
COMPUTER AWARENESS
EPISODE-15
COMPUTER SECURITY

CA FUNSTA
UNBOX THE NEW WAY OF LEARNING

Computer Awareness

Part 7

- Funsta Team

Lets Start

CA FUNSTA
UNBOX THE NEW WAY OF LEARNING

Computer Awareness

Part 1 Intro/Generation/ Classification of Computers

Part 2 Computer Architecture & Memory

Part 3 Computer Hardware

Part 4 Computer Software and System Utilities

Part 5 Number System

Part 6 Computer Codes & Logic Gates

Lets move on to
Next Part

CA FUNSTA
UNBOX THE NEW WAY OF LEARNING

Computer Awareness

Part 7 Introduction to Operating System

Part 8 Operating System

Part 9 Data Communication

Part 10 Computer Networks & Network Topology

Part 11 OSI Layers & Network

Part 12 Database Management System (DBMS)

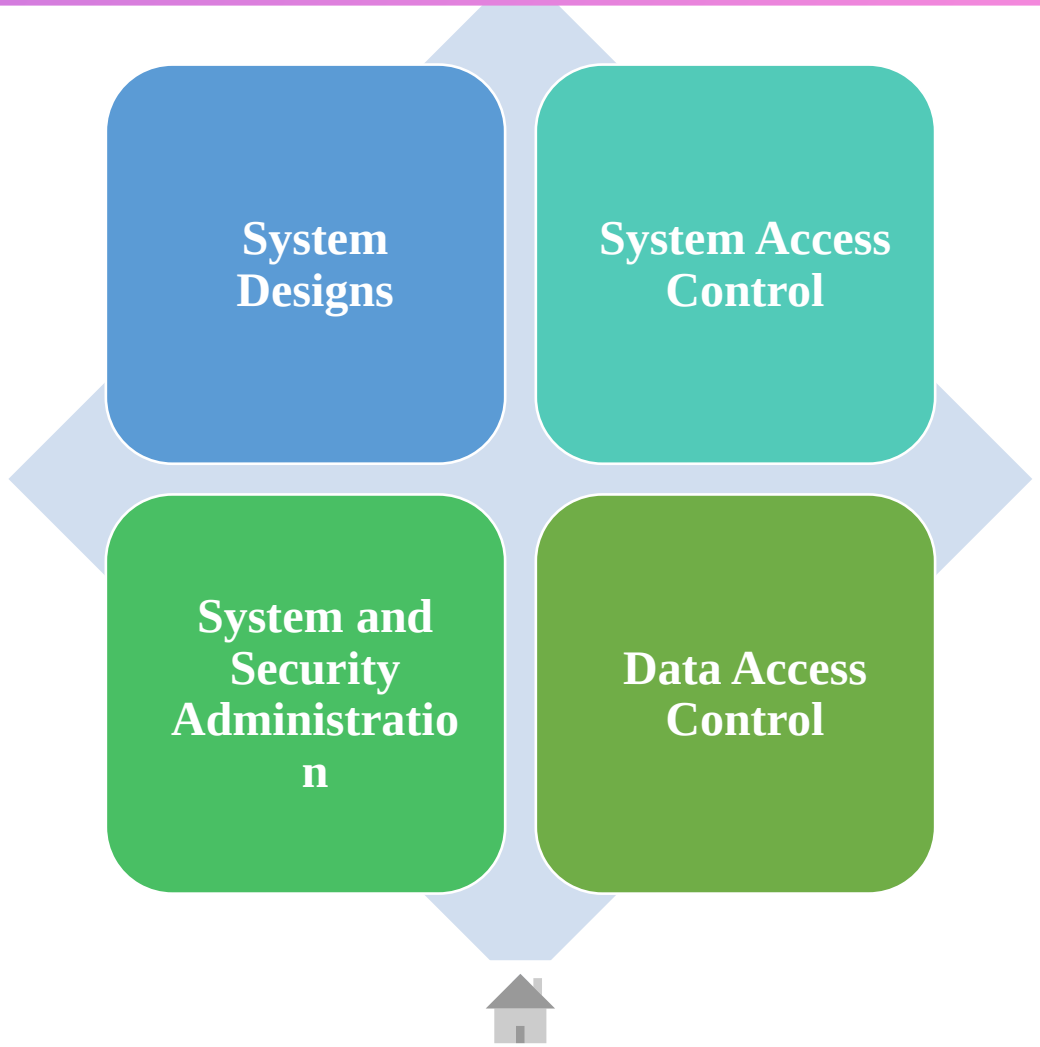
Lets move on to
Next Part

CA FUNSTA
UNBOX THE NEW WAY OF LEARNING

Computer Security

Computer security, also known as cybersecurity or IT **security**, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

Methods of Provide Protection



System Access Control

Access control is a **security** technique that regulates who or what can view or use resources in a computing environment.

