МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх справ
Кафедра мовної підготовки

English for Cybersecurity Students
Навчальний посібник з англійської мови здобувачів вищої освіти першого (бакалаврського) рівня за спеціальністю F5 «Кібербезпека та захист інформації»

Кам’янець-Подільський
2026

УДК: 811.111:004.056(075.8)
П14

Рекомендовано до друку Вченою радою
Харківського національного університету внутрішніх справ
(протокол № 1 від 18.08.2026 року)

Автор:
Павліна Тетяна Володимирівна, старша викладачка кафедри мовної підготовки Харківського національного університету внутрішніх справ

Рецензенти:
Березнева Ірина Миколаївна, доцент кафедри іноземних мов центру мовної підготовки Національної академії Національної гвардії України;
Ірина Леонідівна Кравець, кандидат педагогічних наук, доцент кафедри мовної підготовки Харківського національного університету внутрішніх справ

П14 English for Cybersecurity Students: навчальний посібник з англійської мови для здобувачів вищої освіти першого (бакалаврського) рівня за спеціальністю F5 «Кібербезпека та захист інформації»/ Т. В. Павліна ; Харківський національний університет внутрішніх справ. — Кам'янець-Подільський: ХНУВС, 2026. - 114 с.
Навчальний посібник спрямований на формування та розвиток іншомовної професійної компетентності майбутніх фахівців у сфері кібербезпеки. Матеріали посібника сприяють удосконаленню навичок читання, розуміння, перекладу та аналізу англомовних професійно орієнтованих текстів, розширенню термінологічного словникового запасу й практичному застосуванню граматичних структур. Тематика навчальних матеріалів охоплює основні поняття кібербезпеки, кіберзагрози, захист інформації, кіберзлочинність, інформаційні технології та міжнародну співпрацю у сфері протидії кіберзагрозам. Посібник допомагає здобувачам освіти опановувати сучасну професійну лексику та використовувати англійську мову для роботи з технічною документацією, міжнародними інформаційними ресурсами й науковими матеріалами. Видання може бути використане під час аудиторного навчання та самостійної роботи здобувачів вищої освіти.

ПЕРЕДМОВА

Сучасний світ стрімко змінюється під впливом цифрових технологій, а кіберпростір стає невід'ємною складовою суспільного, економічного та професійного життя. Разом із новими можливостями цифровізації виникають і нові виклики: кібератаки, витоки даних, шкідливе програмне забезпечення, соціальна інженерія та інші кіберзагрози набувають дедалі складніших форм і не визнають державних кордонів. За таких умов підготовка компетентних фахівців у сфері кібербезпеки потребує не лише ґрунтовних технічних знань, а й належного рівня володіння англійською мовою як основним засобом міжнародної професійної комунікації.

Навчальний посібник «English for Cybersecurity Students» підготовлено для здобувачів вищої освіти першого (бакалаврського) рівня за спеціальністю F5 «Кібербезпека та захист інформації» Харківського національного університету внутрішніх справ. Його основною метою є формування та розвиток англомовної комунікативної й професійно орієнтованої компетентності майбутніх фахівців, здатних ефективно працювати з іншомовною інформацією, використовувати професійну термінологію та здійснювати комунікацію у сфері кібербезпеки.

Особливість посібника полягає у поєднанні мовної та фахової підготовки. Англійська мова в ньому розглядається не лише як навчальна дисципліна, а і як практичний інструмент професійного становлення майбутнього фахівця. Саме англійською мовою створюється значна частина сучасної технічної документації, наукових публікацій, стандартів, професійних ресурсів, рекомендацій з інформаційної безпеки та матеріалів міжнародних організацій. Тому здатність читати, розуміти, аналізувати й використовувати англомовні джерела є важливою складовою професійної компетентності фахівця з кібербезпеки.

Матеріали посібника спрямовані на розвиток навичок читання, розуміння, перекладу та аналізу англомовних професійно орієнтованих текстів, розширення словникового запасу, опанування спеціальної термінології, а також систематизацію та практичне застосування граматичних структур, необхідних для професійного спілкування. Значна увага приділяється формуванню вмінь використовувати нову лексику в контексті, визначати основну та другорядну

інформацію, встановлювати логічні зв’язки між частинами тексту, формулювати власні висловлювання та працювати з автентичними матеріалами за фахом.

Тематика посібника охоплює широке коло питань, пов’язаних із розвитком комп’ютерних технологій та сучасної кібербезпеки. Поряд із базовими поняттями про комп’ютери, інформаційні технології, кіберзлочинність і захист інформації розглядаються актуальні напрями цифрового розвитку, зокрема штучний інтелект, робототехніка, безпілотні літальні апарати, квантові обчислення, постквантова криптографія, безпека бездротових мереж, операційних систем та інформаційних систем. Такий тематичний спектр дає змогу студентам поступово формувати професійний тезаурус і водночас ознайомлюватися з технологіями, які визначають сучасний і майбутній розвиток галузі.

Важливим принципом побудови посібника є поступовість і логічне ускладнення матеріалу. На початковому етапі студенти опрацьовують основні поняття та терміни, необхідні для розуміння професійної сфери. Надалі вони переходять до складніших технологічних і прикладних питань, що потребують ширшого словникового запасу, глибшого розуміння змісту та здатності аналізувати професійні тексти. Це сприяє системному формуванню англомовного термінологічного словника майбутнього фахівця та створює підґрунтя для самостійної роботи з іншомовними джерелами.

Запропоновані матеріали можуть використовуватися під час аудиторної та самостійної роботи, на практичних заняттях з англійської мови професійного спрямування, а також як додатковий ресурс для індивідуального опрацювання навчального матеріалу. Завдання можуть адаптуватися відповідно до рівня мовної підготовки студентів, навчальних цілей і формату освітнього процесу.

Очікується, що систематична робота з посібником сприятиме формуванню здатності студентів упевнено орієнтуватися в англомовному професійному середовищі, розуміти спеціалізовану інформацію, коректно використовувати термінологію, аналізувати тексти за фахом і здійснювати професійно орієнтовану комунікацію англійською мовою.

ЗМІСТ	
Передмова	**3**
Unit 1. The origin of cybersecurity	**6**
Unit 2. The evolution of cybercrime	**12**
Unit 3. The history of cybercrime and new threats	**19**
Unit 4. Global cyberpolice	**26**
Unit 5. Cyberpolice in Ukraine	**31**
Unit 6. Evolution of computers	**37**
Unit 7. Computer architecture and I/O devices	**43**
Unit 8. The Quantum leap: the future of quantum computers, and post-quantum cryptography.	**57**
Unit 9. Revision units 1-8	**60**
Unit 10. The history and evolution of artificial intelligence.	**72**
Unit 11. AI and cybersecurity.	**76**
Unit 12. Robots among us: the rise of Intelligent Machines .	**79**
Unit 13. Unmanned drones. The future of robotics.	**84**
Unit 14. Protecting information systems.	**88**
Unit 15 Security in Wi-Fi networks.	**92**
Unit 16. Security in operating systems.	**96**
Unit 17. Malicious software and cyber hygiene.	**100**
Unit 18. Revision units 10-17	**104**
References	**113**

UNIT 1. THE ORIGIN OF CYBERSECURITY

Quiz

1. Which word is connected to the old Greek poet Homer?

a) Virus
b) Domain
c) Trojan
d) Squatting

2. "Cyber" is shortened from --------- meaning in Greek

a) 1 driver
b) 2 steersman
c) 3 pilot
d) 4 player

3. Match words with definitions

Term	**Definition**
1.Cybersecurity	**A.** Criminal activity committed using computers or the internet.
2. Cyberspace	**B.** The use of electronic communication to bully or harass others.
3. Cybercrime	**C.** The practice of protecting digital networks, devices, and data from attacks.
4.Cyberbullying	**D.** The virtual, intangible environment where online communication takes place .

Glossary

Computer worm	Malware that spreads automatically between computers.
Malicious	Intended to cause harm or damage.
Antivirus software	Software designed to detect and remove malware.
Network	A group of connected computers and devices.
Infrastructure	Essential systems such as power, communications, banking, and transport.
Cybersecurity	The protection of computer systems and networks from cyber threats.
Malware	Software designed to damage or disrupt computer systems.

The Origin Of Cybersecurity

The word **cybernetics** was coined in 1947 by an American mathematician named **Norbert Wiener**. He needed a word to describe a new science: the study of how both machines and living organisms control themselves and communicate.

Wiener chose the ancient Greek word **kybernētēs**, which means "steersman" or "the pilot of a ship." He used this as a metaphor. When a pilot steers a boat, they look at the waves, change the rudder, see how the boat responds, and then adjust the steering again. This continuous process of adjusting based on new information is called a **feedback loop**.

Today, cybernetics is everywhere. It explains how a home thermostat keeps a room warm, how the human body maintains its temperature, and how modern Artificial Intelligence (AI) learns from data to make decisions

Cybernetics laid the absolute groundwork for the digital age. Without it, we would not have modern computing, automation, robotics, or Artificial Intelligence (AI). AI operates on cybernetic principles by analyzing data, learning from its mistakes, and optimizing its outputs.

In the early days of computers, security was not a major worry. Computers were massive machines locked in secure rooms, accessible only to a few scientists. However, everything changed in 1971 with the creation of the world's first computer worm, called **Creeper**. Created by researcher Bob Thomas, Creeper was not malicious; it simply traveled between connected computers and displayed the message: *"I'm the creeper, catch me if you can!"*

To solve this problem, a scientist named Ray Tomlinson wrote a program called **Reaper**. Reaper's sole purpose was to travel through the network, find Creeper, and delete it. This was the world's first antivirus software, marking the birth of **cybersecurity**.

Today, cybersecurity is no longer just about catching simple worms. It is the vital practice of protecting digital networks, mobile devices, servers, and data from malicious attacks. Because our modern world relies entirely on the internet for banking, healthcare, and power grids, cybersecurity has become essential for keeping society running safely.

Exercise 1. Match the Terms with Their Definitions

Term	**Definition**
1. Coined	A. A person who steers a boat or ship.
2. Steersman	B. Invented or created a new word or phrase.
3. Metaphor	C. A cycle where a system uses information about its results to adjust itself.
4. Feedback loop	D. A figure of speech used to explain one thing by comparing it with another.

Exercise 2. Complete the Sentences

Use the words from the box.

Word Box: ***cybernetics • feedback loop • thermostat • metaphor • automation***

1. A _____ keeps a room at the desired temperature.
2. Norbert Wiener used a ship's pilot as a _____ to explain cybernetics.

3. A _____ allows a system to learn from previous results.
4. Modern factories often rely on _____ to perform repetitive tasks.
5. _____ studies communication and control in both machines and living organisms.

Exercise 3. True or False
Decide whether the statements are **True (T)** or **False (F).**
1. The word *cybernetics* comes from an ancient Greek word.
2. Norbert Wiener introduced the term in 1947.
3. Cybernetics only studies computers.
4. A feedback loop helps a system improve its performance.
5. Artificial Intelligence uses cybernetic principles.

Exercise 4. Answer the Questions
1. Why did Norbert Wiener create the word *cybernetics*?
2. What does the Greek word *kybernētēs* mean?
3. What is a feedback loop?
4. How does a thermostat demonstrate cybernetic principles?
5. Why is cybernetics important for Artificial Intelligence?

Discussion Task
Discuss the following questions with a partner.
1. Can you think of another example of a feedback loop in everyday life?
2. Why do you think cybernetics is still relevant today?
3. How is learning in humans similar to learning in AI?

Part II. Reading
Reading 2. The Birth of Cybersecurity
(Insert your remaining three paragraphs beginning with "In the early days of computers..." here.)

Vocabulary Exercises
Exercise 5. Match the Terms with Their Definitions

1. Malicious	A. Essential systems needed for society to function.
2.Infrastructure	B. Intended to cause harm.
3. Worm	C. Malware that spreads automatically between computers.
4. Antivirus	D. Software that detects and removes malicious programs.

Exercise 6. Complete the Sentences Use the words from the box.

Word Box: *worm • antivirus • malicious • infrastructure • cybersecurity*

1. A computer _____ can spread across a network by itself.
2. _____ software helps detect and remove malware.
3. Banks and hospitals are part of a country's critical _____.
4. Some hackers create _____ software to damage systems.
5. _____ protects networks, devices, and digital information.

Exercise 7. Multiple Choice

Choose the correct answer.

1. Why was security not a major concern for early computers?

a) They were physically protected.
b) They had no operating systems.
c) They were connected to the internet.

2. What was Creeper?

a) The first antivirus
b) The first computer worm
c) The first firewall

3. What was the purpose of Reaper?

a) To steal passwords
b) To spread through the network
c) To remove Creeper

4. Why has cybersecurity become essential today?

a) Because computers are becoming smaller.
b) Because society depends on digital systems.
c) Because antivirus software is expensive.

Task 8. Case Study: *The Cuckoo's Egg* – How a 75-Cent Error Exposed a Cyber Spy

In 1986, system administrator Clifford Stoll noticed a small accounting error of just 75 cents on a university computer system. Instead of ignoring the discrepancy, he began investigating its cause.

His investigation revealed that an unauthorized user had gained access to the university's network. Over the following months, Stoll carefully monitored the intruder's activities and worked with law enforcement agencies to trace the hacker. Eventually, the investigation uncovered an international cyber espionage operation in which stolen military and scientific information was being passed to Soviet intelligence.

The case became one of the first well-documented examples of cyber espionage and demonstrated that even a minor irregularity in a computer system could indicate a serious security breach. Stoll later described the investigation in his book *The Cuckoo's Egg*, which remains a classic in the field of cybersecurity.

Answer the questions.

1. What unusual event first attracted Clifford Stoll's attention?
2. Why did Stoll decide to investigate such a small accounting error?

3. What did the investigation ultimately reveal?
4. Why is this case considered an important milestone in the history of cybersecurity?
5. What lesson can cybersecurity professionals learn from this incident?

Discuss the following questions in pairs or small groups.
1. Why is attention to detail an important skill for cybersecurity professionals?
2. What might have happened if Clifford Stoll had ignored the 75-cent discrepancy?
3. Can a small technical problem sometimes indicate a much larger security issue? Give an example.

Task 9. Discussion
1. Why do you think cybersecurity has become more important than physical security for many organizations?
2. Which devices in your daily life require cybersecurity protection?
3. What would happen if hospitals or power stations lost their computer systems for one day?

Grammar focus: Irregular plurals of Latin and Greek origin

Many English nouns come from **Latin or Greek**. Some of these nouns keep their original plural forms instead of taking the usual **-s** or **-es** ending.

1. Latin-origin nouns

Singular	Plural	Example
criterion	**criteria**	The criteria are strict.
phenomenon	**phenomena**	These phenomena are difficult to explain.
analysis	**analyses**	The researchers conducted several analyses.
crisis	**crises**	Several crises affected the system.
hypothesis	**hypotheses**	The scientists tested several hypotheses.
thesis	**theses**	The students presented their theses.
diagnosis	**diagnoses**	Doctors made several diagnoses.
medium	**media**	Social media can spread information quickly.
datum	**data**	The data are stored securely.
formula	**formulae / formulas**	The researchers used different formulas.
index	**indices / indexes**	The database contains several indices.

Common patterns

-on → -a
phenomenon → phenomena
criterion → criteria

-um → -a
datum → data
medium → media

-is → -es
analysis → analyses
crisis → crises
hypothesis → hypotheses
thesis → theses

2. Greek-origin nouns
Many Greek nouns also have special plural forms.

Singular	Plural	Example
analysis	**analyses**	The analyses revealed a vulnerability.
crisis	**crises**	The organisation faced several crises.
hypothesis	**hypotheses**	The researchers developed two hypotheses.
phenomenon	**phenomena**	These phenomena require further research.
criterion	**criteria**	The system must meet several criteria.
thesis	**theses**	The students defended their theses.
diagnosis	**diagnoses**	The doctors made several diagnoses.

Important
Some nouns have **two accepted plural forms**, especially in modern English.
formula → formulae / formulas
index → indices / indexes
appendix → appendices / appendixes
In technical and academic English, the traditional Latin forms are often preferred.

Exercise 1. Write the plural form
1. criterion → _____
2. analysis → _____
3. phenomenon → _____
4. crisis → _____
5. hypothesis → _____
6. datum → _____
7. medium → _____
8. thesis → _____
9. diagnosis → _____
10. formula → _____
11. index → _____
12. appendix → _____

Exercise 2. Choose the correct form
1. The researchers conducted several **analysis / analyses** of the cyberattack.
2. The system must satisfy several security **criterion / criteria**.
3. The database contains millions of pieces of **data / datum**.
4. Several economic **crisis / crises** can affect cybersecurity investment.

5. The scientists tested three different **hypothesis / hypotheses**.
6. These natural **phenomenon / phenomena** are difficult to explain.
7. Social **medium / media** can be used to spread misinformation.
8. The doctors made several **diagnosis / diagnoses**.
9. The researchers compared different mathematical **formulae / formulas**.
10. The database uses several **indices / indexes** to improve performance.

Unit Summary

In this unit, you learned:

- the origin of the word *cybernetics*;
- how feedback loops work;
- why cybernetics became the foundation of AI and automation;
- how the first computer worm led to the creation of the first antivirus software;
- why cybersecurity is essential in the modern digital world

UNIT 2. THE EVOLUTION OF CYBERCRIME.

	Glossary
Phreaker	**A person who illegally manipulates telephone networks to make free calls or access telecommunications services.**
Vulnerability	**A weakness in a computer system that attackers can exploit.**
Worm	**A type of malware that spreads automatically across networks without user action.**
Identity theft	**The crime of stealing someone's personal information for fraudulent purposes.**
Phishing	**A cyberattack that tricks people into revealing sensitive information through fake emails or websites.**
Botnet	**A network of infected computers controlled remotely by cybercriminals.**
Distributed Denial of Service (DDoS) attack	**An attack in which many compromised devices flood a server or website with traffic, making it unavailable to users.**
Cybercrime syndicate	**An organized group of criminals involved in cybercrime activities.**
Ransomware	**Malware that encrypts files and demands payment to restore access.**
Cryptocurrency	**A digital currency secured by cryptography, such as Bitcoin.**

Cyberwarfare	**The use of cyberattacks by states to damage or disrupt another country's digital infrastructure.**

The Evolution of Cybercrime; from pranks to global threats

Cybercrime is one of the fastest-growing threats in the modern world. Today, hackers steal millions of dollars, disrupt government systems, and compromise personal data. However, the digital underworld did not appear overnight. It evolved over several decades, moving from innocent curiosity to highly organized global crime.

In the early days of computing, cybercrime as we know it today did not exist. The earliest hackers were often university students or technology enthusiasts. **In the 1970s**, "phreakers" hacked the telephone network to make free long-distance phone calls.

By the 1980s, the first computer viruses appeared. In 1986, two brothers from Pakistan created the "Brain" virus. It is considered the first virus for IBM-compatible computers. They did not want to steal money; they just wanted to protect their medical software from piracy. During this era, most hackers were motivated by curiosity or fame, not financial gain.

The 1990s changed everything with the birth of the World Wide Web. As businesses and individuals connected to the internet, new vulnerabilities emerged. In 1988, just before the decade started, the Morris Worm infected about 10% of all computers connected to the internet, causing massive slowdowns.

In the late 1990s, the first major email viruses arrived. The "Melissa" virus in 1999 spread through Microsoft Word documents, overloading email servers worldwide. This period marked the transition from harmless pranks to expensive digital disruptions. Governments began to realize that cybersecurity was a national priority.

In the 21st century, cybercrime became a business. Hackers stopped looking for fame and started looking for money. Credit card theft, identity theft, and phishing emails became mainstream tools for criminals.

This era saw the rise of botnets—networks of infected computers controlled remotely by a single hacker. Criminals used botnets to launch Distributed Denial of Service (DDoS) attacks, crashing banking and e-commerce websites. Cybercrime syndicates formed, operating like professional corporations with their own developers and support staff.

Today, cybercrime is a sophisticated industry. The most dangerous development of recent years is ransomware. This malware encrypts a victim’s files and demands payment in cryptocurrency to unlock them. Major institutions, including hospitals, schools, and city governments, regularly fall victim to ransomware.

Furthermore, cyberwarfare has emerged. State-sponsored hackers now target critical infrastructure, such as power grids and election systems. The line between independent criminals and government military operations has become blurred.

Exercise 1. Answer the questions

1. How has cybercrime changed since the early days of computing?
2. Who were the first hackers, and what motivated them?
3. What was the purpose of the "Brain" virus?

4. Why was the Morris Worm considered significant?
5. How did the Melissa virus spread?
6. What changes occurred in cybercrime during the 21st century?
7. What is a botnet, and how is it used?
8. How does ransomware affect its victims?
9. What is cyberwarfare?
10. Why has cybersecurity become a national priority?

Exercise 2. Decide whether the statements are **True (T)** or **False (F)**.

1. The earliest hackers were mainly interested in making money.
2. Phreakers hacked telephone systems.
3. The Brain virus was created to steal bank account information.
4. The Morris Worm spread automatically through the internet.
5. The Melissa virus spread through email attachments.
6. Botnets consist of computers controlled remotely by hackers.
7. Ransomware deletes files permanently without asking for payment.
8. Cyberwarfare often targets critical infrastructure.
9. Modern cybercrime is frequently organized like a business.
10. The distinction between cybercriminals and state-sponsored hackers is always clear.

Exercise 3. Match the Terms with Their Definitions

A	**B**
1. Phishing	a. A network of infected computers
2. Botnet	b. A weakness in a computer system
3. Vulnerability	c. Malware that demands payment
4. Ransomware	d. Deceptive messages used to steal information
5. Cyberwarfare	e. Government-sponsored cyber operations

Exercise 4. Complete the Sentences

Use the words from the box.

Word Box: phishing, ransomware, botnet, vulnerability, cyberwarfare, virus

1. A _____ can spread from one computer to another by infecting files.
2. Criminals use _____ emails to trick victims into revealing passwords.
3. A _____ is a weakness that attackers can exploit.
4. A _____ consists of many infected computers controlled by a hacker.
5. _____ encrypts files and demands payment for their recovery.
6. _____ involves cyberattacks carried out by or on behalf of governments.

Task 5. Put the Events in Chronological Order

Arrange the following events from the earliest to the most recent.

- Rise of ransomware
- Creation of the Brain virus

- The Melissa virus outbreak
- Phone phreaking
- Growth of botnets and DDoS attacks
- The Morris Worm

Task 6. Discussion Questions

1. Why do you think the motivations of hackers changed over time?
2. Which type of cybercrime described in the text do you consider the greatest threat today? Why?
3. How can individuals protect themselves from phishing and ransomware attacks?
4. Should governments cooperate internationally to combat cybercrime? Explain your opinion.
5. How do cyberattacks differ from traditional crimes?

Task 7. Vocabulary in Context

Choose the correct answer.

