Al-Mustaqbal University / College of Technical Engineering
Department (Department of Cybersecurity Techniques Engineering)
Class (First)
Ethics for the Information Age/ Code -UOMU0208025
Lecturer (Dr. Ahmed Hasan Al-Janabi & Msc. Heba Hussien)

2nd term – Lecture 4 Internet Interaction

Lecture4

Internet Interaction

Ethics for the Information Age

Department of Cybersecurity Engineering Techniques

First Year

Email (heba.hussein.abdalabbas@uomus.edu.iq)

1.Introduction to Internet Interaction

What is Internet Interaction?

Internet Interaction refers to communication and data exchange between users, devices, and systems through the Internet. This fundamental concept underpins virtually every online activity we engage in today, from simple email exchanges to complex cloud computing operations. Understanding internet interaction is essential for anyone navigating the modern digital landscape, particularly those studying cybersecurity and information ethics.

It includes any activity performed online such as:

- Sending emails - asynchronous communication across the globe
- Browsing websites - accessing information and services
- Using social media - connecting and sharing with others
- Online shopping - e-commerce transactions
- Cloud storage - storing and accessing data remotely
- Mobile applications - portable software services
- Online banking - financial transactions and management
- Video conferencing - real-time audio-visual communication

The Internet is a global network connecting millions of computers, enabling seamless communication and resource sharing across geographical boundaries.

2. How the Internet Works

When a user opens a website, the following steps occur:

1. The user enters a URL in the browser
2. The browser sends a Request to the server
3. The data is divided into Packets for transmission
4. Packets travel through the network via routers
5. Packets reach the Server
6. The server sends a Response back

7. The webpage appears in the browser

Main Components of Internet Communication

- Client - The device or software requesting services
- Server - The computer providing resources or services
- IP Address - Unique numerical identifier for devices
- DNS - Domain Name System that translates domain names to IP addresses
- Router - Device that directs data packets between networks
- Protocols - Standardized rules for communication

Important Internet Protocols

Protocol	Function
HTTP	Transfer web pages
HTTPS	Secure transfer of web pages with encryption
FTP	File transfer between computers
SMTP	Send email messages
TCP/IP	Data transmission across networks
DNS	Convert domain names to IP addresses

3. Types of Internet Interaction

The modern internet supports a diverse range of interaction types, each serving different purposes and user needs. Understanding these various forms of interaction helps users navigate online services more effectively and recognize potential security considerations associated with each type.

Types of Online Interaction

- Email Communication - formal and informal electronic messaging
- Web Browsing - accessing websites and online content
- Social Media - connecting and sharing on platforms
- Online Chat - real-time text-based communication
- E-Commerce - buying and selling goods online
- Cloud Computing - remote computing services
- Video Streaming - watching video content online
- Online Education - learning through digital platforms
- Online Gaming - multiplayer gaming experiences
- Remote Work Systems - professional collaboration tools

All these services depend on Internet Interaction and require users to be aware of associated security risks and ethical considerations.

4. Ethical Issues in Internet Interaction

The proliferation of internet usage has given rise to numerous ethical challenges that users, organizations, and society must address. Understanding these issues is critical for developing responsible digital citizenship and maintaining a safe online environment for all participants.

Issue	Description
Privacy Violation	Accessing personal data without permission
Identity Theft	Stealing personal identity for fraudulent purposes
Cyberbullying	Online harassment and intimidation of others
Piracy	Illegal copying of software and digital content

Issue	Description
Fake News	Spreading false information deliberately
Hacking	Unauthorized access to systems or data
Spam	Sending unwanted messages to many users
Malware	Creating and distributing malicious software

📌 *Ethical behavior is very important when using the Internet. Every user has a responsibility to act with integrity and respect toward others in the digital space.*

5. Spam and Phishing

Spam

Spam is unwanted email messages sent to many users, often for advertising purposes or to distribute malware.

Phishing

Phishing is a cyber attack that tries to steal sensitive information such as passwords, credit card numbers, bank accounts, and personal information. Attackers typically disguise themselves as trustworthy entities to trick victims into revealing confidential data. Phishing attacks have become increasingly sophisticated, often mimicking legitimate communications from banks, social media platforms, and other trusted sources.

Example of a Phishing Attempt:

> *An email says: "Your account will be suspended. Click here to login."*

When the user clicks the link, they are directed to a fake website that captures their login information. The attacker can then use these credentials to access the victim's real account and potentially steal additional information or funds.

6.Cyber Threats During Internet Interaction

Understanding cyber threats is essential for anyone using the internet. These threats can compromise personal data, financial assets, and even national security. Cybersecurity professionals must understand these threats to effectively protect systems and users.