Physical **access control** limits **access** to campuses, buildings, rooms and physical IT assets.

Logical **access control** limits connections to **computer** networks, **system** files and data.

Back to
Methods of Provide Protection

Data Access Control

Database **access control** is a method of allowing **access** to company's sensitive **data** only to those people (database users) who are allowed to **access** such **data** and to restrict **access** to unauthorized persons.

It includes two main components: **authentication and authorization**.

Back to
Methods of Provide Protection

System and Security Administration

A **system administrator**, or sysadmin, is a person who is responsible for the upkeep, configuration, and reliable operation of computer **systems**; especially multi-user computers, such as servers.

Back to
Methods of Provide Protection

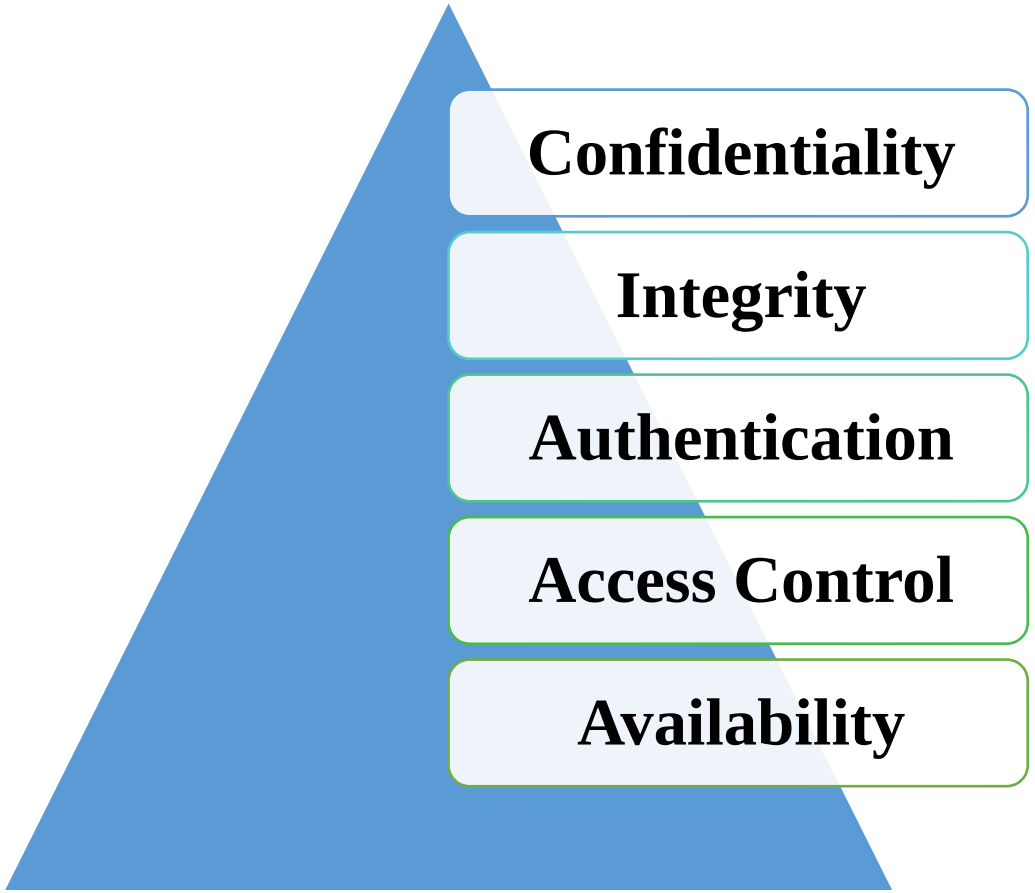
System Designs

Systems design is the process of defining the architecture, modules, interfaces, and data for a **system** to satisfy specified requirements.

Systems design could be seen as the application of **systems** theory to product development.

Back to
Methods of Provide Protection

Components of Computer Security



Confidentiality

- **Confidentiality** is the concealment of information or resources.
- Also, there is a need to keep information secret from other third parties that want to have access to it, so just the right people can access it.