1. A **vulnerability** is:

a) a computer program
b) a security weakness
c) a type of virus

2. A **botnet** is controlled by:

a) antivirus software
b) internet providers
c) a cybercriminal

3. **Ransomware** mainly aims to:

a) improve computer performance
b) encrypt files and demand money
c) block advertisements

4. **Cyberwarfare** usually involves:

a) online shopping
b) government-backed cyber operations
c) software development

5. **Phishing** attacks usually attempt to:

a) steal sensitive information
b) repair damaged files
c) speed up internet connections

USE OF ENGLISH: Phrasal Verbs and idioms for Cybersecurity

Phrasal verb	Meaning
break into	enter a computer system illegally
break down	stop working
carry out	perform an action or attack
come across	find something unexpectedly

Phrasal verb	Meaning
find out	discover information
log in	enter a computer system or account
log out	leave a computer system or account
back up	make a copy of data
set up	create or prepare a system
shut down	turn off a computer or system
take over	gain control of something
wipe out	completely delete or destroy something

Useful set expressions

Expression	Meaning	Example
get to the bottom of something	discover the real cause of a problem	Investigators are trying to **get to the bottom of** the attack.
leave no stone unturned	make every possible effort to find something	The investigators **left no stone unturned** when searching for evidence.
raise a red flag	indicate a possible problem or danger	The unusual login **raised a red flag**.
a red flag	a warning sign	Multiple failed logins were **a red flag**.
a wake-up call	an event that makes people realise they must act	The attack was **a wake-up call** for the company.
stay one step ahead	remain more advanced than an opponent	Security teams must **stay one step ahead** of cybercriminals.
stay ahead of the game	remain successful by anticipating changes	Organisations need to **stay ahead of the game** as threats evolve.
be in the loop	be informed about what is happening	Keep the security team **in the loop**.
keep someone in the loop	keep someone informed	Please **keep me in the loop** about the investigation.
a weak link	the least secure or strongest part of a system/group	Human error can be **the weak link** in cybersecurity.
the weakest link	the least reliable part	An organisation's employees can sometimes be **the weakest link**.
open the door to something	create an opportunity for something, often negative	Poor security can **open the door to** attackers.
close the door on something	prevent something from happening	Strong authentication can **close the door on** many attacks.

Expression	Meaning	Example
a loophole	a weakness or gap in a rule/system	Attackers found **a loophole** in the security policy.
a grey area	a situation where the rules are unclear	The legal use of some hacking tools remains **a grey area**.
tip someone off	give someone secret information or a warning	The unusual network activity **tipped the investigators off**.
cover your tracks	hide evidence of what you have done	The attacker tried to **cover their tracks**.
leave a digital footprint	leave information or evidence of online activity	Criminals often **leave a digital footprint**.
connect the dots	understand how separate pieces of information are related	Investigators eventually **connected the dots** between the attacks.
follow a lead	investigate information that may help solve a case	The police decided to **follow a new lead**.

Risk, Problems and Incidents

Expression	Meaning	Example
a ticking time bomb	a serious problem that may cause trouble at any moment	The unpatched server was **a ticking time bomb**.
a disaster waiting to happen	a situation likely to end badly	Poor password management is **a disaster waiting to happen**.
a nightmare scenario	a very bad possible situation	A complete loss of customer data would be **a nightmare scenario**.
back to square one	back to the beginning after a failure	The backup was corrupted, so the team was **back to square one**.
put out fires	deal with problems as they appear	The IT team spends too much time **putting out fires**.
under pressure	experiencing stress or difficulty	Security teams often work **under pressure** during an attack.
a close call	a situation in which something bad almost happened	Losing the backup server was **a close call**.
in hot water	in serious trouble	The company was **in hot water** after the data breach.
take the heat	receive criticism or blame	The security manager had to **take the heat** after the breach.

Expression	Meaning	Example
bite the bullet	face a difficult situation and take necessary action	The company had to **bite the bullet** and replace its outdated systems.

Exercise 8. Choose the correct phrasal verb.
break into • carry out • find out • back up • set up • shut down • take over • log in • come across • wipe out

1. The hackers tried to _____ the company's database.
2. The security team will _____ an investigation into the attack.
3. Users should regularly _____ important files.
4. The administrator had to _____ the infected server.
5. The police are trying to _____ who launched the attack.
6. The company needs to _____ a secure network for its employees.
7. The researchers _____ an unusual piece of malware during their investigation.
8. The attacker managed to _____ the administrator's account.
9. The malware could _____ all the files on the computer.
10. Employees must _____ before accessing the secure system.

EXERCISE 9. Idioms and Set Expressions
Complete the sentences with the correct expression from the box. **Use each expression once.**
raise a red flag | get to the bottom of something | stay one step ahead | keep someone in the loop | the weakest link | open the door to something | cover your tracks | leave a digital footprint | connect the dots | follow a lead | a ticking time bomb | a smoking gun

1. The company failed to update its old server for several years. It was basically _____.
2. The unusual login from another country _____ and the security team immediately investigated it.
3. Cybersecurity professionals must constantly learn about new technologies if they want to _____ of cybercriminals.
4. The suspect deleted the files and used several anonymous accounts to _____.
5. Investigators discovered an email that directly connected the suspect to the attack. It was _____.
6. Employees who use weak passwords can become _____ in an organisation's security system.
7. The police decided to _____ after receiving information about a suspicious online account.
8. Investigators analysed the messages, payment records and IP addresses and eventually managed to _____.
9. Poor access controls can _____ unauthorised users.
10. Even when people delete their social media posts, they may still _____.

11. The investigation team is working to _____ the data breach and identify its source.
12. Please _____ about any new developments in the investigation.

Exercise 10. Choose **five expressions** from **exercise 9** and write your own sentences. At least:

- **two** sentences should be about cybersecurity;
- **one** should be about a police investigation;
- **one** should be about an everyday situation;
- **one** can be about any topi

UNIT 3. HISTORY OF CYBERCRIME AND NEW THREATS.

Over the past decade, cybercrime has become a big business — a $1.5T industry with an entire ecosystem of criminal organizations run like legitimate organizations**.**

The average cost of a data breach is now $4.45 million. 82% of breaches involve the cloud. Cybercriminals are frequently targeting healthcare, which is now the top attacked industry.

Ransomware made up 24% of attacks in 2023 and is constantly growing.

Yet, while the cybercrime industry has exploded in the past ten years, the truth is that cybercrime is not a new kind of threat.

Here are some of the “historic” cyber-attacks.

1. The Citibank Hack (1994) – *The First Online Bank Robbery*

- **The Culprit**: **Vladimir Levin**, a Russian computer programmer working from his apartment in St. Petersburg.
- **The Attack**: Levin bypassed Citibank's telecommunications network to steal corporate security codes.
- **The Impact**: He transferred over **$10 million** from corporate customers into various international bank accounts before being caught by the FBI. It showed the world that banks were no longer safe from remote criminals.

2. The NASA and Pentagon Breach (1999) – *The Teenage Infiltrator*

- **The Culprit**: **Jonathan James** (known by his online alias "c0mrade"), a 15-year-old American boy.
- **The Attack**: James hacked into the networks of the **U.S. Department of Defense** and **NASA**. He installed a hidden "backdoor" into a Pentagon weapons server to intercept sensitive emails.
- **The Impact**: He downloaded software worth $1.7 million, forcing NASA to shut down its entire computer network for 21 days. He became the first juvenile to be jailed for a cybercrime in the US.

3. The "ILOVEYOU" Worm (2000) – *The Heartbreaker Virus*

- **The Culprit**: Two young computer programmers from the Philippines.
- **The Attack**: They created a script that spread via email with the subject line "ILOVEYOU" and an attachment named LOVE-LETTER-FOR-YOU.TXT.vbs.

When clicked, it deleted random files and sent itself to every contact in the user's address book.

- **The Impact**: It infected roughly **10% of all internet-connected computers** in the world, including systems at the UK Parliament and the Pentagon. It caused an estimated **$10 billion** in global damage. Ironically, the creators could not be charged with a crime because the Philippines had no laws against cybercrime at the time.

4. Project Rivolta / MafiaBoy (2000) – *The Internet Shutdown*

- **The Culprit**: **Michael Calce** ("MafiaBoy"), a 15-year-old Canadian high school student.
- **The Attack**: He launched a series of massive Distributed Denial of Service (**DDoS**) attacks.
- **The Impact**: He managed to crash the world's biggest websites at the time, including **Yahoo!, Amazon, eBay, CNN, and Dell**. The attack caused about **$1.2 billion** in economic damage and proved how vulnerable the global e-commerce infrastructure was.

5. Operation Aurora (2009) – *State-Sponsored Corporate Espionage*

- **The Culprit**: Highly sophisticated hackers originating from China.
- **The Attack**: A targeted cyber attack directed at more than 30 major tech companies, using zero-day vulnerabilities in Internet Explorer.
- **The Impact**: **Google** publicly announced that its corporate infrastructure had been breached and its intellectual property stolen. This marked a major historical shift where cybercrime moved from rogue teenagers to highly organized, state-sponsored political espionage.

6. Stuxnet (2010) – *Malware Destroys Physical Machinery*

- **The Culprit**: Widely believed to be a joint cyber weapon developed by the **United States and Israel**.
- **The Attack**: A highly complex computer worm designed to target industrial control systems (SCADA) via USB drives.
- **The Impact**: It specifically targeted Iran's nuclear facility at Natanz, forcing the centrifuges to spin out of control and physically self-destruct. It is famous for being the **first malware in history to cause physical damage** to real-world infrastructure.

It's clear that cybercrime has evolved rapidly, and while advances in cybersecurity continue to happen, it's a constant battle between overworked, understaffed security departments and threat actors".

Russia's cyberwar against Ukraine

Since 2014, and especially after the full-scale invasion in 2022, cyberattacks have become an important part of Russia's military strategy against Ukraine. Unlike traditional attacks that target physical infrastructure, cyberattacks aim to disrupt communication, damage critical systems, steal sensitive information, and create fear among the population.

On **24 February 2022**, just before the start of Russia's full-scale invasion of Ukraine, a major cyberattack targeted the **KA-SAT satellite communications network**, which was operated by Viasat. The attack disrupted satellite internet services

used by Ukrainian government agencies, military units, emergency services, and businesses. It also affected thousands of users in several European countries.

Russian state-sponsored hacker groups have targeted Ukrainian government institutions, banks, energy companies, telecommunications providers, and transportation systems. Their methods include phishing campaigns, malware infections, distributed denial-of-service (DDoS) attacks, and destructive malware known as "wipers," which permanently erase data from infected computers.

The cyber conflict has also highlighted the importance of cyber hygiene. Regular software updates, strong passwords, multi-factor authentication, secure backups, and employee cybersecurity awareness help reduce the risk of successful attacks. Even simple security measures can prevent many cyber incidents.

The war has shown that cybersecurity is no longer only a technical issue—it is a matter of national security. Future cybersecurity professionals play a crucial role in protecting critical infrastructure, defending digital assets, investigating cyber incidents, and ensuring that essential services remain operational during crises.

Exercise 1. Choose the correct answer.

1. **What motivated the earliest hackers of the 1970s and 1980s?**

A) Making money through ransomware
B) Intellectual curiosity and fame
C) State-sponsored corporate espionage
D) Stealing credit card information

2. **Why did the creators of the 1986 "Brain" virus write the software?**

A) To steal millions from international banks
B) To shut down NASA's computer network
C) To protect their own medical software from piracy
D) To launch a Distributed Denial of Service (DDoS) attack

3. **What made Vladimir Levin's 1994 attack on Citibank historically significant?**

A) It used cryptocurrency for the first time.
B) It was considered the first remote online bank robbery.
C) It destroyed physical machinery in the bank.
D) It was executed by a 15-year-old school student.

4. **Which cybercriminal was the first juvenile (minor) to be jailed for a cybercrime in the US?**

A) Michael Calce ("MafiaBoy")
B) Vladimir Levin
C) Jonathan James ("c0mrade")
D) The creators of the "Brain" virus

5. **Why were the creators of the devastating "ILOVEYOU" worm (2000) unable to be charged with a crime?**
A) They were never identified by the authorities.
B) The Philippines did not have cybercrime laws at the time.
C) They were protected by state-sponsored organizations.
D) The virus did not cause any real financial damage.
6. **What did "Project Rivolta" (MafiaBoy) prove to the global business community?**
A) Email attachments are always unsafe.
B) E-commerce infrastructure was highly vulnerable to DDoS attacks.
C) Banks could easily be hacked from a home apartment.
D) Nuclear facilities could be shut down remotely.

7. **How did the Stuxnet worm (2010) differ from all previous malware?**
A) It spread exclusively through Microsoft Word documents.
B) It was written by two teenagers from Pakistan.
C) It was the first malware to cause physical damage to real-world infrastructure.
D) It demanded a ransom payment in Bitcoin to unlock corporate files.

Exercise 2: State whether the following statements are True (T) or False (F) based on the texts.
1. **[ ]** In the 1970s, "phreakers" manipulated telephone networks to avoid paying for long-distance calls.
2. **[ ]** The Melissa virus of 1999 primarily spread by infecting physical USB drives.
3. **[ ]** A botnet refers to a single, highly powerful supercomputer used by the military to launch cyberwarfare.
4. **[ ]** Operation Aurora (2009) represented a shift in cybercrime from rogue individuals to state-sponsored corporate espionage.
5. **[ ]** Modern ransomware attacks only target private citizens and rarely affect public institutions like hospitals or schools.

Exercise 3. Put the following historical milestones in order from oldest (1) to most recent (5).
- **[ ]** The rise of cryptocurrency-fueled ransomware targeting cities and hospitals.
- **[ ]** The creation of the "Brain" virus to prevent software piracy.
- **[ ]** High schooler "MafiaBoy" crashes major e-commerce websites like Amazon and eBay.
- **[ ]** Telephone "phreakers" hacking long-distance phone lines.
- **[ ]** The Stuxnet worm physically destroying centrifuges in a nuclear facility.

Exercise 4: Answer the questions using your own words in complete sentences.
1. Explain how the shift to the **"Age of Monetization"** in the 2000s changed the structure and organization of cybercriminal groups.

2. Compare the actions of Jonathan James (NASA/Pentagon breach) with Operation Aurora. How do their targets and motivations show the evolution of cybercrime?

Task 5. **A**nswer the questions in complete sentences.

1. When did the cyberattack take place?
2. Which company operated the KA-SAT satellite network?
3. Who were the main users affected by the attack in Ukraine?
4. How did the attack affect people outside Ukraine?
5. Why was disrupting satellite communications significant at that time?

Task 6. Imagine you are a cybersecurity analyst asked to explain the incident to an international audience.

Write **150–200 words** answering the following questions:

- Why are satellite communication systems important for governments and emergency services?
- What challenges can a cyberattack on critical infrastructure create during a conflict?
- What lessons can governments and companies learn from the KA-SAT cyberattack to improve cybersecurity in the future?

Grammar focus: Degrees of Comparison of Adjectives

There are 3 **degrees of comparison** of adjectives:

1. Positive degree

The **positive degree** describes one person or thing without comparing it.

- Cybercrime is **dangerous**.

2. Comparative degree

We use the **comparative** to compare **two** people, things or situations.

Short adjectives

Add **-er + than**.

Adjective	Comparative
fast	faster
small	smaller
safe	safer

- Modern computers are **faster than** early computers.
- A strong password is **safer than** a simple password.

Adjectives ending in -y

Change **-y** → **-i** and add **-er**.

- risky → **riskier**
- likely → **likelier**

Modern cyberattacks are **more sophisticated and riskier than** attacks in the past.

Longer adjectives

Use **more + adjective + than**.

- sophisticated → **more sophisticated**
- effective → **more effective**
- complicated → **more complicated**

Ransomware attacks are becoming **more sophisticated than** they were in the past.

3. Superlative degree

We use the **superlative** to compare **three or more** people or things.

Short adjectives

Use **the + adjective-est**.

- fast → **the fastest**
- safe → **the safest**

Encryption is one of **the safest** ways to protect sensitive information.

Adjectives ending in -y

Change **-y** → **-i** and add **-est**.

- easy → **the easiest**
- likely → **the likeliest**

Phishing is one of **the riskiest** forms of social engineering.

Longer adjectives

Use **the most + adjective**.

- dangerous → **the most dangerous**
- sophisticated → **the most sophisticated**
- complex → **the most complex**

AI-powered attacks may become **the most sophisticated** cyber threats in the future.

4. Irregular comparison

Some common adjectives have irregular comparative and superlative forms.

Positive	Comparative	Superlative
good	better	the best
bad	worse	the worst
far	farther/further	the farthest/furthest
little	less	the least
much/many	more	the most

- This was **the worst** cyberattack the company had experienced.
- Criminals now have **more** sophisticated tools.
- This solution requires **the least** technical knowledge.

Exercise 1. Complete the sentences

Use the correct comparative or superlative form of the adjective in brackets.

1. Modern cyberattacks are _____ than attacks carried out twenty years ago. (sophisticated)
2. Phishing is one of _____ methods used by cybercriminals. (common)
3. Strong passwords are _____ than simple passwords. (secure)
4. Ransomware can be _____ than ordinary malware. (dangerous)
5. Artificial intelligence is becoming _____ in detecting suspicious activity. (effective)

6. This was _____ cyberattack the company had experienced. (serious)
7. Older operating systems are often _____ than modern ones. (vulnerable)
8. Cybercriminals are becoming _____ at hiding their activities. (good)
9. The _____ a network is, the harder it is for attackers to penetrate it. (secure)
10. Social engineering can be _____ to detect than a technical attack. (difficult)
11. This type of attack requires _____ technical knowledge than a zero-day exploit. (little)
12. Of all the threats discussed in the article, ransomware is _____. (dangerous)

Exercise 2. Find and correct the mistakes

Each sentence contains **one mistake** involving the comparison of adjectives. Rewrite the sentences correctly.

1. Cybercrime is becoming more dangerouser every year.
2. Phishing is one of the more common cyber threats.
3. Modern malware is much sophisticated than older malware.
4. This attack was the most serious than the previous one.
5. A strong password is more safer than a short password.
6. AI-powered attacks may be the dangerousest threats in the future.
7. Older systems are not as secure than modern systems.
8. The more connected a device becomes, the vulnerable it may be.
9. Ransomware is one of the most dangerousest forms of malware.
10. Cybercriminals now have more better tools than they had in the past.

Exercise 3. Complete the text

Complete the text with the correct form of the adjectives in brackets.

The Changing Face of Cybercrime

Cybercrime has become one of _____ (serious) problems of the digital age. In the past, many attacks were relatively simple, but modern attacks are much _____ (complex) and _____ (difficult) to detect.

One of _____ (significant) changes has been the development of ransomware. Modern ransomware is _____ (dangerous) than many early forms of malware because it can encrypt large amounts of data in a very short time.

Artificial intelligence is also changing cybercrime. Criminals can use AI to create _____ (convincing) phishing messages and _____ (realistic) fake images and voices. As a result, it is becoming _____ (hard) for ordinary users to recognise fraudulent content.

At the same time, cybersecurity technologies are becoming _____ (advanced). AI-powered security systems can analyse _____ (much) data and identify suspicious behaviour _____ (quickly) than traditional systems.

Experts believe that the _____ (effective) approach to cybersecurity will combine advanced technology with human knowledge. The _____ (aware) users are of cyber threats, the _____ (difficult) it will be for criminals to deceive them.

UNIT 4. GLOBAL CYBERPOLICE

Glossary

ally	**A country or organisation that works together with another.**
approach	**A method of dealing with a problem.**
asymmetric threats	**Threats where attackers have different advantages than defenders.**
attribution	**Identifying who is responsible for a cyberattack.**
authority	**The legal power to take action.**
battle-tested	**Proven to work in difficult situations.**
borderless	**Not limited by national borders.**
coordinate	**To organise people or activities to work together.**
critical infrastructure	**Essential systems such as energy, transport, and communications.**
cyberattack	**An attempt to damage or access computer systems illegally.**
data breach	**Unauthorised access to confidential information.**
decentralized	**Managed by several organisations rather than one central authority.**
digital forensics	**Investigating digital devices to collect evidence.**
dismantle	**To destroy or break up an illegal organisation.**
encrypted	**Protected by code so only authorised users can read it.**
hybrid warfare	**A conflict using military, cyber, and information attacks.**
identity theft	**Stealing another person's personal information.**
jurisdiction	**The legal authority to enforce laws in a certain area.**
leverage (v.)	**To use something effectively to gain an advantage.**
malware	**Harmful software designed to damage systems or steal data.**
ransomware	**Malware that blocks access to files until money is paid.**
resilient	**Able to recover quickly after difficulties.**
state-sponsored	**Supported or directed by a government.**
syndicate	**An organised criminal group.**
threat intelligence	**Information about cyber threats used to prevent attacks.**
wiper malware	**Malware that permanently deletes data.**

Abbreviations

FBI **Federal Bureau of Investigation (USA)**

CISA	**Cybersecurity and Infrastructure Security Agency (USA)**
NCA	**National Crime Agency (UK)**
NCCU	**National Cyber Crime Unit (UK)**
NCSC	**National Cyber Security Centre (UK)**
EC3	**European Cybercrime Centre (Europol)**
SSSCIP	**State Service of Special Communications and Information Protection of Ukraine**
SBU	**Security Service of Ukraine**
GRU	**Russian Military Intelligence Agency**

Global Cyberpolice: Protectors of the Digital Frontier

As we noted earlier, the rise of global internet networks has created a new type of borderless criminal. Today, cyberattackers target banks, critical infrastructure, and private citizens from anywhere in the world. To fight these asymmetric threats, nations have established specialized cyberpolice units. While these organizations share the same ultimate goal of securing the digital realm, their operational structures, methods, and strategic focuses vary significantly across regions like the United States, Great Britain, Europe, and Ukraine.

In the United States, cybercrime enforcement relies on a decentralized, federal approach split among several major agencies. **The Federal Bureau of Investigation (FBI)** serves as the lead agency for investigating domestic cyberattacks, ransomware, and high-profile data breaches, operating dedicated **Cyber Task Forces** in all 56 of its field offices. Alongside the FBI, the **Cybersecurity and Infrastructure Security Agency (CISA**) works as the nation's primary defensive mechanism, protecting government networks and private industry utilities. This American model heavily leverages public-private partnerships, encouraging commercial tech giants to proactively share real-time threat intelligence with law enforcement.

Across the Atlantic, Great Britain utilizes a highly centralized model to coordinate national defense and unmask sophisticated state-sponsored threats. **The National Cyber Crime Unit (NCCU)**, a branch of **the National Crime Agency (NCA),** leads the UK's response to major cyber incidents. The NCCU works in close tandem with **the National Cyber Security Centre (NCSC)** to provide immediate support to victims. Crucially, the NCSC has been instrumental in exposing global cyberterrorism. By combining technical forensic evidence with international threat intelligence, the NCSC successfully unmasked Russian military intelligence units (such as the GRU) for deploying destructive wiper malware against Ukrainian infrastructure. Alongside high-stakes attribution, British authorities focus heavily on prevention through "Cyber Choices" programs, which redirect talented young coders away from illegal activities and into legitimate cybersecurity careers.

On the continental mainland, the European Union recognizes that because Europe consists of many independent nations, cross-border cooperation is essential. To bridge these borders, Europol hosts **the European Cybercrime Centre (EC3**) in The Hague. EC3 does not possess the legal authority to arrest criminals directly. Instead, it serves

as a centralized intelligence data hub, providing advanced digital forensics, specialized tools, and operational support to the police forces of individual EU member states. When a ransomware syndicate strikes targets across multiple European countries simultaneously, EC3 coordinates the joint international operations necessary to dismantle their infrastructure.

This global network of cooperation becomes a vital lifeline for countries operating on the digital frontlines, most notably Ukraine. **The Cyberpolice Department of the National Police** of Ukraine operates in a unique, high-intensity environment. Facing persistent, advanced hybrid warfare, Ukrainian cyberpolice have evolved into a highly resilient, battle-tested force. While they continuously investigate domestic financial fraud and identity theft, their primary mission involves working alongside the State Service of Special Communications and Information Protection (SSSCIP) and the **Security Service of Ukraine (SBU)**. Together with international allies like the British NCSC, they counter state-sponsored cyberwarfare and defend critical national infrastructure from hostile digital sabotage.

Ultimately, cyberpolice forces worldwide face identical systemic challenges, including encrypted communications, anonymous cryptocurrency transactions, and strict jurisdictional limits. Because modern hackers respect no physical borders, the future of global digital security relies entirely on international treaties, instantaneous data sharing, and unified joint operations.

Exercise 1. Choose the correct answer:

1. **Which agency leads the investigation of high-profile data breaches and ransomware inside the United States?**

A) CISA
B) FBI
C) NCSC
D) Europol

2. **What is unique about Great Britain's "Cyber Choices" program?**

A) It helps businesses buy defensive software.
B) It forces hackers to go to prison immediately.
C) It redirects talented young coders into legal cybersecurity careers.
D) It allows the government to read encrypted messages.

