

Threats to Information Security: Complete Glossary (CMA Part 1 Study Guide)

FREE STUDY NOTE · CMA PART 1 · KNOWLEDGE VALLEY

Using the internet exposes an entity's systems, devices, and documents to attack. CMA Part 1, Section E expects you to identify each threat precisely — many exam questions hinge on the difference between two similar-sounding terms (virus vs. worm, sniffing vs. man-in-the-middle). This glossary organizes them so the differences stick.

The three goals of information security

Goal	Meaning
Availability	Authorized users can access the system when needed.
Confidentiality	Secrecy of information — only authorized eyes see it.
Integrity	Preventing unauthorized or accidental modification of programs or data.

Malware: the malicious software family

Malware is software installed without the user's knowledge or consent — often bundled with a legitimate download. The exam tests each type's distinctive behavior:

Threat	What it does	Key exam distinction
Virus	Destroys or modifies data, deletes files; spreads through human interaction (email attachments, downloads, USB, shared files).	Needs a host + human action to spread.
Worm	Self-replicates across networks without human interaction; slows systems by multiplying. Lives inside other files (e.g., Word/Excel).	No human click needed — unlike a virus.
Trojan horse	Disguised as a legitimate program (e.g., a game); secretly installs code letting hackers take over or steal data. Targets a specific computer.	Does NOT self-replicate; built for targeted access.
Logic bomb	Dormant code that activates on a trigger — a date, time, or system condition — then destroys data.	Cannot spread on its own; needs a trigger event.
Spyware	Hides on a device, monitors activity, and steals sensitive info (passwords, bank details) for advertisers or criminals.	Goal is silent data collection, not destruction.
Ransomware	Locks the system and demands payment to restore access.	A criminal money-making scheme, often via malicious email links.
Back door	A deliberately built entry point (e.g., for emergency maintenance) that hackers discover and exploit.	Created intentionally — then abused.

Attacks on data and systems

Threat	What it does
Input manipulation	Errors in system design or data input that corrupt processing.
Program alteration	Unauthorized changes made to a program itself.
Direct file alteration	Data changed directly in a data file.
Data theft	Stealing trade secrets, customer lists, formulas.
Sabotage	Destroying the system for no personal gain — e.g., a disgruntled programmer injecting a logic bomb.
Theft (hardware)	Physical theft of laptops and devices.
Phishing	Fake messages/emails tricking users into revealing IDs, passwords, card numbers.
Password cracker	Software trying letter/number combinations — or whole dictionaries — to guess passwords.
Denial of Service (DoS)	Flooding a network with artificial traffic so legitimate users are locked out. Often uses Trojan-infected machines.
Buffer overflow	Sending more data than memory can hold — crashing the system or letting hackers seize control.
Spoofing (IP spoofing)	Faking a trusted website's identity (name or IP) to harvest credentials or damage a competitor's reputation.
Sniffing	Passively capturing and analyzing network traffic to steal info.
Man-in-the-middle (MitM)	Actively intercepting AND altering communication between two parties. Encryption defeats it.

Exam-critical distinction: sniffing is passive (only monitors); a man-in-the-middle attack is active (intercepts, monitors, and alters).

Exam tips: how CMA tests this topic

- Virus vs. worm vs. trojan vs. logic bomb is the single most tested set — learn the 'key exam distinction' column cold.
- Sniffing (passive) vs. man-in-the-middle (active) is a favorite pair.
- Phishing = tricking humans; spoofing = faking identity; pharming-style DNS tricks are out of scope — don't overthink.
- DoS = availability attack (it hits the 'A' of the CIA triad); ransomware = money extortion; spyware = silent theft.

Frequently asked questions

What are the three goals of information security?

Availability (authorized access), confidentiality (secrecy), and integrity (no unauthorized modification).

What is the difference between a virus and a worm?

A virus needs human interaction and a host file to spread; a worm self-replicates across networks with no human action.

What is a logic bomb?

Dormant malicious code that activates on a specific trigger — a date, time, or system condition — and then destroys data. It cannot spread by itself.

How does a man-in-the-middle attack differ from sniffing?

Sniffing passively monitors traffic; a man-in-the-middle attack actively intercepts and alters communication. Encryption defeats MitM attacks.

Study CMA (USA) with Knowledge Valley

These notes come straight from our CMA (USA) live classes. If you want the full Section E — taught live, with exam-focused short notes, 4,000+ practice MCQs and 14 mock exams — book a free orientation and trial class at knowledgevalley.net. 10+ years coaching CMA candidates across Pakistan, the Gulf and worldwide.