Cybersecurity Department

Faculty of Applied Science

Fundamentals of Cybersecurity

Dr. Taha Basheer Taha

Chapter 1: Introduction and Fundamentals

What is Cybersecurity?

Simple Definition

Cybersecurity means protecting computers, networks, systems, and data from digital attacks.

These attacks may try to:

- Steal information
- Damage systems
- Stop services from working
- Control devices without permission
- Use someone's identity or account

Cybersecurity is like locking your house, but in the digital world. Your phone, email, social media accounts, bank app, university account, and even smart devices all need protection.

Why Cybersecurity is Important

Today, most of our lives are connected to technology. The internet is used for studying, banking, shopping, communication, and entertainment. This means that a lot of personal and sensitive information is stored online.

Cybersecurity is important because attackers may try to access this information and use it for harmful purposes.

Three Levels of Cyber Protection

1. Personal Level

At the personal level, cybersecurity protects:

- Your identity
- Your phone and laptop
- Your photos and messages
- Your bank account
- Your email and social media accounts

Example:
If someone steals your Instagram password, this is a personal cybersecurity problem.

2. Organizational Level

At the organizational level, cybersecurity protects:

- Company data
- Customer information
- Financial records
- Employee accounts
- Reputation of the organization

Example:
If a university database is hacked and student records are stolen, this is an organizational cybersecurity problem.

3. Government Level

At the government level, cybersecurity protects:

- National security
- Government systems
- Citizen data
- Electricity systems
- Water systems
- Transportation systems

Example:
If attackers shut down a city's electricity system, this becomes a national cybersecurity problem.

Quick Questions

Q1. Cybersecurity means:
A. Making computers faster.
B. Protecting systems and data from digital attacks. *
C. Designing websites.
D. Buying new devices.

Q2. Protecting your Instagram account is an example of:
A. Government protection.
B. Organizational protection.

C. Personal protection. *
D. Military protection.

Section 2: Personal Data and Digital Identity

What is Personal Data?

Personal data is any information that can identify you.

Examples include:

- Full name
- Phone number
- Address
- Date of birth
- Place of birth
- National ID
- Passport number
- Driver license number
- Photos
- Private messages
- Bank information
- Medical information
- Educational records

A simple explanation:

If information can tell others who you are, where you are, or how to contact you, then it is personal data.

Offline Identity

Your offline identity is your real-life identity.

It includes the information people around you know in daily life, such as:

- Your real name
- Your family
- Your address
- Your school or university
- Your workplace

- Your age

Example:
Your classmates know your face, name, and maybe your department. This is part of your offline identity.

Online Identity

Your online identity is how you appear on the internet.

It includes:

- Your usernames
- Your profile pictures
- Your posts
- Your comments
- Your online behavior
- Your accounts
- Your email address

Example:
Your Facebook profile, Instagram account, Gmail account, and gaming username are parts of your online identity.

Important Point

Some people may say:

“I do not have social media, so I do not have an online identity.”

This is not correct.

If you use the internet, you have an online identity. Even if you only use Google, YouTube, email, or online learning platforms, you still leave digital traces.

Exercise

What is personal data?

A. Only photos

B. Information that identifies you *

C. Only passwords

D. Only emails

What is online identity?

A. Your physical address

B. Your behavior on internet

C. Your ID card

D. Your house

Discussion Question

What can your online identity be if you don’t use social media?

Where is your Data

Data Does Not Stay in One Place

Many people think that when they take a photo, the photo is only on their phone. But this is not always true.

For example:

1. You take a photo on your phone.
2. You send it to five friends.
3. Each friend downloads it.
4. One friend posts it online.
5. The photo is now stored on different devices and servers.

So, the photo is no longer fully under your control.

The Important Lesson

Once data is shared online, it becomes difficult to control. Even if you delete the photo from your phone, other people may still have copies.

Examples of Data Locations

Your data may exist in:

- Your phone
- Your laptop
- Your friend’s phone
- Cloud storage
- Social media servers
- Messaging apps
- Backup systems
- Company databases

Smart Devices and Data

Smart devices can also collect data about you.

Examples:

- Smartwatch
- Fitness tracker
- Smartphone
- Smart TV
- Smart camera
- Smart speaker
- Smart home devices

These devices may collect:

- Location
- Heart rate
- Sleep patterns
- Activity level
- Voice commands
- Search history
- Usage habits

Privacy and Convenience

Technology makes life easier, but there is a price: privacy.

For example, social media platforms can show targeted advertisements because they analyze user behavior.

When an app is free, your data may be part of the business model.

Section 3 Exercise

Activity: “Follow the Photo”

Imagine this situation:

A student takes a photo in class and sends it to two friends. One friend posts it on Instagram. Another friend sends it to a group chat.

1. Where is the photo now?
2. Who can access it?
3. Can the original student fully delete it?
4. What could go wrong?

Quick Questions

Q1. Once a photo is shared online:
A. It always stays only on your phone
B. It may be copied and stored in many places *
C. It disappears after one day
D. It cannot be downloaded

Q2. Which device may collect health-related data?
A. Smartwatch *
B. Chair
C. Paper notebook
D. Wall clock

What Do Attackers Want?

Attackers Want Valuable Data

Cybercriminals do not attack randomly all the time. Usually, they want something valuable.

They may want:

- Money
- Passwords
- Bank accounts
- Personal identity
- Credit card numbers
- Medical records
- Photos
- Company secrets
- Login credentials

Money Theft

Attackers may try to steal money directly or indirectly.

Examples:

- Stealing credit card information
- Taking over bank accounts
- Sending fake messages asking for money
- Pretending to be a family member in need
- Using stolen airline miles or reward points

Identity Theft

Identity theft means that someone uses your personal information to pretend to be you. This can be very dangerous.

Attackers may use your identity to:

- Open bank accounts
- Take loans
- Use medical insurance
- Create fake profiles
- Commit fraud
- Damage your reputation

Medical Identity Theft

Medical identity theft happens when someone uses another person’s medical information or insurance.

This is dangerous because false medical records may be added under your name.

Example:
Someone uses your medical insurance for treatment. Later, your medical history contains incorrect information.

Banking Identity Theft

Attackers may use private data to access:

- Bank accounts

- Credit cards
- Tax records
- Online accounts
- Social media profiles

This can cause financial damage and long-term problems.

Who Else Wants Your Data?

It is not only criminals.

Other groups may also want data, such as:

1. Internet Service Providers

They may track online activity. In some countries, they may share or sell certain types of data.

2. Advertisers

Advertisers want to understand your interests so they can show targeted ads.

3. Websites

Websites use cookies to remember your activity and preferences.

Exercise

Pair Work: “What Does the Attacker Want?”

identify what the attacker wants in the following situations:

1. A fake message asks for your bank card number.
2. A fake Facebook page asks you to log in.
3. A stranger asks for your university email password.
4. A fake travel website asks for passport details.

Expected Answers

1. Money / bank information
2. Social media account
3. University account access
4. Identity information

Discussion Questions

1. Why are passwords valuable? How can be strengthen?
2. Why are medical records valuable?
3. Why do companies want user data for advertising?

Organizational Data

What is Organizational Data?

Organizational data is information that belongs to a company, university, hospital, bank, or any institution.

It may include:

- Customer data
- Employee data
- Financial records
- Sales information
- Product designs
- Research documents
- Business plans
- Student records
- Patient records

Traditional Data

Traditional data is data that organizations normally create and use.

Examples:

1. Transactional Data

This includes information related to business operations.

