Cybersecurity Badges

Glossary

Abstraction—the principle of removing any unnecessary information.

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

Barcode—a black-and-white code that can contain a variety of different types of data, which can be read by a machine.

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

Data hiding—the principle of keeping information from being observed or accessed by certain users.

Data packet—a piece of a message (called a unit of data) which is transmitted through the Internet.

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

Domain separation—the principle of keeping things (like processes or user accounts) separate from each other.

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

Hops—a computer networking term that refers to the number of routers that a packet (a portion of data) 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 cyber attack, whether or not they mean to.

IP address—IP stands for "Internet Protocol." An IP address is a series of numbers unique to that device. Any device connected to a network has its own IP address.

Layering—the principle of using multiple strategies to protect something. For example, a castle is protected by a moat, guards, fences, etc.

Least privilege—the principle of giving as few people as necessary access to digital content.

Minimization—the principle of reducing the number of ways that someone can hack a digital device or software.

Modularity—the principle of dividing software programs into small "modules" or components, so that you can edit them more easily.

Privileges—defining who can and cannot use an object.

Process—a program running on a computer.

Process isolation—the principle that states that every process runs in its own area of a computer's memory.

Resource encapsulation—the principle of labeling digital objects based on their use (what can use it), privilege (who can use it), and operations (how it should be used).

Rube Goldberg Machine—machine, contraption, invention, device, or apparatus that is deliberately over-engineered or overdone to perform a very simple task in a very complex fashion, usually including a chain reaction. The expression is named after American cartoonist and inventor Rube Goldberg (1883–1970).

Security vulnerability—a weakness in a device or program through which it could be hacked or exploited.

Simplicity—the principle of making designs as simple, streamlined, and intuitive as possible.

Smart devices—electronics that are connected to the Internet, like phones, tablets, laptops, smart watches, smart TVs, smart thermostats, home security systems, etc.

Stakeholder—a person who is affected by an organization's actions and policies. For example, if a chain of stores is hacked, the company's stakeholders include their customers, suppliers, and shareholders.

Traceroute—a list created by a computer that shows the path data travels from one website or device to another.