Shoug Alomran

Comprehensive Glossary

Table of Contents

Introduction to Ethics

Term	Definition	Example
Autonomy	The principle that individuals should have control over their own lives and be allowed to make decisions that apply to their lifestyle.	A patient chooses whether to accept or refuse a medical treatment.
Beneficence	An ethical principle requiring actions that promote the well-being of others and contribute positively to society.	A software engineer fixes a security vulnerability to protect users from harm.
Cultural Relativism	The view that an action is morally right if a person's culture approves of it; it denies the existence of objective moral principles.	A custom accepted in one country may be considered unethical in another.
Directives	Micro-level ethical rules specifically designed to guide the actions of individuals.	"Do not harm others."
Divine Command Theory	An ethical theory asserting that moral judgments are derived from God's commandments and that "good" is aligned with God's will.	Lying is wrong because God forbids it.
Ethics	The philosophical and rational study of morality, focusing on evaluating moral beliefs and behaviors.	Deciding whether collecting users' personal data without consent is morally acceptable.
Impartiality	A feature of a moral system requiring that rules apply equally to all people without bias or favoritism.	A university applies the same cheating policy to every student regardless of status.
Informal	A feature of a moral system where moral rules are generally not enforced by law but by society and personal conscience.	People may criticize someone for being dishonest even if no law was broken.
Justice	An ethical principle stating that decision-makers should focus on actions that are fair to all parties involved.	Two employees with the same performance receive equal pay.
Least Harm	An ethical principle stating that when every option causes some harm, the morally preferable choice is the one that minimizes overall harm.	During a disaster, doctors prioritize patients they can realistically save.
Morality	A system consisting of rules of conduct and principles of evaluation used to prevent harm and promote human flourishing.	Society generally agrees that stealing and murder are morally wrong.
Public	A feature of a moral system requiring that moral rules be publicly known and understood by everyone.	Traffic laws are published so every driver knows the rules.
Rational	A feature of a moral system requiring moral decisions to be based on logical reasoning rather than emotions alone.	A judge bases a verdict on evidence rather than personal feelings.
Respect	An ethical principle requiring individuals to recognize the dignity, rights, and autonomy of others.	A company asks for a user's consent before collecting personal information.
Social Policies	Macro-level ethical rules used to establish guidelines for society as a whole.	"Software should be protected by copyright laws."
Subjective Relativism	The theory that an action is morally right if an individual personally approves of it; right and wrong are entirely personal.	A person believes cheating is acceptable because they personally see nothing wrong with it.

Ethical Theories and Moral Systems

Term	Definition	Example
Act Utilitarianism	An ethical theory stating an act is morally right if its consequences produce the greatest good for the greatest number of people.	Sacrificing one road lane to build a hospital that benefits thousands of people.
Categorical Imperative	A universal moral law identified by Kant that must be followed regardless of desires or circumstances.	Never lie, even if telling the truth is difficult.
Deontology	Derived from the Greek word *deon* (duty); an ethical framework based on following universal moral laws and obligations.	Returning a lost wallet because it is your duty, not because you expect a reward.
End in Itself	The Kantian principle of treating people with respect for their dignity and autonomy, rather than using them merely as a means to achieve a goal.	A company asks for employees' consent before collecting personal data instead of secretly monitoring them.
Golden Mean	Aristotle's principle that virtue lies between two extremes: excess and deficiency.	Courage is the balance between cowardice and recklessness.
Good Will	For Kant, the only thing that is always good in itself; the motivation to do what is right because it is a duty.	Returning extra change because it is the right thing to do, even if nobody would notice.
Human Flourishing (Eudaimonia)	Aristotle's idea that the ultimate goal of life is to achieve excellence and live a virtuous, fulfilling life.	A person develops honesty, courage, and wisdom to become the best version of themselves.
Imperfect Duty	A moral obligation that should generally be followed but allows flexibility in how and when it is fulfilled.	Helping those in need when reasonably able to do so.
Intellectual Virtues	Virtues associated with reasoning, wisdom, and the pursuit of truth, as identified by Aristotle.	Critical thinking and good judgment when solving ethical dilemmas.
Moral Virtues	Habits or dispositions formed through repeated virtuous actions, such as honesty and courage.	A person becomes honest by consistently telling the truth.
Negative Right	A right that others respect by refraining from interfering with an individual.	Freedom of speech—others must not prevent you from expressing your opinion.
Perfect Duty	An absolute, unconditional obligation that must always be followed, often expressed as a prohibition.	Do not steal, regardless of the circumstances.
Positive Right	A right that requires others to provide a service or perform an action.	The right to receive public education.
Principle of Utility	The "Greatest Happiness Principle"; an action is morally right if it maximizes overall happiness for those affected.	Choosing a policy that benefits the majority of society.
Rule Utilitarianism	An ethical theory stating an action is right if it follows a rule that, if universally followed, would produce the greatest overall good.	Following traffic laws because society is safer when everyone obeys them.

