MINISTRY FOR DEVELOPMENT OF INFORMATION TECHNOLOGIES
AND COMMUNICATION OF THE REPUBLIC OF UZBEKISTAN

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES
NAMED AFTER MUHAMMAD AL-KHWARIZMI

ABDUVAKHABOVA D.N.

English in Cyber security

**Course book for undergraduate students majoring in
5330300-Informartion security**

Tashkent 2020

LBC

D.N.Abduvakhabova. English in Cyber security–T.:«ALOQACHI»,2020,192 pages.

ISBN

“English in Cyber security ” is accessible for intermediate level students and above of the Information security specialization. This book includes exercises for developing reading, writing and speaking skills. It aims to help these students to extend and develop a wide variety of language skills and to acquire a knowledge of cyber security in English.

LBC Reviewers:

– PhD docent. N.Tukhtakhodjayeva

– PhD docent. A.Sharipova

ISBN

CONTENTS

PREFACE

"English in Cyber security" is dedicated to students of the Information security specialization.

The purpose of the course book is to form profession-oriented competence of students, enlarge their professional vocabulary and improve their academic English. It aims to help these students to extend and develop a wide variety of language skills and to acquire a knowledge of cyber security in English. Reach selection of motivating and informative, authentic and semi-authentic texts to improve both reading and listening skills with variety topics are presented in themed topics.

The book consists of 12 topical lessons and each lesson starts with colorful lead-in activity shifting students' focus on the topic. Lead-in activity followed by listening and speaking, reading and writing activities respectively. As well as these aspects, there is a range of material which can be used according to student's needs and time available. Students are given useful language to keep changing the phrases they use to express their opinion, agreement and disagreement.

All texts are adapted from scientific articles and refer to students' specialization.

Map of the book

Lesson	Speaking	Listening
1.Cyber security	The differences between Cyber security and Info security	Types of Cyber security
2.Cryptography	Importance of cryptography	What is cryptography
3. Symmetric and asymmetric cryptosystems	The differences between symmetric and asymmetric key cryptography	Cryptosystems
4. Authentication	What’s authentication	How authentication is used
5. Password retention and password attacks.	Discussing various attacks on password	Digital keys
6.Encrypt files and disks	Hardware and software encryption	Full Disk Encryption
7. Network security vulnerabilities and threats	Discussing about network security threats	Computer security
8. Wireless network security	Discussing about the best security mode for WiFi	The importance of wireless security
9. Recovery and backup of data and information	Explaining why is data recovery important	The phases of date recovery
10. Information security policy and its management	The types of security policies	Information security concept is being developed in Uzbekistan
11. Risk management	Discussing about the Importance of risk management	5 steps of risk management process
12.Cyber crime	Describing pictures about Cyber crime	What is Cyber crime

Reading	Writing	Grammar
Common Cyber security measures	About myself	Present Simple Tense
History of Cryptography	CV	Present Continuous Tense
Symmetric and asymmetric encryption	A letter to a friend	Article
Authentication and authorization	A description	Have/have got
A social engineering attack	An application letter	Comparative and Superlative Adjectives
What Is Encryption	A complaint letter	Future Simple Tense
Passive and active threats	E- mail	Past Simple Tense
Why Is Wireless Network Security A Concern?	A summary	Present Perfect Tense
Importance of Backup and Recovery	A composition	Modal verbs: can, must, may
Why is network security policy management necessary?	A review	Verb patterns
Threat Identification	An opinion essay	Voice (Active/Passive)
How Cyber Crime Has Evolved	A report	Relative clause

LESSON 1. CYBER SECURITY

1.In pairs discuss these questions.

1.How would you define Cyber security?

2.What are the differences between Cyber security and Info security?

3. What are the elements of cybersecurity?

2.Match the words with their definitions.

Word/Term	Definition
1. patch	a. a string of characters that allows access to a computer system or service
2. cyberattack	b. the state of being free from public attention
3.password	c. An update or change or an operating system or application.
4. malicious	d. the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.
5.domain	e. an attempt by hackers to damage or destroy a computer network or system.
6.bug	f. characterized by malice; intending or intended to do harm
7.cybersecurity	g. an error, flaw or fault in a computer program or system that causes it to produce an incorrect or unexpected result
8.Spyware	h. Anything used as part of a security response strategy which addresses a threat in order to reduce risk.

9.security control	i. an area of territory owned or controlled by a particular ruler or government.
10.privacy	j. software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive

1	2	3	4	5	6	7	8	9	10

T. 1.1 Listen and check your answers and pronunciation.

T. 1.2 Listen about Cyber security and complete the table.

Types of Cyber security	keywords
1.Information Security	________________ ________________
2.Network Security	________________ ________________
3.Application Security	________________ ________________

T.1.3 Listen again about Cyber security and complete the sentences with ONE or TWO words.

Cyber Security is classified into the following types:

1.Information Security

Information security aims to protect the users' private information from unauthorized access,1________________. It protects the privacy of data and hardware that handle, store and transmit that data. Examples of Information security include User 2________________and Cryptography.

2.Network Security

Network security aims to protect the usability,3______________, and safety of a network, associated components, and data shared over the network. When a network is secured, potential threats gets blocked from entering or spreading on that network. Examples of 4_________________ includes Antivirus and 5_______________ programs, Firewall that block unauthorized access to a network.

3.Application Security

Application security aims to protect software applications from vulnerabilities that occur due to the flaws in application design, development, 6.______________, upgrade or maintenance phases.

5.When you read a text, you will often see a new word that you don't recognize. If you can identify what type of word it is (noun, verb, adjective, etc.) It can help you guess the meaning.

Find the words (1-10) in the text above. Can you guess the meaning from context? Are they nouns, verbs, adjectives or adverbs? Write n, v, adj. or adv. next to each word.

1.protecting______	2.security________
3.innovative______	4.enforce_________
5.restrict_________	6.application______
7.attachments_____	8.effectively______
9.malware________	10.detect_________
11.malicious______	12.slips__________

6.Read the text and translate into your native language. If necessary use a dictionary.

Common Cyber security measures

Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Implementing effective cyber security measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative. Essential cyber security measures:

1.Use strong passwords. Strong passwords are vital to good online security.

2.Create a password policy for your business to help staff follow security best practice. Look into different technology solutions to enforce your password policy.

3.Control access. Make sure that individuals can only access data and services for which they are authorized. For example, you can:

-control physical access to premises and computers network;

-restrict access to unauthorized users;

-limit access to data or services through application controls;

-restrict what can be copied from the system and saved to storage devices;

-limit sending and receiving of certain types of email attachments.

Modern operating systems and network software will help you to achieve most of this, but you will need to manage the registration of users and user authentication systems - passwords.

4.Put up a firewall. Firewalls are effectively gatekeepers between your computer and the internet, and one of the major barriers to cyber threats such as viruses and malware. Make sure that you set up your firewall devices properly or they may not be fully effective. Read more about firewalls in server security.

5.Use security software. You should use security software, such as anti-spyware and anti-virus programs, to help detect and remove malicious code if it slips into your network. Discover how to detect spam, malware and virus attacks.

(techtarget.com/tutorial/Network-security-lesson-2-Common-security-measures)

7.Read the text and define whether statements are True or False.

1. Cyber security is the theory of protecting systems, networks, and programs from digital attacks.

2. Strong passwords are important for good online security.

3. You should control that people can only access data and services for which they are authorized.

4. Modern operating systems and network software will help you, but you will need to manage the registration of users and user authentication systems - passwords.

5. If you don't set up your firewall devices properly, they won't be fully effective.

6. You needn't use security software, such as anti-spyware and anti-virus programs.

8.Read questions about cyber security and choose the correct answer. Discuss your answer.

1.The way I operate my computer can affect other people.

A. True B. False

2. You just got a new computer which has antivirus software already installed. Is it safe to use on the internet immediately?