Back to
Components of Computer Security

Integrity

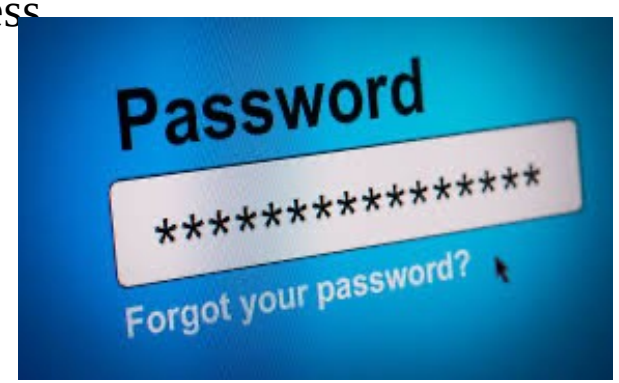
Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change.

Integrity includes data **integrity** (the content of the information) and origin **integrity** (the source of the data, often called authentication).

Back to
Components of Computer Security

Authentication

- Regarding **computer** systems, authenticity or **authentication** refers to a process that ensures and confirms the user's identity.
- The process begins when the user tries to access data or information.
- The user must prove access rights and identity. Commonly, usernames and passwords are used for this process.



Back to
Components of Computer Security

Access Control

Access control is a **security** technique that regulates who or what can view or use resources in a **computing** environment.

It is a fundamental concept in **security** that minimizes risk to the business or organization. There are two types of **access control**: physical and logical.

Back to
Components of Computer Security

Availability

Availability refers to the ability to access data of a resource when it is needed, as such the information has value only if the authorized people can access at right time.

Denying access to data nowadays has become a common attack.

Back to
Components of Computer Security

Worms

- A computer **worm** is a standalone malware computer program that replicates itself in order to spread to other computers.
- **Worms** almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
- The ILOVEYOU, Michelangelo, and MSBlast **worms** are famous **examples**

Trojan

- A **Trojan** horse or **Trojan** is a type of malware that is often disguised as legitimate software.
- **Trojans** can be employed by cyber-thieves and hackers trying to gain access to users' systems.
- Users are typically tricked by some form of social engineering into loading and executing **Trojans** on their systems.

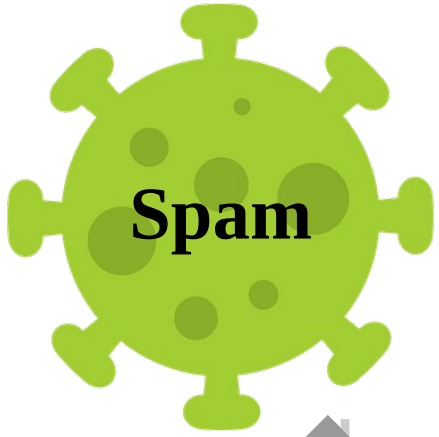
Spyware

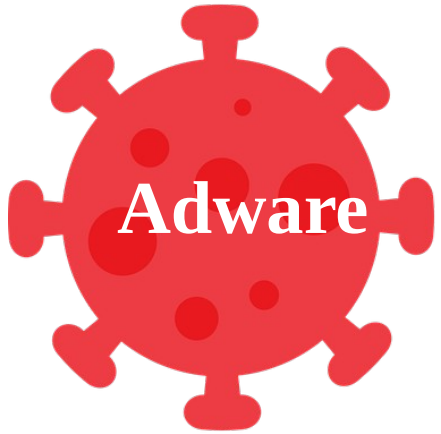
- Spyware is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information.
- Spyware is classified as a type of **malware** — **malicious software** designed to gain access to or damage your computer, often without your knowledge.
- Eg: CoolWebSearch (CWS) , Gator (GAIN),180search Assistant, ISTbar/AUpdate

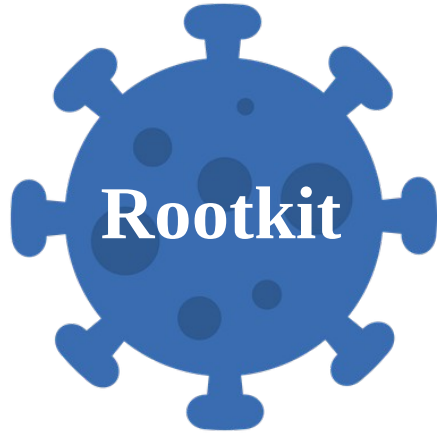
Symptoms of Malware Attack

- **Slow** computer. Are your operating systems and programs taking a while to start up?
- Blue screen of death (BSOD)
- Lack of storage space.
- Suspicious modem and hard drive activity.
- **Pop-ups**, websites, toolbars, and other unwanted programs.
- You're sending out spam.

