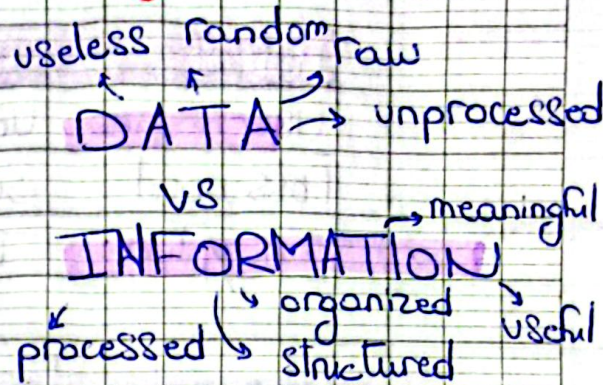


Chapter 1: Security Concepts

Data Threats:

Can be anything from:

- Virus attacks
- Stealing Information
- "Acts of God" (Fires, Flood, ...)



Cyber Crime

download legal music software

stealing confidential info on the internet

Any type of illegal activity using a computer, the internet, a private or public network

Hacking

- Get unauthorized access to info.
- No harm intended

Cracking

- Taking hacking one step further by causing harm

Ethical Hacking

- Companies employ hackers to help them identify threats

All crackers are hackers, not all hackers are crackers.

Threats to data

1) Force Majeure

- Natural Disasters
- Can't be controlled by humans

2) Insider Threats

- From inside the businesses
 - ↳ Employees
 - ↳ Service providers (external contractors with access)
 - ↳ External Insiders (From outside, with access)

Identity Theft

- Stealing personal info (name, address, tel, date of birth)

- purpose: using these info to commit fraud
- Methods: Information Diving, Dumpster Diving (from trash), Mail Theft, Social Media, Skimming (credit card data), Phishing

→ Information Diving

- 1) Dumpster Diving: go through someone's garbage to obtain info
- 2) Mail Theft: target mailbox, get mails with personal info
- 3) Social Media

→ Skimming

Capturing personal info associated with credit cards

→ Pretexting

create false scenario to manipulate someone into revealing sensitive info.

→ Measures to prevent unauthorized access

Method	Description
Username	Unique name to identify who's logging in
Password	Sequence of characters to verify user identity
Encryption	Translation of data into secret code

→ Characteristics of Information Security

• Confidentiality

Ensures that only those with privileges have access

• Integrity

Quality of being whole, complete and uncorrupted (data hasn't been tampered with)

• Availability

Reliable and timely access to data

→ Social Engineering

The art of manipulating people to give up personal and confidential information

• Methods:

↳ Phone calls (Vishing)

↳ Fraudulent emails/websites (Phishing)

↳ Watching someone enter information (Shoulder Surfing)

→ Phishing

- Sending emails that appear to be from legitimate sources, but are actually fake
- Include link to fake websites
- Requires users to manually click a link to activate code

→ Vishing (Phone Calls)

- Use phone calls to trick individuals into revealing sensitive info
- Impersonate representatives from trusted organization to gain trust.

→ Shoulder Surfing

- direct observation technique / watching someone enter information