A. Yes B. No C. Maybe

3. Why might someone break into (hack) your computer?

A. They don't like you.

B. To commit a crime

C. Random vandalism

D. To use it to distribute porn, malicious programs, etc.

E. All of the above

4. If you receive an email claiming to need your username and/or password, what should you do?

A. Report it as phishing/spam through your email provider

B. Delete the message

C. Reply to the message with your email and password

5. Both email attachments and downloaded files can spread malware.

A. True B. False

6. What is the best way to protect your information when you are away from your computer?

A. Lock the computer with a password

B. Activate the screen saver

C. Turn the monitor off

7. What is a firewall?

A. wall that is reinforced and cannot catch on fire.

B. program that protects against viruses.

C. A filter for an internet connection that monitors outgoing and incoming activity.

8. A strong password should contain:

A. Both uppercase and lowercase letters.

B. A word that is easy to remember, such as the name of a pet.

C. At least 8 characters, and a combination of letters, numbers, and characters.

9.Dos and Don'ts

Cyber security is the shared responsibility of every agency employee and business unit. Which of these are good actions for cyber security and which of these are not so good? Write Do or Don'ts before each one.

1.___________ use hard-to-guess passwords or passphrases.

2.___________ share your passwords with others or write them down. You are responsible for all activities associated with your credentials.

3.___________ leave sensitive information lying around the office.

4.___________ leave printouts or portable media containing private information on your desk.

5.___________ post any private or sensitive information, such as credit card numbers, passwords or other private information.

6.___________ click on links from an unknown or untrusted source. Cyber attackers often use them to trick you.

7.___________ be tricked into giving away confidential information. It's easy for an unauthorized person to call and pretend to be an employee or business partner.

8.___________ respond to phone calls or emails requesting confidential data.

9.___________ destroy information properly when it is no longer needed.

10.__________ be aware of your surroundings when printing, copying, faxing or discussing sensitive information.

11.__________ install unauthorized programs on your work computer. Malicious applications often pose as legitimate software.

12.________ lock your computer and mobile phone when not in use.

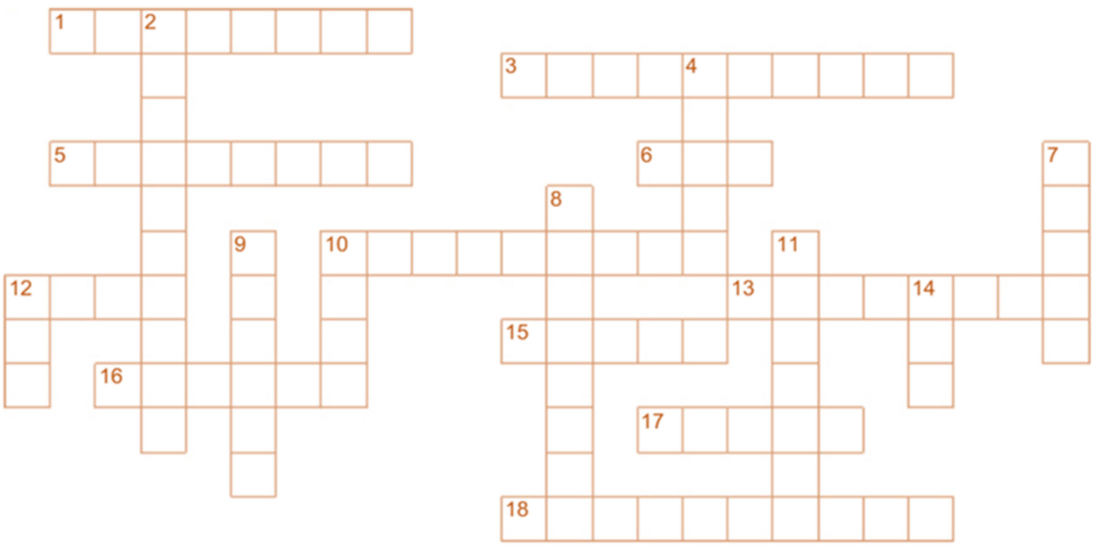
13.________leave devices unattended. Keep all mobile devices, such as laptops and cell phones physically secured. DON'T leave wireless or Bluetooth turned on when not in use.

14.________ report all suspicious activity and cyber incidents to your security representative.

10.Work with your partner and make a list of Dos and Don'ts of Information Security Awareness.

Dos	Don'ts
______________________________	______________________________
______________________________	______________________________

11.Using the Across and Down clues, write the correct words in the numbered grid below.



ACROSS

1.software that can be copied and used without payment to the author(8)

3.file which is linked to, and sent with, an e-mail message (10)

5.a computer program that prevents un authorisedentry into a computer system, stealing information or causing damage (8)

6.frequently asked questions (3)

10.the amount of data that can pass through a channel at one time(9)

12.to start up a computer (4)

13.1024 kilobytes or one million bytes (8)

15.temporary memory used to access frequently used instructions, thus speeding up processing time. Also denotes temporary storage of worldwide web pages by browser software (5)

16.a small file that a website automatically sends to your computer when you connect to the website, containing information about your use of the Internet (6)

17.a program that enters your computer and damages and destroys stored information (5)

18.clarity and sharpness of pictures and text asthey appear on the screen or on paper, often measured in dots per inch (dpi) (10)

DOWN

2.conversion of data into a format that cannot be read except with a special program. Used on the internet for secure transactions (10)

4.sudden failure of software or hardware, often resulting in no response to mouse or keyboard actions (5)

7.the smallest unit of an image on a computer screen (5)

8.1024 megabytes or one thousand million bytes(8)

9.a copy of information on your computer that you make in case you lose the information (6)

10.unit of information equal to eight bits (4)

11.computer or software settings as set in the factory or by the software creator (7)

12.the smallest unit of computer information (3)

14.error or fault in computer software which causes it to malfunction (3)

EnglishGrammar

<table>
<tr><th colspan="2">Present Simple Tense</th></tr>
<tr><th>Positive and negative</th><th>Question</th></tr>
<tr><td>
<table>
<tr><td>I
You
We
They</td><td>live
don’t live</td><td rowspan="2">near here.</td></tr>
<tr><td>He
She
It</td><td>lives
doesn’t
live</td></tr>
</table>
</td><td>
<table>
<tr><td rowspan="2">Where</td><td>do</td><td>I
you
we
they</td><td rowspan="2">live?</td></tr>
<tr><td>He
She
It</td><td>he
she
it</td></tr>
</table>
</td></tr>
<tr><td>Do you like English?
Does he speak French?
Short answer
Yes, I do.
No, he doesn’t.</td><td>1. a habit
I get up at 7:30.
He works too much.
2. a fact which is always true.
Vegetarians don’t eat meat.
We come from Samarkand.
3. a fact which is true for a long time.
I live in Tashkent.
He works in a bank.</td></tr>
</table>

Grammar exercise 1. Fill in the gaps with the correct form of the verb.

Cyber security

Cybersecurity standards are techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organization. This environment 1)…………….. users themselves, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. Computer security, cybersecurity or information technology security (IT security) 2)………. the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they 3)……….. The field is becoming more important due to increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things". Owing to its complexity, both in terms of politics and technology, cybersecurity 4)………. also one of the major challenges in the contemporary world. The principal objective is to reduce the risks, including prevention or mitigation of cyber-attacks. These published materials 5)…………. of collections of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies.

1. a) has included b) has been included c)include d)includes
2. a) has been b) had been c)is d)was
3. a)provide b) providing c)provides d)was provided
4. a) is b) had been c)to be d)was
5. a)consisted b) consists c)consist d)has consisted

Grammar exercise 2. Complete the sentences in Present Simple Tense using the words in brackets.