Social Contract	An implicit agreement among individuals to follow moral rules and accept government enforcement for mutual benefit.	Citizens obey traffic laws in exchange for safer roads and public order.
Universalizability	The requirement that a moral rule must be one that everyone could logically follow without contradiction.	If everyone broke promises whenever convenient, promises would lose all meaning.
Vice	A character trait that prevents human flourishing; often an excess or deficiency of a virtue.	Greed is a vice because it represents an excess of desire for wealth.
Virtue Ethics	An ethical theory emphasizing the development of excellent character traits rather than focusing only on rules or consequences.	A person tells the truth because they strive to be an honest person, not because of punishment or reward.

Professional Ethics

Term	Definition	Example
Agency Model	A relationship model where the professional acts as an agent, carrying out exactly what the client instructs them to do.	A software consultant builds only the features requested by the client without offering alternatives.
Causal Responsibility	Responsibility assigned to individuals because their actions (or failure to act) directly caused an event.	A programmer introduces a bug that causes the system to crash.
Code of Ethics	A statement of principles and core values that guides the ethical behavior of members of a profession.	The ACM Code of Ethics guides software engineers in making ethical decisions.
Due Care	Taking reasonable precautions and exercising the level of care expected from a competent professional to prevent harm.	A software engineer thoroughly tests a medical system before deployment.
Due Diligence	The continuous process of identifying risks, maintaining security measures, and ensuring due care is consistently applied.	A company regularly performs security audits and installs software updates.
External Whistleblowing	Reporting illegal, harmful, or unethical activities to outside authorities, such as government agencies or the media, usually after internal efforts have failed.	An employee reports environmental violations to a government regulator after management ignores the issue.
Internal Whistleblowing	Reporting unethical or illegal behavior to someone within the organization in an attempt to resolve the issue internally.	An employee reports accounting fraud to the company's ethics committee.
Legal Responsibility	Responsibility imposed by law, regardless of personal opinions or intentions.	A company is legally liable for injuries caused by a defective product.
Moral Responsibility	A personal obligation to consider the ethical consequences of one's actions; it cannot simply be transferred to someone else.	A software engineer refuses to release unsafe software despite pressure from management.
Paternalistic Model	A relationship model where the professional makes decisions on behalf of the client, believing they know what is best.	A doctor chooses a treatment without consulting the patient.
Professional Ethics	The ethical standards and responsibilities that guide members of a particular profession.	A software engineer protects confidential client information even after leaving the company.
Role Responsibility	Responsibility arising from the duties and expectations associated with a particular job or role.	A system administrator is responsible for protecting company servers.
Trust Model	A relationship model where the professional provides advice and options while the client participates in the final decision.	A financial advisor explains investment options, and the client chooses which one to follow.
Utilitarianism	An ethical approach that evaluates actions by comparing their overall benefits and harms to achieve the greatest good for the greatest number.	Choosing a software update that benefits millions of users even though it temporarily inconveniences a small number.
Whistleblower	A person who discloses harmful, illegal, or unethical practices within an organization to protect the public interest.	An employee exposes a company for knowingly selling unsafe software.

Technical and Ethical Issues in Systems Analysis and Design

Term	Definition	Example
Cancelled Vacation Syndrome	A situation where managers pressure employees to sacrifice personal time and money to meet unrealistic project deadlines.	A manager cancels everyone's vacation so a medical software project can be completed before release.
Deontological Approach	An ethical approach based on following duties, rules, and professional obligations regardless of the consequences.	A software engineer refuses to release unsafe software because it violates professional duties.
Ethical Behavior	Acting in accordance with moral values, professional standards, and accepted ethical principles.	A developer reports a serious security flaw instead of hiding it.
Hazard Log	A document used to record identified hazards, monitor their status, and ensure every hazard is resolved before deployment.	Engineers document every possible failure in an aircraft control system and verify each one has been addressed.
Informed Consent	The principle that users should understand how a system works, what information is collected, and the consequences of using it before agreeing.	A hospital explains how patient data will be stored before asking patients to sign a consent form.
LOPSA	The League of Professional System Administrators, an organization that provides a Code of Ethics for system administrators.	A system administrator follows the LOPSA Code of Ethics when handling confidential company data.
N-version Programming	A fault-tolerance technique where multiple independent teams develop the same software requirements, and a voting mechanism selects the correct output.	Three separate teams develop aircraft control software, and the system compares their outputs before executing a command.
Quality Assurance (QA)	Activities performed throughout the software development process to ensure the final product meets required quality standards.	QA engineers perform repeated testing before a banking application is released.
Red Lies	Knowingly making false statements about the status, quality, or progress of a project.	A manager tells the client that the software has been fully tested even though testing is incomplete.
Redundancy	Providing multiple interchangeable components so that if one fails, another immediately takes over.	An aircraft has multiple flight control computers so it can continue operating if one fails.
Requirements Engineering	The process of gathering, analyzing, documenting, and managing software requirements before development begins.	Developers identify that students must complete prerequisites before enrolling in a course.
Risk Analysis	The process of identifying possible failures, estimating their likelihood and impact, and planning methods to prevent or reduce those risks.	Engineers analyze what could happen if a hospital's life-support system suddenly loses power.
Safety-Critical Systems	Systems whose failure could result in injury, death, environmental damage, or major financial loss.	Air traffic control software or a pacemaker.