Examples:

- Buying and selling records
- Production activities
- Employment decisions
- Customer orders

2. Intellectual Property

This includes ideas and products that give the organization an advantage.

Examples:

- Patents
- Trademarks
- Product designs
- Research results
- New product plans

If competitors steal this information, the company may lose its advantage.

3. Financial Data

This includes information about the financial health of the organization.

Examples:

- Income statements
- Balance sheets
- Cash flow statements
- Budgets

IoT and Big Data

IoT means Internet of Things. It refers to physical devices connected to the internet.

Examples:

- Smart cameras
- Sensors
- Smart watches

- Smart cars
- Smart home devices
- Industrial machines

These devices collect and share data.

Big Data means very large amounts of data collected from many sources. Because IoT devices generate huge amounts of data, they increase the importance of cybersecurity.

Exercise

Activity: “Classify the Data”

Classify the following as personal data, organizational data, or both.

1. Student grades
2. Company sales report
3. Employee salary
4. Customer phone number
5. Product design document

Suggested Answers

1. Both
2. Organizational
3. Both
4. Both
5. Organizational

The McCumber Cube

What is the McCumber Cube?

The McCumber Cube is a model used to understand information security.

It helps organizations think about security from three directions:

1. What security principle do we need?

2. What state is the data in?
3. What method (Mechanism) will we use to protect it?

Dimension 1: Security Principles (CIA Triad)

1. Confidentiality

Confidentiality means keeping information private. Only authorized people should access the data.

Examples:

- Passwords
- File permissions
- Encryption
- Two-factor authentication

Simple example:
Your university grades should be seen by you and authorized staff only.

2. Integrity

Integrity means keeping information correct and unchanged. Data should not be modified by unauthorized people.

Examples:

- Checksums
- Hash functions
- logs

Simple example:
A student's grade should not be changed by an attacker.

3. Availability

Availability means that systems and data are accessible when needed.

Examples:

- Backups
- Updates
- Maintenance
- Hardware repair
- Reliable internet connection

Simple example:
Students should be able to access the learning system before an exam.

Dimension 2: States of Data

1. Data in Processing

This is data currently being used.

Example: When a system calculates your final grade.

2. Data in Storage

This is data saved somewhere.

Example: A file saved on a hard drive, cloud, or USB.

3. Data in Transmission

This is data moving from one place to another.

Example: Sending an email or uploading a file.

Dimension 3: Security Measures

1. Awareness, Training, and Education

Users must learn about threats and safe behavior.

Example:
Teaching employees (People) how to recognize cyber-attacks as phishing emails. (*This can be your first duty dear student, yes, even if you still in the first year!)*

2. Technology

Technology includes tools used to protect systems.

Examples:

- Firewalls
- Antivirus
- Encryption
- Authentication systems

3. Policies and Procedures

These are rules and plans for security.

Examples:

- Password policy
- Backup policy
- Incident response plan

Simple Way to Explain the Cube

The cube asks three questions:

1. What do we protect?
   Confidentiality, integrity, or availability?
2. Where is the data?
   Stored, moving, or being processed?
3. How do we protect it?
   Training, technology, or policy?

Section 6 Exercise

Activity: “Build the Cube”

A university wants to protect student grades stored in a database.

1. Which principle is important?
2. What state is the data in?

Suggested Answer

1. Integrity and confidentiality
2. Storage

Quick Questions

Q1. Which principle means keeping data private?
A. Availability
B. Confidentiality *
C. Scalability
D. Speed

Q2. Data sent by email is:
A. Data in storage
B. Data in transmission *
C. Data in processing only
D. Deleted data

Q3. Backups mainly support:
A. Availability *
B. Decoration
C. Advertising
D. Username design

Types of Attackers

Attackers are individuals or groups who attempt to exploit vulnerability for personal or financial gain. They are interested in **everything**, from credit cards to product designs!

Amateurs

The term 'script kiddies' emerged in the 1990s and refers to amateur or inexperienced hackers who use existing tools or instructions found on the Internet to launch attacks. Some script kiddies are just curious, others are trying to demonstrate their skills and cause harm. While script kiddies may use basic tools, their attacks can still have significant consequences.

Hackers

This group of attackers break into computer systems or networks to gain access. Depending on the intent of their break in, they can be classified as white, gray or black hat hackers.

- **White hat attackers** break into networks or computer systems to identify any weaknesses so that the security of a system or network can be improved. These break-ins are done with prior permission and any results are reported back to the owner.
- **Gray hat attackers** may set out to find vulnerabilities in a system but they will only report their findings to the owners of a system if doing so coincides with their agenda. Or they might even publish details about the vulnerability on the internet so that other attackers can exploit it.
- **Black hat attackers** take advantage of any vulnerability for illegal personal, financial or political gain.

Organized hackers

- These attackers include organizations of cyber criminals, hacktivists, terrorists and state-sponsored hackers. They are usually highly sophisticated and organized, and may even provide cybercrime as a service to other criminals.
- Hacktivists make political statements to create awareness about issues that are important to them.
- State-sponsored attackers gather intelligence or commit sabotage on behalf of their government. They are usually highly trained and well-funded and their attacks are focused on specific goals that are beneficial to their government.

Identify the hat color:

- After hacking into ATM systems remotely using a laptop, then, this attacker worked with the ATM manufacturers to resolve the identified security vulnerabilities.
- This attacker transferred $10 million into their bank account using customer account and PIN credentials gathered from recordings.
- This attacker's job is to identify weaknesses in a company's computer system.
- This attacker used malware to compromise a company's system and steal credit card information that was then sold to the highest bidder. Black
- While carrying out some research, this attacker stumbled across a security vulnerability on an organization's network that he/she is authorized to access.

Internal and External Threats

Cyber attacks can originate from within an organization as well as from outside of it.

Internal

Employees, contract staff or trusted partners can accidentally or intentionally:

- mishandle confidential data
- facilitate outside attacks by connecting infected USB media into the organization's computer system
- invite malware onto the organization's network by clicking on malicious emails or websites
- threaten the operations of internal servers or network infrastructure devices.

External

Amateurs or skilled attackers outside of the organization can:

- exploit vulnerabilities in the network
- gain unauthorized access to computing devices

use social engineering to gain unauthorized access to organizational data.

Chapter 2: Malwares

Employee: We are under cyber attack

Boss: which type of cyber-attack is this?

You : _____ (in such scenarios you should know the answer)

Types of Malwares

Cybercriminals use many different types of malicious software, or malware, to carry out their activities. Malware is any code that can be used to steal data, bypass access controls, or cause harm to or compromise a system. Knowing what the different types are and how they spread is key to containing and removing them.

1-Spyware

Designed to track and spy on you, spyware monitors your online activity and can log every key you press on your keyboard, as well as capture almost any of your data, including sensitive personal information such as your online banking details. Spyware does this by modifying the security settings on your devices.

It often bundles itself with legitimate software or Trojan horses.

2- Adware

is often installed with some versions of software and is designed to automatically deliver advertisements to a user, most often on a web browser. You know it when you see it! It's hard to ignore when you're faced with constant pop-up ads on your screen.

It is common for adware to come with spyware.

3- Backdoor This type of malware is used to gain unauthorized access by bypassing the normal authentication procedures to access a system. As a result, hackers can gain remote access to resources within an application and issue remote system commands.

A backdoor works in the background and is difficult to detect.

4-Ransomware This malware is designed to hold a computer system or the data it contains captive until a payment is made. Ransomware usually works by encrypting your data so that you can't access it.

Some versions of ransomware can take advantage of specific system vulnerabilities to lock it down. Ransomware is often spread through phishing emails that encourage you to download a malicious attachment or through a software vulnerability.