3. **What is the primary operational limitation of Europe's EC3 agency?**

A) It cannot share data with other countries.
B) It does not have the legal authority to arrest criminals directly.
C) It only investigates financial fraud.
D) It is not allowed to use digital forensics tools.

4. **According to the text, which organization provided vital forensic evidence to hep Ukraine expose Russian state-sponsored cyberterrorism?**

A) The European Cybercrime Centre (EC3)
B) The Federal Bureau of Investigation (FBI)
C) The British National Cyber Security Centre (NCSC)
D) Commercial tech giants

5. **Why have the Ukrainian cyberpolice evolved into a highly resilient, battle-tested force?**
A) They have the largest budget in the world.
B) They constantly face advanced, state-sponsored hybrid warfare threats.
C) They focus exclusively on cryptocurrency transactions.
D) They operate without any domestic legal restrictions.

Exercise 2. True or False (Write T or F)
6. _____ The U.S. model of cybersecurity relies heavily on cooperation between government agencies and private tech companies.
7. _____ The British NCSC unmasked Russian military intelligence (GRU) for deploying ransomware to steal money from Ukrainian citizens.
8. _____ Europol's EC3 serves as a centralized intelligence data hub for European Union member states.
9. _____ Modern cybercriminals are easy to arrest because they always respect geographic and jurisdictional borders.

Exercise 3. Complete the sentences
Word Bank: **Attribution | Wiper malware | Critical infrastructure | Jurisdiction | Data breach**
1. The hospital could not access patient files because the hackers deployed destructive _____ to permanently erase the servers.
2. Power grids, water plants, and public transportation networks are all examples of a nation's _____.
3. Determining exactly which nation or group launched a cyberattack is a difficult process known as _____.
4. A local police officer cannot arrest a cybercriminal living across the world because the criminal is outside of their legal _____.
5. The credit card company suffered a massive _____, exposing millions of customer passwords.

Exercise 4. Answer the questions using your own words in complete sentences.
1. How does the technical assistance from organizations like the UK's NCSC help a country like Ukraine prove that a cyberattack was an act of state-sponsored terrorism rather than an independent hacker group?
2. Which country's model of cyber policing (decentralized like the US, centralized like the UK, or cooperative like the EU) do you think is the most effective against modern threats?
3. Should tech companies be legally forced to give cyberpolice access to encrypted user data to help solve global crimes, or does this violate citizen privacy?
4. How can law enforcement agencies better incentivize young IT specialists to choose defensive cybersecurity over lucrative illegal hacking?

Grammar focus. Comparison of adjectives structures:

Comparison with as ... as

We use **as + adjective + as** to say that two things are equal.

A tablet can be **as vulnerable as** a computer if it is not protected.

For a negative comparison, use **not as ... as**.

Older systems are **not as secure as** modern systems.

Less ... than and the least ...

We can use **less + adjective + than** to show a lower degree.

This type of malware is **less dangerous than** ransomware.

The least + adjective shows the lowest degree among three or more things.

Of these three threats, this one is **the least serious**.

Intensifiers with comparatives and superlatives

We can make comparisons stronger with:

much, far, considerably, significantly, a lot + comparative

- Cyberattacks are **much more sophisticated** today.
- Modern malware is **far more difficult** to detect.
- AI can make attacks **significantly more dangerous**.

We can use:

by far + superlative

- Ransomware is **by far the most serious** threat to this organisation.

one of + the + superlative + plural noun

Phishing is one of **the most common cybercrime techniques**.

comparative + and + comparative

This shows that something is continuously changing.

Cyberattacks are becoming **more frequent and more sophisticated**.

the + comparative ..., the + comparative ...

The more connected devices become, **the more vulnerable** networks may become.

Exercise 5. Complete each sentence with the correct structure: **as ... as, not as ... as, less ... than, the least, much/far/considerably/significantly/a lot + comparative**, or **by far + superlative**.

4. A well-trained employee can be _____ important _____ advanced security software.
5. Traditional passwords are _____ secure _____ multi-factor authentication.
6. My new laptop is _____ fast _____ my old one.
7. Travelling by train is often _____ expensive _____ travelling by plane.
8. This exercise is _____ difficult _____ the previous one.
9. Of all the restaurants in this area, this one is _____ expensive.
10. Winter days are usually _____ short _____ summer days.
11. Online shopping has become _____ more popular in recent years.
12. My new flat is _____ more comfortable than my previous one.

Exercise 6. **Rewrite each sentence using the word or structure in brackets. Do not change the meaning.**

Task 6. Complete the cybersecurity discussion

Officer A: Which cyber threat do you think is the biggest problem for organisations today?

Officer B: Ransomware is probably **(1)** _____ (by far / serious) threats. It can cause **(2)** _____ (much / financial) damage than many other attacks.

Officer A: I agree. But phishing is **(3)** _____ (common) ransomware, isn't it?

Officer B: Yes. In fact, phishing is one of **(4)** _____ (common / cybercrime techniques). It is often **(5)** _____ (less / technically complex) a direct attack on a computer system.

Officer A: But it can be **(6)** _____ (just / dangerous) a technical attack if employees reveal sensitive information.

Officer B: Exactly. And AI is making the situation **(7)** _____ (far / difficult) for users. AI-generated messages are becoming **(8)** _____ (convincing and convincing).

Officer A: So, **(9)** _____ (more / sophisticated) AI becomes, **(10)** _____ (difficult) it may be to identify fake content.

Officer B: That's right. At the same time, cybersecurity tools are becoming **(11)** _____ (advanced and advanced). The best solution is probably to combine technology with well-trained employees.

UNIT 5. CYBER POLICE IN UKRAINE. COOPERATION WITH GLOBAL CYBER POLICE

Discuss the questions.

1. Why do countries need special cyber police units?
2. Can cybercrime be stopped by one country alone? Why or why not?
3. What international organizations help fight cybercrime?

Glossary

Exercise 1. Match the terms with their definitions.

Term	Definition
1. Cyber Police	a. illegal activities carried out using computers or the Internet
2. Cybercrime	b. a request for assistance between law enforcement agencies
3. Digital evidence	c. electronic information used during an investigation
4. Investigation	d. cooperation between countries to solve crimes
5. Malware	e. harmful software used to attack computer systems
6. International cooperation	f. the process of collecting information about a crime

Term	Definition
7. Law enforcement	g. government agencies responsible for enforcing laws
8. Cybersecurity awareness	h. knowledge of online threats and safe behaviour
9. Incident response	i. actions taken after a cyberattack
10. Mutual legal assistance	j. a police unit specializing in cybercrime

Cyber Police in Ukraine and International Cooperation

As technology becomes more advanced, cybercrime is becoming a serious challenge for every country. Criminals use computers and the Internet to steal money, spread malware, attack computer systems, and commit online fraud. Because cybercriminals often operate across national borders, countries need specialized law enforcement units that can investigate these crimes. In Ukraine, this role is performed by the **Cyber Police**.

The Cyber Police of Ukraine is a specialized unit of the National Police. Its main mission is to prevent, detect, investigate, and combat cybercrime. Cyber police officers investigate crimes such as hacking, identity theft, online fraud, phishing attacks, ransomware infections, illegal online trading, and the distribution of malicious software. They also help collect digital evidence that can be used in court.

Besides investigating cybercrime, the Cyber Police work to increase cybersecurity awareness. They organize educational campaigns, publish online safety recommendations, and encourage people to report suspicious online activity. By teaching citizens how to recognize cyber threats, the Cyber Police help prevent many attacks before they happen.

Cybercrime is rarely limited to one country. A phishing campaign may begin in one country, use servers in another, and target victims around the world. For this reason, international cooperation is essential. Ukraine works with many international organizations and foreign law enforcement agencies to exchange information, identify cybercriminals, and coordinate investigations.

One of the most important international partners is INTERPOL, which helps police agencies in many countries share intelligence about cybercrime. Another important organization is Europol, which supports European law enforcement agencies in combating organized cybercrime. Ukraine also cooperates with international cybersecurity experts, computer emergency response teams (CERTs), and private technology companies.

International cooperation includes exchanging digital evidence, conducting joint investigations, identifying criminal networks, and providing mutual legal assistance. Since cybercriminals can quickly move data across borders, timely information sharing is essential for successful investigations.

The fight against cybercrime requires not only modern technology but also skilled professionals and responsible Internet users. Cyber police officers, international organizations, businesses, and ordinary citizens all play an important role in creating a safer digital environment. Strong cooperation between countries makes it more

difficult for cybercriminals to hide and helps protect people, organizations, and critical infrastructure from cyber threats.

Exercise 2. Reading Comprehension

Answer the questions.

1. Why has cybercrime become a global problem?
2. What is the main mission of the Cyber Police in Ukraine?
3. Name five cybercrimes investigated by the Cyber Police.
4. Why is digital evidence important?
5. How does the Cyber Police improve cybersecurity awareness?
6. Why is international cooperation necessary?
7. What role does INTERPOL play in fighting cybercrime?
8. What does Europol do?
9. What activities are included in international cooperation?
10. According to the text, who is responsible for improving cybersecurity?

Exercise 3. True or False

Write **T** (True) or **F**.

1. Cybercrime affects only one country at a time.
2. The Cyber Police investigate phishing attacks.
3. Digital evidence may be used in court.
4. Cyber Police only investigate crimes and do not educate the public.
5. INTERPOL supports international police cooperation.
6. Europol helps European countries combat cybercrime.
7. Information sharing is important during cybercrime investigations.
8. Ordinary Internet users also contribute to cybersecurity.

Exercise 4. Complete the Sentences

Use the words below.

investigate • awareness • evidence • phishing • cooperation • malware • cybercrime • law enforcement

1. The Cyber Police _____ online crimes.
2. _____ attacks often steal passwords.
3. Digital _____ is used during criminal investigations.
4. Educational campaigns improve cybersecurity _____.
5. Countries need international _____ to fight cybercrime.
6. _____ can damage computer systems.
7. Cyber Police are part of _____ agencies.
8. Modern _____ crosses national borders.

Exercise 5. Match the Halves

1. Cyber Police
2. INTERPOL
3. Europol

4. Digital evidence
5. International cooperation

a. supports police cooperation worldwide
b. investigates cybercrime
c. helps solve crimes across borders
d. is used in criminal investigations
e. supports European law enforcement agencies

Exercise 6. Multiple Choice

Choose the correct answer.

1. The Cyber Police are responsible for

a) repairing computers
b) investigating cybercrime
c) designing websites
d) selling software

2. Which organization supports police cooperation worldwide?

a) Microsoft
b) INTERPOL
c) Linux
d) Google

3. Digital evidence is

a) a computer virus
b) electronic information used in investigations
c) antivirus software
d) a firewall

4. Cyber Police improve cybersecurity by

a) publishing safety recommendations
b) creating malware
c) disabling networks
d) selling hardware

5. International cooperation helps

a) hide cybercriminals
b) identify criminal networks
c) reduce Internet speed
d) replace operating systems

Exercise 7. Translate into English. Translate the following phrases into English using the vocabulary from the text.

1. кібербезпека
2. кіберполіція
3. інформаційна безпека
4. правоохоронна діяльність
5. цифрові технології
6. розслідування кіберзлочинів

7. практична підготовка
8. онлайн-шахрайство
9. інформаційні системи
10. національна безпека

Exercise 8. Case Study
A Ukrainian company becomes the victim of a ransomware attack. The attackers demand payment in cryptocurrency. Investigators discover that the malicious software was sent from servers in another country, and the money was transferred through several international accounts.
Answer the questions.
1. Why is this an international cybercrime case?
2. Which Ukrainian organization would investigate the attack?
3. Why would international cooperation be necessary?
4. Which organizations could assist in the investigation?
5. What digital evidence should investigators collect?

Exercise 9. Discussion
Discuss the questions.
1. Why is cybercrime difficult to investigate?
2. Should countries always cooperate in cybercrime investigations?
3. What qualities should a cyber police officer have?
4. How can universities help improve cybersecurity awareness?

Grammar focus. Articles with abbreviations and proper nouns.

1. Articles with abbreviations
An abbreviation can be pronounced in two main ways:
- as a **word**: NATO, UNESCO, NASA
- as individual **letters**: FBI, EU, UK, BBC, AI, VPN

The choice of article depends on **how the abbreviation is used**, not simply on how it is written.
A. Abbreviations pronounced as individual letters
Use **the** when referring to organisations, institutions, or groups whose names normally require **the**.
- **the FBI** – the Federal Bureau of Investigation
- **the BBC** – the British Broadcasting Corporation
- **the EU** – the European Union
- **the UN** – the United Nations
- **the UK** – the United Kingdom
- **the USA** – the United States of America

The FBI investigates serious cybercrime in the United States.
The UK is a member of several international cybersecurity organisations.
However, some abbreviations do **not** normally take an article:
- NATO

- NASA
- UNESCO
- Microsoft
- IBM
- Google
- AI
- IT
- GPS
- Wi-Fi
- VPN

NATO has developed cybersecurity initiatives.
AI is increasingly used to detect cyber threats.
GPS can be vulnerable to interference.

B. When an abbreviation is used as a countable noun
Use **a/an** when an abbreviation refers to **one example, device, system, qualification, etc.**
Use **a** before a consonant sound and **an** before a vowel sound.

- **a VPN** /viː piː enˌ/
- **a USB device** /juː es biː/
- **a URL** /juː ɑː el/
- **an AI system** /eɪ aɪ/
- **an FBI agent** /ef biː aɪ/
- **an HTML document** /eɪtʃ tiː em el/

The company uses **a VPN** to protect remote workers.
She is **an FBI agent**.
The researchers developed **an AI system** for detecting fraud.

Remember
The article depends on the **sound**, not the first written letter:

- **a** USB device → /juː.../
- **a** URL → /juː.../
- **an** FBI officer → /ef.../
- **an** AI tool → /eɪ.../

EXERCISE 10. COMPLETE THE SENTENCES WITH **A, AN, THE, OR – (NO ARTICLE)**.

1. ___ FBI is investigating the cyberattack.
2. The company uses ___ VPN to protect its employees.
3. She works as ___ FBI investigator.
4. ___ NATO has developed new cybersecurity initiatives.
5. They developed ___ AI system for detecting suspicious activity.
6. ___ AI is becoming increasingly important in cybersecurity.
7. He sent ___ email containing a suspicious URL.
8. She opened ___ PDF file attached to the message.

9. ___ BBC reported the cyberattack yesterday.
10. The company uses ___ GPS to track its delivery vehicles.
11. He works for ___ EU cybersecurity agency.
12. They installed ___ USB device to transfer the data.
13. ___ UN promotes international cooperation against cybercrime.
14. She is ___ IT specialist.
15. ___ NASA uses advanced computer systems in its space missions.
16. The employee connected to the network through ___ VPN.
17. ___ FBI officer interviewed the suspect.
18. ___ UNESCO supports international educational and cultural programmes.

Exercise 11. Complete the text

Complete the text with **a, an, the, or – (no article)**.

INTERNATIONAL CYBERSECURITY COOPERATION

Cybercrime is an international problem, so countries need to cooperate. **(1) ___ United Nations** supports international efforts to improve cybersecurity. **(2) ___ NATO** also works on cyber defence and considers cyberspace an important security domain.

In **(3) ___ United Kingdom**, organisations such as **(4) ___ National Cyber Security Centre (NCSC)** provide advice about cyber threats. In **(5) ___ United States**, **(6) ___ FBI** investigates many types of cybercrime.

Technology companies also play an important role. **(7) ___ Microsoft**, for example, develops security tools and regularly publishes information about new threats. Modern organisations often use **(8) ___ VPN** when employees work remotely.

International police cooperation is also important. **(9) ___ Interpol** helps law-enforcement agencies exchange information and coordinate operations. **(10) ___ European Union** also supports cooperation between its member states.

UNIT 6. THE EVOLUTION OF COMPUTERS: FROM VACUUM TUBES TO QUANTUM SECURITY

The history of computing is a story of exponential growth, hardware minimization, and scaling connectivity. For cybersecurity professionals, studying this evolution is not just a history lesson; it is a roadmap of how modern vulnerabilities were born. As computer hardware transformed from massive mechanical gears into microscopic silicon transistors, the methods required to protect data changed forever.

In the 1940s and 1950s, the first generation of computers, such as the famous ENIAC, relied on thousands of fragile vacuum tubes to control electrical currents and used magnetic drums for memory. These giant machines filled entire rooms, possessed no operating systems, and required technicians to program them by physically rewiring cables and inputting paper punch cards. Because these early systems were completely offline and isolated, network security did not exist. Instead, physical security was the only true cybersecurity. Heavy mechanical locks, armed guards, and restricted room access were completely sufficient to protect digital data from unauthorized hands.

Between the 1950s and 1970s, this isolated reality shifted dramatically during the second and third generations of computing. The invention of the solid-state transistor replaced vacuum tubes, making computers smaller, faster, and more reliable. Soon after, engineers developed the Integrated Circuit (IC), which packed thousands of transistors onto a single silicon chip. This hardware revolution birthed powerful centralized mainframes like the IBM System/360. For the first time, computers utilized primitive operating systems that supported "timesharing," allowing multiple users to log into the same hardware simultaneously. As a direct result, software-based access controls became necessary. This era introduced the world to user passwords, restricted file permissions, and the very first experimental malware, such as the self-replicating "Creeper" program on the early ARPANET network.

The fourth generation, spanning from **the late 1970s** to the present day, arrived with the creation of the microprocessor,

Today, we stand on the doorstep of the fifth generation: the era of quantum computing. **Quantum computers** do not process data using traditional binary bits of 0s and 1s. Instead, they utilize quantum bits, or "qubits," which exist in a state of superposition. This allows them to perform complex calculations at speeds unimaginable with today's fastest silicon supercomputers. However, this technological leap poses an existential threat to modern cryptography. A powerful quantum computer could easily crack current RSA and ECC encryption algorithms, which protect global banking systems, government secrets, and everyday internet communications. Consequently, the modern evolution of hardware has triggered an urgent global race to develop "Post-Quantum Cryptography" (PQC) to protect digital infrastructure before quantum threats become operational.
https://www.vc3.com/blog/the-evolution-of-artificial-intelligence-in-cybersecurity

Exercise 1: Choose the correct answer:

1. **Why was physical security considered completely sufficient for first-generation computers?**

A) The machines were completely isolated from external networks.
B) The operating systems had built-in advanced firewalls.
C) The data was encrypted using post-quantum cryptography.
D) Vacuum tubes were naturally immune to electronic hacking.

2. **What technical milestone allowed multiple users to access a mainframe simultaneously?**

A) The invention of the punch card
B) Primitive operating systems and timesharing
C) The creation of the internet perimeter
D) Quantum superposition

3. **What destroyed the traditional cybersecurity perimeter during the fourth generation?**

A) The transition from magnetic drums to silicon
B) The replacement of transistors with vacuum tubes
C) Global internet connectivity and remote access

D) The introduction of simple user passwords

4. **How do quantum computers differ fundamentally from traditional microprocessors?**

A) They rely on physical cables and punch cards.
B) They are much larger than first-generation ENIAC computers.
C) They use qubits in a state of superposition instead of binary bits.
D) They do not require any operating systems to function.

5. **According to the text, what is the main threat quantum computing poses to current cybersecurity?**

A) It will make firewalls completely obsolete.
B) It can easily crack modern encryption algorithms like RSA.
C) It will cause physical hardware components to overheat.
D) It prevents commercial tech giants from sharing threat intelligence.

Task 2: Match the cybersecurity/computing term on the left with its correct definition on the right.

Integrated Circuit	___ __	**A.** Malicious code designed to wipe out or permanently erase server data.
Perimeter	___ __	**B.** A basic unit of quantum information that can exist in multiple states simultaneously.
Qubit	___ __	**C.** A small semiconductor chip packed with thousands of interconnected transistors.
Mainframe	___ __	**D.** The traditional boundary line that separates a safe internal network from the outside world.
Wiper Malware	___ __	**E.** A massive, powerful computer built to process vast amounts of data for many users at once.

Task 4 Case study. Can AI Think? – The Turing Test

Background.

In 1950, British mathematician and computer scientist Alan Turing proposed a simple way to evaluate machine intelligence. Instead of asking whether a machine can *think*, he suggested asking whether it can **convince a human that it is also human** during a conversation.

This became known as the **Turing Test**. In the test, a human judge communicates through text with two hidden participants: one human and one artificial intelligence (AI). If the judge cannot reliably identify which participant is the machine, the AI is said to have passed the test.

Today, advanced AI chatbots can hold long, natural conversations, answer questions, and even write stories or computer code. Some people believe modern AI systems are close to passing the Turing Test, while others argue that they only imitate human language and do not truly understand what they say.

Task A: Imagine that you are a member of a national cyberpolice unit evaluating a new AI chatbot before it is allowed to assist citizens online.
Your team conducts a Turing Test with the chatbot. During a 10-minute text conversation, the AI answers questions about travel, hobbies, current events, and emotions. Five judges participate in the test.

- Three judges believe they were talking to a human.
- Two judges correctly identify the chatbot as AI.
- The chatbot gives fluent and polite answers but invents several facts and provides incorrect legal advice.

Your team must decide whether the chatbot should be used to communicate with the public.
Discussion: Discuss the following questions with a partner:

- Does passing the Turing Test mean that AI is truly intelligent? Why or why not?
- Should AI be allowed to advise people on legal or police matters?
- What are the benefits of using AI in law enforcement?
- What risks should cyberpolice consider before using AI systems?

Grammar focus. Articles with proper nouns

Proper nouns are names of **people, places, countries, cities, organisations, companies, institutions, streets, languages, etc.**
We usually **do not use an article** with singular proper nouns.
People

- **Leonardo da Vinci**
- **William Shakespeare**
- **Albert Einstein**

However, there are several important exceptions.
Albert Einstein developed the theory of relativity.

Use	Example	Meaning
Person's name	**John Smith**	one person
Whole family	**the Smiths**	Smith family
Unknown person with surname	**a Mr Smith**	a man called Smith
Person similar to a famous person	**a Sherlock Holmes**	someone like Sherlock Holmes
Work by an artist	**a Picasso**	a Picasso painting
Famous person's work	**two Picassos**	two works by Picasso
Title + name	**Professor Smith**	no article
Title used alone	**the professor**	common noun
Name used metaphorically	**a real Einstein**	a very intelligent perso

Cities. We normally use **no article** with the names of cities.

- Kyiv

- London
- Paris

Most countries

Most country names do not take an article.

- Ukraine
- France
- Germany
- Poland
- Japan
- Canada

Ukraine has developed its cybersecurity capabilities.

Countries with the

Use **the** with:

- **the United Kingdom**
- **the United States**
- **the Netherlands**
- **the Philippines**
- **the Czech Republic**
- **the United Arab Emirates**

The United States has a large cybersecurity industry.

3. Geographical names

Rivers, seas, oceans and canals

Use **the**:

- the Dnipro
- the Thames
- the Danube
- the Black Sea
- the Mediterranean Sea
- the Atlantic Ocean
- the English Channel
- the Suez Canal

The Dnipro is one of the longest rivers in Europe.

Mountain ranges

Use **the** with mountain ranges:

- the Alps
- the Carpathians
- the Himalayas
- the Andes

The Ukrainian part of **the Carpathians** attracts many tourists.

But individual mountains normally have **no article**:

- Mount Everest
- Mount Snowdon

Mount Everest is the highest mountain in the world.

Deserts
Use **the**:
- the Sahara
- the Gobi
- the Arabian Desert

The Sahara is the largest hot desert in the world.