Software Engineer	A professional who applies engineering principles to design, develop, test, maintain, and improve software systems.	A software engineer develops an online banking application.
Software Maintenance	Modifying software after deployment to fix bugs, improve performance, or adapt to new requirements.	Releasing an update to patch a security vulnerability.
Software Requirements	A documented description of the functions, constraints, and behaviors a software system must satisfy.	"Only students who have completed the prerequisite course may enroll."
Sweep It Under the Rug	Ignoring known problems in the hope that they disappear instead of resolving them.	Management releases software despite knowing it contains critical bugs.
System Safety Engineer	A specialist responsible for identifying hazards, evaluating risks, maintaining hazard logs, and ensuring safety requirements are satisfied throughout development.	A safety engineer reviews every subsystem of a nuclear reactor before deployment.
Systems Analyst	A professional who analyzes business problems and designs information system solutions that satisfy organizational needs.	A systems analyst gathers requirements before developers begin coding.
Technical Issues	Problems related to the design, implementation, testing, or operation of software and hardware systems.	A database vulnerability allows unauthorized access to customer information.
Validation	The process of determining whether the correct system has been built by checking that it satisfies user needs and requirements.	Users test a university portal to confirm it supports course registration correctly.
Verification	The process of determining whether the system has been built correctly according to its specifications and design.	Developers review code and perform unit testing to ensure each module meets its specification.

Network Security and Countermeasures

Term	Definition	Example
Application-layer Attack	An attack targeting applications running on servers or workstations, often using malware such as viruses, worms, or Trojans.	Exploiting a vulnerability in a web application to steal customer data.
Backdoor	A hidden method of bypassing normal authentication to gain unauthorized access to a system.	A programmer secretly creates an administrator account that only they know about.
Biometrics	Authentication based on unique physical or behavioral characteristics, such as fingerprints, facial recognition, or iris scans.	Unlocking a smartphone using Face ID.
Compromised-Key Attack	An attack where an attacker obtains a user's private cryptographic key and uses it to decrypt communications or impersonate the user.	A hacker steals an employee's private key and reads encrypted emails.
Cyber-piracy	The unauthorized copying, distribution, or use of copyrighted software or digital content.	Downloading and distributing cracked software.
Cyberterrorism	Politically motivated cyberattacks intended to cause widespread fear, disruption, or economic damage.	Attacking a country's power grid for political purposes.
Denial of Service (DoS)	An attack in which a **single attacker** overwhelms a system or service with traffic, making it unavailable to legitimate users.	One computer repeatedly sends requests until a website becomes unavailable.
Dictionary Attack	A password attack that repeatedly guesses passwords using common words or predictable combinations.	Trying thousands of common passwords like "password123" until one works.
Distributed Denial of Service (DDoS)	A resource attack in which **multiple compromised systems** simultaneously flood a server or network until it becomes unavailable.	A botnet launches millions of requests against an online shopping website.
Eavesdropping	The unauthorized interception of communications while they are being transmitted.	An attacker secretly listens to an unencrypted Wi-Fi conversation.
Email Bombing	A form of DoS attack where an inbox is flooded with massive numbers of emails to prevent legitimate communication.	Sending thousands of emails to fill an employee's mailbox.
Exploit Attack	An attack that takes advantage of software bugs, vulnerabilities, or misconfigurations to gain unauthorized access.	Exploiting an unpatched operating system vulnerability.
Insider Threat	A security threat originating from someone within the organization, either intentionally or accidentally.	An employee accidentally gives confidential information to a scam caller.
IP Address Spoofing	The act of disguising a packet's true source by forging its IP address.	An attacker pretends to be a trusted company server.
Logic Attack (Logic Bomb)	Malicious code designed to execute only when a specific condition or event occurs.	A programmer inserts code that deletes company files if they are fired.

Man-in-the-Middle (MitM)	An attack where an attacker secretly intercepts and may modify communications between two parties.	A hacker intercepts data sent over an insecure public Wi-Fi network.
Password	A secret sequence of characters used to authenticate a user's identity.	Logging into an online banking account using a password.
Phishing	A social engineering attack that tricks users into revealing sensitive information by pretending to be a trusted organization.	A fake bank email asks a customer to "verify" their password.
Resource Attack	An attack that consumes excessive system resources, making services slow or unavailable.	A DDoS attack exhausts a server's CPU and bandwidth.
Script Kiddie	An inexperienced attacker who uses existing hacking tools without fully understanding how they work.	Downloading a hacking tool from the Internet and running it without modification.
Security Hole (Vulnerability)	A weakness in software, hardware, or system configuration that attackers can exploit.	Leaving default administrator credentials unchanged.
Sniffing (Snooping)	Using software to capture and read unencrypted network traffic.	Capturing usernames and passwords transmitted over HTTP.
Social Engineering	Manipulating people into revealing confidential information by exploiting trust rather than technical weaknesses.	Calling an employee while pretending to be IT support to obtain a password.
Stealth Backdoor	A specially designed backdoor that hides its presence and avoids detection during normal audits.	Malware secretly creates a hidden administrator account that does not appear in normal account listings.
Strong Password	A password containing uppercase and lowercase letters, numbers, special characters, and no easily guessed personal information.	**M!7qZ@4Lp2$**
Structured Hacker	A skilled attacker who carefully plans attacks, researches targets, and possesses advanced programming and networking knowledge.	Spending months studying a company's network before launching an attack.
Technical Weakness	A flaw or vulnerability in hardware, software, or network configuration that may be exploited by attackers.	A router left with its default password.
Time Bomb	A malicious program that remains inactive until a specific time or condition triggers its execution.	Code that activates after an employee stops logging into the system.
Unstructured Hacker	An inexperienced attacker with limited technical knowledge who performs attacks with little planning.	A teenager randomly trying hacking tools downloaded from the Internet.
Weak Password	A password that is easy to guess because it uses common words, personal information, or simple patterns.	**football123** or **password**