5- A virus is a type of computer program that, when executed, replicates and attaches itself to other executable files, such as a document, by inserting its own code. Most viruses require end-user interaction to initiate activation and can be written to act on a specific date or time.

Viruses can be relatively harmless, such as those that display a funny image. Or they can be destructive, such as those that modify or delete data.

Viruses can also be programmed to mutate in order to avoid detection. Most viruses are spread by USB drives, optical disks, network shares or email.

6-Trojan Horse This malware carries out malicious operations by masking its true intent. It might appear legitimate but is, in fact, very dangerous. Trojans exploit your user privileges and are most often found in image files, audio files or games.

Unlike viruses, Trojans do not self-replicate but act as a trap to sneak malicious software past unsuspecting users.

7- Worms This is a type of malware that replicates itself in order to spread from one computer to another. Unlike a virus, which requires a host program to run, worms can run by themselves. Other than the initial infection of the host, they do not require user participation and can spread very quickly over the network.

Worms share similar patterns: They exploit system vulnerabilities, they have a way to propagate themselves, and they all contain malicious code (payload) to cause damage to computer systems or networks.

Worms are responsible for some of the most devastating attacks on the Internet. In 2001, the Code Red worm had infected over 300,000 servers in just 19 hours.

In brief:

Malware designed to track your online activity and capture your data	Spyware
Software that automatically delivers advertisements	Adware
Malware that holds a computer system captive until a payment is made to the attacker	Ransomeware
Malicious code that attaches to legitimate programs and usually spreads by USB drives, optical media, network shares or email	virus
Malicious code that replicates itself independently by exploiting vulnerabilities in networks	worm

There are many different malware types that pose a threat to your organization but how can cybercriminals get into your networks and systems in the first place? They have many means at their disposal.

Some Methods of infiltration:

2.2.1 Social Engineering

Social engineering is the manipulation of people into performing actions or divulging confidential information. Social engineers often rely on people's willingness to be helpful, but they also prey on their weaknesses. For example, an attacker will call an authorized employee with an urgent problem that requires immediate network access and appeal to the employee's vanity or greed or invoke authority by using name-dropping techniques in order to gain this access.

2.2.2 Denial-of-Service

Denial-of-Service (DoS) attacks are a type of network attack that is relatively simple to carry out, even by an unskilled attacker. A DoS attack results in some sort of interruption of network service to users, devices or applications. As sending enormous amount of data rate to a network which it cannot handle. This causes a slowdown in transmission or response, or the device or service to crash.

2.2.3 Distributed DoS

A Distributed DoS (DDoS) attack is similar to a DoS attack but originates from multiple, coordinated sources. For example:

- An attacker builds a network (botnet) of infected hosts called zombies, which are controlled by handler systems.
- The zombie computers will constantly scan and infect more hosts, creating more and more zombies.
- When ready, the hacker will instruct the handler systems to make the botnet of zombies carry out a DDoS attack.

2.2.4 Botnet

A bot computer is typically infected by visiting an unsafe website or opening an infected email attachment or infected media file. A botnet is a group of bots, connected through the Internet, that can be controlled by a malicious individual or group. It can have tens of thousands, or even hundreds of thousands, of bots that are typically controlled through a command and control server.

These bots can be activated to distribute malware, launch DDoS attacks, distribute spam email, or execute brute-force password attacks. Cybercriminals will often rent out botnets to third parties for nefarious purposes.

Many organizations. like Cisco, force network activities through botnet traffic filters to identify any botnet locations.

Security vulnerabilities

are any kind of software or hardware defect. A program written to take advantage of a known vulnerability is referred to as an *exploit*. A cybercriminal can use an exploit against a vulnerability to carry out an *attack*, the goal of which is to gain access to a system, the data it hosts or a specific resource.

Chapter 3: Protecting your device and network

Cybersecurity is not only about installing antivirus software or memorizing technical terms. At its heart, cybersecurity is about **control**. To make your device safe and secure, you should:

- turn the firewall on
- install antivirus and antispyware
- manage your operating system and browser
- set up password protection.

Cybersecurity is not only about installing antivirus software or memorizing technical terms. It is mainly about **controlling your data** and protecting it before, during, and after using digital devices and online services.

Every time you use a laptop, connect to Wi-Fi, upload a photo, save a password, or click "I agree," you are making a security decision. Some decisions protect your data, while others expose it to risk.

This chapter explains seven important cybersecurity topics:

1. Encryption
2. Backup
3. Secure deletion
4. Passwords and two-factor authentication
5. Public Wi-Fi and Bluetooth
6. Terms of Service
7. OAuth login

The goal is to understand how everyday digital habits can either protect or expose personal information.

---

1. Encryption: Lock the Meaning

Encryption is the process of changing readable information into an unreadable form so that unauthorized people cannot understand it. If someone steals a file, encryption may not stop the theft itself, but it can stop the thief from reading the content.

This means encryption protects the **meaning** of the data, not just the physical file. For example, if a laptop contains private photos, university documents, or saved personal information, encryption makes that data unreadable without the correct key, password, or authorized account.

A simple way to understand encryption is this: the attacker may see the file, but cannot understand what is inside it. The file becomes like a message written in a locked language. Figure 1 shows a diagram for encryption / decr

Windows also provides a feature called **Encrypting File System**, or **EFS**. This feature can encrypt files and connect access to a specific user account. Only the authorized user can access the encrypted files.

Basic encryption and decryption process:

Plain Text
This is the original readable message, like:

Hello

Encryption Algorithm
This is the method used to hide the message.

Key
The key is a secret value used by the algorithm to lock or unlock the message.

Cipher Text
This is the encrypted message. It looks unreadable, for example:

X7a@91k

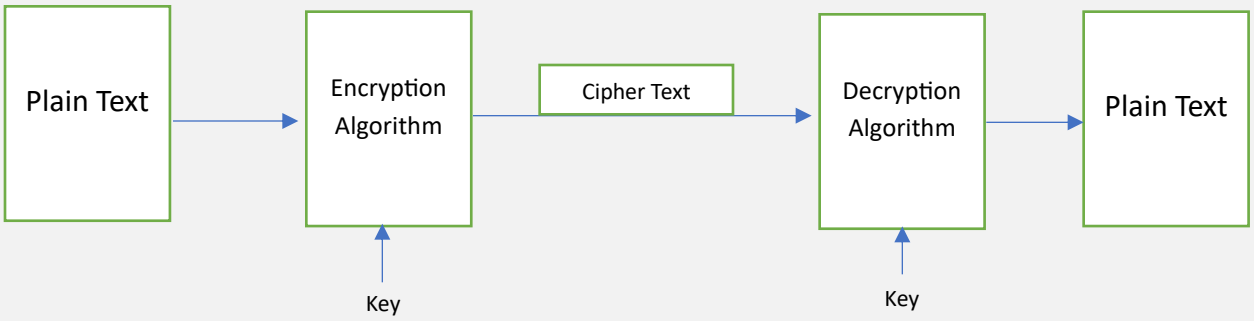
Decryption Algorithm
This uses a key to convert the cipher text back into the original message.

So the idea is:

Plain Text + Encryption Algorithm + Key → Cipher Text

Then: **Cipher Text + Decryption Algorithm + Key → Plain Text**

The diagram below shows **the basic encryption and decryption process**



Classical Encryption Example: Caesar Cipher

- One of the **earliest substitution ciphers**, used by **Julius Caesar** (100–44 BC).
- Each letter in the plaintext is shifted by a fixed number of positions in the alphabet.

