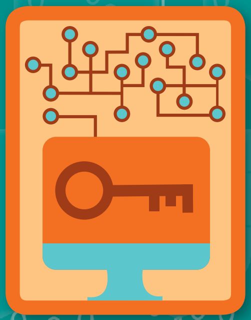

Badge 1: Cybersecurity Basics

If you want to stop hackers from stealing information or disrupting other people's computers, you need to know about how computers and computer programs work. Learn how computer programmers write code and set up systems to slow down or stop hackers.

Steps

1. Find out how computers run multiple programs
2. Identify functions and privileges
3. Learn how computers hide information
4. Design a layered security system
5. Design a Rube Goldberg machine

Purpose

When I've earned this badge, I'll know the principles of cybersecurity and how cybersecurity experts use them to protect computer networks and information.

STEP 1 Find out how computers run multiple programs

Imagine getting ready for school in the morning while you're talking to your mom, packing your lunch, and trying to find your cell phone. That's called multitasking.

The problem is that our brains aren't designed to multitask. You're more likely to make mistakes when you multitask.

Computers often have to multitask, too. When a computer multitasks, it creates an opportunity for hackers to break in. Every program you're running or website you're using provides a kind of entry point to your computer. Computer programmers have developed ways to help computers run multiple programs more efficiently and more safely.

- Each **process**, or program running, is separated into its own space in the computer's memory. You can see a form of this when you have multiple tabs open on your computer running different programs. This is called **process isolation**. Every program gets to work in its own space.
- **Domain separation** is another way programmers help computers multitask more efficiently. Domain separation helps prevent large data breaches by keeping different types of data separate, such as credit card numbers and social security numbers. Domain separation also restricts employees from having access to different kinds of data. For example, employees who work on the website may be restricted from accessing customer data, to prevent customer data from getting published on the website.

WORDS TO KNOW

Address space an area of the computer's memory that only one program can access

Bar code a black-and-white code that can contain a variety of different types of data and be read by a machine

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

Data packet a piece of a message (called a unit of data) that's transmitted through the internet

Digital object anything that is stored on a computer. This might be data, user information, software programs, etc.

Faraday cage a box or enclosure made of metal that conducts electricity and prevents electromagnetic charges from reaching whatever is inside it

Hops the number of routers that a packet passes through from its source to its destination

Hotspot a wireless access point, typically in a public location, that provides internet access to laptops, smartphones, or other devices

Insider threat a current or former employee, contractor, or other business partner who has access to an organization's data or network information. Because of this access, they could be involved in a cyberattack

IP address IP stands for internet protocol. It's a series of numbers unique to that device. Any device connected to a network has its own IP address

Privileges defining who can and cannot use an object

Process a program running on a computer

Security vulnerability a weakness in a device or program through which it can be hacked or exploited

Smart devices electronics that are connected to the internet, like phones, tablets, laptops, smart watches, smart TVs, smart thermostats, or home security systems

Stakeholder a person who is affected by an organization's actions and policies

Traceroute a list that shows the path data packets travel from one website or device to another

GenCyber's First Principles of Cybersecurity

Hackers constantly look for new ways to break into other people's computers. Cybersecurity experts have to make hacking as hard as possible. These ten principles of cybersecurity, created by the National Security Agency (NSA) and the National Science Foundation (NSF), cover different aspects of computing to make a computer system safer.

Abstraction removing any unnecessary information

Data hiding keeping information from being seen or accessed by certain users

Domain separation keeping things (like processes or user accounts) separate from each other

Layering using multiple strategies to protect yourself or your digital stuff

Least privilege giving as few people as necessary access to digital content

Minimization reducing the number of ways someone can hack a digital device or software

Modularity dividing software programs into small "modules," or components, so that you can edit them more easily

Process isolation running every computer program in its own area of a computer's memory

Resource encapsulation labeling a digital object, like a file or folder, based on who can use it and how it should be used

Simplicity making designs as simple, streamlined, and easy to understand as possible

DOES YOUR COMPUTER KNOW WHAT TIME IT IS?

GPS, or the Global Positioning System, is a group of satellites in space that work together to provide exact locations on earth. It's why the map app on your phone works, but is also really important in a lot of other ways.

For example, each satellite has a special clock in it, and they work together to give computers on earth the EXACT time down to the billionth of a second. Banks, airlines, fire stations, police departments, TV stations, and the military are just a few of the organizations that use computers or other technology that depend on the GPS clocks.

In 2016, a computer glitch caused some GPS satellites to transmit bad timing data. Computers on earth started shutting down. Cell phone towers stopped working. Radio stations lost their signals. Computers at all kinds of organizations—from businesses to government agencies—were affected.