1. Cyber security ……. (protect) the integrity of a computer's internet-connected systems, hardware, software and data from cyber attacks.
2. Cybersecurity ……..(to be) the practice of protecting systems, networks, and programs from digital attacks.
3. Cyber security …….(refer) to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals.
4. Spyware is a program running in the background that ……(monitor) the user's computer activities.
5. Anti-Virus Software that ……(attempt) to identify and eliminate computer viruses and other malicious software by:

6. Every one …….(use) electronic communications in some manner; whether it be to check a bank account on a mobile phone, to make reservations at a restaurant, or just browsing social media sites.
7. Personal Use of Cyber Security On personal computers cyber security ………(include) the encryption of information.
8. Commercial use of Cyber Security Companies and corporations ……(rely) on different aspects of cyber security in order to protect the shipments of their products ,and more importantly, the financial information of their customers.
9. Network penetration …….(to be) a very important aspect of infrastructure integrity.
10. Cyber security ……… (make) use of security standards which ……(help) organizations in following best security practices and techniques to be used in order to minimize the number of successful cyber attacks.

T.1.4 Listen and check.

WRITING "About myself"

Answer the questions below.

1.What is a good introduction?

2.What is personal introduction?

3.How do you introduce yourself?

How to Write Shortly About Yourself. Tips.

Writing about yourself can be tough, because there is so much you can say. You have a lifetime of experiences, talents, and skills to summarize in a paragraph, or two. Whatever kind of writing you are planning on doing, whatever your purpose, just think about it like you are introducing yourself to a stranger. What do they need to know?

Here are some examples of things you can say about yourself:

My name's ...

I'm from ... / I live in ...

I was born in ...

I’m ... years old.

I study at……….

I like ... because ...

I don’t like ... because ...

In my free time I ...

My best friends are ... because ...

My favourite (subject, actor, pop group, sport) is ... because ...

I have ... brothers and sisters.

In the future, I’d like to ... because ...

TASK. Write about yourself using tips and examples given above. Answer questions like:

- Who are you?
- What is your background?
- What are your interests?
- What are your talents?

LESSON 1. CYBER SECURITY

CAN YOU: ***REVISE AND CHECK***

...give definition of:

patch____________________

cyberattack_______________

malicious_______________

password_______________

cybersecurity_____________

domain_________________

bug____________________

spyware_________________

privacy__________________

… speak about Cyber security and common Cyber security measures? What are the differences between Cyber security and Info security?

… write about yourself

….do these tests

1.Which type of cyber attack is commonly performed through emails?

A. Trojans

B. Phishing

C. Worm

D. Ransomware

2. For maximum security, passwords should be made up of:

A. Lower case letters only

B. Memorable names and dates

C. A sequence of numbers or letters

D. Upper and lower case letters numbers and symbols

3. Which of the following is the best answer for how to secure your router?

A. Change the default name and password of the router.

B. Turn off the router's remote management.

C. Log out as the administrator once the router is set up.

D. All of the above.

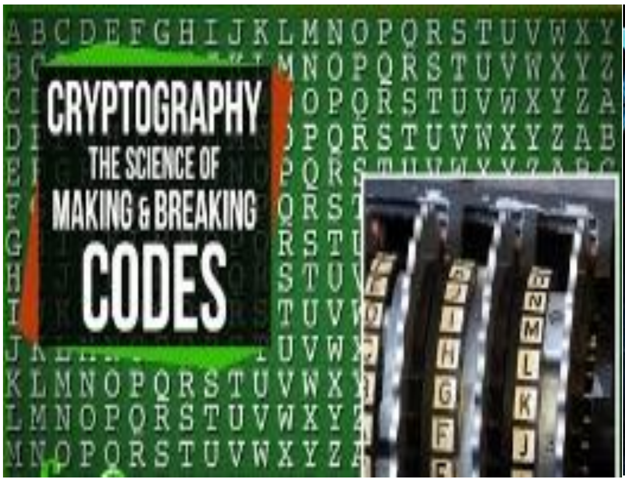
LESSON 2. CRYPTOGRAPHY

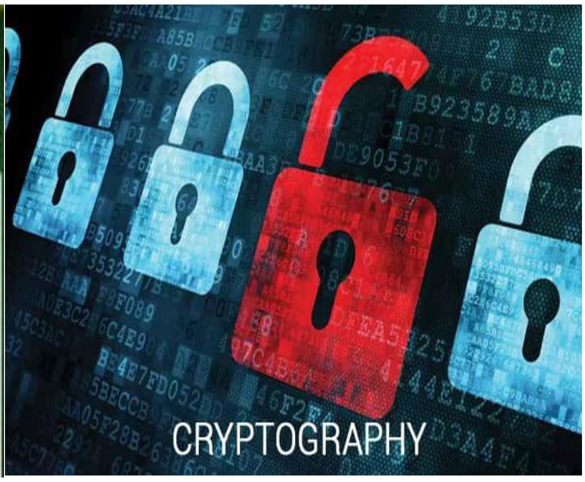
1.In pairs discuss this questions.

1.What do you know about Cryptography?

2.What is the Importance of Cryptography?

3.What are Ciphers?





2.This glossary includes some of the most important words and vocabulary used in crypto space read and translate them into your native language using dictionary.

1.A-label-The ASCII compatible encoded (ACE) representation of an internationalized (unicode) domain name. A-labels begin with the prefix xn--.

2.Authentication-The process of verifying that a message was created by a specific individual (or program). Like encryption, authentication can be either symmetric or asymmetric. Authentication is necessary for effective encryption.

3.Bytes-like-A bytes-like object contains binary data and supports the buffer protocol. This includes bytes, byte array, and memory view objects.

4.Cipher – A cipher is an algorithm, which changes the normal order and arrangement of letters within a message.

5.Cryptography – Cryptography is the study of hiding the meaning of a message by changing the content of the message using rules. It involves ciphers and codes.

6.Decryption-The process of converting cipher text to plaintext.

7.Encryption-The process of converting plaintext to ciphertext.

8.Key-Secret data is encoded with a function using this key. Sometimes multiple keys are used. These must be kept secret, if a key is exposed to an attacker, any data encrypted with it will be exposed.

9.Nonce-A nonce is a number used once. Nonce is used in many cryptographic protocols. Generally, a nonce does not have to be secret or unpredictable, but it must be unique. A nonce is often a random or pseudo-random number .

10.Plaintext-User-readable data you care about.

T.2.1 Listen and check your pronunciation.

T.2.2 Listen and choose the best answer for the blanks.

1. Cryptography, the use of codes and …………. to protect secrets, began thousands of years ago.

a. ciphers

b. sinuses

c. causes

2. Cryptography involves creating written or generated codes that allow ………….. to be kept secret.

a. information

b. informatics

c. informs

3. Information ………….. uses cryptography on several levels.

a. sensor

b. cyber security

c. security

4. The information maintains its …………… during transit and while being stored.

a. infinity

b. integrity

c. information

T. 2.3 Listen again and fill in the gaps with ONE or TWO words.

What is cryptography?

Cryptography, the use of codes and ciphers to (1)_______________, began thousands of years ago. Until recent decades, it has been the story of what might be called (2)______________ — that is, of methods of encryption that use pen and paper, or perhaps simple mechanical aids.

Cryptography(3)________________ creating written or generated codes that allow information to be kept secret. Cryptography (4)_____________ data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a (5)__________________, thus compromising the data. Information security uses cryptography on several levels. The information cannot be read without a key to (6)________________ it. The information maintains its (7)____________________ during transit and while being stored. Cryptography also aids in nonrepudiation. This means that the sender and the (8)________________ of a message can be verified.

5.Read the text and complete the text with the expressions given below.

a) proliferation of cryptographic techniques
b) evolution of cryptography as well
c) science of information security
d) by messages written in hieroglyph
e) the applications of cryptography
f) As civilizations evolved
j) Improved coding techniques
h) This rule became a key

History of Cryptography

The art of cryptography is considered to be born along with the art of writing. **1**……………………human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics.