Privacy in Cyberspace

Term	Definition	Example
Biometrics	Systems designed to identify or verify individuals using unique physical or behavioral characteristics such as fingerprints, iris scans, facial recognition, voice, or DNA.	Unlocking a smartphone using Face ID.
Cloud Computing	A computing model where data and programs are stored and accessed over the Internet rather than locally, raising concerns about data ownership, privacy, and legal jurisdiction.	Saving files to Google Drive instead of storing them only on your computer.
Computer Matching	The process of cross-checking information from multiple unrelated databases to identify matching records ("hits").	Comparing passport records with criminal databases to identify suspects.
Computer Merging	Also called **Data Banking**; combining information from multiple unrelated databases into one composite database.	Combining hospital, banking, and university records into one file.
Contextual Integrity	The principle that personal information should only be used for the purpose and in the context in which it was originally collected.	A hospital shares patient records with advertisers without the patient's permission.
Cookies	Small files stored on a user's device that remember browsing preferences and other information for future visits.	A website remembers your preferred language after you return.
Cross-Device Tracking	The practice of linking a user's activities across multiple devices to create a single profile for advertising or analytics.	Searching for shoes on your phone and seeing the same ads later on your laptop.
Cyber-Privacy	The protection and control of personal information collected, stored, shared, and exchanged through digital technologies.	Choosing who can access your personal information online.
Data Banking	Another term for **Computer Merging**, where multiple databases containing personal information are integrated into one central database.	A government combines tax, healthcare, and education databases into one system.
Data Mining	The analysis of large datasets to discover hidden patterns, relationships, and trends that can be used to predict behavior.	An online store recommends products based on your previous purchases.
Dataveillance	The continuous monitoring of people's activities through computer technology to collect and analyze personal data.	Software records every website an employee visits during work hours.
Device Fingerprint	A unique combination of hardware and software characteristics used to identify and track a device without storing cookies.	A website recognizes your computer based on installed fonts and browser settings.
E-Government	The use of information technology by governments to provide online public services and interact electronically with citizens.	Renewing your passport through an online government portal.

First-Party Cookie	A cookie created by the website the user is currently visiting to improve functionality and remember preferences.	Amazon remembers the items in your shopping cart.
Flash Cookie (Supercookie)	A persistent cookie that cannot normally be removed by clearing browser history or deleting standard cookies.	A website still recognizes your device after you've cleared your browser cookies.
Government Surveillance	The monitoring of citizens by government agencies using technology for purposes such as security, law enforcement, or intelligence gathering.	Security cameras and facial recognition used in airports.
Information Privacy	The degree of control an individual has over how their personal information is collected, stored, shared, and exchanged.	Deciding whether an app may access your location.
Internet of Things (IoT)	A network of Internet-connected physical devices that collect and exchange data automatically.	A smart thermostat that adjusts your home's temperature remotely.
Online Behavioural Tracking	Monitoring a user's browsing activities across multiple websites to build profiles for advertising and analytics.	Advertisers tracking the websites you visit to show targeted ads.
P3P (Platform for Privacy Preferences)	A protocol allowing websites to declare their privacy policies so browsers can compare them with users' privacy preferences.	A browser warns that a website's privacy policy conflicts with your settings.
Privacy	The fundamental right to be left alone and free from unwanted interference or intrusion.	Choosing not to share your medical history with others.
Profiling	Creating a profile of an individual by analyzing patterns discovered through data mining.	A bank predicts that a customer is a high-risk borrower based on spending habits.
RFID (Radio Frequency Identification)	Technology using a microchip (tag) and reader communicating via radio waves to identify and track objects or people.	A public transport card that is scanned when entering a train station.
Surveillance Drone (UAS)	An unmanned aerial system equipped with cameras or sensors to monitor people or locations from the air.	A police drone monitoring traffic during a public event.
Surveillance Technology	Hardware or software used to secretly monitor or record people's activities.	Malware that activates a victim's webcam without permission.
Third-Party Cookie	A cookie created by an external organization, usually an advertising network, to track users across multiple websites.	Facebook or Google ads following your browsing activity on different websites.
Tracking Cookie	A third-party cookie designed specifically to monitor browsing behavior and deliver targeted advertisements.	Seeing ads for a product after visiting an online shopping website.
Web 2.0	The interactive web where users generate content and often exchange personal information in return for online services.	Posting photos and comments on Instagram or Facebook.