Example:
Shift by 3 →
Plaintext: **MEET ME AFTER THE PARTY**
Ciphertext: **PHHW PH DIWHU WKH SDUWB**

Brute force attack to find the key

A brute-force attack is a method for gaining unauthorized access by systematically trying every possible combination of credentials (passwords, keys, PINs, etc.) until the correct one is found.

Multiple-Choice Question

A student stores private photos and university files on a laptop. The laptop is stolen, but the files were encrypted before the theft.

What is the best explanation?

A) Stealing the laptop automatically means the files are readable.
B) Encryption makes the stolen files unreadable without the correct key.
C) Encryption deletes the files permanently.
D) Encryption and passwords are exactly the same thing.

---

2. Backup: When Protection Fails, Recovery Wins

A backup is another copy of important data stored in a separate place. Even if a user protects a device carefully, problems can still happen. A laptop may fail, a phone may be stolen, files may be deleted by mistake, or ransomware may lock important data.

Backup is important because it allows users to recover data after failure, damage, theft, or attack. Without backup, one damaged or stolen device can mean the loss of important files forever.

Backups can be stored in different ways. An external hard drive gives the user control, but it can also be lost, damaged, or stolen. Network storage can be useful in homes, offices, or labs. Cloud storage protects data if the original device is damaged or stolen, but it depends on account security.

The best question is not:

“Do I have my files now?”

The better question is:

“If this device stops working today, can I recover my files tomorrow?”

Multiple-Choice Question

A teacher keeps all exam files on one laptop. There is no copy anywhere else. The laptop suddenly stops working the night before the exam.

What is the main security problem?

A) One device became a single point of failure.
B) The files were saved on the desktop folder.
C) The teacher forgot the file names.
D) Backup is only needed for photos, not exams.

Correct Answer: A

3. Secure Deletion: Delete Does Not Always Mean Gone

Many users think that deleting a file means it has disappeared forever. This is not always true. When a file is deleted and even when the Recycle Bin is emptied, the operating system may only remove the visible path to the file.

The data may still exist on the storage device until it is overwritten. This means that special recovery or forensic tools may still recover deleted files.

For example, a student may delete personal photos from an old laptop, empty the Recycle Bin, and then sell the laptop. The student may think the data is gone, but the files may still be recoverable.

Secure deletion means removing data in a way that makes recovery very difficult. This can involve overwriting old data with new meaningless data. For very sensitive information, physical destruction of the storage device may be the strongest option.

Multiple-Choice Question

A student sells an old laptop after deleting personal files and emptying the Recycle Bin.

What is the main risk?

A) Emptying the Recycle Bin guarantees all data is impossible to recover.
B) Deleted files may still be recoverable with forensic tools.
C) Selling the laptop automatically removes all security risks.
D) Recovery tools only work on phones, not laptops.

Correct Answer: B

---

4. Passwords and Two-Factor Authentication: One Lock Is Not Enough

A password is usually the first lock on an account. However, many users weaken this lock by using the same password for several accounts, choosing weak passwords, writing passwords in unsafe places, or sharing them with others.

One of the most dangerous habits is password reuse. If one password is leaked from one service, attackers may try the same password on other accounts such as email, social media, or university systems.

Two-factor authentication, or **2FA**, adds a second proof of identity. This may be a code sent to a phone, an authentication app, a fingerprint, face recognition, or a physical security key.

A password proves something the user knows. Two-factor authentication adds another proof that the user is really the account owner.

However, 2FA is not magic. Attackers may still use phishing, malware, or social engineering to trick users into giving away codes or approving fake login requests.

Multiple-Choice Question

A student uses the same password for Facebook, Gmail, and university email. The password is also written in a notebook.

What is the main risk?

A) One leaked password can open many accounts.
B) A written password is always safer than memory.
C) Using one password is easier, so it is more secure.
D) Two-factor authentication is only useful for banks.

Correct Answer: A

5. Public Wi-Fi and Bluetooth: Free Connection Can Hide Expensive Risk

Public Wi-Fi is useful, but it should not be treated like a trusted private network. Public Wi-Fi may be found in cafés, airports, universities, hotels, and shopping malls. The problem is that public networks may expose users to monitoring, fake networks, or unsafe sharing.

Users should avoid sensitive actions on public Wi-Fi, such as logging into bank accounts, sending private files, entering important passwords, or sharing personal information.

Bluetooth can also create risk if it is left on unnecessarily. Attackers may try to exploit open wireless connections. A simple safe habit is to turn Bluetooth off when it is not being used.

Public Wi-Fi is like a public place. It may be useful, but users should be careful about what they do there.

Multiple-Choice Question

A student joins free café Wi-Fi, logs into important accounts, sends private files, and keeps Bluetooth turned on.

What is the main problem?

A) Free Wi-Fi is always protected by the café.
B) Public networks and open Bluetooth increase exposure.
C) Bluetooth cannot be attacked if the phone screen is locked.
D) Public Wi-Fi only affects speed, not privacy.

Correct Answer: B

6. Terms of Service: You May Own It, But You May Also Give Permission

Most users click **"I agree"** without reading the Terms of Service. This is risky because Terms of Service explain the rules between the user and the service provider.

Terms of Service may explain what the company can do with uploaded data, what rights the user keeps, what permissions the user gives, and what happens when the account is closed.

A key idea is the difference between **ownership** and **license**.

Ownership means the content belongs to the user.
License means the user gives the platform permission to use the content in certain ways.

For example, a student may still own a photo uploaded to an app. However, the platform may have permission to store it, resize it, display it, recommend it, or use it according to the policy and privacy settings.

The danger is not always losing ownership. The danger is giving permission without understanding what that permission means.

Multiple-Choice Question

A student uploads personal photos to a free app and clicks "I agree" without checking the Terms of Service or privacy settings.

What is the main risk?

A) The student may have granted broad permission without understanding it.
B) "I agree" means the company can never use the photos.
C) Uploading always means full private control forever.
D) Terms of Service are only important for paid services.

Correct Answer: A

7. OAuth Login: Login Without Giving Your Password Everywhere

OAuth allows users to sign in to a third-party website or app using another account, such as Google, Facebook, Apple, or Microsoft.

For example, a website may allow the user to choose:

“Login with Google.”

In this case, the user does not give the website the actual Google password. Instead, Google verifies the user and allows the website limited access.

OAuth can be useful because the user does not need to type the same password into many websites. However, the risk appears when users click **Allow** without reading the requested permissions.

Some apps may ask for access to:

- Name
- Email address
- Profile photo
- Contacts
- Files
- Other account information

Before approving OAuth login, users should check what permissions the app is requesting and refuse unnecessary access.

Multiple-Choice Question

A student uses “Login with Google” on an unknown website and accepts all requested permissions quickly.

What is the main risk?

A) OAuth always gives the safest minimum permission automatically.
B) The student may approve unnecessary access to personal data.
C) Google login means the website is always trustworthy.
D) Permissions do not matter after login.

Correct Answer: B

Chapter 4: Network Security

Network security is the protection of devices, users, services, and data while they are connected to a network. It focuses especially on data in transmission: data moving between phones, laptops, servers, websites, and cloud services.

In previous lectures, you learned about cybersecurity basics, data, attackers, malware, DoS/DDoS, botnets, encryption, and passwords. This lecture continues from there. It does not repeat those topics in detail. Instead, it shows how networks are protected, monitored, and investigated when suspicious communication happens.

1. What Is Network Security?

A network is a group of connected devices that can communicate with each other. Examples include a home Wi-Fi network, a university lab network, a company network, and the internet.