4. Universities, airports, stations and streets
Universities Some university names use **no article**:
- Oxford University
- Cambridge University
- Harvard University

She studied at **Oxford University**.
But names containing **University of ...** normally use **the**:
- the University of Oxford
- the University of Cambridge
- the University of Warsaw

He works at **the University of Warsaw**.
Airports
Many airport names use **no article**:
- Heathrow Airport
- London City Airport
- Warsaw Chopin Airport

They arrived at **Heathrow Airport**.
Streets and squares
Usually no article:
- Baker Street
- Oxford Street
- Trafalgar Square
- Independence Square

The embassy is on **Baker Street**.

Exercise 7. Exercise Articles with proper names
Complete the sentences with **a, an, the, or – (no article)**.
1. ___ Ukraine has developed new cybersecurity initiatives.
2. ___ United Kingdom has a national cybersecurity strategy.
3. ___ Kyiv is the capital of Ukraine.
4. ___ Dnipro is one of the longest rivers in Europe.
5. ___ Black Sea is an important geographical feature of the region.
6. ___ Carpathians attract many tourists every year.
7. ___ Mount Everest is the highest mountain in the world.
8. ___ United States is one of the world's largest economies.
9. ___ Poland shares a border with Ukraine.
10. ___ Netherlands is famous for its canals and cycling culture.

11. ___ London is one of the world's largest cities.
12. ___ Danube flows through several European countries.
13. She studied at ___ University of Cambridge.
14. He studied at ___ Cambridge University.
15. ___ Microsoft develops a wide range of cybersecurity products.
16. ___ European Union supports cooperation between its member states.
17. They travelled across ___ Atlantic Ocean by ship.
18. ___ Japan is famous for its advanced technology.

EXERCISE 8. ARTICLES WITH NAMES OF PEOPLE

Complete the sentences with **a, an, the, or – (no article)**.

1. ___ William Shakespeare is one of the most famous writers in English literature.
2. ___ Shakespeare wrote many famous plays.
3. The museum has ___ Picasso on display.
4. He thinks he is ___ Newton, but he is not particularly good at solving scientific problems.
5. ___ Smiths invited us to dinner last weekend.
6. ___ Smith called earlier and left a message for you.
7. ___ Mr Brown wants to speak to the manager.
8. ___ Professor Johnson gave a lecture on artificial intelligence.
9. ___ professor gave us some useful advice about the project.
10. ___ Queen Elizabeth II was one of the UK's longest-reigning monarchs.
11. ___ Queen visited the university last year.
12. The exhibition contains several works by ___ Leonardo da Vinci.
13. This painting is ___ Rembrandt.
14. She hopes to become ___ Marie Curie of the modern era.
15. ___ Beatles became one of the most influential bands in music history.
16. There was ___ Johnson among the candidates for the position.
17. She is sometimes described as ___ Agatha Christie of modern crime fiction.
18. ___ Agatha Christie wrote numerous detective novels.
19. ___ Inspector Brown interviewed the witness.
20. ___ inspector who interviewed the witness was very experienced.

UNIT 7. COMPUTER ARCHITECTURE AND I/O DEVICES

Glossary

architecture	The basic design and structure of a computer system.
volatile memory	Memory that loses its data when the power is turned off.
encrypt	To protect data by converting it into a secret code.
peripheral	A device connected to a computer, such as a keyboard or printer.
input device	A device used to enter data into a computer.
output device	A device that displays or produces information from a computer.

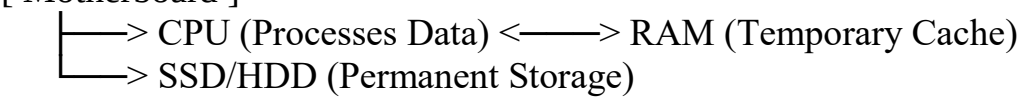
biometric scanner	A device that identifies a person using fingerprints, face, or other biological features.
firmware	Software permanently stored inside a hardware device.
keylogger	Hardware or software that secretly records keystrokes.
BadUSB	A cyberattack in which a USB device is reprogrammed to execute malicious commands.
supply-chain attack	An attack that targets hardware or software before it reaches the user.
vulnerability	A weakness that attackers can exploit.

Before securing a network, a cybersecurity professional must understand the physical machine. Every computer relies on a core architecture to process data, alongside specialized devices to interact with the outside world. For security experts, each hardware component and device represents a potential entry point for malicious actors.

What is Inside a Computer?

The internal components of a computer work together to execute instructions, store data, and manage system resources:

- **The Motherboard:** The main circuit board that acts as the computer's central nervous system. It connects and allows communication between all internal components.
- **The Central Processing Unit (CPU):** The "brain" of the computer. It executes program instructions and processes data. From a security standpoint, vulnerabilities in CPU design (like Spectre and Meltdown) can allow attackers to steal sensitive data directly from the processor's memory.
- **Random Access Memory (RAM):** Temporary, volatile memory. It holds data that the CPU actively uses. When the computer turns off, RAM clears. Cybercriminals often target RAM using "volatile memory analysis" to extract encryption keys before they vanish.
- **Storage Drives (HDD/SSD):** Permanent, non-volatile storage where the operating system, applications, and user files live. Hard Disk Drives (HDDs) use magnetic platters, while Solid State Drives (SSDs) use flash memory. Security teams encrypt these drives to prevent data theft if a physical device is stolen.



Input and Output (I/O) Devices

Computers require peripherals to interact with users and external networks. These are divided into input and output functions:

- **Input Devices:** Components that send data *into* the computer. Examples include keyboards, mice, microphones, webcams, and biometric scanners (fingerprint readers).
- **Output Devices:** Components that receive data *from* the computer to display or project it. Examples include monitors, printers, speakers, and headphones

The Cybersecurity Risks of Peripherals

In cybersecurity, input and output devices are highly vulnerable to physical and digital supply-chain attacks:

- **Keyloggers:** Malicious software or a physical USB hardware adapter attached between a keyboard and a computer. It secretly records every keystroke to steal passwords and credit card numbers.
- **BadUSB Attacks:** Attackers reprogram the firmware of innocent-looking USB flash drives. When plugged in, the computer recognizes the USB as an **input device** (like a keyboard) and automatically executes malicious terminal commands in seconds.
- **Hardware Sniffing:** Sophisticated spies can intercept electromagnetic or acoustic signals from monitors and printers to recreate the secret documents being printed or displayed.

Exercise 1: Vocabulary Matching Quiz

Match the hardware component with its correct function or security risk.

1. CPU	**A.** Volatile memory that holds active data; targeted for encryption keys.
2. RAM	**B.** The main circuit board connecting all internal computer parts.
3. Motherboard	**C.** An input exploit where a USB spoof-mimics a keyboard to run commands.
4. Keylogger	**D.** The processor or "brain" of the machine executing system tasks.
5. BadUSB	**E.** A spy tool or malware used to capture secret keystrokes and passwords.

Exercise 2: Categorization Challenge

Classify each device into the correct category: ***Input Device****,* ***Output Device****, or* ***Internal Component****.*

1. Biometric Fingerprint Scanner: _____
2. Solid State Drive (SSD): _____
3. Computer Monitor: _____
4. Network Printer: _____
5. Central Processing Unit (CPU): _____

Exercise 3. Read the statements and decide whether they are **True (T)** or **False (F).** Correct the false statements.

a) The motherboard stores all user files permanently.
b) RAM loses its contents when the computer is switched off.
c) SSDs use magnetic platters to store information.
d) Keyloggers can be hardware devices or software.
e) A BadUSB attack tricks a computer into recognising a USB drive as another device.
f) Cybersecurity professionals only need to protect software, not hardware.

Exercise 4. Complete the Sentences Choose the correct word from the box.

- **CPU • RAM • motherboard • SSD • keylogger • biometric scanner**

1. The _____ executes program instructions.
2. The _____ connects all internal computer components.
3. A _____ identifies users by their fingerprints.
4. A _____ secretly records everything a user types.
5. Files remain on an _____ even after the computer is turned off.
6. Programs currently in use are stored in _____.

Exercise 5. Answer the questions in one or two sentences.

1. Why is RAM called **volatile memory**?
2. What is the difference between an HDD and an SSD?
3. Why do organisations encrypt storage drives?
4. How can a BadUSB attack infect a computer?
5. Why are input devices considered a cybersecurity risk?

Grammar focus. The pronouns.

A **pronoun** is a word that replaces a noun or a noun phrase. Pronouns help us avoid repetition and make texts more natural and concise.

1. Personal pronouns

Personal pronouns refer to people, animals or things.

Subject	Object	Possessive adjective	Possessive pronoun
I	me	my	mine
you	you	your	yours
he	him	his	his
she	her	her	hers
it	it	its	–
we	us	our	ours
you	you	your	yours
they	them	their	theirs

Subject pronouns are normally used before a verb:
They detected a suspicious connection.
It contains sensitive information.
Object pronouns are used after verbs and prepositions:
The administrator contacted **them**.
The attacker sent the message to **him**.

2. Possessive pronouns and possessive adjectives

Possessive adjectives are followed by a noun:
This is **our** network.
The hacker stole **their** data.
Possessive pronouns replace the noun phrase:

This network is **ours**.
The data is **theirs**.
Compare:
This is **my password**.
This password is **mine**.
Do not use a noun after a possessive pronoun:
This password is **mine**. ✓
This password is **mine password**. ✗

3. Reflexive pronouns

Reflexive pronouns are:
myself, yourself, himself, herself, itself, ourselves, yourselves, themselves
They are used when the subject and object are the same person or thing:
The program automatically updates **itself**.
The students tested the application **themselves**.
They can also be used for emphasis:
The cybersecurity specialist **herself** analysed the incident.

4. Demonstrative pronouns

The main demonstrative pronouns are:

- **this** – one thing/person near the speaker
- **that** – one thing/person further away
- **these** – several things/persons near the speaker
- **those** – several things/persons further away

This is a secure server.
That is the old operating system.
These are the latest security updates.
Those were the original files.
They can also be used before nouns as demonstrative determiners:
This system is vulnerable.
Those devices are outdated.

5. Indefinite pronouns

Indefinite pronouns refer to people or things without identifying them specifically.
People

- **someone / somebody** – one unspecified person
- **anyone / anybody** – any person
- **no one / nobody** – not one person
- **everyone / everybody** – all people

Someone has accessed the account.
Nobody knows the original password.
Everyone must follow the security policy.
Things

- **something**
- **anything**
- **nothing**
- **everything**

There is **something** wrong with the network.
We couldn't find **anything** suspicious.
Everything is protected by encryption.
Indefinite pronouns referring to people are normally treated as **singular**:
Everyone **is** responsible for cybersecurity.
Somebody **has** changed the settings.
However, **they/their** are commonly used when the gender of the person is unknown or irrelevant:
Everyone should protect **their** account.

6. Interrogative pronouns

Interrogative pronouns are used to ask questions.

- **who** – people as the subject
- **whom** – people as the object, mainly in formal English
- **whose** – possession
- **which** – a choice from a limited number
- **what** – general information

Who detected the attack?
Whose account was compromised?
Which system was affected?
What caused the failure?
In everyday English, **who** is often used instead of **whom**:
Who did you contact?

7. Relative pronouns

Relative pronouns introduce relative clauses.

- **who** – people
- **which** – things and animals
- **that** – people or things in defining relative clauses
- **whose** – possession
- **whom** – people as an object in formal English

The analyst **who** investigated the incident found the problem.
The software **which** we installed is more secure.
The vulnerability **that** was discovered yesterday has been fixed.
The researcher **whose** work influenced the project is giving a presentation.
That is common in defining relative clauses:
The device **that** connects to the network is infected.

8. Reciprocal pronouns

Reciprocal pronouns express a mutual relationship between two or more people.

- **each other**
- **one another**

The security teams shared information with **each other**.
The systems communicate with **one another**.
In modern English, **each other** and **one another** are often interchangeable.

9. Distributive pronouns

The main distributive pronouns are **each** and **either/neither**.

Each refers to members of a group individually:
Each of the students has a security key.
Either means one of two:
Either of these methods can be used.
Neither means not one and not the other:
Neither of the passwords is secure.
After **each, either** and **neither**, the verb is normally singular:
Each of the devices **is** protected.
Neither of the servers **was** available.

10. Quantifying pronouns

Some pronouns express an indefinite quantity:

- **all**
- **both**
- **some**
- **any**
- **none**
- **many**
- **much**
- **few**
- **a few**
- **little**
- **a little**
- **several**

Many of the systems were affected.
Some of the data was corrupted.
None of the passwords was strong enough.
Both is used with two people or things:
Both of the servers are online.
All can refer to three or more people or things:
All of the devices have been updated.

Exercise 6. Personal pronouns

Choose the correct pronoun.

1. The security analyst examined the logs and then sent ___ to the administrator.

a) they
b) them
c) their
d) themselves

2. The server is offline because ___ has been attacked.

a) it
b) them
c) they
d) its

3. The police officers contacted the system administrator and asked ___ some questions.
a) he
b) his
c) him
d) himself
4. The students are studying cybersecurity because ___ want to work in the IT sector.
a) them
b) their
c) themselves
d) they
5. The company asked ___ to change our passwords.
a) we
b) us
c) our
d) ours

Exercise 7. Possessive forms
Choose the correct answer.
1. This is ___ new security policy.
a) our
b) ours
c) us
d) we
2. The laptop belongs to Sarah. It is ___.
a) her
b) hers
c) she
d) herself
3. These are ___ encrypted files.
a) they
b) them
c) their
d) theirs
4. This server belongs to our department. It is ___.
a) our
b) ours
c) us
d) we
5. The hacker tried to access ___ account.
a) he
b) him

c) his
d) himself
6. The company has changed ___ cybersecurity policy.
a) it
b) its
c) it's
d) itself

Exercise 8. Reflexive pronouns
Complete the sentences with the correct reflexive pronoun.
1. The program can update _____ automatically.
2. The students carried out the penetration test _____.
3. The administrator _____ discovered the vulnerability.
4. We should protect _____ from phishing attacks.
5. You should ask _____ whether the password is strong enough.
6. The hackers accidentally exposed _____ during the attack.

Exercise 9. Demonstrative pronouns
Choose **this, that, these** or **those**.
1. _____ is the new firewall configuration on my screen.
2. Look at _____ servers over there. They are very old.
3. _____ are the latest security updates.
4. Can you see _____ device at the other end of the room?
5. _____ is an example of a strong password.
6. _____ files on my computer are encrypted.

Exercise 10. Indefinite pronouns
Complete the sentences with:
someone, anyone, no one, everyone, something, anything, nothing, everything
1. _____ has changed the configuration of the server.
2. Is there _____ suspicious in the network traffic?
3. _____ in the organisation must follow the cybersecurity policy.
4. We searched the computer, but we found _____ unusual.
5. _____ knows who created the malware.
6. The system is working perfectly. _____ is under control.
7. The administrator heard _____ moving files during the night.
8. If _____ contacts you and asks for your password, do not give it to them.

Exercise 11. Interrogative pronouns
Choose the correct word.
1. _____ discovered the vulnerability?
a) Who
b) Which

c) Whose
d) What
2. _____ computer was infected?
a) Who
b) Whom
c) Whose
d) What
3. _____ caused the network failure?
a) Who
b) What
c) Whose
d) Which
4. _____ of these two security tools is more effective?
a) What
b) Who
c) Which
d) Whose
5. _____ did the administrator contact after the attack?
a) Whom
b) Whose
c) Which
d) What

Exercise 12. Relative pronouns
Complete the sentences with **who, which, that** or **whose**.
1. The analyst _____ investigated the attack works for the cyber police.
2. The malware _____ infected the computer has been removed.
3. The company _____ systems were attacked reported the incident.
4. This is the software _____ we use to monitor the network.
5. The engineer _____ designed the system is an expert in cybersecurity.
6. The vulnerability _____ was discovered last week has been fixed.
7. The researcher _____ discovered the vulnerability published a report.
8. The server _____ stores the data is protected by several security mechanisms.

Exercise 13. Reciprocal and distributive pronouns
Choose the correct answer.
1. The two security teams regularly communicate with ___.
a) each other
b) themselves
c) itself
d) one
2. The three departments support ___.
a) each

b) one another
c) themselves
d) either
3. ___ of the students has completed the cybersecurity test.
a) Each
b) Both
c) Several
d) Many
4. ___ of the two servers is available. Both are offline.
a) Either
b) Neither
c) Each
d) All
5. You can use ___ of these two authentication methods.
a) neither
b) either
c) both
d) all
6. The members of the team shared their findings with ___.
a) each other
b) themselves
c) either
d) neither

Exercise 14. Quantifying pronouns
Choose the correct answer.
1. ___ of the computers have been updated.
a) Both
b) Much
c) Little
d) Any
2. ___ of the information was useful.
a) Many
b) Few
c) Some
d) Several
3. ___ of the passwords were strong enough.
a) None
b) Much
c) Little
d) Every
4. There are ___ suspicious files on the server.
a) much
b) several

c) little
d) a little
5. ___ of the two systems can be used as a backup.
a) Both
b) All
c) Several
d) Many
6. We have very ___ time to investigate the incident.
a) few
b) little
c) many
d) several

Exercise 15. Mixed pronouns
Choose the correct answer.
1. The cybersecurity expert ___ discovered the attack immediately informed the police.
a) which
b) who
c) whose
d) whom
2. The company has introduced a new security policy. ___ requires all employees to use MFA.
a) They
b) It
c) Them
d) Its
3. ___ should be responsible for protecting their own account.
a) Everyone
b) Everything
c) Nothing
d) Someone
4. The two administrators checked the logs ___.
a) themselves
b) each other
c) one
d) either
5. The data belongs to the company. It is ___.
a) their
b) theirs
c) them
d) they
6. ___ of the two methods is suitable for this system?
a) Who

b) Whose
c) Which
d) What

7. The device ___ was connected to the network has been isolated.

a) who
b) whose
c) which
d) whom

8. The administrator changed the password ___.

a) himself
b) itself
c) themselves
d) each other

9. ___ of the students has received an individual access code.

a) Both
b) Each
c) Many
d) Several

10. The hacker sent the malicious file to ___.

a) we
b) our
c) us
d) ourselves

Exercise 16. Find and correct the mistakes

Each sentence contains **one mistake** involving a pronoun. Correct it.

1. The administrator checked the logs by him.
2. This files contain sensitive information.
3. Everyone should protect his or her account or their account from attack.
4. The company changed theirs security policy.
5. The two teams shared information with themselves.
6. The researcher which discovered the vulnerability published a report.
7. Neither of the servers are available.
8. Someone has left their password on the desk.
9. The students completed the task theirselves.
10. The laptop belongs to me, so it is my.

Exercise 17. Pronouns in cybersecurity texts

Complete the text with suitable pronouns.

Cybersecurity is everyone's responsibility. **(1)** _____ employee should understand the basic security rules and follow **(2)** _____ every day. If **(3)** _____ receives a suspicious email, they should report **(4)** _____ immediately. Employees should never give their passwords to **(5)** _____, even if the person claims to be a system administrator.

Organisations also need to protect **(6) _____** networks and data. **(7) _____** of the security systems should be regularly updated and tested. If a company discovers a vulnerability, **(8) _____** should fix it as soon as possible. Security teams must also cooperate with **(9) _____** because cyberattacks can affect several organisations at the same time.

Good cybersecurity requires cooperation. No organisation can protect **(10) _____** completely without the help of others.

Exercise 18. Rewrite the sentences

Rewrite the sentences using a suitable pronoun to avoid repetition.

1. The security team analysed the security team's report.
2. The company updated the company's software.
3. The students tested the system by the students.
4. The two administrators helped the two administrators during the investigation.
5. The researcher found a vulnerability. The vulnerability was critical.
6. All employees must protect all employees' accounts.
7. The server belongs to our department. The server is not operational.
8. The analyst contacted the analyst's manager after the incident.

Case Study: The Infected USB Drive

A large company receives promotional USB flash drives from a new supplier. An employee plugs one of the USB drives into an office computer to view the files. Within a few seconds, the computer begins executing unknown commands. Several user accounts are created without permission, security software is disabled, and confidential documents are copied to an external server.

A cybersecurity investigation reveals that the USB drive had been modified with **BadUSB firmware** before it was delivered to the company.

Task A. Identify the Attack. Answer the questions.

- What type of cyberattack was used?
- Which computer component was exploited?
- Why did the operating system trust the USB device?

Task B. Analyse the Incident. Complete the table.

Question	**Answer**
What was the main security mistake?	
What information was at risk?	
What were the consequences of the attack?	
Which hardware component allowed the attack?	

Task C. Recommend Security Measures

Work in pairs and suggest **at least four** ways to prevent similar attacks.

UNIT 8. THE QUANTUM LEAP: THE FUTURE OF QUANTUM COMPUTERS AND POST-QUANTUM CRYPTOGRAPHY

Quantum computers process data in fundamentally new ways compared to classical machines, utilizing bizarre phenomena from quantum physics. For cybersecurity students, understanding these mechanics is essential. They are the very tools that will soon empower devastating cyberattacks, while simultaneously providing the next generation of unbreakable digital defense.

Instead of classical bits that must represent an absolute zero (\(0\)) or one (\(1\)), quantum computers use **qubits** (quantum bits). To grasp how qubits achieve their massive processing power, we must look at two famous physics principles:

- **The Double-Slit Experiment:** When subatomic particles are fired through two slits at a screen, they behave like waves. They pass through *both* slits simultaneously and create an interference pattern. This wave-like ability to explore multiple paths at once is known as **superposition**. In computing, it allows a qubit to exist as a fluid combination of \(0\) and \(1\) at the same time.
- **Schrödinger's Cat Experiment:** This famous thought experiment envisions a cat locked in a box with a vial of poison, where the cat is considered both simultaneously alive and dead until the box is opened. Similarly, a qubit remains in a suspended state of superposition, holding millions of calculation outcomes at once. The system only "collapses" into a single, definite state when it is observed or measured.

[Classical Bit] ⟶ Absolute State ⟶ Either 0 OR 1

[Quantum Qubit] ⟶ Superposition ⟶ Both 0 AND 1 (Until Measured)

The Cryptographic Crisis and "Harvest Now, Decrypt Later"

The processing power unlocked by superposition allows quantum computers to evaluate vast numbers of possibilities simultaneously. Using **Shor's Algorithm**, a sufficiently powerful quantum computer will easily break widely used asymmetric encryption methods (such as RSA and ECC) that currently secure the global internet.

This has triggered an urgent cybersecurity threat known as **Harvest Now, Decrypt Later (HNDL)**. Adversaries and nation-states are actively intercepting and storing encrypted network traffic today. While they cannot read it right now, they will decrypt it the moment a functional quantum computer becomes available. Consequently, any data with a long shelf-life—such as state secrets, health records, and banking data—is already at risk.

The New Defense (Post-Quantum Cryptography)

To survive this threat, the cybersecurity industry is migrating to **Post-Quantum Cryptography (PQC)**. PQC consists of purely software-based algorithms designed to secure our existing internet infrastructure against both classical and quantum attacks.

Unlike **Quantum Key Distribution (QKD)**—which relies on physics and expensive fiber-optic hardware—PQC relies on complex mathematical problems that are inherently "hard" for quantum processors to solve:

- **Lattice-Based Cryptography:** Hides data inside complex, multi-dimensional geometric structures (lattices) consisting of millions of hidden points. Finding the hidden key is virtually impossible for any computer.
- **Hash-Based Cryptography:** Uses the secure, one-way mathematical properties of traditional cryptographic hash functions to build unbreakable digital signatures.
- **Code-Based Cryptography:** Relies on the extreme difficulty of decoding error-correcting codes that have random errors intentionally injected into them.

The U.S. National Institute of Standards and Technology (NIST) has finalized the first official PQC standards to replace vulnerable systems, including **ML-KEM** (for general encryption) and **ML-DSA** (for digital signatures).