Cloud Computing: Services, Security, and Ethical Frameworks

Term	Definition	Example
Account Hijacking	The unauthorized acquisition of user credentials to eavesdrop on, manipulate, or falsify cloud-based data and transactions.	A hacker steals an employee's Microsoft 365 password and accesses company files.
Availability	Ensuring that cloud services and data remain accessible to authorized users whenever they are needed.	A cloud provider uses backup servers so users can still access Gmail during hardware failures.
Cloud Computing	A computing model where IT resources and services are delivered over the Internet instead of being hosted locally.	Using Google Drive instead of storing files only on your computer.
Compliance	Adhering to laws, regulations, organizational policies, and industry standards throughout the development and operation of cloud systems.	A hospital cloud system complies with healthcare privacy regulations.
Confidentiality	Protecting information from unauthorized disclosure by ensuring only authorized users can access it.	Encrypting patient records stored in the cloud.
Data Breach	An incident in which confidential information is accessed, disclosed, or stolen by unauthorized individuals.	A hacker leaks customer credit card information from a cloud database.
EaaS (Equipment as a Service)	A cloud service model that facilitates connecting and managing Internet of Things (IoT) devices and equipment over the Internet.	A company remotely manages thousands of smart sensors installed in factories.
Hybrid Cloud	A cloud deployment model combining public and private cloud services to balance flexibility and security.	A company stores sensitive employee data in a private cloud while hosting its website in a public cloud.
IaaS (Infrastructure as a Service)	A cloud service model that provides virtualized computing resources such as servers, storage, networking, and processing power.	Renting virtual servers from Amazon EC2.
Integrity	Ensuring that information remains accurate, complete, and unaltered except by authorized users.	Preventing unauthorized modifications to financial records stored in the cloud.
Malware Injection	Malicious code inserted into cloud services that executes as though it were a legitimate cloud instance.	An attacker uploads a malicious virtual machine to steal cloud data.
Multi-Tenancy	A cloud architecture where multiple customers share the same physical infrastructure while their data remains logically separated.	Several companies use the same cloud server without accessing each other's data.
PaaS (Platform as a Service)	A cloud service model providing the platform, operating system, and development tools needed to build and deploy applications.	Developing a web application using Google App Engine.
Private Cloud	A cloud environment dedicated exclusively to a single organization for greater control and security.	A bank hosts its own private cloud for customer financial records.

Privacy	The right of users to control how their personal information is collected, stored, processed, and shared within cloud environments.	Choosing whether a cloud provider may collect usage statistics.
Public Cloud	A cloud environment owned and operated by a third-party provider and made available to the general public.	Microsoft Azure or Amazon Web Services (AWS).
SaaS (Software as a Service)	Cloud-hosted software applications delivered directly to end users over the Internet.	Gmail, Microsoft 365, or Dropbox.
Security	The protection of cloud systems, applications, and data against unauthorized access, attacks, and misuse.	Using firewalls and encryption to secure cloud storage.
Sustainability	The ability of cloud infrastructures to reduce environmental impact by minimizing physical hardware, energy consumption, paper usage, and commuting.	Companies reduce electricity consumption by moving servers to energy-efficient cloud data centers.
Trust	The confidence users place in cloud providers to securely store, manage, and protect their information.	A hospital chooses a trusted cloud provider to host patient records.
Utilitarianism	An ethical approach suggesting that cloud policies should maximize benefits for the greatest number of users while minimizing harm.	A cloud provider implements stronger security measures even if they slightly inconvenience users because it protects millions of accounts.
Virtualization	The technology that allows multiple virtual machines or operating systems to run on a single physical server, forming the foundation of cloud computing.	One physical server hosts dozens of independent virtual servers.

Social Media Ethical, Legal, and Security Issues

Term	Definition	Example
Background Check	The process of reviewing a person's online presence, including social media, to verify qualifications or identify information relevant to employment decisions.	An employer reviews a candidate's LinkedIn profile before hiring them.
Digital Marketing	The use of social media and other online platforms to promote products, strengthen brand loyalty, and gather customer insights.	A company advertises a new product on Instagram and TikTok.
Electronic Word-of-Mouth (eWOM)	Online recommendations, reviews, and opinions shared by users that influence others' purchasing decisions.	A customer posts a positive review about a restaurant on Google Maps.
Facebook Exchange (FBX)	Facebook's advertising system that uses real-time bidding and browsing history to display retargeted advertisements.	After visiting a shoe store website, Facebook shows advertisements for the same shoes.
Hashtag	A keyword preceded by the # symbol used to categorize content and improve its discoverability on social media.	**#CyberSecurity** or **#ETHC303**
Marketplace Ads	Traditional Facebook advertisements displayed in the side column containing a headline, description, and image.	A clothing company advertises a seasonal sale using a Marketplace Ad.
Nomophobia	The fear or anxiety of being without a mobile phone or unable to use it.	Feeling stressed because your phone battery dies while you're away from home.
Privacy Settings	User-controlled settings that determine who can view, share, or interact with personal information on social media.	Setting your Instagram account to **Private** so only approved followers can view your posts.
Promoted Posts	Paid Facebook posts that increase the visibility and reach of existing content.	A business pays to promote an announcement about a new product launch.
Reputation Management	The process of monitoring and maintaining an individual's or organization's online image.	A company responds professionally to negative online reviews to protect its reputation.
Retargeting	An online advertising technique that shows advertisements to users based on websites or products they previously visited.	Looking at a laptop online and later seeing ads for that same laptop on Facebook.
Social Media	Online platforms that allow users to create, share, and interact with content and communicate with others.	Facebook, Instagram, X, TikTok, and LinkedIn.
Social Networking	The creation of online communities that enable people to communicate, collaborate, and share information regardless of geographic location.	Students joining a Facebook group to discuss a university course.
Social Networking Use Policy	An organization's formal policy defining acceptable employee behavior, security requirements, and the appropriate use of social media.	A company prohibits employees from sharing confidential information on social media.
Social Signals	User interactions such as likes, shares, comments, and reposts that search engines and platforms may use to evaluate content popularity and relevance.	A blog post with thousands of shares ranks higher in search results.