Some Other Threats to Computer Security







Spoofing

Spoofing, as it pertains to cybersecurity, is when someone or something pretends to be something else in an attempt to gain our confidence, get access to our systems, steal data, steal money, or spread malware.

Spoofing attacks come in many forms, primarily: Email **spoofing**.

Back to
Some Other Threats
to Computer Security

Hacking

Hacking is an attempt to exploit a **computer** system or a private network inside a **computer**. Simply put, it is the unauthorized access to or control over **computer** network **security** systems for some illicit purpose.

Black hat **hackers hack** to take control over the system for personal gains.

Back to
Some Other Threats
to Computer Security

Cracking

A **cracker** is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent.

Back to
Some Other Threats
to Computer Security

Phishing

- **Phishing** is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.
- It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

Back to
Some Other Threats
to Computer Security

Spam

- **Spam** is any kind of unwanted, unsolicited digital communication, often an email, that gets sent out in bulk.
- **Spam** is a huge waste of time and resources.

Back to
Some Other Threats
to Computer Security

Adware

- **Adware**, or advertising supported software, is software that displays unwanted advertisements on your **computer**.
- **Adware** uses the browser to collect your web browsing history in order to 'target' advertisements that seem tailored to your interests.

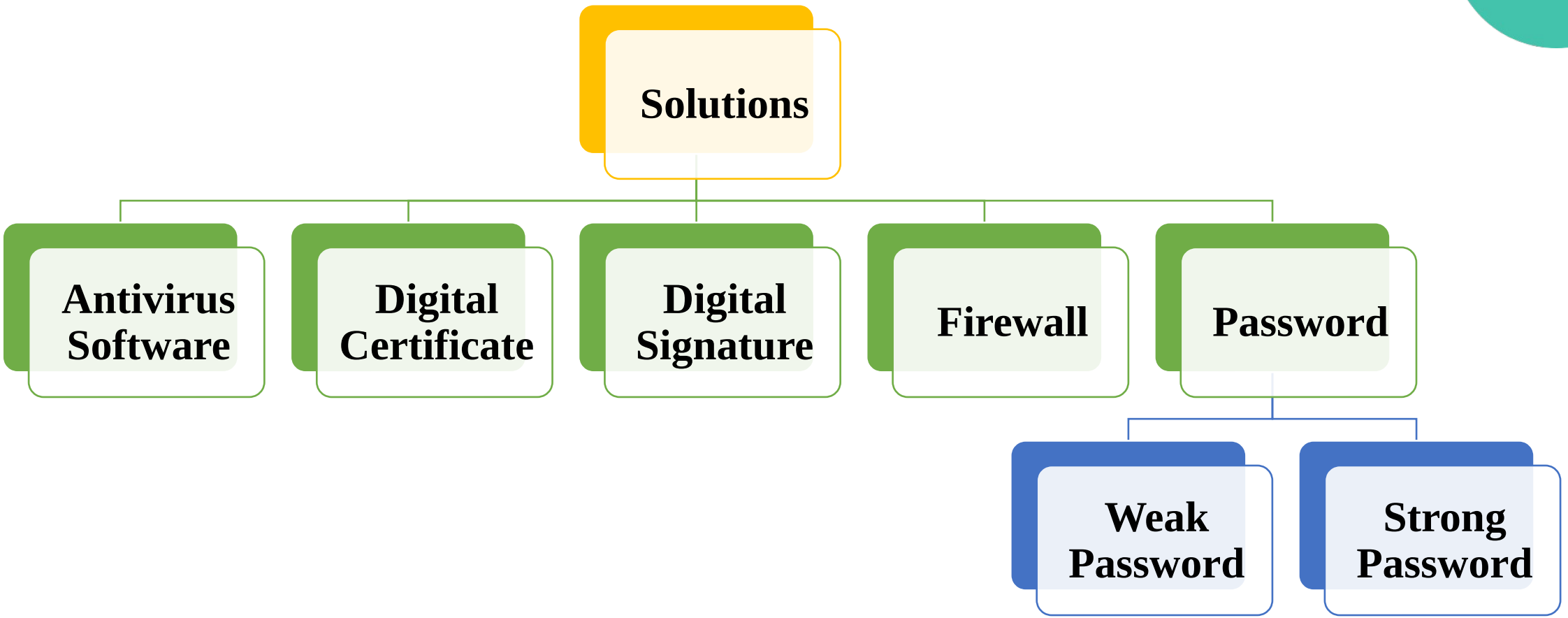
Back to
Some Other Threats
to Computer Security

Rootkit

- A **rootkit** is a clandestine **computer** program designed to provide continued privileged access to a **computer** while actively hiding its presence.
- Today **rootkits** are generally associated with malware – such as Trojans, worms, viruses – that conceal their existence and actions from users and other system processes.