As future cybersecurity professionals, implementing PQC will be one of the largest IT migrations you will face. The transition is complicated by three major bottlenecks:

1. **Larger Data Footprints:** PQC public keys are exponentially larger than RSA keys, causing network packet fragmentation and latency.
2. **Resource Constraints:** Legacy routers and embedded Internet of Things (IoT) devices often lack the RAM and processing power to compute PQC algorithms.
3. **Cryptographic Hybridization:** To minimize risk during the transition, organizations are deploying hybrid systems. Data is encrypted with *both* a classical algorithm (like ECC) and a PQC algorithm simultaneously. If the new PQC math contains an undiscovered flaw, the classical layer still protects it from everyday hackers.

Ultimately, the quantum revolution proves the "observer effect" highlighted by Schrödinger's cat: in the quantum era, the very act of trying to intercept, measure, or steal data changes the state of the system itself, paving the way for a brand-new era of digital defense.

Exercise 1: Match the cybersecurity and physics terms on the left with their correct definitions on the right.

1. Qubit	**A.** The threat of intercepting encrypted data today to decrypt it years later.
2. Superposition	**B.** A software-based algorithm designed to resist quantum computer attacks.
3. Lattice-Based	**C.** A quantum bit that can exist as a combination of 0 and 1 simultaneously.
4. HNDL	**D.** The state of existing in multiple possibilities at once until measured.
5. PQC	**E.** A type of cryptographic math hiding data in multi-dimensional geometry.

Task 2: Answer the following questions in complete sentences based on the text.

1. Why does Shor's Algorithm pose such a severe threat to modern internet security?

2. What is the main physical difference between implementing QKD and implementing PQC?
3. hybridization protect data if a new PQC algorithm turns out to have a hidden flaw**?**

Task 3: Fill in the blanks using the following words:
collapses, **hybrid**, **asymmetric**, **wave-like**, **footprints**.

The Double-Slit experiment proved that subatomic particles have a 1. _____ behavior, which allows qubits to hold multiple states at once. However, when someone observes a quantum system, the superposition 2. _____ into a single state. Quantum processors will easily break traditional 3. _____ encryption methods like RSA. To fix this, IT professionals are switching to PQC, though they face challenges like larger data 4. _____. For safety during this transition, many companies deploy 5. _____ systems that combine both old and new encryption layers.

Task 4. **Watch the video and choose the correct answer.**
https://www.youtube.com/watch?v=UjaAxUO6-Uw&t=65s
1. Why did Erwin Schrödinger propose the cat experiment?
a) To prove that cats have special abilities.
b) To explain how to care for laboratory animals.
c) To demonstrate the strange consequences of quantum mechanics.
d) To show that atoms are visible.
2. Inside the box, the cat's fate depends on:
a) a computer program.
b) a radioactive atom.
c) a laser.
d) an electric battery.
3. According to the Copenhagen interpretation, before the box is opened the cat is:
a) definitely alive.
b) definitely dead.
c) both alive and dead in a quantum superposition.
d) asleep.
4. What does the thought experiment mainly question?
a) Whether animals can understand physics.
b) How quantum effects relate to the everyday world.
c) Whether radiation is dangerous.
d) How to build a better laboratory.
5. Schrödinger designed the experiment mainly to:
a) support the Copenhagen interpretation.
b) criticise and challenge it.
c) discover a new particle.
d) explain Einstein's theory of relativity.
6. Which statement is TRUE?

a) The experiment was actually performed with a real cat.
b) It is a thought experiment rather than a real experiment.
c) Scientists proved that the cat would survive.
d) The box was transparent.

Task 2. Discuss the questions in pairs or small groups.

1. Why did Erwin Schrödinger create the "cat in the box" thought experiment?
2. What does the cat represent in the experiment?
3. Why do many people find the idea of the cat being both alive and dead difficult to understand?
4. Do you think the thought experiment explains quantum mechanics clearly? Why or why not?
5. Why is observation so important in the experiment?
6. Do you think a thought experiment can be as valuable as a real scientific experiment? Explain your opinion.
7. How does Schrödinger's Cat challenge our everyday understanding of reality?
8. Why do scientists still discuss this experiment more than 90 years after it was proposed?
9. How has Schrödinger's Cat influenced modern science and technology?
10. What questions about the universe does this experiment leave unanswered?

UNIT 9. REVISION UNITS 1–8

Part 1. Vocabulary Revision

Task 1. Match the terms with their definitions.

1. Cybersecurity
2. Cybercrime
3. Cybercriminal
4. Vulnerability
5. Malware
6. Phishing
7. Cyberpolice
8. Digital evidence
9. Operating system
10. Processor
11. Input device
12. Output device
13. Quantum computer
14. Encryption
15. Cryptography
16. Post-quantum cryptography

a. software designed to damage or compromise a computer system
b. a person who commits crimes using computers or networks
c. protection of systems, networks and digital information
d. a weakness that can be exploited by an attacker
e. a person or organisation responsible for investigating cybercrime
f. criminal activity involving computers or digital networks
g. information stored digitally that can be used as evidence
h. a system that manages computer hardware and software
i. a device used to enter information into a computer
j. a device that presents information from a computer
k. the main component that processes instructions
l. a method of protecting information by converting it into a secure form
m. the science of protecting information through mathematical methods
n. a computer using quantum principles to process information
o. cryptographic methods designed to resist attacks from quantum computers
p. a fraudulent attempt to obtain information by pretending to be trustworthy

Task 2. Complete the sentences. ***Use the words below.***
cybersecurity • cybercrime • malware • vulnerability • digital evidence • processor • encryption • phishing • quantum computer • cyberpolice

1. _____ investigates crimes committed using computers and networks.
2. A serious software _____ allowed attackers to access the database.
3. Strong _____ protects sensitive information from unauthorised users.
4. The police collected _____ from the suspect's computer.
5. _____ messages often attempt to steal passwords and financial information.
6. A modern computer's _____ performs billions of operations every second.
7. The organisation improved its _____ after suffering a cyberattack.
8. The laboratory is researching how a _____ could affect modern cryptography.
9. The police officer specialises in investigating _____.
10. The infected computer contained several types of _____.

Part 2. Reading Revision
From the First Computers to Quantum Cybersecurity

Cybersecurity has developed together with computer technology. When computers first appeared, they were large, expensive machines used mainly by governments, universities and research organisations. Security was not initially the main concern because computers were not connected to global networks.

As computers became smaller and more affordable, they entered businesses and homes. The development of the internet created enormous opportunities for communication and information sharing, but it also created new opportunities for criminals. Hackers could attack systems from a distance, steal information and disrupt services.

The history of cybercrime includes many different stages. Early computer criminals often experimented with systems to gain unauthorised access. Later, criminals began creating viruses, worms, Trojans and other types of malware. As online banking and e-commerce developed, criminals increasingly targeted financial information and personal data.

Phishing became one of the most common methods of cybercrime. Criminals began sending messages that appeared to come from banks, government agencies or other trusted organisations. Their aim was usually to persuade victims to reveal passwords, payment details or other sensitive information.

The growth of cybercrime led to the development of specialised cyberpolice units. International cooperation became essential because cybercriminals can operate in one country while attacking victims in another. Police organisations and international agencies exchange information, investigate digital evidence and cooperate in cross-border operations.

Ukraine has also developed specialised cyberpolice capabilities. Ukrainian cyberpolice officers investigate online fraud, hacking, malware distribution, identity theft and other forms of cybercrime. Cooperation with international law-enforcement organisations is particularly important because many cybercrime investigations involve foreign servers, platforms or suspects.

At the same time, computer technology continues to evolve. Modern computers contain powerful processors, memory systems and a wide range of input and output devices. Smartphones, tablets, servers and cloud systems have become essential parts of modern society.

The next major technological development may be quantum computing. Unlike classical computers, quantum computers use quantum bits, or qubits. In theory, sufficiently powerful quantum computers could solve certain problems much faster than classical machines. This could have major consequences for cryptography.

Some current encryption systems rely on mathematical problems that are extremely difficult for classical computers to solve. A sufficiently powerful quantum computer could potentially break some of these systems. For this reason, researchers are developing **post-quantum cryptography**, which aims to protect information against future quantum attacks.

The evolution of computers therefore creates a continuous cybersecurity challenge. Every technological advance can provide new opportunities for society, but it can also create new vulnerabilities. Cybersecurity professionals must understand both the history of technology and the threats that may emerge in the future.

Part 3. Comprehension

Task 3. Answer the questions.

1. Why was cybersecurity less important when early computers were developed?
2. How did the internet change cybercrime?
3. What types of information do cybercriminals commonly target?
4. Why is international cooperation important in cybercrime investigations?
5. What types of crimes does cyberpolice investigate?

6. Why is cyberpolice cooperation particularly important for Ukraine?
7. What is a qubit?
8. Why could quantum computers create problems for modern cryptography?
9. What is post-quantum cryptography?
10. Why must cybersecurity professionals understand technological development?

Task 4. True or False

1. Early computers were normally connected to the internet.
2. The development of the internet created new opportunities for cybercriminals.
3. Phishing can be used to steal passwords.
4. Cybercriminals always operate in the same country as their victims.
5. International cooperation can help investigate cross-border cybercrime.
6. Cyberpolice investigate only computer viruses.
7. Quantum computers use qubits.
8. Quantum computing may affect some existing cryptographic systems.
9. Post-quantum cryptography is designed to prepare for future quantum attacks.
10. Technological progress can create both opportunities and cybersecurity risks.

Task 5. Find the evidence

Find information in the text supporting these statements.

1. The internet changed the nature of cybercrime.
2. Cybercrime investigations often require international cooperation.
3. Cybersecurity is connected to technological development.
4. Quantum computing may change the future of information security.

Write **one or two sentences** for each answer.

Part 4. Grammar. Plural Forms of Nouns

Task 6. Write the plural form.

Pay particular attention to **Latin and Greek-origin nouns**.

1. virus → _____
2. analysis → _____
3. crisis → _____
4. phenomenon → _____
5. criterion → _____
6. hypothesis → _____
7. database → _____
8. technology → _____
9. device → _____
10. network → _____
11. medium → _____
12. datum → _____
13. diagnosis → _____
14. thesis → _____

Task 7. Choose the correct form.

1. The security team analysed several **(criterion / criteria)**.
2. Researchers conducted several **(analysis / analyses)** of the malware.
3. Cybersecurity professionals must understand different **(phenomenon / phenomena)**.
4. The database contains millions of **(datum / data)**.
5. Several **(virus / viruses)** infected the computers.
6. The researchers developed new **(hypothesis / hypotheses)**.
7. The scientists discussed several possible **(crisis / crises)**.
8. The system uses different **(medium / media)** for communication.

Part 5. Articles

Task 8. Choose a, an, the or —.

1. Cybersecurity is ___ important part of modern computing.
2. ___ internet has changed the nature of cybercrime.
3. A hacker discovered ___ vulnerability in the system.
4. ___ vulnerability allowed attackers to access the database.
5. Quantum computing is ___ rapidly developing field.
6. He works as ___ cybersecurity specialist.
7. ___ cybercrime can affect individuals, businesses and governments.
8. Ukraine has developed ___ specialised cyberpolice unit.
9. ___ encryption protects sensitive information.
10. Researchers are developing ___ new approach to post-quantum cryptography.

Part 6. Adjectives and Adverbs

Task 9. A. Choose the correct form.

1. The security team responded **quick / quickly** to the attack.
2. This is a **serious / seriously** vulnerability.
3. The system operates **efficient / efficiently**.
4. The researchers conducted a **careful / carefully** analysis.
5. The hacker worked **secret / secretly**.
6. Quantum computers may become extremely **powerful / powerfully**.
7. The officer examined the digital evidence **thorough / thoroughly**.
8. Cybercriminals often use **complex / complexly** methods.

B. Complete the text

Complete the text with the correct comparative or superlative structure.

Life in the Digital Age

Life today is very different from life 30 years ago. Smartphones are **(1) _____** (powerful) the mobile phones of the past, and they can perform **(2) _____** (many) functions.

However, modern life is not always easier. People are often **(3) _____** (busy) they were in the past, and many spend **(4) _____** (much) time looking at

screens. Working from home can be **(5) _____** (comfortable) working in an office, but it can also make it difficult to separate work from personal life.

Online shopping is another major change. It is often **(6) _____** (convenient) going to a shop, especially for people who live far from city centres. However, visiting a shop can be **(7) _____** (enjoyable) shopping online because customers can see and try products before buying them.

Transport is changing too. Electric cars are becoming **(8) _____** (common and common), while public transport is becoming **(9) _____** (environmentally friendly). The **(10) _____** (efficient) public transport becomes, the **(11) _____** (attractive) it will be to people who normally drive.

Technology has also changed communication. Sending a message is **(12) _____** (much / quick) making a phone call, but a face-to-face conversation can be **(13) _____** (personal) a text message.

In the future, everyday life may become **(14) _____** (even / convenient), but people will still need to decide how much technology they really want to use. After all, the **(15) _____** (important) technology is not always the technology that makes life the easiest.

Part 7. Pronouns

Task 10. Choose the correct pronoun.

Demonstrative pronouns

1. _____ devices are connected to the secure network.

a) This
b) These
c) That

2. _____ information was collected during the investigation.

a) These
b) Those
c) This

Indefinite pronouns

3. _____ gained unauthorised access to the server.

a) Someone
b) Anyone
c) Nothing

4. The police could not find _____ suspicious on the computer.

a) anyone
b) anything
c) someone

5. _____ should follow basic cybersecurity rules.

a) Everyone
b) Nothing
c) Something

Reciprocal pronouns

6. The two security teams shared information with _____.

a) themselves
b) each other
c) anyone

Relative pronouns

7. The officer _____ investigated the case collected the digital evidence.

a) who
b) which
c) where

8. The computer _____ was infected has been isolated.

a) who
b) which
c) where

9. The company _____ systems were attacked contacted the police.

a) whose
b) who
c) which

10. This is the laboratory _____ the researchers study quantum technology.

a) who
b) which
c) where

Part 8. Numerals

Task 11. Write the numbers in words.

- 1950
- 1969
- 1986
- 2,500
- 10,000
- 3.5 million
- 21st century
- 64-bit
- 128-bit
- 1,000,000

Part 9. Prepositions

Task 12. Choose the correct preposition.

1. Cybercriminals often attack systems **through / at / by** the internet.
2. The officer specialises **in / on / at** cybercrime investigations.
3. The computer was protected **from / of / with** malware.
4. The hacker gained access **to / at / on** the server.
5. The police collected evidence **from / by / at** the computer.
6. The organisation is responsible **for / of / to** network security.
7. Researchers are working **on / at / for** post-quantum cryptography.

8. The attack occurred **in / on / at** 2025.
9. The system was developed **by / from / with** a team of engineers.
10. The data was stored **on / at / in** a secure server.

Part 10. Question Words
Task 13. Choose the correct question word.
who • what • where • when • why • which • whose • how

1. _____ discovered the vulnerability?
2. _____ did the cyberattack happen?
3. _____ was the system attacked?
4. _____ did the criminals gain access?
5. _____ information was stolen?
6. _____ computer was infected?
7. _____ type of malware was used?
8. _____ is responsible for investigating the case?

Part 11. There is / There are
Task 14. Complete the sentences.

1. _____ a vulnerability in the operating system.
2. _____ several suspicious files on the computer.
3. _____ an international cyberpolice organisation investigating the case.
4. _____ millions of connected devices around the world.
5. _____ some important evidence on the server.
6. _____ two possible explanations for the attack.

Part 12. Used to
Task 15. Complete the sentences with used to, didn't use to or the correct present form.
1. Early computers _____ be extremely large.
2. People _____ use smartphones for online banking.
3. Cybercriminals _____ have access to today's advanced AI tools.
4. Computers _____ be connected to global networks.
5. Today, people _____ rely heavily on digital technology.
6. Cybercrime _____ be as complex as it is today.

Part 13. Be Going To
Task 16. Complete the sentences.
1. Researchers _____ develop new post-quantum algorithms.
2. The cyberpolice _____ investigate the suspicious activity.
3. The company _____ upgrade its security system.
4. The university _____ introduce a new cybersecurity course.
5. The engineers _____ test the quantum computer tomorrow.

Use: **am / is / are going to + verb**

Part 14. Gerund or Infinitive

Task 17. Choose the correct form.

1. Cybersecurity professionals must avoid **(sharing / to share)** passwords.
2. Researchers want **(developing / to develop)** stronger encryption.
3. The officer decided **(investigating / to investigate)** the case further.
4. Users should avoid **(opening / to open)** suspicious attachments.
5. The team finished **(analysing / to analyse)** the digital evidence.
6. The company plans **(introducing / introducing)** new security measures.
7. Cybercriminals often try **(stealing / to steal)** sensitive information.
8. Experts recommend **(using / to use)** multi-factor authentication.

Part 15. Types of Verbs

Task 18. Identify the type of verb.

Write: **action verb, linking verb, auxiliary verb or modal verb**

1. The hacker **accessed** the server.
2. The system **is** secure.
3. The researchers **are** testing the device.
4. Users **must** protect their passwords.
5. The officer **examined** the computer.
6. The technology **became** more advanced.
7. The company **has** developed a new system.
8. Cybersecurity professionals **can** prevent many attacks.

Part 16. The Verb To Be

Task 19. Complete the sentences with the correct form of to be.

1. Cybersecurity _____ essential for modern organisations.
2. These devices _____ connected to the network.
3. The computer _____ infected yesterday.
4. The researchers _____ working on a new project.
5. There _____ several vulnerabilities in the system.
6. There _____ a serious problem with the server.
7. The police officer _____ responsible for collecting evidence.
8. Quantum computers _____ expected to affect cryptography.

Part 17. Irregular Verbs

Task 20. Complete the table.

Infinitive	Past Simple	Past Participle
arise	_____	_____
bear	_____	_____
bind	_____	_____
breed	_____	_____

Infinitive	Past Simple	Past Participle
cast	_____	_____
cling	_____	_____
deal	_____	_____
flee	_____	_____
forbid	_____	_____
foresee	_____	_____
freeze	_____	_____
grind	_____	_____
hide	_____	_____
lay	_____	_____
lead	_____	_____
mean	_____	_____
overcome	_____	_____
seek	_____	_____
shake	_____	_____
shrink	_____	_____
slide	_____	_____
spin	_____	_____
split	_____	_____
spread	_____	_____
steal	_____	_____
swear	_____	_____
undergo	_____	_____
undertake	_____	_____
withdraw	_____	_____
withstand	_____	_____

Part 18. Mixed Grammar Revision

Task 21. Choose the correct answer.

1. There _____ several vulnerabilities in the system.

a) is
b) are
c) be
d) was

2. The police have collected several pieces of digital _____.

a) evidences
b) evidence

c) evidenceses
d) evidential
3. Researchers _____ develop stronger cryptographic systems in the future.
a) are going to
b) used to
c) are
d) have
4. Early computers _____ much larger than modern devices.
a) used to be
b) use to be
c) were use to
d) used be
5. The officers are responsible for _____ digital evidence.
a) collect
b) to collect
c) collecting
d) collected
6. The researcher _____ discovered the vulnerability reported it immediately.
a) which
b) who
c) where
d) whose
7. The two teams exchanged information with _____.
a) themselves
b) each other
c) someone
d) anything
8. The system contains several _____.
a) analysis
b) analyses
c) analysises
d) analysi
9. A quantum computer may _____ modern cryptography.
a) affect
b) affecting
c) to affecting
d) affected
10. The police _____ going to investigate the attack.
a) is
b) are
c) be
d) was
11. _____ is responsible for protecting the database?

a) What
b) Who
c) Which
d) Where

12. The officer examined the evidence _____.

a) careful
b) carefully
c) care
d) carefulness

Part 19. Error Correction

Task 22. Find and correct the mistakes.

1. There is several vulnerabilities in the system.
2. The police collected many digital evidences.
3. Early computers used to was very large.
4. The researchers are going develop a new algorithm.
5. Cybersecurity specialists recommend to use strong passwords.
6. The officer which investigated the case collected the evidence.
7. The two teams shared information with themselves.
8. There were several serious cybercrime in the region.
9. The researcher made several important analysises.
10. Someone have accessed the server.
11. These information is highly confidential.
12. The cyberpolice is going to investigate the attack.

Part 20. Final Integrated Revision

Task 23. Complete the text. Use the correct form of the words or structures.

The Future of Cybersecurity

Cybersecurity _____ (be) one of the most important areas of modern technology. In the past, computers _____ (use) mainly by governments, universities and large organisations. Today, _____ are millions of connected devices around the world.

Cybercriminals _____ (become) increasingly sophisticated. They use malware, phishing and other methods to attack individuals and organisations. Security professionals recommend _____ (use) strong passwords and multi-factor authentication.

International cyberpolice organisations work with _____ to investigate cross-border crimes. Officers _____ (collect) digital evidence and analyse computer systems.

At the same time, researchers _____ (develop) new technologies. Quantum computers _____ (be) potentially capable of breaking some current encryption systems. Because of this, scientists _____ (go) to develop post-quantum cryptography.

The future _____ (be) likely to bring both new opportunities and new threats. Cybersecurity professionals _____ (need) to understand how technology develops and how criminals can misuse _____ technologies.

Part 21. Final Speaking Task
Cybersecurity: From the Past to the Future
Work in groups.
Prepare a **3–4 minute presentation** about the development of cybersecurity.
Your presentation should include:
1. The past
- early computers;
- the beginning of cybercrime;
- early forms of malware;
- the development of the internet.

2. The present
- modern cybercrime;
- global cyberpolice;
- cyberpolice in Ukraine;
- protection of computers and information systems.

3. The future
- quantum computers;
- post-quantum cryptography;
- new cyber threats;
- future international cooperation.

UNIT 10. THE HISTORY AND EVOLUTION OF ARTIFICIAL INTELLIGENCE.

Glossary

Artificial Intelligence (AI)	**The ability of computers to perform tasks that normally require human intelligence, such as learning, reasoning, and problem-solving.**
AI Agent	**An AI system that can perform tasks independently to achieve a specific goal.**
algorithm	**A sequence of instructions a computer follows to solve a problem or complete a task.**
artificial neural network	**A computing system inspired by the structure of the human brain that learns from data.**
autonomously	**Acting independently without direct human control.**

automation	**The use of technology to perform tasks with little or no human involvement.**
data privacy	**The protection of personal or sensitive information from unauthorised access or misuse.**
database	**A structured collection of data stored electronically for easy access and management.**
Deep Learning	**A type of machine learning that uses multi-layered neural networks to recognise patterns and make decisions.**
Expert System	**An AI program that imitates the knowledge and decision-making abilities of a human expert.**
Generative AI	**AI that creates new content, including text, images, music, videos, or computer code.**
Graphics Processing Unit (GPU)	**A specialised processor designed to perform many calculations simultaneously, making it ideal for AI applications.**
Large Language Model (LLM)	**An AI model trained on vast amounts of text to understand and generate human language.**
Machine Learning (ML)	**A branch of AI that enables computers to learn from data and improve their performance without being explicitly programmed.**
multimodal AI	**AI capable of processing and combining different types of information, such as text, images, audio, and video.**
pattern recognition	**The ability of AI to identify regularities, relationships, or structures in data.**
processor	**The hardware component that executes instructions and performs calculations in a computer.**
productivity	**The ability to complete tasks efficiently and effectively.**
strategic task	**A task that requires planning, analysis, and decision-making to achieve a goal.**

Turing Test	**A test proposed by Alan Turing to evaluate whether a machine can communicate in a way that is indistinguishable from a human.**

Abbreviations

AI Artificial Intelligence
ML Machine Learning
LLM Large Language Model
GPU Graphics Processing Unit
IBM International Business Machines
IT Information Technology

Artificial Intelligence (AI) feels like a brand-new technology, but its roots go back more than 70 years. What started as a mathematical theory in university labs has become a technology that changes how we live and work. Understanding where AI came from helps us understand where it is going next.

The journey of AI officially began in **1950** when British mathematician **Alan Turing** published a famous paper. He asked a simple question: *"Can machines think?"* [4] He created the "Turing Test" to measure a machine's intelligence.

