



# Senior Cybersecurity Basics

**Pillar:** STEAM

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

**Seniors will earn their badge by learning how computers and computer programs work in order to write code and stop hackers. As cybersecurity is one of the defining issues of our time, experts help people, companies, and nations protect their networks and information.** 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. Find out how computers run multiple programs. We multitask all the time when we are doing several things at once. The problem is, our brains are not designed to multitask, as this causes more errors. The same happens with computers. When they multitask, they allow opportunities for hackers to break in – a weak spot. Each program or website you are using allows a different entry point for hackers. Computer programmers have developed ways to protect this from happening.
  - a. Each program running, called a **process**, is separated into its own space in the computers' memory. This is called **process isolation**, where every program gets to work in its own space. For example, when you have multiple tabs open and they are all running different programs.
  - b. **Domain separation** is another way programmers help computers multitask efficiently. This helps prevent large data breaches by keeping different types of data separate, such as credit card numbers and social security numbers. Even employees working at the same company do not have access to all your information, so they cannot see it all, which keeps you safer.
  - c. Hackers are always looking for new ways to break into computers. Cybersecurity experts try to make this as difficult as possible. Read the [ten principles of cybersecurity](#) created from the National Science Foundation and National Security Agency or see [this poster](#) to summarize.
2. Identify functions and privileges
  - a. There are certain processes and certain pieces of equipment we use for specific purposes. We would not use flippers to skate with or bake a cake after icing it. That is the concept of **resource encapsulation**. This idea labels parts of a program or data according to who can use it and how. This protects a code or data from revealing too much information. Programmers bundle, or encapsulate, data and label it.
  - b. Another concept is **least privilege**, whereas few people as necessary have access to certain data. Limiting how programs and data can be used also limits how hackers can make trouble.
3. Learn how computers hide information
  - a. One-way programmers do this is called **abstraction**, where they hide anything on the screen that is unnecessary and can distract or be used incorrectly. It is so much easier to just see a pretty website rather than all the code and formulas, isn't it? This is the idea with abstraction – you do not have to see how it is done; you just see the finished product.
  - b. Another way to hide information is called **data hiding**. Essentially, programmers hide information from those that do not need to access it. So, when you go the bank, the bank teller can only see as much information as they need to complete your transaction, not everything in your account.



4. Design a layered security system. Trying to hack a computer system is like trying to break out of an escape room, but in reverse. You are both trying to solve a series of puzzles in an order.
  - a. Using multiple security strategies is called **layering**. Cybersecurity experts create a series of obstacles, like firewalls and antivirus software to protect the computer system, or passwords and resource encapsulation. Have you ever been locked out of a website from trying too many incorrect passwords? This is a layering technique.
  - b. **Modularity** is another technique where computer programs are broken into smaller parts called **modules**. If there is a problem, the programmer can edit just that one module instead of having to rewrite or fix the entire program. Modularity makes computers and programs easier to fix and limits the damage a hacker can do.
  
5. Design a Rube Goldberg Machine. [Rube Goldberg Machines](#) are overly complicated ways to do simple things. This is the opposite of what you would want for cybersecurity. It is difficult to monitor and easier to break.
  - a. In cybersecurity, less is more, a concept known as **simplicity**. The simpler, the easier to notice and fix problems, which makes programs more secure.
  - b. **Minimization** is similar; it means reducing the ways that software can be attacked. By minimizing the programs and limiting access to data, you minimize the opportunities for hackers to break in.

**Additional online resources:**

- If this is a potential career interest, check out National Security Agency’s high school and college [internship opportunities](#)

**When you’re finished:** Congratulations, you have earned your badge! You can purchase by emailing [shopdept@gksmo.org](mailto:shopdept@gksmo.org) or at <https://www.girlscoutshop.com/senior-cybersecurity-basics-badge>

No shipping charges apply at this time.

---