These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous **2**……………………… The roots of cryptography are found in Roman and Egyptian civilizations.

The first known evidence of cryptography can be traced to the use of 'hieroglyph'. Some 4000 years ago, the Egyptians used to communicate **3**…………………………... This code was the secret known only to the scribes who used to transmit messages on behalf of the kings. One such hieroglyph is shown below.

Hieroglyph

Later, the scholars moved on to using simple mono-alphabetic substitution ciphers during 500 to 600 BC. This involved replacing alphabets of message with other alphabets with some secret rule. **4**………………………….. to retrieve the message back from the garbled message.

The earlier Roman method of cryptography, popularly known as the **Caesar Shift Cipher,** relies on shifting the letters of a message by an agreed number (three was a common choice), the recipient of this message would then shift the letters back by the same number and obtain the original message.

It is during and after the European Renaissance, various Italian and Papal states led the rapid **5**……………………… Various analysis and attack techniques were researched in this era to break the secret codes. **6**……………………… such as Vigenere Coding came into existence in the 15th century, which offered moving letters in the message with a number of variable places instead of moving them the same number of places.

Original message

a	**t**	**t**	**a**	**c**	**k**		**a**	**t**	**d**	**a**	**w**	**n**

Each letter is shifted by "2"

c	**v**	**v**	**c**	**e**	**m**	**c**	**v**	**f**	**c**	**y**	**p**

Secret message

-Only after the 19th century, cryptography evolved from the ad hoc approaches to encryption to the more sophisticated art and **7**……………………….

-In the early 20th century, the invention of mechanical and electromechanical machines, such as the Enigma rotor machine, provided more advanced and efficient means of coding the information.

-During the period of World War II, both cryptography and cryptanalysis became excessively mathematical.

With the advances taking place in this field, government organizations, military units, and some corporate houses started adopting **8**……………………… They used cryptography to guard their secrets from others. (https://en.wikipedia.org/wiki/History_of_cryptography)

6.Read the text again and answer the question.

1.Where can be found the roots of cryptography?

2.What did mono-alphabetic substitution ciphers involve?

3. When was Vigenere Coding appeared?

4.What was purpose of using cryptography during World War II?

7. Writing Secret Messages Using Ciphers

-Write out the entire alphabet in a line.

-Choose a number to be your "rotation" amount. For example 7 ...

-Under your first line, starting at the letter you "rotated" to, rewrite the alphabet. ...

-Decide what your message is going to say and write it on a piece of paper. ...

-To decode a message, you do the process in reverse.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Ex. I have a big secret.   - B ATOX T UBZ LXVKXM.

8.Write a secret message and exchange letters with your friend. Try to read and understand each others secret messages.

EnglishGrammar

<table>
<tr><th colspan="2">Present Continuous</th></tr>
<tr><td colspan="2">Form. am/is/are + ing (present participle)</td></tr>
<tr><td>Positive and negative</td><td>Question</td></tr>
<tr><td>
<table>
<tr><td>I</td><td>`m (am)<br>`m not</td><td rowspan="3">working.</td></tr>
<tr><td>He
She
It</td><td>`s (is)
isn’t</td></tr>
<tr><td>You
We
They</td><td>`re (are)
aren’t</td></tr>
</table>
</td><td>
<table>
<tr><td rowspan="3">What</td><td>am</td><td>I</td><td rowspan="3">wearing?</td></tr>
<tr><td>is</td><td>he
she
it</td></tr>
<tr><td>are</td><td>you
we
they</td></tr>
</table>
</td></tr>
</table>

Short answer. Are you going? **Yes**, I **am**. / **No**, ~~I`m not~~. NOT Yes, I`m.

Is Saida working? **Yes**, she **is**. / No, she **isn’t**. N~~OT Yes,~~ she`s.

Use. The Present Continuous is used to express:

1. an activity happening now.

*They’***replaying** *football in the garden.*

*She can’t talk now because she’***s washing** *her hair.*

2. an activity happening around now; but perhaps not at the moment of speaking.

*He’***s studying** *maths at university.*

*I`***m reading** *a good book at the moment.*

3. a planned future arrangement.

*I`***m seeing** *the doctor at 10.00 tomorrow.*

What ***are*** *you* ***doing*** *this evening?*

Grammar exercise 1. Fill in the blanks with the appropriate form of the verb.

1. Jamila …………………. in the garden.

a.works b.is working c.are working

2. I ………………….. Oliver Twist at the moment.

a.is reading b.am reading c.are reading

3. He ………………… TV.

a.is watching b.am watching c.are watching

4. Who ……………….. the violin?

a.is playing b.are playing c.am playing

5. Don't make noise. The baby …………………

a.is sleeping b.are sleeping c.am sleeping

6. I ………………… in the park now.

a.is waiting b.am waiting c.are waiting

7. Karim and Saida ………………… in the kitchen.

a.is cooking b.are cooking c.am cooking

8. He ………………… pizza at the moment.

a.is making b.are making c.am making

9. Mother ………………….. a sweater.

a.is knitting b.are knitting c.am knitting

10. Sevara and her friend …………………. over for lunch.

a.is coming b.are coming c.am coming

T.2.4 Listen and check.

Grammar exercise 2. Make the present continuous - positive, negative or question.

1) (they / not / read)

2) (I / cook tonight)

3) (he / see the doctor tomorrow)?

4) (you / eat chocolate)?

5) (what / you / do)?

6) (we / make a mistake)?

7) (you / come tomorrow)

8) (it / snow)

9) (John / sleep at the moment)

10) (he / not / dance)

11) (how / they / get here)?

12) (when / it / start)?

13) (I / not / speak Chinese at the moment)

14) (I / stay with a friend for the weekend)

15) (they / come to the party)?

16) (we / not / study)

Writing a CV. Discuss with a partner. Are these sentences True or False?.

1. A CV is a document with information about you.T/F
2. You use a CV to get a job.T/F
3. You should put your photo on your CV.T/F
4. Your CV should be 3 or 4 pages long.T/F
5. It’s OK to have mistakes (spelling, grammar) on your CV.T/F
6. All information on your CV must be in full sentences.T/F

A CV is a document that lists your qualifications previous and current employment. It is included as part of a job application and is intended help to you sell yourself and your abilities to a potential

Here is a sample CV. Use this template and design your own.

Bobokulov Akmaljon CV

I am a multimedia programmer with qualifications and experience. I am looking for a job in computer programming sphere in Tashkent.

Personal details

Address: 56/8/3 Chilanzar, Tashkent, Uzbekistan

Email: akmaljondjj@gmail.com

Phone: +998998591804

Date of birth: 18 April 1995

Education and qualifications

2010-2013: Shakhrisabz Lyceum of Information Technology, Kashkadarya (Uzbekistan). Diploma in Telecommunication engineer

2017-present: student of Tashkent University of Information Technology 4th course, Telecommunication Technology faculty

Work experience

2011-2012: engineer of Exchange in Shakhrisabz.

2017-present: network administration for the Internet Provider (EVO company) in Tashkent.

Skills

Languages: Uzbek(fluent); English (advanced); Russian(elementary);

Computers: Microsoft Office (Word, Excel and PowerPoint), Network administration(Cisco CCNA,CCNP):

UZ driving license

Interests

I enjoy football and played for the men's team at university.

References

Mr Khurshid Urakov, English Lecturer, Everest company: khurshidurakov@mail.ru

Mr Umrullo Alayev, main network administration of Uztelecom, in Tashkent uztelecom@mail.uz

…………………. CV

I am……………………………………………………………………………….

Personal details

Address: ……………………………….

Email: ………………………………….

Phone: ………………………………

Date of birth: …………………………..

Education and qualifications

year: …………………………………………………………………..………

year:……………………………………………………………….…………

Work experience

year: ……………………………………………………………..……………

year:…………………………………………………………..………………….

Skills

Languages: ……………………………………………………………………

Computers: …………………………………………………………………...