Sponsored Stories	Facebook advertisements that highlight a user's interaction with a business (such as liking a page or checking in) and display it to their friends.	Your friend likes a restaurant, and Facebook shows that interaction as an advertisement.
Web of Trust (WOT)	A browser extension that evaluates and warns users about potentially malicious or untrustworthy websites.	WOT warns that a website has a poor reputation before you visit it.

Principles of Business Ethics

Term	Definition	Example
Business Ethics	The application of moral principles and ethical standards to business decisions and organizational conduct.	A company refuses to use child labor even if it reduces costs.
Code of Ethics	A formal document that outlines the ethical principles and expected standards of behavior for members of an organization.	Employees sign and follow the company's Code of Ethics.
Corporate Social Responsibility (CSR)	A company's commitment to operating ethically while contributing positively to society, the environment, and the economy.	A company funds environmental conservation projects and community education programs.
Ethical Leadership	Leadership that demonstrates honesty, integrity, fairness, and ethical decision-making while setting an example for others.	A CEO openly admits a company mistake and takes responsibility for correcting it.
Fairness	The ethical principle of treating all individuals and stakeholders equally, impartially, and without discrimination.	Two employees with equal qualifications receive the same promotion opportunity.
Global Ethics	The application of ethical principles while respecting cultural differences and international business practices.	A multinational company follows local labor laws while maintaining universal human rights standards.
Integrity	Acting honestly, consistently, and according to strong moral principles, even when no one is watching.	A manager reports an accounting error that benefits the company financially.
Organizational Ethics	The ethical values, principles, and culture that guide decision-making within a specific organization.	A company prioritizes customer privacy in all of its business decisions.
Professional Ethics	Ethical standards governing the behavior of members of a particular profession.	An accountant refuses to falsify financial records.
Stakeholder	Any individual or group that is affected by or has an interest in an organization's decisions and activities.	Customers, employees, shareholders, suppliers, and the local community.
Sustainability	Conducting business in a way that meets current needs without compromising the ability of future generations to meet their own needs.	A company reduces energy consumption and switches to renewable energy sources.
Transparency	The practice of communicating honestly and openly with stakeholders about business activities and decisions.	A company publicly reports a data breach instead of hiding it.
Whistleblowing	Reporting unethical, illegal, or harmful activities within an organization to protect the public interest.	An employee reports that the company is knowingly violating environmental regulations.

Understanding Social Engineering

Term	Definition	Example
Dumpster Diving	The practice of searching through discarded materials to find sensitive information such as documents, passwords, hardware, or storage devices that can aid an attack.	An attacker finds employee contact lists in a company's trash bin.
Impersonation	Pretending to be another person or authority to gain trust, information, or physical access.	An attacker pretends to be an IT technician to obtain an employee's password.
Malware	Malicious software designed to damage systems, steal information, or gain unauthorized access to a computer.	A Trojan secretly steals online banking credentials.
PBX (Private Branch Exchange)	A private telephone network within an organization that attackers may exploit to make fraudulent calls appear to originate internally.	A scammer manipulates the PBX so a call appears to come from the company's IT department.
Phishing	A social engineering attack that uses fraudulent emails or websites to trick victims into revealing sensitive information.	A fake bank email asks users to "verify" their login credentials.
Phishing Test	A simulated phishing attack conducted by an organization to assess employee awareness and improve security training.	A company sends fake phishing emails to employees as part of cybersecurity training.
Phone Spoofing	The technique of falsifying caller ID information so a phone call appears to come from a trusted source.	An attacker makes a call appear to come from the victim's bank.
Pretexting	Creating a believable but false scenario or identity to convince a victim to disclose information or grant access.	An attacker pretends to be an HR employee requesting personal information.
Shoulder Surfing	Obtaining confidential information by watching someone enter passwords or other sensitive data.	An attacker watches someone type their ATM PIN.
Smishing	A phishing attack carried out through SMS text messages that encourages immediate action using fear, urgency, or rewards.	A text message claims your bank account has been locked and asks you to click a link.
Social Engineering	The manipulation of people into revealing confidential information or performing actions that compromise security by exploiting human psychology rather than technical vulnerabilities.	An attacker convinces an employee to reveal their password over the phone.
Spear Phishing	A highly targeted phishing attack directed at a specific individual or organization using personalized information.	A fake email addressed specifically to a company's finance manager requesting a bank transfer.
Vishing	A social engineering attack conducted over the telephone, often using phone spoofing to appear legitimate.	An attacker pretends to be a bank representative and asks for a customer's verification code.
Whaling	A phishing attack targeting high-ranking executives or government officials to gain access to valuable information or systems.	A CEO receives a fake email requesting confidential financial information.