Attack	Description
Phishing	Steal user information through deceptive means
Malware	Malicious software designed to damage or disrupt
Ransomware	Encrypt files and demand payment for decryption
DDoS Attack	Overwhelm servers with traffic to cause downtime
Man-in-the-Middle	Intercept and alter communication between parties
Password Attack	Attempt to guess or crack passwords
Identity Theft	Steal personal identity for fraud
Spyware	Monitor user activity without consent

Most cyber attacks occur during Internet Interaction. Being aware of these threats is the first step in protecting yourself and others from becoming victims.

7. HTTP vs HTTPS

Understanding the difference between HTTP and HTTPS is crucial for secure internet browsing. HTTPS provides encryption and authentication that protects users from various types of attacks.

HTTP	HTTPS
Not secure	Secure
No encryption	Encryption enabled
Data can be stolen	Data protected
Port 80	Port 443

HTTPS uses:

- SSL (Secure Sockets Layer) - cryptographic protocol for secure communication
- TLS (Transport Layer Security) - successor to SSL with improved security
- Encryption - converting data into unreadable format for unauthorized parties

📌 *Always use HTTPS websites, especially when entering sensitive information such as passwords or credit card numbers.*

8. Safe Internet Interaction

Practicing safe internet habits is essential for protecting yourself and others from cyber threats. Following these security rules can significantly reduce the risk of becoming a victim of cybercrime.

How to Use the Internet Safely

Important security rules:

1. Use strong passwords - combine letters, numbers, and symbols
2. Enable Two-Factor Authentication - add an extra layer of security
3. Do not share personal information - protect your privacy
4. Do not click unknown links - they may lead to malicious sites

5. Install Antivirus software - protect against malware
6. Update operating system - patch security vulnerabilities
7. Use VPN - encrypt your internet connection
8. **Avoid public Wi-Fi - they are often unsecured**
9. Check HTTPS websites - ensure secure connections
10. Logout from public computers - prevent unauthorized access

9. Internet Ethics

Ethical use of the internet is fundamental to maintaining a safe and productive digital environment. Every user has a responsibility to act with integrity and consideration for others online.

Ethical Use of the Internet

Users should:

- Respect others online - treat people with courtesy and dignity
- Do not cyberbully - never harass or intimidate others
- Do not hack accounts - respect others' digital property
- Respect privacy - protect personal information
- Do not spread fake news - verify information before sharing
- Do not download pirated software - respect intellectual property
- Do not distribute malware - never create or spread malicious software
- Use the Internet legally - comply with laws and regulations

10. Cybersecurity Ethics

Cybersecurity professionals bear a special responsibility due to their knowledge and access to systems. Ethical conduct is paramount in this field, as the same skills that protect systems can also be used to harm them.

Ethics for Cybersecurity Students

Cybersecurity students must:

• Not hack systems without permission - always obtain proper authorization

- Protect user data - safeguard confidential information
- Report security vulnerabilities - disclose responsibly to affected parties
- Follow laws and regulations - comply with legal requirements
- Maintain confidentiality - keep sensitive information private
- Use knowledge for protection, not attacks - apply skills ethically

Types of Hackers

Hacker Type	Description
White Hat	Ethical hacker - works with authorization to find vulnerabilities
Black Hat	Criminal hacker - exploits systems for malicious purposes
Gray Hat	Between both - may hack without permission but not for harm

11. Advantages of Internet Interaction

Internet interaction has transformed modern society, offering numerous benefits that have reshaped how we communicate, work, learn, and live. Understanding these advantages helps us appreciate the value of digital connectivity while remaining aware of the need for responsible use.

- Fast communication - instant messaging and email across the globe
- Online education - accessible learning opportunities worldwide
- E-commerce - convenient shopping and business transactions
- Cloud storage - accessible data from anywhere
- Remote work - flexible employment opportunities
- Information sharing - knowledge accessible to all
- Entertainment - streaming, gaming, and social media

- Online services - banking, healthcare, government services

12. Disadvantages of Internet Interaction

While internet interaction offers tremendous benefits, it also presents significant challenges and risks that users must navigate. Understanding these disadvantages is essential for developing appropriate safeguards and maintaining a balanced perspective on digital engagement.

- Cybercrime - various forms of digital criminal activity
- Privacy problems - personal data exposure and misuse
- Internet addiction - excessive use affecting daily life
- Fake news - misinformation spreading rapidly
- Malware - malicious software threats
- Data theft - unauthorized access to personal information
- Identity theft - fraudulent use of personal identity
- Security threats - various risks to digital safety

13. Discussion Questions

The following questions are designed to stimulate critical thinking about internet interaction and its ethical implications. Consider these questions carefully and be prepared to discuss them in class.

1. What is Internet Interaction?
2. What is the difference between HTTP and HTTPS?
3. What is phishing?
4. What are cyber threats?
5. Why are ethics important on the Internet?
6. What is the difference between White Hat and Black Hat hackers?