In **1956**, the term "Artificial Intelligence" was used for the first time. Scientists gathered at the **Dartmouth Summer Research Project** to discuss creating an artificial brain. Early AI programs could solve algebra word problems and play checkers. However, early computers were too slow and expensive. By the 1970s, funding decreased, and AI entered its first "AI Winter"—a period where progress slowed down significantly.

AI returned to life in the 1980s with **"Expert Systems."** [1, 2] These were programs that imitated the decision-making skills of human experts in specific fields, like medicine or finance.

The biggest shift came with the development of **Machine Learning (ML)**. Instead of programmers writing strict rules for every situation, computers were trained to learn from data. A historic moment occurred in **1997** when IBM's supercomputer, **Deep Blue**, defeated the world chess champion, Garry Kasparov. This proved that machines could handle highly complex, strategic tasks.

By the 2010s, two things exploded: the amount of digital data available and the power of computer processors (especially GPUs). This allowed scientists to develop **Deep Learning**, which uses artificial neural networks inspired by the human brain.

Computers suddenly became excellent at recognizing images, translating languages, and understanding speech. In **2016**, Google's **AlphaGo** beat the world champion at Go, an ancient board game infinitely more complex than chess. AI was no longer just analyzing data; it was recognizing complex visual patterns better than humans.

Current Development: The Generative AI Era (2020s–Present)

Today, we are living in the era of **Generative AI**. The release of tools like **ChatGPT** in late 2022 marked a turning point. Modern AI models (known as Large Language Models, or LLMs) do not just analyze data—they create new things. They write essays, generate realistic images, write software code, and compose music in seconds.

Current development is focused on two main areas:

- **Multimodal AI**: Systems that can seamlessly process text, audio, images, and video all at the same time.
- **AI Agents**: Programs that do not just answer questions, but can autonomously complete multi-step tasks, like booking a flight or managing a database.

While AI brings incredible productivity, it also brings modern challenges. Society is now dealing with deepfakes, copyright issues, data privacy concerns, and the fear of automation replacing human jobs.

Exercise 1: Timeline Matching

Match the decade/year on the left with the correct historical event on the right.

1. **1950** — *A) IBM's Deep Blue defeats Garry Kasparov at chess.*
2. **1956** — *B) ChatGPT is released, popularizing Generative AI.*
3. **1997** — *C) Alan Turing publishes his paper proposing the Turing Test.*
4. **2016** — *D) The term "Artificial Intelligence" is coined at Dartmouth.*
5. **2022** — *E) AlphaGo beats the world champion of the game Go.*

Exercise 2: *Choose the correct answer based on the text.*

1. **What was the main problem during the "AI Winter"?**

A) Computers were too dangerous for public use.
B) Computers were too slow, expensive, and funding stopped.
C) AI was banned by governments.
D) Internet connections were too slow.

2. **How does Deep Learning differ from early AI methods?**

A) It requires humans to code every single rule.
B) It operates without using any digital data.
C) It uses neural networks inspired by the human brain to find patterns.
D) It is only used for playing board games.

3. **What is a major feature of modern "Multimodal AI"?**

A) It only works on mobile phones.
B) It can handle text, images, and video at the same time.
C) It does not require any electricity to run.
D) It never makes mistakes or false positives.

Task 3: Answer the questions:

1. What is the difference between older Machine Learning (analyzing data) and modern Generative AI?
2. Mention two societal problems or challenges caused by the rapid development of modern AI.

UNIT 11. AI AND CYBERSECURITY

Glossary

Double-edged sword a situation or technology that has both advantages and disadvantages.
Signatures unique patterns of code or data used by security software to recognise known malware.
Anomaly something unusual or unexpected that differs from normal behaviour.
Isolate to separate a computer, device, or system from a network to stop a cyber threat from spreading.
Generative AI artificial intelligence that can create new content, such as text, images, audio, or computer code.
Deepfake an AI-generated video, image, or audio recording that realistically imitates a real person.
Mutating changing its form or code over time, especially to avoid being detected.
False positive an incorrect result in which harmless activity is identified as a security threat

Artificial Intelligence (AI) is transforming the digital world at an incredible speed. For cybersecurity professionals, the rise of AI is a double-edged sword. This means that while AI provides powerful new tools to defend networks, it also gives cybercriminals advanced methods to launch attacks. The battle between hackers and security experts has entered a new, automated era.

AI as a Shield: Modern Defense

Traditionally, cybersecurity relied on static rules and signatures to detect malware. Security software looked for known threats. However, modern cyberattacks change constantly. This is where AI shines.

AI systems can analyze millions of data points every second. They use machine learning to understand normal network behavior. If a user suddenly downloads thousands of files at 3:00 AM, the AI detects this anomaly immediately. It can automatically lock the user's account and isolate the computer from the network before any data is stolen. AI helps human analysts respond to threats in real time, saving organizations millions of dollars.

AI as a Weapon: Automated Attacks

Unfortunately, cybercriminals are also adopting AI. Hackers use artificial intelligence to automate their attacks, making them faster and harder to detect.

One major threat is AI-powered phishing. In the past, phishing emails were often easy to spot because of bad grammar or spelling mistakes. Today, generative AI tools allow hackers to write perfect, highly convincing emails in any language. Criminals also use deepfake technology to clone the voices or faces of company executives. They use these realistic clones to trick employees into transferring money or revealing passwords. Furthermore, AI can be used to write mutating malware that changes its own code to bypass traditional antivirus software.

The Future: Machine vs. Machine

The future of cybersecurity will be a battle of machine against machine. Human analysts can no longer keep up with the speed of automated AI attacks. Organizations must implement AI defenses just to survive.

However, AI is not a complete replacement for humans. AI systems can still make mistakes, known as false positives, where harmless activity is flagged as a threat. Human expertise is still required to make final strategic decisions and investigate complex breaches. For future cybersecurity professionals, learning how to manage, train, and protect AI systems will be the most critical skill of the decade.

Exercise 1. Choose the correct answer:

1. **Why is AI described as a "double-edged sword" in the text?**

A) It is very expensive to buy and maintain.
B) It helps both the attackers and the defenders in cybersecurity.
C) It only works on advanced operating systems.
D) It replaces human workers but increases system errors.

2. **How does AI detect threats that traditional software might miss?**

A) By searching for old, known malware signatures.
B) By analyzing network behavior and finding anomalies.
C) By asking the user to change their password frequently.
D) By shutting down the entire internet connection every night.

3. **What is "mutating malware"?**

A) Software that damages the computer hardware physically.
B) A virus that can only infect mobile phones.
C) Malicious code that changes itself to avoid detection by security software.
D) A type of deepfake voice recording.

Exercise 2: True or False

1. **[ ]** AI defense systems can automatically block a threat without waiting for a human to do it.
2. **[ ]** Bad grammar is still the easiest way to identify a phishing email created by modern hackers.
3. **[ ]** Deepfakes use AI to impersonate executives to trick employees into giving away passwords.
4. **[ ]** Because of AI, human cybersecurity experts will not be needed at all in the future.

Task 3. Discussion & writing

Answer the following questions in complete sentences to practice your English.

1. Imagine you are a cybersecurity analyst. What is the biggest advantage of having an AI assistant in your daily job?
2. How can companies protect their employees from deepfake attacks? Brainstorm at least two practical solutions.

Task 4. Case study

Background

In 2026, Anthropic introduced **Mythos**, an advanced AI system designed to identify security weaknesses in software. As part of **Project Glasswing**, Mythos was used to analyse thousands of open-source projects and critical software systems used around the world.

The results surprised the cybersecurity community. Within only a few weeks, Mythos identified more than **23,000 potential vulnerabilities** across over **1,000 open-source software projects**. Security experts later confirmed that many of these findings were genuine security flaws, including more than **1,000 high- and critical-severity vulnerabilities**.

Mythos examined millions of lines of source code automatically. Unlike traditional security scanners, the AI was able to understand how software functions worked together and identify complex weaknesses that had remained hidden for years.

Researchers reported that Mythos found vulnerabilities in major software projects, including web browsers, operating systems, multimedia software, and networking tools. Some of these flaws had existed in the code for more than a decade without being discovered by human experts. Mozilla reported fixing **271 vulnerabilities in Firefox** that were identified during its collaboration with Mythos.

The Mythos case demonstrated both the power and the limitations of AI in cybersecurity.

Advantages

- AI could analyse enormous amounts of code much faster than human teams.
- It discovered vulnerabilities hidden in very old software.
- It helped prioritise high-risk code for human review.

Risks

- The large number of false positives created extra work for analysts.
- Attackers could potentially use similar AI tools to find vulnerabilities before defenders do.
- Organisations realised that legacy software may contain many unknown security weaknesses.

Impact on Cybersecurity

After the project, many companies began investing in AI-assisted secure code review. Governments and critical infrastructure operators also started reassessing the security of legacy systems.

The incident strengthened the idea that the future of cybersecurity will involve cooperation between AI and human experts, rather than replacing humans completely.

Task A. Answer the questions.

- What was the main goal of the Mythos project?
- What type of software did Mythos analyse?
- Name three vulnerabilities detected by the AI.
- Were all findings real vulnerabilities?
- Why is legacy software a security concern?

Task B. True or False

- Mythos analysed modern code only.
- The AI found millions of potentially vulnerable code fragments.
- Every finding was confirmed by human experts.
- Some vulnerabilities affected software still in use.
- The case showed that AI can completely replace cybersecurity professionals.

Task C. Discussion

- Should companies be required to review old software with AI tools?
- What is more dangerous: unknown vulnerabilities or false positives?
- How can organisations combine AI analysis with human expertise effectively?

UNIT 12. ROBOTICS, HUMANOID ROBOTS AND ARTIFICIAL INTELLIGENCE

Glossary

Industrial robot a robot designed for manufacturing and repetitive factory work.
Humanoid robot a robot built to resemble and move like a human.
Artificial intelligence (AI) technology enabling machines to learn and make decisions.
Machine learning AI that improves performance by analysing data.
Computer vision AI that recognises images, people, and objects.
Natural language processing AI that understands and produces human language.
Sensor a device that collects information from the environment.
Authentication verifying a user's identity before granting access.
Encryption converting information into a secure unreadable form.
AI hallucination false or inaccurate information generated by artificial intelligence.
Remote control operating a device from another location.
Human supervision monitoring robot actions to ensure safe and correct operation.

Robotics has developed from a scientific idea into one of the fastest-growing technologies of the 21st century. Today, robots build cars, assist surgeons, explore other planets, and even communicate naturally with people. Combined with artificial intelligence (AI), modern robots are becoming increasingly capable of performing tasks that once required human intelligence.

The idea of intelligent machines is much older than computers. Ancient Greek engineers designed simple mechanical devices powered by water and gears. During the Renaissance, **Leonardo da Vinci** sketched plans for a mechanical knight that could move its arms and head. Although it was never built during his lifetime, many historians consider it one of the earliest humanoid robot designs.

The first industrial robots appeared in the 1950s. In 1961, **Unimate**, the world's first industrial robot, began working in a General Motors factory in the United States. It carried out dangerous and repetitive tasks such as lifting hot metal parts and welding. This marked the beginning of modern industrial robotics. Today, millions of industrial robots work in factories producing cars, electronics, and household appliances.

As computer technology improved, robots became more intelligent. Instead of following only simple programmed instructions, they began using sensors, cameras, and artificial intelligence to understand their surroundings. Machine learning allows robots to improve their performance by analysing data, while computer vision enables them to recognise objects, faces, and obstacles. Natural language processing allows some robots to understand spoken language and respond naturally.

One of the most exciting developments is the creation of **humanoid robots**. These robots are designed to resemble humans, with a head, arms, hands, legs, cameras, microphones, and advanced software. Their human-like shape allows them to work in buildings, offices, hospitals, and homes without changing the environment. They can open doors, climb stairs, carry objects, and use tools designed for people.

Several companies have developed advanced humanoid robots. **ASIMO**, created by Honda, became famous for walking, running, climbing stairs, and interacting with people. **Atlas**, developed by Boston Dynamics, can jump, perform acrobatic movements, and maintain its balance on difficult surfaces. **Pepper**, created by SoftBank Robotics, is designed for customer service and can recognise basic human emotions. More recently, companies such as **Tesla**, **Figure AI**, **Agility Robotics**, and **Apptronik** have introduced humanoid robots intended to work in warehouses, factories, and logistics centres.

Today, humanoid robots are used in many industries. In hospitals, they deliver medicine, transport equipment, and assist medical staff. In hotels and airports, they greet visitors, answer questions, and provide directions. In warehouses, robots move heavy packages and help organise inventory. Some schools and universities use robots to support education, while research laboratories use them to test new AI technologies. Robots are also used in dangerous environments such as nuclear power stations, disaster zones, deep-sea exploration, and space missions where sending humans would be risky.

Artificial intelligence has greatly expanded what robots can do. Modern AI allows robots to recognise speech, translate languages, identify objects, plan routes, and even hold conversations using large language models. However, AI is still imperfect. Robots may misunderstand instructions, make incorrect decisions, or generate false information, known as **AI hallucinations**. Because of these limitations, human supervision remains essential in critical situations.

Cybersecurity is becoming increasingly important as robots become connected to the internet. Many robots collect personal information through cameras, microphones, GPS systems, and other sensors. If attackers gain unauthorised access, they could steal sensitive data, disable safety systems, or even control robots remotely. Manufacturers therefore use authentication, encryption, secure software updates, and continuous monitoring to protect robotic systems.

Experts believe that humanoid robots will become much more common during the next decade. Companies expect them to assist elderly people, support healthcare workers, inspect infrastructure, deliver goods, perform dangerous rescue operations, and help astronauts during future missions to the Moon and Mars. Rather than replacing humans completely, most specialists believe robots will work alongside people, taking

over repetitive, physically demanding, or dangerous jobs while humans focus on creativity, communication, and complex decision-making.

Task 1. Answer the questions.

1. Who designed one of the earliest humanoid robot concepts?
2. What was the purpose of Unimate?
3. How has artificial intelligence improved modern robots?
4. Why are humanoid robots designed to resemble humans?
5. Name four companies developing humanoid robots today.
6. Give five examples of where humanoid robots are currently used.
7. What cybersecurity risks are associated with robots?
8. According to the text, how may robots be used in the future?

Task 2. Decide whether the statements are True (T) or False (F).

1. The first industrial robot was introduced in the 1960s.
2. Leonardo da Vinci designed a mechanical knight.
3. Atlas was developed mainly for customer service.
4. Pepper can recognise basic human emotions.
5. Humanoid robots are already used in hospitals.
6. AI enables robots to recognise speech and objects.
7. Human supervision is no longer necessary.
8. Future robots may assist astronauts on space missions.

Task 3. Match the robot with its description.

Robot	**Description**
1. Unimate	a. Customer service robot
2. ASIMO	b. First industrial robot
3. Atlas	c. Humanoid robot famous for walking and running
4. Pepper	d. Agile research robot capable of acrobatic movements

Task 4. Complete the sentences.

Use the words below.

warehouse • AI • sensors • encryption • hospitals • astronauts

1. Modern robots use _____ to collect information about their surroundings.
2. Artificial intelligence helps robots learn and make _____ decisions.
3. Humanoid robots already work in _____ delivering medicine.
4. Some companies use robots in the _____ to move heavy packages.
5. Strong _____ protects robots from cyberattacks.
6. Future robots may help _____ during missions to the Moon and Mars.

Task 5. Discussion

1. Which industry will benefit most from humanoid robots? Why?
2. Should every connected robot have built-in cybersecurity protection?

3. Would you trust a humanoid robot to care for elderly people? Explain.
4. Which jobs should always remain under human control?
5. How might humanoid robots change society over the next twenty years?

TASK 6. CASE STUDY: PHANTOM MK1 — HUMANOID ROBOTS ON THE BATTLEFIELD

Background

In February 2026, two **Phantom MK1 humanoid robots** were reportedly deployed to Ukraine in supporting roles near the front line. According to the source, the robots were developed by the San Francisco startup **Foundation** in just 13 months. The Phantom MK1 was designed for military use but was also intended as a **dual-use** system, meaning that the same technology could be used for both military and civilian purposes.

The Phantom MK1 is 175 cm tall and weighs 80 kg. It can walk at almost 2 metres per second and is controlled by a human operator using a VR headset and hand tracking. The operator can see what the robot sees and makes the critical decisions. The robot has eight cameras and can use different tools or weapons without major modifications.

According to the source, the robots were tested in difficult conditions, including mud, rubble and urban environments. The case raises important questions about the future of warfare, artificial intelligence, human control and cybersecurity.

The Mission

The source describes a mission in which one Phantom encountered a four-person guard team. The AI assessed the situation and the robots reportedly disarmed the guards without fatalities. The two robots then completed the mission and reached the extraction point.

The Phantom is not presented as a completely autonomous system. Human operators remain responsible for important decisions. One operator can reportedly control up to six units simultaneously. The source also states that current US military protocols require human authorisation before lethal action.

Cybersecurity Challenge

The Phantom also creates a new cybersecurity problem. A modern military robot depends on software, sensors, communication systems and networks. If an enemy could hack these systems, it might be possible to interfere with the robot or use it against its operators.

According to the source, the Phantom uses isolated military hardware, encrypted firmware, biometric authentication and a physical system designed to destroy its AI core if tampering is detected.

This means that future conflicts could involve not only physical battles but also **cyberattacks against robotic systems**. The source suggests that controlling or disabling an enemy's robots could become as important as traditional military operations.

Task A. Watch video https://www.youtube.com/watch?v=wqOjGV-t0Lk and answer the questions.

1. When and where were the Phantom MK1 robots reportedly deployed?
2. What was the main purpose of their deployment?
3. How does a human operator control the Phantom?
4. What makes the Phantom a dual-use technology?
5. Why is cybersecurity particularly important for this type of robot?

Task B. Analyse the situation

Imagine that you are a **cybersecurity specialist working for a military organisation**.
Your team is responsible for protecting a fleet of Phantom MK1 robots.
Identify **five possible cyber threats** to the robots.
For each threat, explain:

- what could happen;
- what information or system could be affected;
- how the organisation could reduce the risk.

Task C. Human control or autonomous AI?

Read the statement:
"Humanoid military robots should be allowed to make decisions without direct human control."
Work in groups and prepare arguments **for or against** this statement.
Consider:

- human lives;
- speed of AI decision-making;
- responsibility for mistakes;
- cyberattacks;
- technical failures;
- international law;
- the possibility of saving soldiers' lives.

Task D. Future scenario

Imagine that by **2035** military robots have become much more advanced.
Complete the scenario:
A robotic unit loses communication with its human operator during a military operation. At the same time, the robot detects what it believes is an enemy target.
Discuss:

1. Should the robot continue the mission?
2. Should it make its own decision?
3. Should it stop and wait for human instructions?
4. What could happen if the robot's AI has been hacked?
5. Who should be responsible if the robot makes a wrong decision?

Task E. Final discussion

Discuss the following question:
Will humanoid military robots make warfare safer or more dangerous?
Use at least **three arguments** to support your opinion.
Key vocabulary
humanoid robot — a robot designed to resemble the human body.
dual-use technology — technology that can be used for both civilian and military purposes.
human operator — a person who controls or supervises a machine.
autonomous — able to operate or make decisions without direct human control.
VR headset — a device that creates a computer-generated visual environment.
payload — equipment or materials carried by a robot for a specific mission.
mission module — a specialised unit that gives a robot a particular function.
biometric authentication — security based on physical characteristics such as fingerprints or facial features.
tampering — unauthorised interference with or modification of a system.
attack vector — a possible method of gaining unauthorised access to a system.
human authorisation — official permission given by a person before an action is performed.

UNIT 13. UNMANNED DRONES. THE FUTURE OF ROBOTICS.

Watch the video https://www.youtube.com/watch?v=WbB5ZejLKbg

Listening Comprehension Questions
1. **What is the primary function of the THeMIS robot?** (0:24 - 0:47)
2. **According to the video, what is the 'limiting factor' in using these robots?** (2:25 - 2:35)
3. **How does the video describe the role of human operators in controlling these vehicles?** (1:10 - 1:20)

Vocabulary Match
Match the following terms to their definitions as used in the video context:
- **Autonomous** (1:20): A) A partner or supporter.
- **Wingman** (0:29): B) Able to operate without direct human control.
- **Payload** (1:04): C) The total weight a vehicle can carry.
-

Discussion
- The video mentions that the 'age of the lethal combat robot has arrived.' Based on what you heard, do you think using robots on the battlefield makes war more or less dangerous for humans? Why?

Glossary
Unmanned drone a vehicle that operates without a person physically controlling it.

Autonomous able to operate and make decisions without direct human control.
Remote control controlling a device from another location.
Reconnaissance collecting information about an area or situation.
Surveillance monitoring people, places, or activities for security purposes.
Thermal camera a camera that detects heat and produces thermal images.
Navigation the process of finding and following a route.
Obstacle avoidance technology that allows a drone to detect and avoid objects.
Payload equipment or materials carried by a drone.
Drone delivery transporting goods or supplies using unmanned aerial vehicles.
Authentication checking a user's identity before allowing access.
Encrypted communication protected communication that prevents unauthorised access to data.
Privacy the right to keep personal information and activities protected.
Ground robot an unmanned robot designed to move across land.
Human supervision monitoring and controlling automated systems to ensure safe operation.

Unmanned Drones and the Future of Robotics

Unmanned drones have become one of the most important developments in modern robotics. A drone is an unmanned vehicle that can be controlled remotely or operate partly or completely autonomously. Drones can fly, move across the ground, or operate underwater, but aerial drones are currently the most widely used.

The history of unmanned aerial vehicles is older than many people realise. Early experiments with unmanned aircraft began in the first half of the 20th century. During the Second World War, remotely controlled aircraft were developed for military purposes. Later, improvements in radio communication, cameras, navigation systems, GPS and computer technology made drones smaller, cheaper and more reliable.

For many years, drones were mainly associated with military operations. They were used for reconnaissance, surveillance and intelligence gathering because they could enter dangerous areas without putting pilots at risk. Modern military drones can remain in the air for many hours, collect high-resolution images and transmit information to operators in real time.

Today, drones have many civilian applications. Emergency services use them to search for missing people, monitor disasters and assess damaged buildings. Firefighters can use drones equipped with thermal cameras to locate people in smoke or darkness. Police forces use them for surveillance, traffic monitoring, search-and-rescue operations and documenting crime scenes.

Drones are also becoming important in agriculture. Farmers can use them to photograph fields, monitor crops and identify areas affected by disease, drought or pests. This allows farmers to use water, fertiliser and pesticides more efficiently. In construction, drones can inspect buildings, bridges and other infrastructure without requiring workers to climb dangerous structures.

Another growing application is delivery. Several companies are developing drones that can transport small packages, food and medical supplies. Drone delivery

could be particularly useful in remote areas where roads are poor or where traditional transport is too slow. During emergencies, drones could deliver medicines, blood supplies or other essential equipment to areas that are difficult to reach.

Artificial intelligence is making drones increasingly autonomous. Traditional drones require an operator to control their movements, but AI-powered drones can recognise objects, avoid obstacles, plan routes and respond to changing conditions. Computer vision allows a drone to analyse images, while machine learning can help it improve its ability to navigate and identify objects.

However, autonomous drones also create serious risks. A drone can be hacked, tracked or taken over by an unauthorised user. Attackers could interfere with its navigation system, steal information from its cameras or use it to enter restricted areas. For this reason, drone systems need strong authentication, encrypted communication, secure software and regular updates.

Privacy is another important issue. Drones equipped with cameras can collect images and information about people without their knowledge. Governments and organisations therefore need clear rules about where drones can operate, what data they can collect and how long that data can be stored.

The future of robotics will probably involve cooperation between drones, robots and humans. Instead of operating as separate technologies, drones may work together with ground robots and humanoid robots. For example, an aerial drone could inspect a damaged building, send information to a ground robot, and help the robot navigate inside the building. Human operators could supervise the entire system from a safe location.