………………………………………………………………………………

………………………………………………………………………………

Interests

I enjoy ……………………………………………………………...……

……………………………………………………………………………....

………………………………………………………………………………

………………………………………………………………………………

References

……………………………………………………………………………….

……………………………………………………………………………….

………………………………………………………………………………

………………………………………………………………………………

LESSON 2. CRYPTOGRAPHY ***<u>REVISE AND CHECK</u>***

CAN YOU:

...give definition of:

A-label__________________

Authentication____________

bytes-like________________

cipher__________________

cryptography____________

decryption______________

encryption______________

key_____________________

plaintext_______________

nonce___________________

...talk about cryptography and its importance?

What is cryptography used for?

What is cryptography with example?

What is cryptography and types?

…write CV?

…do these tests

1.This is an encryption/decryption key known only to the party or parties that exchange secret messages.

A. e-signature
B. digital certificate
C. private key
D. security token

2.Today, many Internet businesses and users take advantage of cryptography based on this approach.

A. public key infrastructure
B. output feedback
C. Encrypting File System
D. single signon

3. Cryptanalysis is used ___________

A. to increase the speed

B. to encrypt the data

C. to make new ciphers

D. to find some insecurity in a cryptographic scheme

LESSON 3. SYMMETRIC AND ASYMMETRIC CRYPTOSYSTEMS

1.In pairs discuss this questions.

1.What is asymmetric and symmetric?

2.Is AES asymmetric or symmetric?

3.Look at the figure 1.What are the main differences between symmetric and asymmetric key cryptography?

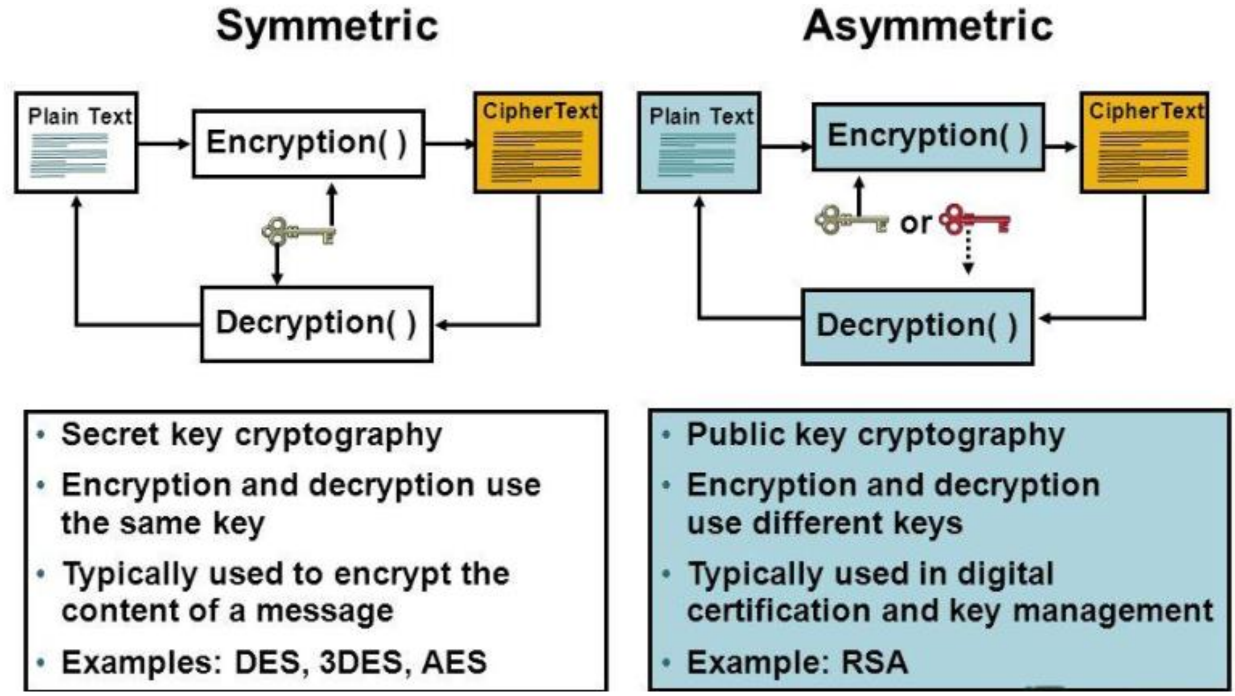


Figure 1

4.Which is better asymmetric or symmetric encryption?

2.Match the words with their definitions.

	Words		**Definitions**
1	decipher	a	not symmetrical; lacking symmetry; disproportioned
2	symmetric	b	the piece of information or parameter that is used to encrypt and decrypt messages in a symmetric encryption
3	asymmetric	c	make (a coded or unclear message) intelligible
4	recipient	d	convert (a text written in code, or a coded signal) into normal language.

5	algorithm	e	a suite of cryptographic algorithms needed to implement a particular security service, most commonly for achieving confidentiality
6	secret key	f	convert (information or data) into a code, especially to prevent unauthorized access
7	cryptosystem	g	made up of exactly similar parts facing each other or around an axis
8	technique	h	a process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer
9	decrypt	i	a person or thing that receives or is awarded something
10	encrypt	j	a way of carrying out a particular task, especially the execution or performance of an artistic work or a scientific procedure

1	2	3	4	5	6	7	8	9	10

T.3.1 Listen and check your answers and pronunciation.

T.3.2 Listen and choose the best answer.

1. A cryptosystem is an implementation of cryptographic______________ and their accompanying infrastructure to provide information security services.

a.technology

b. techniques

c.hightech

2. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the _____________.

a.public key

b.secret key

c. encryption key

3. Symmetric cryptosystems are also sometimes referred to as__________ cryptosystems.

a. secret key

b.public key

c.encryption key

4. The encryption process where different keys are used for encrypting and decrypting the information is known as _____________Encryption.

a. asymmetric key

b.secret key

c.public key

T.3.3 Listen and complete the sentences.

1. A cryptosystem is also referred to as a……………….

2. The main difference between these cryptosystems is the relationship between the encryption and the……………….

3. . It is practically impossible to decrypt the cipher text with the key that is unrelated to the…………….

4. The study of symmetric cryptosystems is referred to as symmetric …………….

5. Even today, its relevance is very high and it is being used extensively in many …………….

6. Though the keys are different, they are mathematically related and hence, retrieving the …………….. by decrypting cipher text is feasible.

5.Read the text and find the words or phrases in the text with the following meanings.

1. _____________ - facts provided or learned about something or someone.

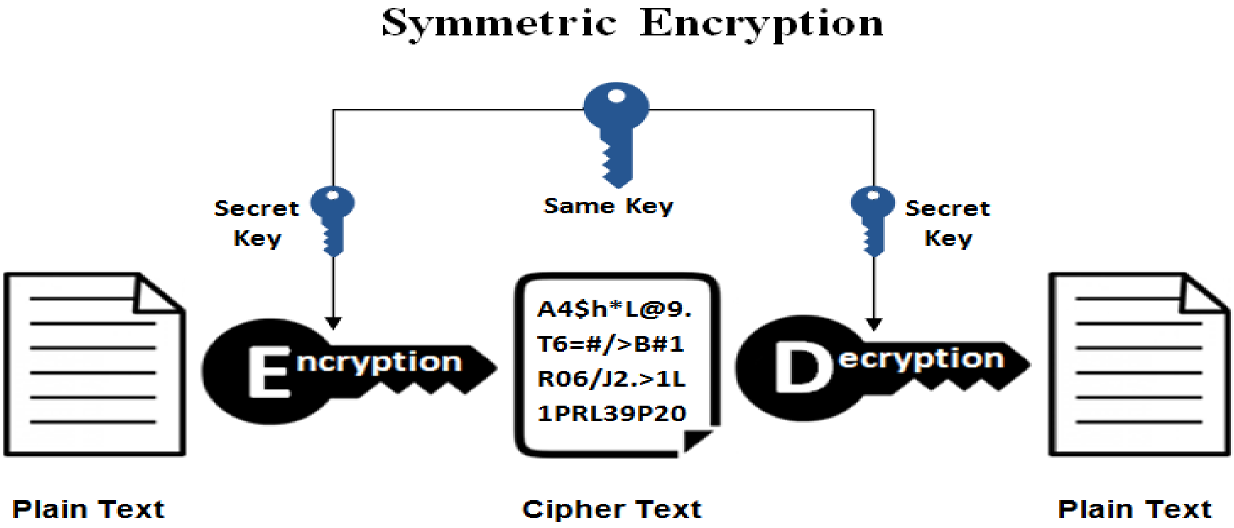
2. _____________- a process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.