The glitch was fixed in less than a day, but it brought a big problem into focus: much of the world's economy and services depends on the GPS clocks. If they fail, it impacts everything. Cybersecurity experts have warned that the all-important role GPS plays also makes it a prime target for hackers.

STEP 2 Identify functions and privileges

Would you wear swimming flippers to go ice skating? Would you try to frost a cake before you baked it? Of course not! You use ice skates for ice skating, not swimming flippers. And you need to bake a cake before you ice it.

These are examples of **resource encapsulation**. This cybersecurity idea labels parts of the program or data based on who can use it and how it's used. This protects the code or data from revealing any more about itself than it needs to run a program. Programmers bundle, or encapsulate, programming and data, and label it. All the contents of the bundle still work, but the user and the rest of the program don't have access to the details.

A related idea is **least privilege**. That means as few people as necessary should have access to digital "stuff." Identifying who can use computer hardware, programs, and data—and limiting how they can be used—limits the ways hackers make trouble.

STEP 3 Learn how computers hide information

Computer programmers use a similar idea called abstraction. The goal is to remove anything on the screen that can distract you or be used incorrectly.

For example, when you open a spreadsheet, you only see the columns and rows, numbers, and mathematical functions. You input your data and tell the spreadsheet to sum up columns or find averages. The program does the mathematical calculations for you, but you don't see how the math gets done. You just see the result of the calculation. When you create an account on a website, you don't see the code that stores your username and password so you can log in again later. You only see the login page.

Programmers want to provide the minimum information necessary to a user to accomplish a task. When you see a little hourglass or spinning circle on your computer screen, that means a part of the program you're using is running (like checking your username and password to log you in), but the programmer hasn't given you access to see it.

Another concept programmers use is called **data hiding**. That just means that programmers hide data from users who don't need access. For example, in banking, a teller will be able to see only data about your account needed to complete your transaction.

STEP 4 Design a layered security system

Trying to break into a computer security system is like trying to get out of an escape room, but in reverse. When you do an escape room activity, you solve a series of puzzles in a particular order to get out. When hackers want to break into a computer, they have to get through a series of security systems in a particular order to reach their goal.

Using multiple security strategies is called **layering**. Cybersecurity experts create a series of obstacles, such as firewalls and antivirus software, to protect the computer system. They also limit access through passwords, multi-factor authentication, and resource encapsulation. Layered security systems may have a time limit to ensure users really know the passwords and aren't just guessing. They may also lock users out after inputting the wrong password too many times.

Programmers also use **modularity** to make computers more secure. Programs are divided into smaller components, or "modules." If there's a problem, the programmer can edit or swap out the module instead of having to rewrite the whole program. Modularity applies to the parts of a computer, too. If your sound card fails, you can replace it. Modularity make computers and programs easier to fix and limits the damage a hacker can do.

STEP 5 Design a Rube Goldberg machine

Rube Goldberg's wacky machines may be great fun to build and play with, but you wouldn't want to be responsible for keeping one running smoothly. All those moving parts mean more for you to monitor and more places where the machine can break down.

In cybersecurity, less is more. That's another way of describing the principle of **simplicity**. The simpler, more streamlined, and easier to understand a program is, the better. When software is simple, it's easier to notice and fix problems. That makes the programs more secure.

Minimization is a cybersecurity concept that's similar to simplicity. It means reducing the number of ways that software can be attacked. When you work to make your programs simple and you limit access to data, you minimize the opportunities hackers have to break into your system.

SOLVE SIMPLE PROBLEMS IN COMPLEX WAYS

Reuben Goldberg was a famous cartoonist. He studied engineering in college and liked to invent things. He drew lots of different types of cartoons throughout his career, including political cartoons and ones about sports. He's most famous for his cartoon strip *The Inventions of Professor Lucifer Gorgonzola Butts*. Professor Butts invented crazy, ridiculously complicated machines to do simple tasks, such as opening an umbrella. The cartoons led to people describing needlessly complicated things as "Rube Goldberg machines."

Rube died in 1970, but people still hold contests to see who can build the best machine. Each contest has a task, such as assembling a hamburger, putting toothpaste on a toothbrush, or putting money in a piggy bank. Inventions are judged on creativity, silliness, and teamwork.

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

- Giving a classroom presentation about what I’ve learned.
- Partnering with a cybersecurity professional to create a video on the ten principles of cybersecurity.
- Developing a workshop for others showing them how to use concepts like least privilege and layering to improve their personal cybersecurity.

I’m inspired to: