

UNIT 1.3

Introduction to Cyber Security?

Cyber Security is a process that's designed to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services.

The world of Cyber Security revolves around the industry standard of confidentiality, integrity, and availability, or CIA. Privacy means data can be accessed only by authorized parties; integrity means information can be added, altered, or removed only by authorized users; and availability means systems, functions, and data must be available on-demand according to agreed-upon parameters.

The main element of Cyber Security is the use of authentication mechanisms. For example, a user name identifies an account that a user wants to access, while a password is a mechanism that proves the user is who he claims to be.

Types of Cyber Crimes

Cybercrime is any unauthorized activity involving a computer, device, or network. The three types are computer-assisted crimes, crimes where the computer itself is a target, and crimes where the computer is incidental to the crime rather than directly related to it.

Cybercriminals usually try to profit off of their crimes using a variety of tactics, including:

- Denial of Service, or DOS

Where a hacker consumes all of a server's resources, so there's nothing for legitimate users to access

- Malware

Where victims are hit with a worm or virus that renders their devices useless

- Man in the Middle

Where a hacker puts himself between a victim's machine and a router to sniff data packets

- Phishing

Where a hacker sends a seemingly legitimate-looking email asking users to disclose personal information

Other types of cyberattacks include cross-site scripting attacks, password attacks, eavesdropping attacks (which can also be physical), SQL-injection attacks, and birthday attacks based on algorithm functions.