Network security means protecting this communication from unauthorized access, misuse, interruption, and data leakage. It answers four basic questions:

Who is allowed to connect?

What traffic is allowed to pass?

What behavior looks suspicious?

What should we do when something suspicious happens?

Network security is not only one tool. It is a combination of people, policies, devices, software, monitoring, and response procedures.

Returning to CIA triad :

Security Goal	Network Security Meaning	Simple Example
Confidentiality	Keep network data private from unauthorized people.	Prevent an attacker on public Wi-Fi from reading login information.
Integrity	Protect network data from unauthorized change.	Prevent an attacker from modifying a file during upload.
Availability	Keep network services working when needed.	Prevent a DDoS attack from making a website unavailable.

Network Traffic: What Moves Inside the Network?

Network traffic means the flow of data packets between devices over a network. A packet is a small unit of data that moves from one device to another.

Each packet may include these important parts:

Part	Meaning	Simple Example
Source IP address	The device that sends the packet.	192.168.1.25
Destination IP address	The device or server receiving the packet.	203.0.113.55
Protocol	The communication rule being used.	TCP, UDP, ICMP
Port number	The application/service door used by the traffic.	443 for HTTPS, 53 for DNS
Payload	The data being transferred.	A web request, file data, message content, or encrypted data

Explanation
If a packet is like a delivery box, the source IP is the sender address, the destination IP is the receiver address, the protocol is the delivery method, the port is the office door, and the payload is what is inside the box.

Simple Example

Network Record	Explanation
10.0.0.15 -> 142.250.185.14, TCP, Port 443	A device inside the network communicated with an external web server using HTTPS.
10.0.0.20 -> 8.8.8.8, UDP, Port 53	A device asked a DNS server to translate a website name into an IP address.
172.16.0.10 -> 203.0.113.55, TCP, Port 443, 620 MB	A device sent a large amount of data to an external IP. This may need investigation.

3. Network Security vs. Network Forensics

Network security and network forensics are connected, but they are not exactly the same.

Area	Main Question	When It Happens	Example
Network Security	How do we protect the network and detect threats?	Before, during, and after incidents	Configure firewall rules, monitor traffic, block suspicious activity.
Network Forensics	What happened, when, and how?	Mainly after suspicious activity or an incident	Analyze logs to reconstruct a timeline of attacker behavior.

For this Fundamentals lecture, we use some ideas from network forensics, but the focus is network security: how to understand traffic, recognize suspicious behavior, and respond correctly.

4. Main Network Devices and Security Tools

Different devices and tools help control or monitor network communication.

Device / Tool	Main Function	Security Role
Switch	Connects devices inside the same local network.	Can help separate traffic using network design and VLANs in larger networks.
Router	Connects different networks together.	Directs traffic between the local network and other networks, including the internet.

Device / Tool	Main Function	Security Role
Firewall	Filters traffic based on rules.	Allows or blocks traffic using IP addresses, ports, protocols, applications, or policies.
IDS	Intrusion Detection System.	Monitors traffic and generates alerts when suspicious behavior is detected.
IPS	Intrusion Prevention System.	Detects suspicious traffic and may block it automatically.

Firewall: The Network Gatekeeper

A firewall is a security control that decides which traffic is allowed and which traffic is blocked. It can protect one device, one network, or cloud services.

Firewalls often record logs such as:

Allowed connections

Blocked connections

Source and destination IP addresses

Ports and protocols

Time of the connection

Firewall Rule Example	Decision	Reason
Allow internal students to access university system on port 443.	Allow	Students need secure web access to learning services.
Block unknown external traffic trying to access internal database port.	Block	The database should not be open to the public internet.
Block traffic from a known malicious IP address.	Block	The IP is associated with harmful activity.

IDS and IPS: Detecting Suspicious Behavior

IDS and IPS systems analyze traffic patterns. They can detect signs such as malware communication, scanning, unusual access attempts, or possible data exfiltration.

Feature	IDS	IPS
Full name	Intrusion Detection System	Intrusion Prevention System
Main action	Detects and alerts	Detects and may block
Example	Alert: possible data exfiltration	Block a suspicious connection automatically
Simple comparison	Like an alarm camera	Like an alarm camera plus an automatic door lock

5. Common Network Security Threats

The following threats are related to network security. Some of them were introduced in previous lectures, so here they are summarized only from the network point of view.

Threat	Network Security Meaning	Example
Unauthorized access	Someone connects to a system or service without permission.	An attacker guesses or steals an account password and logs in remotely.
Eavesdropping	Someone observes network communication.	An attacker monitors unsafe public Wi-Fi traffic.
Rogue or fake Wi-Fi	A fake network is created to trick users into connecting.	A fake network named "University_Free_WiFi" asks users to log in.
Malware movement	Malware spreads or communicates over the network.	A worm moves from one vulnerable computer to another.
Data exfiltration	Sensitive data leaves the organization without permission.	A large upload of financial files to an unknown external IP.
DoS/DDoS	Attackers overload a service so legitimate users cannot access it.	A website becomes unavailable because it receives more traffic than it can handle.
Insider misuse	A trusted account or person uses access in a harmful way.	An admin account sends sensitive data to an external address.

6. Wireless Network Security

Wireless networks are convenient, but they can expose users if they are open, weakly protected, or fake. This section continues the previous topic of public Wi-Fi and Bluetooth without repeating it fully.

Good Wi-Fi Practices

Use trusted networks when logging in to important accounts.

Avoid sensitive actions on unknown public Wi-Fi, such as banking or sending private files.

Use strong Wi-Fi passwords for private networks.

Change default router passwords.

Update router firmware when updates are available.

Use a guest network for visitors instead of sharing the main network password.

Turn Bluetooth off when it is not needed.

Important Point
Free Wi-Fi is not always safe Wi-Fi. A network can be free, fast, and still risky. The question is not only "Does it connect?" The better question is: "Who controls this network, and what can they see or manipulate?"

7. Sources of Network Security Evidence

When suspicious network activity happens, security teams need evidence. Evidence may come from network devices, security tools, and system logs.

Source	What It May Show	Why It Matters
Firewall, router, and switch logs	Allowed/blocked connections, source/destination IPs, ports, protocols, and time.	Helps identify external communication and suspicious connections.
IDS/IPS alerts	Suspicious patterns such as possible data exfiltration, scanning, malware traffic, or policy violations.	Helps detect behavior that normal users may not notice.

Source	What It May Show	Why It Matters
System and security logs	Logins/logouts, privilege usage, file access, file modification, and log clearing.	Helps connect network activity to user or account activity.

8. Indicators of Suspicious Network Activity

In network security, suspicion should be based on behavior, not assumptions. One event alone may not prove an attack, but a pattern of events can be very important.

Indicator	What It Means	Example
Unusual IP addresses	Communication with external or new IP addresses not normally used by the user or organization.	Finance_Admin connects to 203.0.113.55 for the first time.
Large outbound data transfers	A large amount of data leaves the network suddenly.	620 MB sent outside the organization.
High-privilege accounts	Admin accounts perform unusual network communication.	An admin account uploads files to an unknown external server.
Timing anomalies	Activity occurs outside normal working hours or in very fast sequence.	Login, file access, upload, and log clearing happen within 20 minutes.
Anti-forensic actions	Actions that hide or destroy evidence.	Security logs are cleared after a suspicious transfer.

Key Idea
A suspicious event is stronger when it appears with other suspicious events. Example: external IP + large upload + admin account + log clearing is much stronger than external IP alone.