In the future, autonomous robotic systems may be used in disaster response, environmental monitoring, healthcare, agriculture, logistics and space exploration. However, technological progress must be accompanied by responsible development. The more autonomous robots become, the more important cybersecurity, human supervision, safety and ethical rules will be.

Exercise 1. Answer the questions.

1. What is an unmanned drone?
2. When did early experiments with unmanned aircraft begin?
3. Why were drones originally important for military operations?
4. How are drones used by emergency services?
5. How can farmers benefit from drones?
6. What makes modern drones more autonomous?
7. What cybersecurity risks can drones face?
8. Why can drones create privacy problems?
9. How could drones work together with ground robots?
10. What areas may use autonomous robotic systems in the future?

Exercise 2. True or False

1. Drones have only been developed for civilian purposes.
2. Military drones can be used for reconnaissance and surveillance.

3. Firefighters can use thermal cameras mounted on drones.
4. Drones cannot be used in agriculture.
5. AI can help drones avoid obstacles.
6. Autonomous drones are completely protected from cyberattacks.
7. Drone cameras can create privacy concerns.
8. Future robots may cooperate with drones.
9. Human supervision will become unnecessary.
10. Drones can be useful during natural disasters.

Exercise 3. Match the application with the example.

Application	Example
1. Agriculture	a. Delivering medicines to remote areas
2. Emergency response	b. Monitoring crops
3. Construction	c. Inspecting bridges
4. Healthcare delivery	d. Searching for missing people
5. Police work	e. Monitoring traffic

Exercise 4. Complete the sentences.

Use the words below.

autonomous • surveillance • thermal • navigation • authentication • privacy

1. Military drones are often used for reconnaissance and _____.
2. _____ cameras can detect heat in darkness or smoke.
3. AI can make drones more _____.
4. GPS and AI can improve drone _____.
5. Strong _____ can prevent unauthorised users from controlling a drone.
6. Camera-equipped drones can create serious _____ concerns.

Task 5. Find the evidence

Find information in the text to support each statement.

1. Drones can reduce risks for human workers.
2. Drones can improve agricultural efficiency.
3. AI makes drones more independent.
4. Drones can become targets of cyberattacks.
5. Future robots may cooperate with each other.

Write **one or two sentences** for each answer.

Task 6. Case Study: Disaster Response

A large industrial building has collapsed after an explosion. The area is dangerous because parts of the building may collapse again. Several people may still be trapped inside.

A rescue organisation has:

- two camera drones;
- one thermal-imaging drone;

- two ground robots;
- one humanoid robot;
- a remote human control centre.

Your task

Design a rescue operation using these technologies.

Decide:

1. Which robot or drone should be used first?
2. What information should the drones collect?
3. How should the ground robots be used?
4. What should the humanoid robot do?
5. What decisions must remain under human control?
6. How should the robotic systems be protected from cyberattacks?

Prepare a **2–3 minute presentation** of your plan.

Task 7. Discussion

Discuss the following questions.

1. Should police be allowed to use drones for continuous surveillance?
2. Would you trust an autonomous drone to deliver medicine?
3. What should happen if an autonomous drone loses contact with its operator?
4. Should drones be allowed to make important decisions without humans?
5. Which profession will be most affected by drones in the future?

UNIT 14. INFORMATION SYSTEMS PROTECTION.

Modern organizations rely heavily on information systems and computer networks to handle daily operations. An **information system (IS)** is a structured set of interconnected components—including hardware, software, data, people, and processes. These systems store, process, and transmit vast amounts of valuable data.

Information systems support operations, knowledge work, and management in organizations.(figure 1)

However, as technology advances, the threats to these networks grow increasingly complex. Protecting these assets requires a combination of advanced software, robust hardware, and smart human behavior.

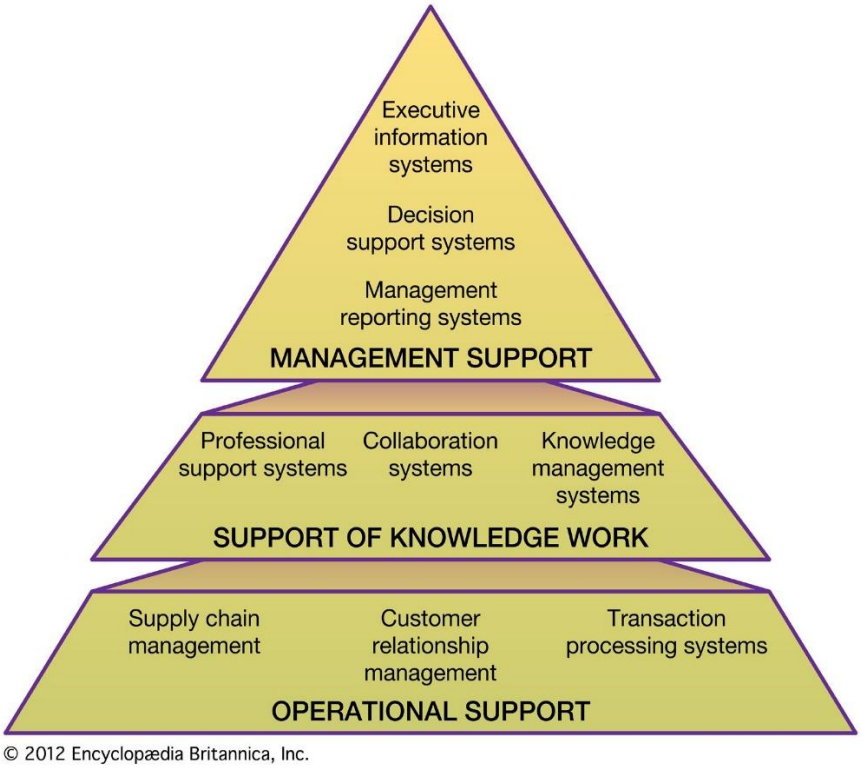
To defend a network effectively, cybersecurity experts implement several layers of protection:

- Firewalls: Hardware or software that monitors and filters incoming and outgoing network traffic.
- Encryption: The process of converting data into unreadable code to prevent unauthorized access.
- Multi-Factor Authentication (MFA): A security system that requires multiple pieces of evidence to verify a user's identity.
- Antivirus Software: Programs designed to detect, block, and remove malicious software like viruses and ransomware.

Cybercriminals continuously develop new methods to breach secure networks. One of the most common threats is **phishing**, where attackers send fraudulent emails to trick employees into revealing sensitive credentials. Another rising danger is ransomware, which locks users out of their systems until a ransom is paid. Additionally, the rise of remote work has expanded the attack surface, making home networks a frequent target for hackers.

Protecting information systems is an ongoing battle. Cybersecurity specialists must constantly monitor networks for unusual activity, perform regular vulnerability assessments, and update security protocols. Because human error remains a leading cause of data breaches, professionals also focus heavily on training staff to recognize social engineering tactics. In this field, staying educated about the latest threat intelligence is essential for survival.

Figure 1.



https://www.britannica.com/topic/information-system

Cloud Computing Security

Today, many organizations store data and run applications in the cloud instead of maintaining their own physical servers. Cloud computing provides flexibility, scalability, and cost savings, but it also introduces new security challenges. Protecting cloud environments requires both cloud service providers and customers to share responsibility for security.

One of the most important aspects of cloud security is **identity and access management (IAM)**. Organizations should ensure that only authorized users can access cloud resources by using strong passwords, multi-factor authentication, and role-based access control. The **principle of least privilege** should be applied so that users receive only the permissions necessary to perform their jobs.

Another critical security measure is **data encryption**. Data should be encrypted both **at rest**, when it is stored, and **in transit**, when it is transmitted over networks. Regular data backups help organizations recover quickly from ransomware attacks, accidental deletion, or hardware failures.

Cloud environments should also be continuously monitored for suspicious activity. Security teams use logging, automated alerts, and security information and event management (SIEM) tools to detect potential threats. Regular security audits, vulnerability scanning, and software updates help reduce the risk of cyberattacks.

Although cloud providers secure the underlying infrastructure, customers remain responsible for protecting their own accounts, applications, and sensitive information. Understanding this **shared responsibility model** is essential for maintaining a secure cloud environment.

Exercise 1. Answer the Questions

1. What are the main components of an information system?
2. Why are firewalls important in network security?
3. What is the purpose of encryption?
4. How does multi-factor authentication improve security?
5. Why has remote work increased cybersecurity risks?
6. What are the benefits of cloud computing?
7. What is the principle of least privilege?
8. Why should data be encrypted both at rest and in transit?
9. What is the shared responsibility model in cloud computing?

Exercise 2 . True or False

Write **T** (True) or **F** (False)

1. Information systems only consist of hardware and software.
2. Firewalls can monitor both incoming and outgoing traffic.
3. Ransomware steals passwords without encrypting files.
4. Multi-factor authentication requires more than one form of verification.
5. Cloud customers are responsible for protecting their own accounts.
6. Security monitoring can help detect suspicious activity.
7. Data backups are useful after ransomware attacks.
8. Cloud providers are responsible for every aspect of customer security.

Match the Terms with Their Definitions

1. Firewall	a. Software that collects and analyzes security events
2. Encryption	b. Protection of data by converting it into unreadable form
3. Phishing	c. Filtering network traffic
4. SIEM	d. Fraudulent attempt to steal information
5. Least privilege	e. Giving users only the permissions they need

D. Complete the Sentences . Use the words below.

firewall • phishing • encryption • ransomware • cloud • authentication • backup • vulnerability

1. A _____ protects a network from unauthorized traffic.
2. _____ converts information into unreadable code.
3. A _____ attack often begins with a fake email.
4. Organizations use _____ to recover lost data.
5. Multi-factor _____ verifies a user's identity.
6. Security experts regularly scan for system _____.
7. Many companies store their data in the _____.
8. _____ can lock users out of their files.

Match the descriptions with the correct cybersecurity term.

1. ____ This security tool scans computers and devices for harmful programs such as viruses, worms, and ransomware. It helps detect, block, and remove malicious software before it can damage the system. Many programs update automatically to recognize new threats. Regular scans improve the security of devices. It is an essential part of everyday cybersecurity.
2. ____ This security technology examines incoming and outgoing network traffic to allow or block connections based on security rules. It helps prevent unauthorized users from accessing a network. Organizations often use it together with other security measures. It can be installed as hardware or software. It is one of the first lines of defense against cyber threats.
3. ____ This process changes readable information into a coded format that can only be understood by authorized users with the correct key. It protects sensitive data while it is stored or transmitted over the internet. Many websites and messaging applications use this technology. It helps prevent unauthorized access to confidential information. Strong algorithms provide a higher level of protection.
4. ____ This security method requires users to prove their identity in more than one way before gaining access to an account or system. For example, a user may enter a password and then confirm a code sent to a mobile phone. It greatly reduces the risk of unauthorized access. Even if one authentication factor is compromised, accounts remain better protected. Many organizations require this security measure for employees and customers.

Choices

A. Encryption
B. Firewall
C. Multi-Factor Authentication (MFA)
D. Antivirus Software
E. Backup
F. Phishing
G. VPN (Virtual Private Network)
H. Spyware

UNIT 15. SECURITY IN WI-FI NETWORKS

Glossary

Wi-Fi network a wireless network that allows devices to connect to the internet without using cables.
Router a device that connects computers and other devices to a network and directs internet traffic.
Wireless signal radio waves that carry data between a router and connected devices.
Encryption the process of converting data into a secure form so that only authorised users can read it.
WPA2 a wireless security standard that protects Wi-Fi networks by encrypting transmitted data.
WPA3 the latest Wi-Fi security standard that provides stronger encryption and better protection than WPA2.
Password a secret combination of letters, numbers, or symbols used to access a device, account, or network.
Administrator account a user account with full permission to manage system or network settings.
VPN a Virtual Private Network that creates an encrypted connection between a device and the internet to protect online privacy.
Public Wi-Fi a wireless network that is available for anyone to use, often in places such as cafés, airports, or hotels.
Hotspot a location or device that provides wireless internet access to nearby devices.
Man-in-the-middle attack a cyberattack in which an attacker secretly intercepts and may alter communication between two parties.
Unauthorized user a person who gains access to a computer system or network without permission.
Network traffic the flow of data sent and received across a computer network

Discuss the questions.

1. Do you usually connect to public Wi-Fi networks? Why or why not?
2. What could happen if a Wi-Fi network is not secure?

How Secure Is Your Wi-Fi Network?

Today, Wi-Fi networks are everywhere. People use them at home, at work, in schools, cafés, airports, and hotels. Wireless Internet allows users to connect laptops, smartphones, tablets, and other devices without cables. Although Wi-Fi is convenient, it also creates security risks if it is not properly protected.

A Wi-Fi router sends and receives data through radio signals. Anyone within the signal range may try to detect the network. If the network is not protected, unauthorized users may connect to it and access shared files, monitor network traffic, or even attack connected devices.

One of the most important methods of protecting a wireless network is encryption. Modern routers usually support WPA2 or WPA3 encryption standards. These technologies convert transmitted data into unreadable code. Even if attackers intercept

the data, they cannot read it without the correct encryption key. WPA3 provides stronger protection than WPA2 because it uses more advanced security features.

A strong Wi-Fi password is another essential security measure. Weak passwords, such as *12345678* or *password*, can be guessed easily by attackers. Security experts recommend using long passwords that combine uppercase and lowercase letters, numbers, and special symbols. Passwords should also be changed regularly and should never be shared with unauthorized people.

Many users forget to change the default administrator password on their wireless router. Manufacturers often use simple default passwords that are publicly available on the Internet. If attackers gain access to the router settings, they can change the network configuration, monitor traffic, or disable security features. Therefore, changing the administrator password immediately after installing a router is an important step in securing a wireless network.

Public Wi-Fi networks present additional risks because anyone can join them. Cybercriminals sometimes create fake Wi-Fi hotspots with names similar to legitimate networks. Unsuspecting users connect to these fake networks and unknowingly send sensitive information directly to attackers. Public Wi-Fi users are also vulnerable to man-in-the-middle attacks, where criminals intercept communication between users and websites.

One way to reduce these risks is by using a Virtual Private Network (VPN). A VPN creates an encrypted connection between the user's device and a secure server. Even when using public Wi-Fi, a VPN helps protect personal information from being intercepted. Users should also avoid online banking, shopping, or entering passwords while connected to unknown public networks.

Wi-Fi security is not only the responsibility of network administrators. Every user plays an important role in protecting wireless networks by choosing strong passwords, updating router software, enabling encryption, and following safe online practices. Good security habits help reduce cyber threats and keep personal and organizational data safe.

Exercise 1. Reading Comprehension

Answer the questions.

1. Why are Wi-Fi networks popular today?
2. How does a router transmit data?
3. What may happen if a Wi-Fi network is not protected?
4. Why is encryption important?
5. What is the difference between WPA2 and WPA3?
6. What makes a password strong?
7. Why should users change the default administrator password?
8. What is a fake Wi-Fi hotspot?
9. How does a VPN improve security?
10. What should users avoid when using public Wi-Fi?

Exercise 2. Match the terms with their definitions.

1. Wi-Fi network	a. a secret code used to connect to a wireless network
2. Router	b. software that protects data sent over the Internet
3. Wireless signal	c. a device that connects a local network to the Internet
4. Password	d. radio waves used to transmit data
5. Encryption	e. technology that converts data into unreadable code
6. Public Wi-Fi	f. someone who uses a computer or network without permission
7. Unauthorized user	g. a wireless network available to everyone
8. VPN	h. a wireless local area network

Exercise 3. True or False

Write **T** (True) or **F** (False).

1. Wi-Fi networks always use cables.
2. WPA3 provides stronger security than WPA2.
3. Weak passwords are difficult to guess.
4. Default router passwords should be changed.
5. Fake Wi-Fi hotspots can steal users' information.
6. VPNs encrypt Internet traffic.
7. Online banking is completely safe on any public Wi-Fi network.
8. Every user is responsible for Wi-Fi security.

Exercise 4. Complete the Sentences

Use the words below.

VPN • router • encryption • password • hotspot • intercepted • wireless • attackers

1. A _____ connects a local network to the Internet.
2. Wi-Fi is a _____ network.
3. _____ protects transmitted information.
4. Users should create a strong _____.
5. Cybercriminals sometimes create fake Wi-Fi _____.
6. Data can be _____ by criminals on insecure networks.
7. A _____ creates an encrypted connection.
8. Strong security makes life more difficult for _____.

Exercise 5. Match the Halves

1. WPA3
2. Public Wi-Fi
3. VPN
4. Router
5. Strong password

a. creates an encrypted Internet connection
b. may expose users to cyber threats
c. should contain letters, numbers, and symbols
d. provides advanced wireless security

e. connects a network to the Internet

Exercise 6. Find the Words in the Text
Find words or phrases in the reading that mean:
1. someone without permission _____
2. secret code protecting data _____
3. people who commit cybercrime _____
4. a network anyone can use _____
5. to stop others from reading information _____

Exercise 7. Discussion
Discuss these questions in pairs.
1. Is public Wi-Fi safe? Why or why not?
2. What mistakes do people often make when using Wi-Fi?
3. Would you recommend using a VPN? Why?
4. What advice would you give to your family about Wi-Fi security?

Exercise 8. Case Study
Maria is working in a café. She connects to a free Wi-Fi network called **Coffee_Free_WiFi**. She logs into her online banking account without using a VPN. She also saves her banking password in the browser.
Answer the questions.
1. What security mistakes did Maria make?
2. What risks does she face?
3. How could she protect herself?
4. Which cybersecurity technologies could help?

Exercise 9. Vocabulary in Context
Choose the correct answer.
1. WPA3 is a type of:
a) malware
b) encryption standard
c) browser
d) operating system
2. A VPN is mainly used to:
a) delete viruses
b) encrypt Internet traffic
c) change passwords
d) update software
3. A fake hotspot is created to:
a) improve Wi-Fi speed
b) steal users' information
c) install antivirus software
d) repair routers

4. Unauthorized users:
a) have permission to access the network
b) access the network without permission
c) create operating systems
d) update routers
5. The administrator password protects:
a) websites
b) router settings
c) browsers
d) email accounts

Exercise 10. Writing
Write **120–150 words** on the following topic:
How can people protect their home Wi-Fi networks?
Include:
- the importance of strong passwords;
- encryption (WPA2/WPA3);
- router updates;
- changing default settings;
- safe use of public Wi-Fi.

Exercise 11.Prepare a 2–3 minute presentation entitled **"Five Ways to Secure a Home Wi-Fi Network.**

UNIT 16. SECURITY IN OPERATING SYSTEMS

Glossary

Operating system (OS) software that manages computer hardware, applications, and user interactions.
Vulnerability a weakness in software that attackers can exploit.
Exploit to use a security weakness for malicious purposes.
Unauthorized access entering a system or network without permission.
Security patch a software update that fixes known security weaknesses.
Administrator account an account with full control over the operating system.
Standard user account an account with limited permissions for everyday computer use.
Access control a system that manages who can use files and resources.
File permissions rules that determine who can view or change files.
Firewall software that blocks unauthorized network connections.
Secure boot a security feature that prevents unauthorized software from starting.
Cyber hygiene safe habits that help protect computers and data from cyber threats.

Discuss the questions.
1. Which operating system do you use most often?
2. Why do operating systems need regular updates?

3. What could happen if an operating system is not protected?
4. Which operating system do you think is the most secure? Why?

Why Operating System Security Matters

Every computer, smartphone, and server uses an operating system (OS). Popular operating systems include Microsoft Windows, Linux, macOS, Android, and iOS. The operating system manages hardware resources, controls software applications, and allows users to interact with their devices. Because it controls the entire system, protecting the operating system is one of the most important tasks in cybersecurity.

Cybercriminals often search for vulnerabilities in operating systems. A vulnerability is a weakness in software that attackers can exploit to gain unauthorized access, steal information, or install malicious software. Software developers regularly discover new vulnerabilities, which is why operating systems require frequent security updates.

Software vendors release security patches to fix known vulnerabilities. Installing these patches as soon as possible helps reduce the risk of cyberattacks. Many operating systems can download and install updates automatically, ensuring that users receive the latest security improvements without delay.

User accounts also play an important role in operating system security. Most systems provide different permission levels. Administrator accounts have full control over the system, while standard user accounts have limited privileges. Cybersecurity experts recommend using a standard account for everyday activities and an administrator account only when system changes are necessary. This approach limits the damage that malware can cause if a user's account is compromised.

Another important security feature is access control. Operating systems allow administrators to define who can access files, folders, applications, and network resources. Proper file permissions prevent unauthorized users from viewing, modifying, or deleting sensitive information.

Modern operating systems also include built-in security tools such as firewalls, encryption, secure boot, and antivirus protection. However, these tools cannot provide complete security if users ignore basic cyber hygiene. Downloading software from untrusted websites, opening suspicious email attachments, or disabling security features can make even the most secure operating system vulnerable.

Keeping an operating system secure requires both technology and responsible user behaviour. Regular updates, strong passwords, careful management of user accounts, and safe browsing habits all help reduce security risks. Together, these practices create a safer computing environment for individuals and organizations.

Exercise 1. Reading Comprehension

Answer the questions.

1. What is the main function of an operating system?
2. What is a vulnerability?
3. Why are security patches important?
4. Why should updates be installed quickly?

5. What is the difference between an administrator account and a standard user account?
6. What is access control?
7. Why are file permissions important?
8. Name four built-in security features mentioned in the text.
9. What user actions can make an operating system less secure?
10. According to the text, who is responsible for operating system security?

Exercise 2. Match the terms with their definitions.

1. Operating system (OS)	a. a weakness that attackers can exploit
2. Vulnerability	b. a program that manages computer hardware and software
3. Security patch	c. a software update that fixes security problems
4. Administrator account	d. an account with full system privileges
5. User account	e. an account with limited permissions
6. Access control	f. rules that determine who can use system resources
7. File permissions	g. settings that define who can read or modify files
8. Software update	h. installation of a newer version of software
9. Malware	i. malicious software designed to damage a system
10. Authentication	j. verification of a user's identity

Exercise 3. True or False

Write **T** (True) or **F** (False).

1. Every computer uses an operating system.
2. Vulnerabilities strengthen computer security.
3. Security patches fix known weaknesses.
4. Administrator accounts have limited privileges.
5. Standard user accounts are safer for daily work.
6. File permissions control access to information.
7. Firewalls are built into many operating systems.
8. Users should disable security features whenever possible.

Exercise 4. Complete the Sentences Use the words below.

updates • administrator • vulnerabilities • permissions • malware • authentication • operating system • access

1. Every computer has an _____.
2. Security _____ fix software weaknesses.
3. Attackers search for _____.
4. An _____ account has full control.
5. File _____ determine who can modify data.
6. _____ verifies the identity of a user.
7. Poor security allows _____ to infect a computer.
8. _____ control limits who can use system resources.

Exercise 5. Match the Halves

1. Security patches
2. Administrator account
3. Access control
4. File permissions
5. Standard user account

a. limits everyday privileges
b. fixes software vulnerabilities
c. controls access to files
d. has full system privileges
e. determines who can use resources

Exercise 6. Multiple Choice

Choose the correct answer.

1. A vulnerability is

a) a security update
b) a weakness in software
c) a password
d) a firewall

2. A security patch

a) creates malware
b) fixes software problems
c) changes passwords
d) deletes files

3. Access control helps

a) increase Internet speed
b) manage user permissions
c) remove viruses
d) create backups

4. Standard user accounts

a) have full administrative rights
b) are recommended for everyday work
c) disable security
d) install operating systems

5. Which action increases security?

a) Ignoring updates
b) Using weak passwords
c) Installing security patches
d) Disabling antivirus software

Exercise 7. Case Study

David downloads free software from an unknown website. During installation, he disables the antivirus program because it reports a warning. He is logged in using an

administrator account. Two days later, his computer becomes slow, and some files disappear.

Answer the questions.