3. _____________- have or include (something) as a necessary or integral part or result.

4. ____________- a verbal, written, or recorded communication sent to or left for a recipient who cannot be contacted directly.

5. ____________- a global computer network providing a variety of information and communication facilities, consisting of interconnected networks.

6. ____________- the imparting or exchanging of information by speaking, writing, or using some other medium.

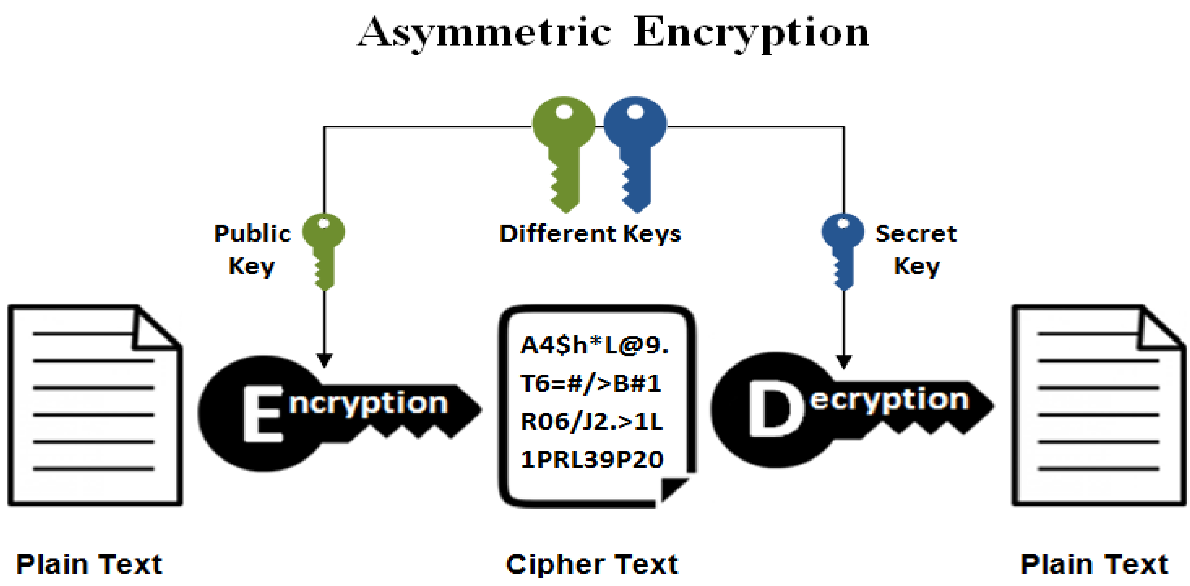


This is the simplest kind of encryption that involves only one secret key to cipher and decipher information. Symmetrical encryption is an old and best-known technique. It uses a secret key that can either be a number, a word or a string of random letters. It is a blended with the plain text of a message to change the content in a particular way. The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages. Blowfish, AES, RC4, DES, RC5, and RC6 are examples of symmetric encryption. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.

The main disadvantage of the symmetric key encryption is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it.

Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetrical encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.

Symmetric encryption is an old technique while asymmetric encryption is relatively new.



Asymmetrical encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption. Asymmetric encryption uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. It ensures that malicious people do not misuse the keys. It is important to note that anyone with a secret key can decrypt the message and this is why asymmetrical encryption uses two related keys to boosting security. A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know.

A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication. Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Asymmetric encryption was introduced to complement the inherent problem of the need to share the key in symmetrical encryption model, eliminating the need to share the key by using a pair of public-private keys. Asymmetric encryption takes relatively more time than the symmetric encryption.

(https://www.clickssl.net/blog/symmetric-encryption-vs-asymmetric-encryption)

6.Read the text and define whether the statements are True or False.

1. Symmetrical encryption is a new and best-known technique.
2. Symmetrical encryption is a blended with the plain text of a message to alter the content in a particular way.
3. Asymmetric encryption is an old technique while asymmetric encryption is relatively new.
4. Symmetric encryption uses two keys to encrypt a plain text.
5. Asymmetric key has a far better power in ensuring the security of information transmitted during communication.
6. Asymmetric encryption takes much time than the symmetric encryption.

EnglishGrammar

Article
1.The indefinite article a or an in used with singular, count nouns to refer to a thing or an idea for the first time. *We are **a cat** and **a dog.**/ There's **a supermarket** in Adam Street.* 2. The definite article the is used with singular and plural, count and uncount nouns when both the speaker and the listener know the thing or idea already. *We have a cat and a dog. The cat is old, but the dog is just a puppy.* *I'm going to the supermarket. Do you want anything? (We both know which supermarket*)
Definite article. The definite article used:
1. before seas, rivers, hotels, pubs, theatres, museums, and newspapers. *the Atlantic* *the British Museum* *The Times* *the Ritz* 2. if there is only one of something *the sun* *the Queen* *the Government* 3. with superlative adjectives. *He's the richest man in the world./ Jane's the oldest in the class*

Indefinite article. The indefinite article is used:
1. with professions. *I'm **a teacher./** She is **an architect.*** 2. with some expressions of quantity. ***a pair of / a little / a couple of / a few*** 3. with some expressions of frequency. ***once a week/ three times a day*** 4. in exclamations with what +a count noun ***What a** lovely **day!/ What a pity!***
No article. There is no article:
1. before plural and uncount nouns when talking about thing in general. ***I like potatoes. / Milk is good for you.*** 2. before countries, towns, streets, languages, magazines, meals, airports, stations and mountains ***I had launch with Jamshid./ I bougth Cosmopolitan at Victoria Station.***
Before some places and with some forms of transport

at home	In/to bed	at/to work
At/to school/university	By bus	By plane
By car	By train	On foot

She goes to work by bus.

so + **adjective/adverb** *I was **so** scared.* *He always drives **so** fast.*	***so many* + plural nouns** *Some children have **so many** toys.*
such a + adjective + singular noun *She's **such** a nice person.*	***so much* + uncountable nouns** *Footballers earn **so much** money these days.*

such + adjective + plural/uncountable noun

*The Smiths are **such** friendly neighbours.*

Note: So and *such* are used for emphasizing an adjective or noun. They are used more in spoken than written English. They are often exclamations, with an exclamation mark(!). *He works so hard!* is stronger than *He works very hard.*

Grammar exercise 1. Choose the correct definite or indefinite article: "the", "a", "an" or "-" (zero article) .

1. I saw …… movie last night.
2. They are staying at ….. hotel.
3. Look at ……. woman over there! She is a famous actress.
4. I do not like …… basketball.
5. That is …… girl I told you about.
6. …… night is quiet. Let's take a walk!
7. John traveled to ….. Mexico.
8. I read …… amazing story yesterday.
9. I live in ……. apartment. …….. apartment is new.
10. I would like …….. piece of cake.

Grammar exercise 2. Put Correct Articles.

