

## SECP1513: Technology Information System

## Mind Map Chapter 7

Semester 1 2024/2025

1<sup>st</sup> December 2024

**Faculty of Computing** 

## Prepared by:

Muhammad Thaqif bin Abdul Aziz	SX231702ECJHF04
Aqilah binti Mohamad Kasim	SX231764ECRHF04
Muhammad Munzir bin Mohamed Dauzkaply Nor	SX240286ECRHS04

		Accuracy: Emphasizes the importance of correct and secure data collection to ensure that the information is reliable and trustworthy.
		Property: Discusses the ownership of data, raising questions about who has the rights to access and control personal information.
		Access: Focuses on the control individuals have over how their data is used, highlighting the need for user consent and transparency.
Shift Towards Cookie-less Tracking: Companies are moving away from	colle gove	e Databases: Refers to extensive ections of data held by entities such as ernments and financial institutions, ch can be used for various purposes.
traditional cookie-based tracking methods to enhance user privacy.  Consumer Control: There is a growing demand from consumers for more control	and prof	rmation Resellers: Companies that buy sell personal data to create detailed iles of individuals, often without their wledge.
over their personal data and how it is used.  Transparency Requirements: Organizations are expected to be transparent about their data collection and usage practices to  Data Privacy  Recent Trends	asso iden	s: Identifies potential dangers ciated with big data, including tity theft and misuse of personal rmation.
Cloud Backup Services: The rise of cloud-based solutions for secure data storage, providing users with reliable options for		Illusion of Anonymity: Explains how users often believe they are anonymous online, while their activities can be tracked.
data protection.		Cookies: Describes how cookies are used for tracking user behavior, distinguishing between first-party and third-party cookies.
Protection of Networks: IT security experts are responsible for safeguarding networks and data systems from threats and breaches.	Internet & Web	Privacy Modes: Introduces features like incognito and private browsing that aim to enhance user privacy online.
Skills Required: A degree in computer science (CS) and practical experience are essential for success in this field.		Spyware: Discusses software that secretly monitors user activities, posing a threat to personal privacy.
Salary Range: The average salary for IT security professionals ranges from \$62,000 to \$101,000, reflecting the demand for skilled workers.  Role of IT Security Professionals  Part 4: Careers in IT Security  Ethics		DoS Attacks: Denial of Service attacks that overload systems, rendering them unusable and disrupting services.
Growth Potential: There is a high demand for security experts due to the increasing prevalence of cyber threats and the need for robust security measures.		Rogue Wi-Fi: Fake wireless networks set up to steal personal data from unsuspecting users who connect to them.
16. Tobast security measures.		
Moral Guidelines: Establishes a framework	Cybercrimes	Identity Theft: Involves stealing personal information for financial fraud, leading to significant financial and emotional distress.
for ethical behavior in technology use, guiding professionals in their decision-making.	Cybercrimes	information for financial fraud, leading to
for ethical behavior in technology use, guiding professionals in their decision-	Cybercrimes	information for financial fraud, leading to significant financial and emotional distress.  Phishing: The practice of creating fake websites to deceive users into providing
for ethical behavior in technology use, guiding professionals in their decision-making.  Copyright & Piracy: Discusses the legal protections for creators and the implications of software piracy on intellectual property rights.  Digital Rights Management (DRM): Technologies that prevent unauthorized use of digital content, ensuring creators  Part 3: Ethics	Cybercrimes	information for financial fraud, leading to significant financial and emotional distress.  Phishing: The practice of creating fake websites to deceive users into providing sensitive information.  Viruses: Malicious software that attaches itself to legitimate programs, spreading
for ethical behavior in technology use, guiding professionals in their decision-making.  Copyright & Piracy: Discusses the legal protections for creators and the implications of software piracy on intellectual property rights.  Digital Rights Management (DRM): Technologies that prevent unauthorized use of digital content, ensuring creators are compensated.  Plagiarism: The unethical act of claiming someone else's work as one's own, which	Malware Types	information for financial fraud, leading to significant financial and emotional distress.  Phishing: The practice of creating fake websites to deceive users into providing sensitive information.  Viruses: Malicious software that attaches itself to legitimate programs, spreading when the infected program is run.  Worms: Self-replicating malware that spreads across networks without needing
for ethical behavior in technology use, guiding professionals in their decision-making.  Copyright & Piracy: Discusses the legal protections for creators and the implications of software piracy on intellectual property rights.  Digital Rights Management (DRM): Technologies that prevent unauthorized use of digital content, ensuring creators are compensated.  Plagiarism: The unethical act of claiming		information for financial fraud, leading to significant financial and emotional distress.  Phishing: The practice of creating fake websites to deceive users into providing sensitive information.  Viruses: Malicious software that attaches itself to legitimate programs, spreading when the infected program is run.  Worms: Self-replicating malware that spreads across networks without needing to attach to a host program.  Trojan Horses: Malicious software disguised as legitimate applications,
for ethical behavior in technology use, guiding professionals in their decision-making.  Copyright & Piracy: Discusses the legal protections for creators and the implications of software piracy on intellectual property rights.  Digital Rights Management (DRM): Technologies that prevent unauthorized use of digital content, ensuring creators are compensated.  Plagiarism: The unethical act of claiming someone else's work as one's own, which undermines academic and professional		information for financial fraud, leading to significant financial and emotional distress.  Phishing: The practice of creating fake websites to deceive users into providing sensitive information.  Viruses: Malicious software that attaches itself to legitimate programs, spreading when the infected program is run.  Worms: Self-replicating malware that spreads across networks without needing to attach to a host program.  Trojan Horses: Malicious software disguised as legitimate applications, tricking users into installing them.  Zombies and Botnets: Networks of compromised computers controlled
for ethical behavior in technology use, guiding professionals in their decision-making.  Copyright & Piracy: Discusses the legal protections for creators and the implications of software piracy on intellectual property rights.  Digital Rights Management (DRM): Technologies that prevent unauthorized use of digital content, ensuring creators are compensated.  Plagiarism: The unethical act of claiming someone else's work as one's own, which undermines academic and professional		information for financial fraud, leading to significant financial and emotional distress.  Phishing: The practice of creating fake websites to deceive users into providing sensitive information.  Viruses: Malicious software that attaches itself to legitimate programs, spreading when the infected program is run.  Worms: Self-replicating malware that spreads across networks without needing to attach to a host program.  Trojan Horses: Malicious software disguised as legitimate applications, tricking users into installing them.  Zombies and Botnets: Networks of compromised computers controlled remotely to perform malicious activities.  Access Control: Techniques such as firewalls, passwords, and biometrics that restrict unauthorized access to systems