to everyone.

5. Explore social engineering. **Social engineering** is a cyberattack strategy that attempts to manipulate or deceive users to give up their personal information. If it sounds too good to be true, it probably is!
    a. Before you click, do your research! If someone contacts you via email, phone, or online ads, research it before you do anything else. Find out if they are legit; the Better Business Bureau (BBB) is a good place to start. If you do fall victim, you can report it to the BBB as well. Some examples are asking you to send money before you can join a contest, or to claim a prize you've "already won", even for college scholarships sites asking for a fee.

**Additional online resources:**

- Cadette Cybersecurity Pinterest Board

**When you're finished:** Congratulations, you have earned your badge! You can purchase by emailing shopdept@gsksmo.org or at https://www.girlscoutshop.com/cadette-cybersecurity-basics-badge

No shipping charges apply at this time.

---