1.Authentication is _____ common technique for masking contents of messages or other information traffic so that opponents cannot extract the information from the message.

a) a
b) the
c) an

2.Replay an attacker performs ____ capture of ___ data unit and its subsequent retransmission to produce an unauthorized effect.

a) the, the
b) a, a
c) an, an

3.Feistel is ___ block cipher structure in DES

a) –
b) the
c) an

4.____ greatest common divisor of two integers is the largest positive integer that exactly divides both integers.

a) the
b) an
c) –

5.___ distribution of bits in a random number sequence should be uniform therefore the frequency of occurrence of ones and zeros should be approximately equal.

a) a
b) –
c) the

6.Miller–Rabin algorithm is typically used to test ___ large number for primality.

a) a
b) the
c) an

T. 3.4 Listen and check.

Grammar Exercise 3. Choose the correct article: a, an, the or - (no article).

1.Are you coming to …… party next Saturday?

2.I bought …… new TV set yesterday.

3.I think ….. man over there is very ill. He can't stand on his feet.

4.I watched …… video you had sent me.

5.She was wearing …… ugly dress when she met him.

6.I am crazy about reading …… history books.

7.She is …… nice girl.

8.Do you want to go to ……. restaurant where we first met?

9.He is …… engineer.

10.He thinks that …….. love is what will save us all.

WRITING a letter to a friend.

1.How do you write a letter to a friend?

2.How do you begin a letter?

3.How do you end a letter to a friend?

4.What are the steps to write a letter?

The 5 steps to Writing a Letter

Step 1. **The Heading:** This includes your address and the date. Write it in the upper-right corner of the page and spell out the name of the month to avoid confusion.

Step 2. The Salutation: This is the "hello" part of your letter and is also known as the greeting. It is located on the next line after the heading, but it is placed on the left side of the page about an inch from the edge. The name of the person should be capitalized and followed by a comma.

Step 3. The Body: Here is where you express thoughts and ideas. In other words, it is the reason for writing the letter. Start under the salutation, an inch from the left edge or the page (5 spaces).

Step 4: The Closing: This is the "good-bye" part of the letter. Usually, words such as "Your truly" or "Love" are used here. Closings should make the reader feel like you really care or that you really mean what you have written.

Step 5: The Signature: Sing the letter in your own handwriting just below the closing.

Task.You want to sell your Laptop. You think that your friend might buy it from you. Write a letter to your friend.

In your letter:

-Explain why you are selling the Laptop;

-Describe the Laptop;

Suggest a date when your friend can come and see it.

Dear (name)____

____

____

____

____

____

____

LESSON 3. SYMMETRIC AND ASYMMETRIC CRYPTOSYSTEMS

REVISE AND CHECK

CAN YOU:

…define the main differences between symmetric and asymmetric key cryptography? Where we can use symmetric and asymmetric keys?

…**write** a letter to a friend?

…give definition of:

Decipher___________________

Symmetric__________________

Asymmetric_________________

Recipient__________________

Algorithm__________________

secret key_________________

cryptosystem_______________

technique__________________

decrypt____________________

encrypt____________________

…do these tests

1.Using the same key to encrypt and decrypt a message is…

A. asymmetric encryption

B. plain text

C. cipher text

D. symmetric encryption

2. A message before decryption is known as…

A. encrypted text

B. plain text

C. original message

D. cipher text

3.In asymmetric key cryptography, the private key is kept by __________

A. sender

B. sender and receiver

C. all the connected devices to the network

D. receiver

4.Asymmetric key cryptography is used for all of the following except:

A.Encryption of data

B.Access control

C.Nonrepudiation

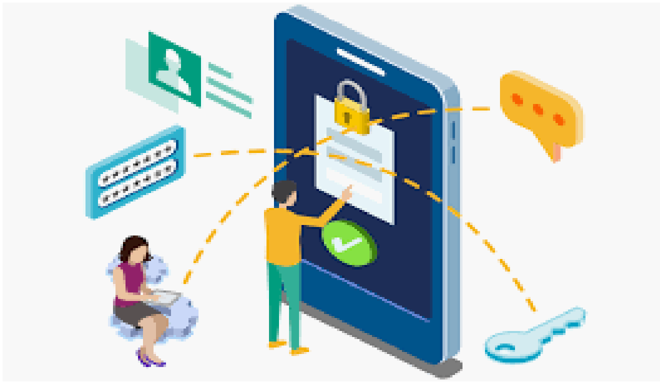
D.Steganography

LESSON 4. AUTHENTICATION

1.In pairs discuss these questions.

1. What's authentication?

2. What's the difference between identification and authentication?



Authentication - MobileConnect

2.Match the words with their definitions.

	Words		Definitions
1	verification	a	give official permission for or approval to (an undertaking or agent).
2	certification	b	a formal written or spoken statement, especially one given in a court of law.
3	corroboration	c	the action of checking or proving the validity or accuracy of something.
4	authorize	d	a certified statement.
5	validation	e	check or prove the validity or accuracy of.
6	verify	f	the state of being verified
7	credential	g	a formal or explicit statement or announcement.
8	testimony	h	a qualification, achievement, quality, or aspect of a person's background, especially when used to indicate their suitability for something.
9	validate	i	evidence which confirms or supports a statement, theory, or finding; confirmation.

10	declaration	j	make sure or demonstrate that (something) is true, accurate, or justified.

1	2	3	4	5	6	7	8	9	10

T.4.1 Listen and check your answers and pronunciation.

T.4.2 Listen and choose the best answer in order to fill in the gaps.

1. Generally, a user has to choose a username or user ID and provide a valid …………… to begin using a system.

a. passport

b. password

c. pass way

2. Many companies use authentication to validate users who log into their ………..

a. own sites

b. sites

c. websites

3. Organizations also use authentication to control which users have access to corporate networks and …………

a. sources

b. resources

c. sites

4. …which grants access to multiple systems with a single set of login ……………

a. credentials

b. credits

c. credence

T.4.3 Listen again and complete the sentences.

Generally, a user has to choose a username or user ID and provide a valid 1)_______________ to begin using a system. User authentication authorizes human-to-machine interactions in operating systems and 2)______________, as well as both wired and wireless networks to enable access to networked and internet-connected systems, applications and resources. Many companies use authentication to validate users who log into their websites. Without the right security 3)_______________, user data, such as credit and debit card numbers, as well as Social Security numbers, could get into the hands of cybercriminals.

Organizations also use authentication to control which users have access to corporate networks and 4)________________, as well as to identify and control which machines and servers have access. Companies also use authentication to enable remote employees to securely 5)_____________ their applications and networks.

For enterprises and other large organizations, authentication may be accomplished using a single sign-on (SSO) system, which grants access to multiple systems with a single set of login 6)_________________.

5.Read the text and find the meaning of these words. If necessary you may use a dictionary.

1. credentials-____________________

2. authorized-____________________

3. application-____________________

4. patching-______________________

5. identity-_______________________

6. authenticate-___________________

What is authentication?

Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

Authentication is important because it enables organizations to keep their networks secure by permitting only authenticated users (or processes) to access its protected resources, which may include computer systems, networks, databases, websites and other network-based applications or services.

Once authenticated, a user or process is usually subjected to an authorization process as well, to determine whether the authenticated entity should be permitted access to a protected resource or system. A user can be authenticated but fail to be given access to a resource if that user was not granted permission to access it.

The terms authentication and authorization are often used interchangeably; while they may often be implemented together the two functions are distinct. While authentication is the process of validating the identity of a registered user before allowing access to the protected resource, authorization is the process of validating that the authenticated user has been granted permission to access the requested resources. The process by which access to those resources is restricted to a certain number of users is called access control. The authentication process always comes before the authorization process.

Authentication and authorization

The terms authentication and authorization are often used interchangeably; while they may often be implemented together the two functions are distinct.

While authentication is the process of validating the identity of a registered user before allowing access to the protected resource, authorization is the process of validating that the authenticated user has been granted permission to access the requested resources. The process by which access to those resources is restricted to a certain number of users is called access control. The authentication process always comes before the authorization process.