1. Which mistakes did David make?
2. How could malware enter the system?
3. Why was using an administrator account risky?
4. What should David have done differently?
5. Which cybersecurity practices from the reading would have prevented the problem?

Exercise 8. Discussion

Discuss with a partner.

1. Why should software updates never be ignored?
2. Is it safe to download software from unknown websites?
3. Should students use administrator accounts every day? Why?
4. Which operating system security feature do you think is the most important?

Exercise 9. Write 120–150 words.

Explain why regular operating system updates are essential for cybersecurity. Give at least three reasons and examples.

UNIT 17. MALICIOUS SOFTWARE AND CYBER HYGIENE

Discuss the questions.

1. Have you ever had a computer virus?
2. How can malware enter a computer?
3. What is cyber hygiene?
4. Which security practices do you follow every day?

Vocabulary

Exercise 1. Match the terms with their definitions.

1. Malware	a. software that protects computers from malicious programs
2. Virus	b. software that secretly collects user information
3. Worm	c. harmful software designed to damage or disrupt systems
4. Trojan	d. malicious software disguised as a legitimate program
5. Ransomware	e. malware that encrypts files and demands payment
6. Spyware	f. malware that spreads by attaching itself to files
7. Antivirus software	g. malware that spreads automatically across networks
8. Phishing	h. fake messages designed to steal personal information
9. Backup	i. a copy of important data
10. Cyber hygiene	j. safe habits that reduce cybersecurity risks

Cyber Hygiene: Your First Line of Defence

Glossary

Malware software designed to damage systems or steal information.
Virus malware that spreads by attaching itself to files or programs.
Worm malware that spreads automatically through computer networks.
Trojan malware disguised as legitimate software to trick users.
Ransomware malware that encrypts files and demands payment for recovery.
Spyware malware that secretly collects personal or sensitive information.
Phishing a cyberattack using fake messages to steal information or install malware.
Cyber hygiene safe online practices that reduce cybersecurity risks.
Antivirus software software that detects, blocks, and removes malware.
Multi-factor authentication (MFA) a security method requiring multiple forms of identity verification.
Backup a copy of data used to restore lost files.
Removable USB drive a portable storage device used to transfer computer files.

Modern computers and mobile devices face many cybersecurity threats every day. One of the greatest dangers is **malicious software**, commonly called **malware**. Malware is any software created to damage computers, steal information, interrupt services, or give attackers unauthorized access to a system. Individuals, businesses, and governments all face the risk of malware infections.

There are several common types of malware. A **virus** attaches itself to files or programs and spreads when infected files are opened. A **worm** can copy itself and spread automatically through computer networks without user action. A **Trojan** looks like a legitimate application but secretly installs malicious code after the user opens it. **Ransomware** encrypts files and demands payment before allowing users to access their data again. Another common threat is **spyware**, which secretly monitors user activity and collects passwords, personal information, or financial data.

Cybercriminals use different methods to distribute malware. One of the most common methods is **phishing**. Attackers send emails or messages that appear to come from trusted organizations, asking users to click a link or download an attachment. If the user opens the file, malware may be installed immediately. Malware can also spread through infected websites, fake software downloads, removable USB drives, and unsecured networks.

Good **cyber hygiene** helps prevent many malware infections. Users should always keep their operating systems and applications updated because software updates often fix security vulnerabilities. Installing reliable antivirus software provides another important layer of protection by detecting and removing malicious programs. Regularly scanning computers helps identify threats before they cause serious damage.

Strong passwords are another essential part of cyber hygiene. Passwords should be unique, difficult to guess, and changed when necessary. Multi-factor authentication (MFA) provides additional security by requiring more than one method of identity verification.

Creating regular **backups** is also very important. If ransomware encrypts important files, users can restore their data from a backup instead of paying criminals. Backups should be stored separately from the main computer, such as on an external drive or in secure cloud storage.

Cyber hygiene is not only about technology. It also depends on responsible user behaviour. People should avoid clicking suspicious links, downloading software from unknown websites, or sharing personal information with unverified sources. By combining secure technology with safe online habits, users can significantly reduce the risk of malware infections and protect both personal and organizational data.

Exercise 1. Reading Comprehension

Answer the questions.

1. What is malware?
2. What is the difference between a virus and a worm?
3. How does a Trojan infect a computer?
4. What does ransomware do?
5. What information can spyware collect?
6. What is phishing?
7. Why should users install software updates?
8. Why are backups important?
9. What is cyber hygiene?
10. Name four good cyber hygiene practices mentioned in the text.

Exercise 2. True or False

Write **T** (True) or **F** (False).

1. Malware is designed to protect computers.
2. Worms can spread automatically through networks.
3. Trojans always look suspicious.
4. Spyware collects information secretly.
5. Phishing emails often appear to come from trusted organizations.
6. Software updates may improve security.
7. Backups help recover data after ransomware attacks.
8. Cyber hygiene only depends on antivirus software.

Exercise 3. Complete the Sentences

Use the words below.

malware • phishing • antivirus • backups • ransomware • spyware • virus • updates

1. A _____ attaches itself to files.
2. _____ encrypts files and demands payment.
3. _____ secretly collects personal information.
4. Users should install software _____ regularly.
5. _____ software detects malicious programs.
6. _____ are copies of important data.
7. _____ emails try to steal information.

8. Good cyber hygiene helps prevent _____ infections.

Exercise 4. Match the Halves

1. Virus
2. Worm
3. Trojan
4. Ransomware
5. Backup

a. spreads automatically through networks
b. protects data after an attack
c. encrypts files for money
d. attaches itself to files
e. pretends to be legitimate software

Exercise 5. Multiple Choice

Choose the correct answer.

1. Which type of malware encrypts files?

a) Spyware
b) Virus
c) Ransomware
d) Worm

2. Which malware collects personal information?

a) Spyware
b) Firewall
c) VPN
d) Patch

3. Phishing usually arrives through

a) USB cables
b) emails or messages
c) operating systems
d) printers

4. Which action improves cyber hygiene?

a) Ignoring updates
b) Using weak passwords
c) Installing antivirus software
d) Downloading software from unknown websites

5. A backup is

a) a virus
b) a copy of important data
c) an operating system
d) a firewall

Exercise 6. Case Study

Emma receives an email saying that her parcel cannot be delivered unless she opens an attached document. The email looks genuine, so she opens the attachment. A few minutes later, all her files become inaccessible, and a message demands payment in cryptocurrency to restore them.

Answer the questions.

1. Which cyberattack did Emma experience?
2. How did the malware infect her computer?
3. Which type of malware is responsible?
4. What could Emma have done to prevent the attack?
5. How would regular backups help in this situation?

Exercise 7. Discussion

Discuss the questions with a partner.

1. Why do people still fall for phishing attacks?
2. Which type of malware do you think is the most dangerous? Why?
3. How often should people back up their files?
4. Which cyber hygiene habits are most important for students?

Exercise 8. Write **120–150 words**.

Describe five cyber hygiene practices that every computer user should follow to protect personal information and devices from malware.

Exercise 9. Prepare a 3-minute presentation entitled **"How to Stay Safe Online: Good Cyber Hygiene Practices.**

UNIT 18. REVISION UNITS 10–17

Part 1. Vocabulary Revision

Task 1. Match the terms with their definitions.

1. Artificial intelligence
2. Machine learning
3. Humanoid robot
4. Unmanned drone
5. Network traffic
6. Encryption
7. Vulnerability
8. Security patch
9. Malware
10. Phishing
11. Ransomware
12. Cyber hygiene
13. Authentication
14. Firewall
15. Anomaly
16. False positive

a. software designed to damage a system or steal information
b. a weakness that attackers can exploit
c. a robot designed to resemble a human
d. a method of protecting data by converting it into a secure form
e. a system that checks a user's identity
f. AI that learns from data
g. a security update that fixes software weaknesses
h. an automated aerial vehicle
i. unusual activity that differs from normal behaviour
j. safe practices that reduce cybersecurity risks
k. malicious software that encrypts files and demands payment
l. technology that enables machines to perform intelligent tasks
m. data moving through a computer network
n. a system that blocks unauthorised network connections
o. a cyberattack using fake messages to obtain information
p. a harmless activity incorrectly identified as a threat

Task 2. Complete the sentences. Use the words below.
AI • encryption • vulnerability • malware • firewall • authentication • drone • ransomware • anomaly • cyber hygiene

1. Strong _____ protects sensitive information from unauthorised users.
2. A security system detected an unusual _____ in the network traffic.
3. The company uses multi-factor _____ to protect administrator accounts.
4. The security team discovered a serious _____ in the operating system.
5. The organisation's _____ blocked the suspicious connection.
6. Regular updates are an important part of good _____.
7. The police used a _____ to search the area from the air.
8. The infected computer was attacked by _____.
9. The hospital uses _____ to analyse medical data.
10. The company restored its files after a _____ attack.

Part 2. Reading Revision

AI and the Future of Cybersecurity

Artificial intelligence is changing both robotics and cybersecurity. Modern AI systems can analyse enormous amounts of information, identify unusual behaviour and assist security professionals in detecting cyberattacks. At the same time, criminals can use AI to automate phishing campaigns, create convincing fake content and develop more sophisticated malware.

AI is also transforming robotics. Humanoid robots can use computer vision, sensors and machine learning to understand their environment and perform physical tasks. Unmanned drones can monitor large areas, transport equipment and assist emergency services. In the future, drones, ground robots and humanoid robots may work together as a single automated system.

However, connected robots and drones create new security risks. If attackers gain access to a robotic system, they may steal information, interfere with its operation or control it remotely. Strong authentication, encrypted communication, secure software and regular updates are therefore essential.

Information systems also require protection against more traditional threats. Operating systems must receive security patches, while user accounts should have appropriate permission levels. Firewalls can control network connections, and antivirus software can detect malicious programs. Users must also practise good cyber hygiene by using strong passwords, avoiding suspicious links and keeping their software updated.

One of the biggest challenges for cybersecurity professionals is the speed of technological change. AI systems can process information much faster than humans, but they can also make mistakes. A false positive may cause harmless activity to be treated as a threat, while an undetected attack can result in serious damage.

The future of cybersecurity will therefore depend on both advanced technology and human expertise. AI, robots and automated security systems can perform many tasks, but humans will continue to be responsible for important decisions, ethical questions and strategic planning.

Task 3. Answer the questions.

1. How can AI help cybersecurity professionals?
2. How can criminals use AI?
3. What technologies allow humanoid robots to understand their environment?
4. How might drones and robots work together in the future?
5. What could happen if a robotic system is hacked?
6. Why are security patches important?
7. What is a false positive?
8. Why will human expertise remain important?

Task 4. Find words in the text that mean:

1. very large in amount
2. unusual
3. connected to a network
4. permission to use a system
5. harmful software
6. protection against computer attacks
7. mistakes or incorrect results
8. information collected by a system

Part 3. Grammar Revision

English Verb Tenses

Task 5. Choose the correct tense.

1. Cybersecurity specialists usually _____ network traffic carefully.

a) monitor

b) are monitoring
c) have monitored
d) monitored

2. The technician _____ the security patch yesterday.
a) installs
b) has installed
c) installed
d) was installing

3. The security team _____ the network when the attack started.
a) monitors
b) monitored
c) was monitoring
d) has monitored

4. The company _____ several vulnerabilities this week.
a) has discovered
b) discovered
c) was discovering
d) discovers

5. The hackers _____ the system for several hours before they were detected.
a) attacked
b) have attacked
c) had been attacking
d) are attacking

6. AI systems _____ cybersecurity for many years by 2030.
a) will improve
b) will have improved
c) improved
d) have improved

7. By next month, the company _____ the new security system.
a) will implement
b) implements
c) will have implemented
d) implemented

8. The researchers _____ the robot since early morning.
a) have been testing
b) tested
c) are testing
d) had tested

9. When the administrator arrived, the malware _____ several files.
a) has encrypted
b) had encrypted
c) encrypts
d) will encrypt

10. At 10 p.m. tomorrow, the security team _____ the new firewall.
a) will test
b) tested
c) will be testing
d) has tested

Task 6. Complete the sentences with the correct form of the verb.
1. Cybercriminals often _____ (use) phishing emails to attack users.
2. The security team _____ (investigate) the incident at the moment.
3. The company _____ already _____ (install) the latest security patch.
4. The technician _____ (repair) the server when the power failed.
5. The attackers _____ (steal) sensitive data before the breach was discovered.
6. The researchers _____ (test) the AI system for three months.
7. By the end of the year, the organisation _____ (upgrade) all its operating systems.
8. At this time tomorrow, the engineers _____ (monitor) the network.
9. The robot _____ (work) for six hours before its battery ran out.
10. By 2035, AI _____ (transform) many areas of cybersecurity.

Task 7. Identify the tense.
Write the name of the tense.
1. The administrator checks the logs every morning.
2. The engineers are testing a new security system.
3. The company has updated its software.
4. The security team has been monitoring the network for two hours.
5. The hacker accessed the server yesterday.
6. The police were investigating the cyberattack.
7. The attackers had deleted the files before the investigation began.
8. The team had been analysing the data for several hours.
9. The company will introduce a new firewall next month.
10. The engineers will be testing the system tomorrow.
11. The organisation will have completed the upgrade by Friday.
12. By next year, researchers will have been developing the system for five years.

Part 4. Present Tenses
Task 8. Choose the correct form.
1. AI systems **analyse / are analysing** millions of data points every second.
2. The security team **checks / is checking** the network right now.
3. The company **has introduced / introduces** a new authentication system this month.
4. Researchers **have been studying / study** AI security for several years.
5. The drone **is transmitting / transmits** video at the moment.
6. Cybercriminals **have developed / develop** new methods of attack recently.

Part 5. Past Tenses

Task 9. Complete the sentences.

1. The first industrial robots _____ (appear) in factories decades ago.
2. The security team _____ (monitor) the network when the attack occurred.
3. The hacker _____ already _____ (gain) access before the administrator noticed.
4. The researchers _____ (test) the drone for several hours before the accident.
5. The company _____ (release) a security patch last week.
6. The police _____ (investigate) the cyberattack when they discovered another vulnerability.

Part 6. Future Tenses

Task 10. Choose the correct future form.

1. In the future, robots _____ more tasks independently.

a) will perform
b) performed
c) have performed

2. By 2030, many companies _____ AI-based security systems.

a) will have adopted
b) adopt
c) adopted

3. At this time tomorrow, the engineers _____ the new drone.

a) will be testing
b) test
c) have tested

4. By next year, researchers _____ the technology for five years.

a) will have been developing
b) developed
c) are developing

Part 7. Modal Verbs

Task 11. Choose the correct modal verb.

1. Users _____ install security updates regularly.

a) should
b) might
c) would

2. An administrator _____ have full access to the system.

a) must
b) can
c) may

3. A hacker _____ exploit an unpatched vulnerability.

a) might
b) should
c) ought

4. Companies _____ protect sensitive personal information.
a) must
b) could
c) might
5. AI _____ make mistakes when analysing complex data.
a) can
b) must
c) should
6. Employees _____ open suspicious email attachments.
a) mustn't
b) don't have to
c) might
7. The security team _____ investigate the unusual network activity.
a) should
b) can't
c) wouldn't
8. A drone _____ be controlled remotely or autonomously.
a) can
b) mustn't
c) shouldn't

Task 12. Complete the sentences with a suitable modal verb.
1. Users _____ use strong and unique passwords.
2. Organisations _____ update operating systems regularly.
3. Cybersecurity professionals _____ monitor unusual network activity.
4. Hackers _____ exploit an unprotected Wi-Fi network.
5. Employees _____ share their passwords with other people.
6. An autonomous robot _____ make a wrong decision.
7. Security experts _____ investigate a serious breach immediately.
8. Companies _____ use encryption to protect sensitive information.

Part 8. Mixed Grammar Revision
Task 13. Choose the correct answer.
1. The cybersecurity team _____ the network for three hours when they discovered the attack.
a) monitored
b) had been monitoring
c) has monitored
d) will monitor
2. The company _____ its operating systems every month.
a) updates
b) is updating
c) updated
d) has updated

3. Look! The drone _____ towards the damaged building.
a) flies
b) flew
c) is flying
d) has flown
4. The technician _____ the vulnerability yesterday.
a) has identified
b) identifies
c) identified
d) is identifying
5. By next Friday, the engineers _____ the new security system.
a) will install
b) installed
c) will have installed
d) install
6. The hackers _____ access to the server before the firewall blocked them.
a) had gained
b) gain
c) have gained
d) were gaining
7. AI systems _____ become more important in cybersecurity in the future.
a) have
b) will
c) were
d) had
8. The security team _____ the suspicious activity since 6 a.m.
a) monitors
b) monitored
c) has been monitoring
d) had monitored
9. Companies _____ ignore critical security updates.
a) should
b) mustn't
c) can
d) may
10. The robot _____ complete the task without human supervision in the future.
a) might
b) mustn't
c) shouldn't
d) can't

Part 9. Error Correction
Task 14. Find and correct the mistake.
1. The company is use AI to detect cyberattacks.

2. The hackers have attacked the server yesterday.
3. The security team was monitor the network when the alarm sounded.
4. By next year, the company will have upgrade all its systems.
5. Users must to install security updates.
6. The robot can to identify objects using computer vision.
7. The researchers have been test the drone since Monday.
8. The administrator had already left when the attack has started.

Part 10. Final Revision Task

Task 15. Complete the text.

Use the correct tense or modal verb.

The Future of Cybersecurity

Cybersecurity _____ (change) rapidly over the last decade. Artificial intelligence _____ already _____ (become) an important tool for security professionals. Today, AI systems _____ (analyse) enormous amounts of network traffic and _____ (identify) unusual behaviour.

However, cybercriminals _____ also _____ (use) AI to improve their attacks. Security experts believe that this competition _____ (continue) in the future.

By 2035, organisations probably _____ (use) much more advanced AI security systems. Security professionals _____ also _____ (work) with robots and autonomous drones.

However, organisations _____ (not / ignore) human supervision. AI systems _____ (make) mistakes, so cybersecurity specialists _____ (check) important decisions.

If organisations want to remain secure, they _____ (must / should) combine advanced technology with responsible human decision-making.

Task 16. Speaking: The Future of Cybersecurity

Work in groups. Discuss the following situation:

It is 2035. Your organisation uses AI, humanoid robots, autonomous drones and advanced information systems.

Prepare a short presentation explaining:

1. How AI protects the organisation.
2. How humanoid robots are used.
3. How drones support security.
4. How Wi-Fi networks are protected.
5. How operating systems are secured.
6. How malware is detected.
7. What role human cybersecurity specialists have.
8. What could happen if the systems are attacked.

Try to use **at least six different English tenses** and **four modal verbs**.

REFERENCES

1. Anthropic. (2026). *Claude Mythos and the future of AI-powered vulnerability discovery*. Anthropic. Available at: https://www.anthropic.com/
2. CISA. (2023). *#StopRansomware Guide*. Cybersecurity and Infrastructure Security Agency. Available at: #StopRansomware Guide
3. Cybersecurity and Infrastructure Security Agency (CISA). *Cybersecurity resources and best practices*. Available at: CISA Cybersecurity Resources
4. ENISA. (2025). *ENISA Threat Landscape 2025*. European Union Agency for Cybersecurity. Available at: ENISA Threat Landscape 2025
5. Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Publications Office of the European Union. Available at: Internet Organised Crime Threat Assessment (IOCTA) 2024
6. Europol. (2025). *The changing DNA of serious and organised crime: EU Serious and Organised Crime Threat Assessment 2025*. Publications Office of the European Union. Available at: EU-SOCTA 2025
7. Kovacs, E. (2026, May 25). *Anthropic: Mythos Detected 23,000 Potential Vulnerabilities Across 1,000 OSS Projects*. SecurityWeek. Available at: SecurityWeek article
8. National Cyber Security Centre. (2022). *Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion*. UK Government. Available at: NCSC – Russia behind cyber attack with Europe-wide impact
9. National Institute of Standards and Technology. (2024). Pascoe, C., Quinn, S., & Scarfone, K. *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper 29. Available at: NIST Cybersecurity Framework (CSF) 2.0
10. National Institute of Standards and Technology. (2024). Rigopoulos, K., Quinn, S., Pascoe, C., Marron, J., Mahn, A., & Topper, D. *NIST Cybersecurity Framework 2.0: Resource & Overview Guide*. NIST Special Publication 1299. Available at: NIST CSF 2.0 Resource & Overview Guide
11. OWASP Foundation. (2025). *OWASP Top 10: The Ten Most Critical Web Application Security Risks*. Available at: OWASP Top 10
12. OWASP Foundation. *OWASP Web Security Testing Guide*. Available at: OWASP Web Security Testing Guide
13. MITRE. *ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge*. Available at: MITRE ATT&CK
14. MITRE. *Common Vulnerabilities and Exposures (CVE)*. Available at: MITRE CVE
15. FIRST. *Common Vulnerability Scoring System (CVSS)*. Forum of Incident Response and Security Teams. Available at: FIRST CVSS
16. IBM. *What is cybersecurity?* IBM. Available at: IBM Cybersecurity
17. Microsoft. *Microsoft Security*. Available at: Microsoft Security
18. Google. *Google Safety Center: Security*. Available at: Google Security
19. Cloudflare. *Learning Center: Cybersecurity*. Cloudflare. Available at: Cloudflare Learning Center

20. Cisco. *Cybersecurity*. Cisco. Available at: Cisco Cybersecurity
21. International Telecommunication Union. *Global Cybersecurity Index*. ITU. Available at: ITU Global Cybersecurity Index
22. European Union Agency for Cybersecurity (ENISA). *Cybersecurity*. Available at: ENISA
23. INTERPOL. *Cybercrime*. International Criminal Police Organization. Available at: INTERPOL Cybercrime
24. Council of Europe. *Cybercrime Programme Office (C-PROC)*. Available at: Council of Europe – Cybercrime Programme Office
25. United Nations Office on Drugs and Crime. *Cybercrime*. UNODC. Available at: UNODC Cybercrime
26. National Police of Ukraine. *Cyber Police Department*. Available at: Cyber Police of Ukraine
27. Computer History Museum. *Computer History Museum*. Available at: Computer History Museum
28. Encyclopaedia Britannica. *Artificial Intelligence*. Available at: Encyclopaedia Britannica – Artificial Intelligence
29. Encyclopaedia Britannica. *Computer*. Available at: Encyclopaedia Britannica – Computer
30. National Institute of Standards and Technology. *Post-Quantum Cryptography*. NIST. Available at: NIST Post-Quantum Cryptography
31. National Institute of Standards and Technology. *Computer Security Resource Center (CSRC)*. Available at: NIST Computer Security Resource Center
32. Internet Engineering Task Force. *RFCs – Internet Engineering Task Force*. Available at: IETF RFCs
33. National Cyber Security Centre. *Guidance and resources*. UK Government. Available at: NCSC Guidance
34. Verizon. (2025). *2025 Data Breach Investigations Report*. Verizon. Available at: Verizon Data Breach Investigations Report
35. Mandiant. *M-Trends: Cybersecurity insights and threat intelligence*. Google Cloud. Available at: Mandiant M-Trends
36. Microsoft. *Microsoft Digital Defense Report*. Available at: Microsoft Digital Defense Report
37. Google Cloud. *Threat Horizons*. Available at: Google Cloud Threat Horizons
38. SANS Institute. *Cybersecurity Training and Resources*. Available at: SANS Institute
39. CERT-UA. *Computer Emergency Response Team of Ukraine*. State Service of Special Communications and Information Protection of Ukraine. Available at: CERT-UA
40. State Service of Special Communications and Information Protection of Ukraine. *Cybersecurity*. Available at: SSSCIP of Ukraine
41. **CyberPol English. Англійська мова для фахівців кіберполіції**: навч. посіб. / В. В. Кочина, О. О. Статівка; Харків. нац. ун-т внутр. справ. — Кам'янець-Подільський: ХНУВС, 2026. 254 с.