Ethical Hacking and Information Security

Term	Definition	Example
Advanced Persistent Threat (APT)	A sophisticated, long-term cyberattack in which an attacker gains unauthorized access and remains hidden while continuously monitoring or stealing information.	A nation-state hacker secretly remains inside a government network for months collecting classified information.
Asset	Anything of value that must be protected from threats, including hardware, software, information, and people.	A company's customer database.
Attack Surface	The total number of possible entry points that an attacker can use to access or compromise a system.	Open network ports, websites, employee accounts, and remote access services.
Availability	Ensuring authorized users can access systems, services, and information whenever needed.	A hospital's patient database remains available 24/7.
Bot	Software capable of performing automated tasks or being remotely controlled by an attacker.	Malware installed on a victim's computer waiting for commands.
Botmaster	The attacker who controls a botnet and issues commands to compromised devices.	A hacker instructs thousands of infected computers to launch a DDoS attack.
Botnet	A collection of compromised devices (zombies) controlled by a botmaster to perform coordinated malicious activities.	Thousands of infected computers simultaneously attack a website.
Confidentiality	Protecting information from unauthorized access or disclosure.	Encrypting patient medical records.
Cyber Attack	Any deliberate attempt to gain unauthorized access to, damage, or disrupt computer systems or networks.	A ransomware attack encrypts company files.
Daisy Chaining	Performing multiple attacks in sequence, where each successful attack provides information that enables the next attack.	A hacker steals login credentials, then uses them to access confidential databases.
Defensive Information Warfare	The protection of information systems against attacks while ensuring confidentiality, integrity, and availability.	Installing firewalls and intrusion detection systems to defend a military network.
Doxing	Collecting and publicly revealing private or identifying information about an individual without permission.	Publishing someone's home address and phone number online.
Exploit	Software or techniques that take advantage of a vulnerability to compromise a system.	Using an unpatched software flaw to gain administrator access.
Hack Value	The attractiveness or importance of a target from the attacker's perspective.	A major bank has a higher hack value than a personal blog.
Information Assurance (IA)	The practice of protecting information by ensuring its confidentiality, integrity, availability, authentication, and non-repudiation.	A government agency uses encryption and digital signatures to protect classified documents.
Information Warfare	The use of information systems and technologies to gain a strategic military, political, or economic advantage over an adversary.	Launching cyber operations to disrupt another country's communication systems.

Integrity	Protecting information from unauthorized modification or destruction while ensuring authenticity and accuracy.	Preventing unauthorized changes to financial records.
Non-repudiation	A security property ensuring that the sender cannot deny sending a message and the receiver cannot deny receiving it.	A digitally signed contract proves who signed it.
Offensive Information Warfare	Actions intended to disrupt, damage, or compromise an opponent's information systems.	Disabling an enemy's communication network during a military conflict.
Payload	The harmful portion of malicious software that performs the intended malicious action after infection.	A ransomware payload encrypts all files on a victim's computer.
Risk	The likelihood that a threat will successfully exploit a vulnerability and cause damage.	An unpatched server is at high risk of being compromised.
Threat	Any potential event, person, or circumstance capable of exploiting a vulnerability and causing harm to a system.	A hacker attempting to steal confidential information.
Vulnerability	A weakness in hardware, software, configuration, or procedures that can be exploited by attackers.	Leaving default administrator credentials unchanged.
Zero-Day Attack	An attack exploiting a previously unknown vulnerability before a security patch becomes available.	Attackers exploit a newly discovered browser vulnerability before the vendor releases an update.
Zombie Computer	A compromised computer secretly controlled by a botmaster as part of a botnet.	An infected home computer participates in a DDoS attack without the owner's knowledge.

Intellectual Property Laws and Ethical Practices

Term	Definition	Example
Competitive Intelligence (CI)	The ethical collection and analysis of information from public and legally obtainable sources to understand competitors and support business decisions.	A company analyzes a competitor's annual report before launching a new product.
Copyright	A legal protection granted to original works of authorship, including books, music, software, films, and artwork, once they are fixed in a tangible medium.	A programmer owns the copyright to software they created.
Copyright Infringement	The unauthorized use, reproduction, distribution, or display of copyrighted material without the owner's permission.	Downloading and distributing pirated software.
Cybersquatting	Registering or using a domain name in bad faith to profit from another person's trademark or brand reputation.	Registering **nike-shoes.com** hoping Nike will buy it.
Derivative Rights	The copyright owner's exclusive right to authorize new works based on the original work.	Turning a novel into a movie with the author's permission.
Digital Millennium Copyright Act (DMCA)	A U.S. law that prohibits bypassing technological protection measures used to protect copyrighted works.	Circumventing DVD encryption to copy a movie illegally.
Digital Rights Management (DRM)	Technologies used to control access to and prevent unauthorized copying of digital copyrighted content.	Netflix encrypts its videos so only subscribers can watch them.
Doctrine of First Sale	A legal principle allowing the owner of a physical copy of a copyrighted work to sell or give away that copy without the copyright owner's permission.	Selling a used textbook to another student.
Fair Use Doctrine	A legal doctrine allowing limited use of copyrighted material without permission for purposes such as criticism, teaching, research, commentary, or news reporting.	Using a short quotation from a book in a research paper.
Intellectual Property (IP)	Creations of the mind, including inventions, artistic works, symbols, designs, and software, protected by intellectual property laws.	A company's logo, patented invention, and software source code.
License	Legal permission granted by the owner of intellectual property specifying how others may use it.	Purchasing a software license to use Microsoft Office.
Open Source Software (OSS)	Software whose source code is publicly available and may be modified and redistributed according to its license.	Linux or Mozilla Firefox.
Patent	A legal right granted to inventors that prevents others from making, using, or selling an invention without permission for a limited period.	A company patents a new battery technology.
Patent Infringement	Using, making, or selling a patented invention without the patent holder's authorization.	Manufacturing a patented medical device without a license.
Plagiarism	Presenting another person's ideas, words, or work as your own without proper acknowledgment.	Copying paragraphs from a website into an assignment without citation.
Proprietary Software	Software owned by an individual or company that restricts modification, copying, and redistribution.	Microsoft Windows.