9. Correlating Network Traffic and User Activity

Network traffic alone shows communication, but it does not always explain who initiated it. System logs alone show user actions, but they do not always show where the data went.

To understand an incident, we correlate different logs together.

Login events

File access events

File modification events

Network connections

Large data transfers

Log clearing or security tool disabling

A simple timeline may look like this:

Timeline Pattern
Login -> file access -> file modification -> external network connection -> large data transfer -> logs cleared

This pattern does not automatically prove guilt, but it strongly suggests that the activity requires investigation.

10. Case Study: Network Security Analysis

Scenario Description

A security analyst reviewed system and network logs related to the account Finance_Admin after unusual network activity was detected. The organization policy states that Finance_Admin accounts must access financial files only from internal network IP addresses.

Log Entries

No.	Time	Event
1	16:10	Finance_Admin logged in from internal IP 172.16.0.10.
2	16:15	Finance_Admin accessed file 'Financials.xlsx'.
3	16:20	Finance_Admin modified file 'Q3_Financials.xlsx'.
4	16:25	Outbound network connection detected from Finance_Admin to external IP 203.0.113.55.
5	16:27	Large data transfer of 620 MB sent to IP 203.0.113.55.
6	16:30	Security logs cleared by Finance_Admin.

11. Prevention, Detection, and Response

Network security work can be organized into three stages.

Stage	Main Question	Examples
Prevention	How do we reduce the chance of attack?	Strong passwords, firewall rules, secure Wi-Fi, patching, least privilege, network segmentation.
Detection	How do we notice suspicious behavior?	Firewall logs, IDS/IPS alerts, unusual IPs, large outbound transfers, timing anomalies.
Response	What do we do after detecting a problem?	Disconnect affected device, preserve logs, reset credentials, block malicious IP, report to security team.

12. Practical Network Security Checklist

For Students and Normal Users

Use trusted Wi-Fi for important accounts.

Do not approve unknown login requests.

Do not share university account passwords.

Turn off Bluetooth when not needed.

Avoid sending sensitive files over unknown networks.

Report strange login alerts or account behavior quickly.

For Organizations

Use firewalls to control traffic entering and leaving the network.

Monitor logs from firewalls, routers, switches, systems, and security tools.

Use IDS/IPS to detect or block suspicious traffic.

Limit admin privileges and monitor high-privilege accounts carefully.

Keep network devices updated.

Separate sensitive systems from general user networks when possible.

Keep backups and incident response procedures ready.

Examples

Example 1: Is It Network Security?

Read each situation and decide if it is mainly network security, device security, account security, or privacy.

Situation	Expected Classification
A student connects to fake university Wi-Fi.	Network security / account security
A laptop has no antivirus.	Device security
An admin account sends 620 MB to an unknown external IP.	Network security / insider misuse
A student clicks "Allow" for an unknown app to access Google contacts.	Privacy / account security
A website is unavailable because too much traffic is sent to it.	Network security / availability

Example 2: Firewall Rule Thinking

Decide whether the firewall should allow or block the following traffic. Explain your reason.

Traffic	Allow or Block?	Reason
Student laptop sent a request to University website, TCP port 443	Allow	Needed secure web access.
Internet sent a request to access internal student grades database	Block	Internal database should not be publicly reachable.
Unknown external IP sent a request to accsess admin login page, many repeated attempts	Block / alert	Possible brute-force or unauthorized access attempt.
Office computer sent data to unknown external IP, 620 MB upload	Alert / investigate	Possible data exfiltration.

Example 3: Suspicious or Normal?

Decide whether each behavior is normal, suspicious, or highly suspicious.

Behavior	Suggested Answer
A student opens the university website at 10:00 AM from university Wi-Fi.	Normal
A finance account sends a large file to a new external IP.	Suspicious / highly suspicious
Security logs are cleared after a large upload.	Highly suspicious
A computer contacts a DNS server to open a website.	Usually normal
An admin account logs in at 3:00 AM and disables security tools.	Highly suspicious

Example 4: Build the Timeline

Arrange according the correct timeline.

Mixed Event	Correct Order
Large outbound data transfer	5
File modification	3
Login	1
Logs cleared	6
File access	2
External network connection	4

Chapter 5: Legal and Ethical Considerations

Cybersecurity is not only about tools, attacks, passwords, firewalls, or malware. It is also about responsibility. A cybersecurity professional may have access to private files, system logs, user accounts, messages, and evidence that can affect people's jobs, reputation, or legal position.

Question

If you found a USB flash drive that might contain stolen company files, what is the first thing you should do: open it quickly to check, or protect it and report it properly? Why?

1. Why Do Law and Ethics Matter in Cybersecurity?

A technical action can be correct from a computer point of view but wrong from a legal or ethical point of view. For example, a student may know how to access another person's account, but that does not make it acceptable. A security employee may know how to read logs or files, but that does not mean they can inspect everything without permission.

Situation	Technical View	Legal / Ethical View
Opening a suspicious USB directly	You may see the files quickly.	You may change evidence, spread malware, or break procedure.
Checking a user's private messages	It may reveal useful information.	It may violate privacy if there is no permission or clear scope.
Copying all files from a laptop	It gives more data to analyze.	It may collect irrelevant private data and create risk.
Writing a report that says "the user is guilty"	It sounds strong.	It is biased unless the evidence truly proves it.

Key Idea

Cybersecurity skill must be controlled by law, ethics, and professional responsibility. Without this control, the investigator can become part of the problem.

2. What Is Digital Evidence?

Digital evidence is any information stored, transmitted, or received in digital form that can help an investigation. It can be found in computers, phones, cloud services, network devices, emails, logs, cameras, smart watches, and many other systems.

Source	Possible Digital Evidence	Simple Example
Computer or laptop	Documents, browser history, deleted files, system logs, USB history	A document shows when it was created or modified.
Smartphone	Messages, photos, calls, GPS, app data	GPS data may show where a person was at a specific time.
Cloud account	Backups, shared files, login history, email records	A deleted photo may still exist in cloud backup.
Network devices	Firewall logs, router logs, connection times, IP addresses	A log shows a large upload to an external IP.
IoT devices	Camera events, smart lock records, smartwatch activity	A smart lock may record when a door was opened.

Digital evidence can answer important questions such as: Who used the account? What file was opened? When did the event happen? Where did the connection go? How did the suspicious activity occur?

3. Why Is Digital Evidence Sensitive?

Digital evidence is powerful, but it is also fragile. It can be changed, deleted, copied, hidden, or misunderstood. This is why investigators must handle it carefully and explain their findings clearly.

Characteristic	Meaning	Simple Example
Easily altered	Small actions may change the data or metadata.	Opening a file may change access time.
Easily deleted	A user or program may remove files or logs.	Security logs are cleared after suspicious activity.
Volatile	Some evidence disappears when power is turned off.	RAM contents may be lost after shutdown.
Easily copied	A copy can be made without obvious physical change.	A file can be copied to USB in seconds.
Hidden	Important data may not be visible to normal users.	Deleted files, caches, metadata, and system artifacts.
Large in volume	There may be too much data to inspect manually.	Thousands of emails or log entries.

Characteristic	Meaning	Simple Example
Global	Data may be stored in another country or cloud provider.	A backup is stored on a foreign cloud server.

Simple Explanation

Digital evidence is like wet ink on paper. If you touch it carelessly, you may change it. If you collect it without documentation, people may doubt it. If you explain it badly, it may mislead others.

4. Legal Considerations: What Are We Allowed to Do?

Legal considerations are about rules, permission, procedure, and admissibility. In cybersecurity, the question is not only "Can I technically access this?" The legal question is "Am I allowed to access this?"