Back to
Some Other Threats
to Computer Security

Solutions to Computer Security Threats



Antivirus Software

- **Antivirus software** helps protect your **computer** against malware and cybercriminals.
- **Antivirus software** looks at data — web pages, files, **software**, applications — traveling over the network to your devices.
- It searches for known threats and monitors the behavior of all programs, flagging suspicious behavior.
- Eg: Avast, K7, McAfee

Back to
Solutions to Computer Security Threats

Digital Certificate

- A digital certificate provides information about the identity of an entity.
- A digital certificate is issued by a Certification Authority (CA).
- Examples of trusted CA across the world are **Verisign**, **Entrust**, etc.
- The CA guarantees the validity of the information in the certificate.

Back to
Solutions to Computer Security Threats

Digital Signature

Digital Signature is a process that guarantees that the contents of a message have not been altered in transit.

When you, the server, digitally sign a document, you add a one-way hash (encryption) of the message content using your public and private key pair.

Back to
Solutions to Computer Security Threats

Firewall

- A **firewall** is a security device — **computer** hardware or software — that can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on your **computer**.
- Three basic types of firewalls —**packet filtering**, application, and **packet** inspection— are designed to control traffic flows.
- The previous descriptions provide general functionality of the operation of these types of firewalls

Back to
Solutions to Computer Security Threats

Password

- **PASSWORD**. - Personal Access Security Service Without Regscloseular Decloser.
- A **password** is a string of characters used for authenticating a user on a **computer** system.
- For example, you may have an account on your **computer** that requires you to log in.
- Most **passwords** are comprised of several characters, which can typically include letters, numbers, and most symbols, but not spaces
- There are two Types.
  - Weak Password
  - Strong Password

Back to
Solutions to Computer Security Threats

Weak Password

A **password** that is easy to detect both by humans and by **computer**.

People often use obvious **passwords** such as the names of their children or their house number in order not to forget them.

Examples of weak passwords: qwert12345, Gbt3fC79ZmMEFUFJ, 1234567890, 987654321, nortonpassword.

Back to Password

Back to Solutions to Computer Security Threats

Strong Password

A **password** that is hard to detect both by humans and by the **computer**.

Two things make a **password** stronger: (1) a larger number of characters, and (2) mixing numeric digits, upper and lower case letters and special characters ($, #, etc.).

An **example of a strong password** is “Cartoon-Duck-14-Coffee-Glvs”. It is long, contains all 4 character types, and is easy to remember.

There are 4 uppercase letters, 19 lowercase letters, 2 numbers, and 4 symbols totaling 27 characters.

Back to Password

Back to Solutions to Computer Security Threats

File Access Permission

File permissions control what user is permitted to perform which actions on a **file**.

In the traditional method, **files** have attributes describing the owner of the **file** and the group the **file** is in, as well as **permissions** for the owner, group, and everyone else.

It has three types

- Read Permission
- Write Permission
- Execute Permission

Read Permission

Read will allow you to open the file, view its attributes, owner, and **permissions**

Back to
File Access Permission

Write Permission

Write will allow you to **write** data to the file, append to the file, and **read** or change its attributes.

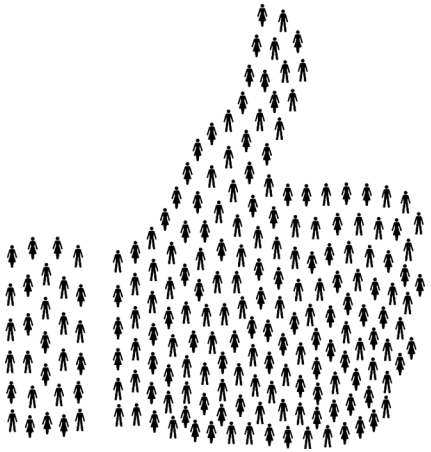
Back to
File Access Permission

Execute Permission

- **Execute permission** on files means the right to **execute** them, if they are programs. (Files that are not programs should not be given the **execute permission**.)
- For directories, **execute permission** allows you to enter the directory (i.e., cd into it), and to access any of its files.

Back to
File Access Permission

‘Hurrah!’
We completed this section.



Next Section

Coming Soon...