Public Domain	Creative works that are no longer protected by copyright and may be used freely by anyone.	A novel whose copyright has expired.
Reverse Engineering	Analyzing a product or software to understand how it works so it can be studied, improved, or made compatible.	Studying hardware to develop compatible replacement components.
Service Mark	A trademark used to identify and distinguish services rather than physical products.	The logo of an airline or consulting company.
Software License	A legal agreement specifying the rights and restrictions governing the use of software.	Accepting the End User License Agreement (EULA) before installing software.
Trade Dress	Protection for the distinctive appearance, packaging, or overall visual presentation of a product or business.	The unique layout and appearance of an Apple Store.
Trade Secret	Valuable confidential business information that provides a competitive advantage and remains protected as long as it is kept secret.	Coca-Cola's secret formula.
Trademark	A legally protected word, symbol, phrase, logo, or design used to identify the source of goods or services.	The Nike "Swoosh" logo.

Anti-Cyber Crime Law in Saudi Arabia

Term	Definition	Example
Computer Fraud	The use of computers or information systems to commit dishonest or illegal acts for financial or personal gain.	Altering payroll records to increase your own salary.
Cyber Defamation	Publishing false or harmful statements about a person or organization through electronic means with the intent to damage their reputation.	Posting false accusations about a business on social media.
Cyber Extortion	Demanding money, services, or other benefits by threatening to damage, expose, or disable computer systems or digital information.	A hacker demands payment to avoid leaking stolen company data.
Cyber Stalking	Using the Internet or electronic communication to repeatedly harass, threaten, or intimidate another person.	Continuously sending threatening messages through social media.
Cybercrime	Any criminal activity carried out using computers, networks, or digital technologies.	Stealing banking credentials through phishing emails.
Data Diddling	The unauthorized modification of data before, during, or after it is entered into a computer system.	An employee changes payroll data before salaries are processed.
Denial of Service (DoS)	An attack that prevents legitimate users from accessing a computer system or network by overwhelming its resources.	Flooding a government website with requests until it becomes unavailable.
Email Bombing	Sending an extremely large number of emails to overwhelm a mailbox or email server.	Filling a company's mailbox with thousands of spam emails.
Email Spoofing	Forging the sender's email address so that an email appears to come from a trusted source.	A scam email appears to come from a bank instead of a criminal.
Hacking	Gaining unauthorized access to a computer system or network by bypassing security controls.	Breaking into a company's internal network without permission.
Identity Theft	Illegally obtaining another person's personal information to impersonate them for fraud or other crimes.	Using someone's national ID number to open a bank account.
Logic Bomb	Malicious code that remains inactive until a specified condition or event triggers its execution.	Code deletes company files after an employee's account is removed.
Malware	Malicious software designed to damage systems, disrupt operations, or gain unauthorized access.	Installing spyware that secretly steals passwords.
Phishing	Fraudulently pretending to be a trusted organization to obtain sensitive information such as passwords or banking details.	A fake PayPal email asks users to log in using a malicious website.
Salami Attack	A fraud technique involving many very small unauthorized transactions that individually go unnoticed but collectively produce significant gains.	Deducting one cent from thousands of bank accounts each day.
Software Piracy	The unauthorized copying, distribution, installation, or sale of copyrighted software.	Installing one licensed software copy on hundreds of computers.
Spamming	Sending unsolicited bulk electronic messages, usually advertisements or scams.	Sending thousands of promotional emails without recipients' consent.
Trojans (Keyloggers)	Malicious software that secretly records a user's keystrokes to steal passwords, banking information, and other sensitive data.	A keylogger records online banking credentials as they are typed.

Unauthorized Access	Accessing a computer system, network, or information without permission or legal authorization.	Logging into another employee's account without their permission.
Unauthorized Interception	Secretly intercepting electronic communications or data transmissions without authorization.	Capturing confidential emails transmitted over a network.
Web Jacking	Taking unauthorized control of a website by compromising administrator credentials and preventing the legitimate owner from accessing it.	A hacker changes a company's website and demands payment to restore access.