Legal Concept	Simple Meaning	Cybersecurity Example
Authorization	Having permission or legal authority to perform an action.	A company gives the security team permission to review firewall logs.
Scope	The limit of what you are allowed to check.	Investigate the suspected laptop, not every employee device.
Admissibility	Whether evidence can be accepted in court or formal investigation.	A log may be rejected if it was collected incorrectly.
Jurisdiction	The legal area or country whose rules apply.	Cloud data may be stored in another country.
Policy compliance	Following organization rules and procedures.	Using approved tools and writing an incident report.

Important Point

A cybersecurity student or employee should never investigate accounts, devices, or networks without proper permission. Curiosity is not authorization.

5. Ethics: What Should We Do?

Ethics is about responsible behavior even when the law is not very clear. Sometimes a person may have technical access to data, but using that access would still be wrong. Ethical cybersecurity protects systems and also protects people.

Ethical Principle	Meaning	Example
Privacy	Respect personal information.	Do not open unrelated personal photos during a file investigation.
Confidentiality	Do not share sensitive information casually.	Do not tell friends about a student or employee case.
Minimum access	Access only what is needed.	Check relevant logs instead of copying all personal files.
Objectivity	Do not assume guilt before evidence is reviewed.	Write “the evidence suggests” instead of “he is guilty.”
Honesty	Report what you found and what you did not find.	Mention missing logs or uncertainty.
Professional care	Use accepted methods and protect evidence.	Work on a copy and preserve the original.

Ethical Question

If you are able to see private information during an investigation, should you look at everything? A professional answer is no. You should stay within the purpose and scope of the investigation.

6. Authorization and Scope

Authorization means permission to act. Scope means the boundary of that permission. Both are essential. Without authorization, investigation can become illegal. Without scope, investigation can become uncontrolled.

In real organizations, authorization may come from management, legal department, incident response policy, signed consent, or official law enforcement procedure. Students should understand the principle: do not investigate someone else’s device, account, or network just because you have the ability.

Scenario	Allowed or Not?	Reason
A security analyst reviews firewall logs after an official alert.	Usually allowed	It is part of authorized security monitoring.

Scenario	Allowed or Not?	Reason
A student opens a classmate's email account to check for malware.	Not allowed	No permission and account privacy is violated.
An investigator copies only the approved project folder from a company laptop.	Allowed if authorized	The action is within scope.
An employee reads unrelated personal photos during a case.	Not ethical	The data is outside the investigation need.
A teacher asks students to analyze fake sample logs in class.	Allowed	The data is educational and does not expose real people.

7. Admissibility of Electronic Evidence

Evidence is not useful only because it exists. In formal investigations or court, electronic evidence must be acceptable. Admissibility means the evidence can be used because it is relevant, reliable, and collected properly according to the rules that apply.

A simple way to think about admissibility is to ask four questions:

Question	Meaning	Example
1. Is it relevant?	Does it help prove or disprove something important?	A message confirming a planned meeting may be relevant.
2. Is it more useful than harmful?	Does it clarify the issue more than it confuses or unfairly damages?	Hundreds of unrelated browsing logs may confuse the case.
3. Was it legally obtained?	Was it collected with permission, warrant, consent, or proper policy?	Evidence taken by unauthorized hacking may be rejected.
4. Is it reliable and explainable?	Can the source, method, and meaning be defended?	A hash value and documented process support reliability.

Simple Rule

Bad handling can destroy good evidence. A file may show something important, but if it was collected illegally or changed accidentally, it may lose value.

8. Chain of Custody

Chain of custody is the documented history of evidence. It records who collected the evidence, when it was collected, where it was stored, who handled it, and whether it was changed. The goal is to show that the evidence stayed trustworthy from collection to reporting.

Chain of Custody Question	Why It Matters
Who collected the evidence?	Identifies responsibility.
When was it collected?	Supports the investigation timeline.
Where was it collected from?	Connects evidence to the case location or system.
Who handled it after collection?	Shows whether unauthorized people accessed it.
How was it stored?	Shows whether evidence was protected from change or loss.
Was a copy created and verified?	Supports analysis without changing the original.

Time	Action	Person
10:00	USB flash drive found on office desk.	Officer A
10:05	USB placed in evidence bag and labeled.	Officer A
10:20	USB delivered to digital forensics lab.	Officer B
10:35	Forensic copy created and hash value recorded.	Analyst C
11:00	Analysis started on the copy, not on the original.	Analyst C

Key Idea

If the chain of custody is broken, people may ask: Was the evidence changed? Was something added? Was something removed? Can we still trust it?

9. Evidence Integrity and Hash Values

Integrity means that evidence has not been changed. In digital forensics, investigators often use a hash value to help verify integrity. A hash is like a digital fingerprint of a file or disk image. If the data changes, the hash value should change.

Term	Simple Meaning	Example
Original evidence	The actual device or file collected from the scene.	The suspect USB flash drive.

Term	Simple Meaning	Example
Forensic copy / image	A careful copy used for analysis.	A copy of the USB used in the lab.
Hash value	A digital fingerprint used to verify that data did not change.	Hash before analysis equals hash after analysis.
Write protection	A method to prevent changes to storage media.	Using a write blocker when copying a drive.

Important Point

In a simple classroom explanation: do not work directly on the original evidence if you can avoid it. Preserve the original and analyze a verified copy.

10. Privacy and Confidentiality

Cybersecurity investigations can expose sensitive personal or organizational information. The investigator may see private messages, photos, browsing history, medical information, financial documents, or personal accounts. This creates a serious ethical duty.

Risk	What Can Go Wrong?	Responsible Action
Over-collection	Collecting more data than needed.	Collect only what is necessary for the case.
Curiosity browsing	Looking at private data unrelated to the incident.	Stay within scope and document reasons.
Gossip or leakage	Sharing case details with people who do not need to know.	Keep findings confidential.
Misinterpretation	Taking data out of context.	Correlate with other evidence and mention uncertainty.
Unsecured storage	Evidence or reports are lost or exposed.	Store evidence in protected locations.

Professional Rule

Access does not mean permission. Permission does not mean unlimited access. Investigation must be limited, documented, and justified.

11. Objectivity and Bias

A good cybersecurity analyst does not begin with the conclusion. The analyst begins with the evidence. If the analyst already decided that a person is guilty, they may ignore evidence that points in another direction.

Bad Reporting Style	Better Reporting Style
The employee stole the files.	The account uploaded 620 MB to an external IP after accessing financial files. This may indicate data exfiltration and requires further investigation.
The student hacked the system.	The logs show repeated failed login attempts from the student's device, followed by one successful login. More context is needed.
The audio proves confession.	The audio appears to contain a confession, but authenticity and chain of custody must be verified.
The user deleted evidence.	Security logs were cleared by the account at 16:30. The reason is not yet confirmed.

Key Sentence

A professional report should separate facts, interpretation, and conclusion. It should not exaggerate what the evidence can prove.

12. Case Study: The USB Evidence Problem

Scenario Description

A local company reports that confidential customer data was stolen. The security team finds a USB flash drive on the desk of an employee who had access to the customer database. Everyone wants to open the USB immediately. However, the team must handle the situation legally and ethically.

No.	Event	Question
1	USB found on employee desk.	Who should collect it and how should it be documented?
2	Manager wants to open it quickly on a normal laptop.	What risk does this create?
3	Security analyst says a forensic copy should be created first.	Why is this better?
4	The USB contains customer files and personal photos.	Which files should be examined and which should be avoided?

