

Introduction to ICT Security Threats

Introduction to ICT Security Threats

Information and Communication Technology (ICT) security focuses on protecting data, devices, networks, and services from unauthorized access, disruption, or damage. Understanding the landscape of threats is the first step toward building effective defenses.

1. Core Concepts

Concept	Description
Threat	Any potential danger that could exploit a vulnerability to cause harm.
Vulnerability	Weakness in a system, process, or control that can be exploited.
Risk	The likelihood that a threat will exploit a vulnerability <i>and</i> the impact of that exploitation.
Asset	Anything of value that needs protection (e.g., data, hardware, reputation).
Countermeasure	Technical, procedural, or administrative actions taken to mitigate risk.

2. Classification of Threats

Category	Typical Examples	Primary Impact
Malware	Viruses, worms, ransomware, trojans, spyware	Data loss, system downtime, extortion
Network-Based Attacks	Denial-of-Service (DoS/DDoS), Man-in-the-Middle (MITM), ARP spoofing	Service interruption, data interception
Social Engineering	Phishing, pre-texting, baiting, tailgating	Credential theft, unauthorized access
Insider Threats	Malicious employees, careless staff, compromised accounts	Data leakage, sabotage
Physical Threats	Theft of devices, hardware tampering, environmental hazards	Loss of equipment, data exposure
Supply-Chain Threats	Compromised third-party software, hardware implants	Broad compromise across multiple organizations

Introduction to ICT Security Threats

3. Common Attack Vectors

1. Email & Messaging

- Phishing links, malicious attachments, business email compromise (BEC).

2. Web & Browsers

- Drive-by downloads, malicious scripts, compromised websites (watering hole attacks).

3. Removable Media

- Infected USB drives, external hard disks.

4. Remote Access

- Weak VPN configurations, exposed RDP ports, insecure SSH keys.

5. Software Vulnerabilities

- Unpatched operating systems, outdated libraries, zero-day exploits.

6. Cloud Services

- Misconfigured storage buckets, insecure APIs, credential leakage.
-

4. Threat Lifecycle (Kill Chain)

1. **Reconnaissance** – Gather information about targets (public records, social media).
2. **Weaponization** – Create or acquire exploit tools (malware, exploit kits).
3. **Delivery** – Transmit the weapon (email, drive-by download, USB).
4. **Exploitation** – Trigger vulnerability to gain foothold.
5. **Installation** – Deploy persistent malicious code (backdoors, rootkits).
6. **Command & Control (C2)** – Establish communication with attacker's server.
7. **Actions on Objectives** – Data exfiltration, encryption, sabotage, espionage.

Understanding each stage helps defenders disrupt the chain early.

Introduction to ICT Security Threats

5. Impact Categories

Impact Type	What It Affects	Example Consequences
Confidentiality	Unauthorized disclosure of data	Data breach, privacy violations
Integrity	Unauthorized alteration of data	Corrupted records, false financial statements
Availability	Disruption of services	Outage, loss of productivity
Accountability	Loss of traceability	Difficulty attributing actions