No.	Event	Question
5	The report says “employee is guilty.”	What is wrong with this wording?
6	The chain of custody form is incomplete.	How does this affect trust in the evidence?

Suggested Analysis

No.	Suggested Answer
1	The USB should be collected by an authorized person, labeled, sealed, and recorded in the chain of custody.
2	Opening the USB directly may change metadata, spread malware, or weaken evidence integrity.
3	A forensic copy protects the original and allows analysis to be repeated or verified.
4	Investigators should focus on relevant customer files and avoid unrelated personal data unless it becomes clearly relevant and authorized.
5	The report should describe evidence and avoid declaring guilt. Guilt is a legal conclusion, not a technical shortcut.
6	An incomplete chain of custody creates doubt about whether the evidence was changed, lost, or accessed by unauthorized people.

Conclusion

The strongest cybersecurity work is not only technical. It is careful, legal, ethical, and well documented.

13. Case Study: The Voice Case

A digital audio clip is leaked online. The clip seems to contain a person confessing to a crime. The clip spreads quickly on social media, and many people believe it immediately. The question is: should this audio be accepted as evidence?

Concern	Question to Ask
Authenticity	Is the audio original, edited, generated, or taken out of context?
Source	Who recorded it and how was it obtained?
Chain of custody	Who handled the file from the time it was created until now?
Metadata	Does the file metadata support the claimed time, device, and source?
Fairness	Could the audio mislead people if presented without context?
Privacy and legality	Was it recorded or leaked legally?

14. Practical Checklist for Cybersecurity Students

Before handling digital evidence or suspicious data, use this simple checklist.

Question	Yes / No
Do I have permission or authority to access this data?	
Do I understand the scope of what I am allowed to check?	
Am I avoiding unrelated private information?	
Am I documenting what I did and when I did it?	
Am I preserving the original evidence when possible?	
Am I analyzing a copy instead of changing the original?	
Can I explain my method clearly to another person?	
Am I reporting facts separately from opinions?	
Am I honest about uncertainty or missing information?	
Am I keeping the case confidential?	

Simple Rule to Remember

Before you click, copy, open, delete, share, or report: ask yourself whether the action is authorized, necessary, documented, and fair.

Examples

Example 1: Legal, Ethical, or Both?

Read each situation and decide if the main issue is legal, ethical, both, or acceptable.

Situation	Expected Classification	Reason
A student tries to access a classmate's account to "test security."	Legal and ethical problem	No authorization and privacy is violated.
A security analyst reviews firewall logs after a real alert.	Acceptable if authorized	Monitoring logs is part of approved security work.
An employee shares investigation details with friends.	Ethical problem	Confidentiality is violated.
An investigator collects personal photos unrelated to the case.	Ethical and possibly legal problem	Outside scope and violates privacy.
A report says "possible data exfiltration" because evidence is not complete.	Acceptable	The wording acknowledges uncertainty.

Example 2: Stay Within Scope

The investigation is about a leaked file named Customers.xlsx. Decide whether each action is inside or outside the investigation scope.

Action	Inside or Outside Scope?	Reason
Check access logs for Customers.xlsx.	Inside	Directly related to the leaked file.
Inspect all family photos on the laptop.	Outside	Not related to the case.
Review USB connection history around the time of the leak.	Inside	May show file copying activity.
Read unrelated private chat messages.	Outside unless specifically authorized and relevant	Privacy risk.
Create a report explaining what was checked and why.	Inside	Documentation is part of responsible procedure.

Example 3: Is the Evidence Strong?

Decide whether each item is weak, useful, or strong evidence. Explain why.

Evidence Item	Suggested Answer	Reason
A screenshot shared on social media.	Weak alone	May be edited and has unclear source.
Firewall log showing a large upload to an external IP.	Useful	Shows network behavior but needs correlation.
Hash-verified forensic copy of a USB containing the leaked file.	Strong	Integrity and relevance are supported.
A rumor that an employee was angry.	Weak	Not technical evidence and may be biased.
Timeline showing login, file access, USB connection, and file copy.	Strong	Multiple events support each other.

Example 4: Build a Chain of Custody

Arrange the following actions in the correct order.

Mixed Event	Correct Order
Analyze the forensic copy.	5
Find the USB on the desk.	1
Place the USB in an evidence bag and label it.	2
Create a forensic copy and record hash value.	4
Deliver the USB to the lab and record the transfer.	3
Write the final report with methods and findings.	6

Final Summary

Cybersecurity is not only a technical field. It is a trust field. Students must learn that digital evidence can help reveal the truth, but only when it is collected and explained legally, ethically, and carefully.

Legal considerations answer: Am I allowed to do this?

Ethical considerations answer: Should I do this, and how can I do it responsibly?

Digital evidence must be protected because it can be changed, copied, deleted, hidden, or misunderstood.

Authorization, scope, privacy, chain of custody, integrity, and objective reporting are essential.

The best cybersecurity professional is not only skilled, but also careful, fair, and honest.

Chapter 6: Cyberpsychology: The Human Brain as the Last Firewall

Cybersecurity is not only about firewalls, passwords, encryption, and networks. It is also about attention, fear, curiosity, trust, habit, design, fatigue, and the small human decision before a click.

What Cyberpsychology Means

Definition: Cyberpsychology studies how people think, feel, and behave around digital technology, and how digital systems influence human decisions.

In cybersecurity, it explains why users click suspicious links, reuse passwords, ignore warnings, accept permissions, or trust fake pages.

Main idea: attackers often do not hack the computer first; they hack emotion, attention, trust, urgency, curiosity, or fatigue.

Important line: the human brain is not a bug. It uses shortcuts to survive quickly, but attackers can turn these shortcuts into vulnerabilities.

Psychological Buttons Used in Cyber Attacks

Button	Typical message	Human effect
Urgency	"Confirm now or lose access."	Reduces thinking time.
Fear	"Your account is infected/leaked."	Narrows attention.
Authority	"Message from IT / bank / university."	Reduces questioning.
Curiosity	"Your result/photo is attached."	Creates an information gap.
Reward	"Free gift / free software."	Makes desire argue with security.
Fatigue	Repeated MFA prompts.	Turns security into noise.

Smart Devices and Behavioral Data

Smart devices may collect or infer patterns, not only content: typing rhythm, scroll style, touch pressure, pauses, phone angle, motion, location routine, and app habits.

Positive side: behavioral biometrics can help detect account misuse when the password is correct but the typing or interaction style is unusual.

Risk side: the same behavior patterns can profile stress, routine, mood, or private habits if collection is unclear.

Dark Patterns: When the Interface Becomes the Attacker

Dark patterns are interface choices that push, hide, confuse, or exhaust the user into decisions they may not really want.

Examples: large “Accept all” button with hidden reject option; easy subscription but difficult cancellation; fake countdown timers; pre-selected permission boxes.

Human biases involved: scarcity, social proof, default bias, loss aversion, urgency, and framing.

Ethical contrast: good design clarifies choices; manipulative design hides consequences.

Defending the Brain

Design for real humans: tired, busy, distracted, emotional, and under pressure.

Make safe choices easy and risky actions slower. Use clear language instead of frightening or confusing messages.

Reduce alert fatigue. Too many prompts can train people to approve automatically.

Teach a pause routine: Stop -> name the emotion -> verify through another channel -> report suspicious activity.

The 5-second firewall

Before clicking, ask: Who benefits if I click now? What emotion is being pushed? Can I verify somewhere else? Is this permission necessary? What would happen if I wait 5 minutes?