Authorization includes the process through which an administrator grants rights to authenticated users, as well as the process of checking user account permissions to verify that the user has been granted access to those resources. The privileges and preferences granted for the authorized account depend on the user's permissions, which are either stored locally or on the authentication server. The settings defined for all these environment variables are set by an administrator.

Systems and processes may also need to authorize their automated actions within a network. Online backup services, patching and updating systems and remote monitoring systems, such as those used in telemedicine and smart grid technologies, all need to securely authenticate before they can verify that it is the authorized system involved in any interaction and not a hacker. (en.wikipedia.org.Authentication)

6.Read the text and decide whether the statements are True or False.

1. Authentication technology controls systems to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.___

2.Twice authenticated, a user or process is usually subjected to an authorization process as well, to determine whether the authenticated entity should be permitted access to a protected resource or system._______

3. The process by which access to those resources is restricted to a certain number of users is called access control._______

4. The terms authentication and authorization are never used interchangeably._____

5. The authorization process always comes before the authentication process._____

6. Systems and processes may also need to authorize their automated actions within a network.________

7.Authentication quiz

1. Which authentication mechanism is the easiest to deploy and the easiest to break?

a.shared secrets (passwords and PINs)

b.biometrics

c.tokens

d.geo-location

2. Which of the following publishes internal IDs to the outside world or external business partner IDs internally, or both?

a.application-specific directories

b.OS-specific directories

c.departmental directories

d.border directory

3. True or False: Tokens and smart cards have identical capabilities today.

a.True b.False

4. What should you consider when deploying an LDAP structure?

a. Using a unique User ID across the entire structure

b. Using LDAP chaining

c. Making the people database space as flat as possible

d.All of the above

5. Which of the following is not a best practice for using tiered groups to control user access?

a.Apply policies to each layer individually.

b.Keep the group structure as simple as possible.

c.Don't nest OUs or groups more than a few layers deep.

d.Keep the number of groups to a minimum.

EnglishGrammar

<table>
<tr><th colspan="2">The verb have/have got</th></tr>
<tr><th>Have \ has – (formal)</th><th>Have got\ has got - informal</th></tr>
<tr><th colspan="2">Formation</th></tr>
<tr><td>Positive form
I, You, We/ They + have + a lesson today.
She, he, it + has + a big house.
Negative form
I, You, We, They + don’t + have + a lesson on Sunday.
She, he, it+ doesn’t + a big house.
Question form
Do + I, you, we, they+ have a lesson on Sunday? – No, I, you, we. they + don’t. / Yes, I, we, they +do.
Does + she, he, it+ a big house? – Yes, she, he, it+ does. / No, she, he, it+ doesn’t.</td><td>Positive form
I, You, We, They + have got+ two siblings.
She, he, it + has got + an expensive car.
Negative form
I, You, We. They + haven’t got two siblings.
She, he, it+ hasn’t got + an expensive car.
Question form
Have+ I, you, we, they+ got+ two siblings? – No, I, you, we, they + haven’t / Yes, I, we + have. Has + she, he, it+ got + an expensive car? – Yes, she, he, it+ has got. / No, she, he, it+ hasn’t.
P.S. We don’t use got in short answers.
Have you got a mobile phone?
- Yes, I have. ~~got/~~ No, I haven’t.</td></tr>
<tr><td colspan="2">Both of these verbs are used to talk about:
1. possession.
I have a meeting today. / I have got a meeting today.
Karim has the latest model of PC. / Karim has got the latest model of PC.
2. relationship.
Do you have any siblings? / Have you got any siblings?
Nodir has five aunts and two uncles. / Nodir has got five aunts and two uncles.
3. illnesses.
My brother has got the flu now. / My brother has the flu now.
I’ve got a terrible headache. / I’ve a terrible headache.
4. characteristics or appearance.
Our room in the hotel has got a nice view./Our room in the hotel has a nice view.
Why do you have a tattoo? / Why have you got a tattoo?
My elder daughter has blue eyes.
5. things we do (meals, holidays…) and with a bath, a shower, or a wash.
I with my family usually have a breakfast at 7.
Alisher can’t answer the phone now. He is having a shower.</td></tr>
</table>

Grammar exercise 1. Fill in the gaps with the correct form of have/has got.

1. ….. an item for sale in a reputable store implicitly attests to it being genuine, the first type of authentication.

A)Have B)Having C) Has D)Being

2. The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something the user knows, something the user ….. , and something the user is.

A) have B) had C)has D) can

3. The ownership factors - Something the user ….. wrist band, ID card, security token, implanted device, cell phone with built-in hardware token, software token, or cell phone holding a software token.

A) have B) has C)had D) can

4. The term digital authentication …… another meaning as electronic authentication or e-authentication, refers to a group of processes where the confidence for user identities is established and presented via electronic methods to an information system.

A) has B) have C)had D) can

5. Authorization …… the process which is distinct from that of authentication.

A) have got B) has got C) had got D) don't have got

6. A full authentication protocol ……. a number of *attributes* about this user, such as a unique identifier, an email address.

A) has B) have C)had D) can

7. We …… two ways to send the authentication token to an API. You can include it as a query parameter, access token=$token, or as an HTTP header Authorization: Bearer $toke. The header method is recommended.

A) has B) have C)had D) can

8. Users ….. a user ID which are usually identified with, and authentication is accomplished when the user provides a credential, for example a password, that matches with that user ID.

A) have got B) has got C)had D) to be

9.Most users ….. the familiarity with using a password, which, as a piece of information that should be known only to the user, is called a knowledge authentication factor.

A) has B) have C)had D) can

10.Authentication is important because it ..... enabling organizations to keep their networks secure by permitting only authenticated users to access its protected resources, which may include computer systems, networks, databases, websites and other network-based applications or services.

A) has B) have C)had D) can

Grammar exercise 2. Fill the gaps with: *have / has / have got / has got.*

1. Organizations also use authentication to control which users ……… access to corporate networks and resources.
2. An old security adage ……… it that authentication factors can be "something you know, something you have or something you are."
3. This approach to authentication ……… several drawbacks, particularly for resources deployed across different systems.
4. Now that you ……… routes and views setup for the included authentication controllers.
5. Many smartphones ……… a fingerprint sensor that allows you to unlock your phone.
6. Some facilities ……… retinal scanners, which require an eye scan to allow authorized individuals to access secure areas.

T. 4.4 Listen and check.

WRITING a description.

1.What is an example of a description?

2.How do you write a description?

3.What makes a good description?

4.What is effective description?

5. What is the use of description?

6. What are some descriptive words?

Planning A Description

1)Print a copy of the structure of a description

2. Plan your writing task by writing notes near each section.

3) Write your description.

Task.Describe a piece of modern technology you own.

You should say:

-what it is

-what you use it for

-how long you have owned it and explain why it is important to you.

LESSON 4. AUTHENTICATION ***REVISE AND CHECK***

CAN YOU:

…give definition of:

Verification________________

Certification________________

Corroboration______________

Authorize__________________

Validation_________________

Verify____________________

Credential_________________

Testimony_________________

Validate___________________

Declaration________________

…give definition for authentication?

What is the purpose of authentication?

What are the three types of authentication?

How is authentication done?

…**write** a description

…do these tests

1.Which of the following is the verification of a person's identity?

A. Authorization C. Accountability

B. Password D. Authentication

2.Which of the following is the final step a user needs to take before that user can access domain resources?

A.Verification C. Validation

B.Authentication D. Authorization

3.To gain access to your network, users must provide a thumbprint and a username and password. What type of authentication model is this?

A. Biometrics C. Domain logon

B. Single sign-on D. Multifactor

LESSON 5. PASSWORD RETENTION AND PASSWORD ATTACKS

1.Work in pairs and discuss these questions.

1.What is password guessing attack?

2.How do hackers hack passwords?

3.What is a high strength password?

4.What are various attacks on password?

2.Match the words with their definitions.

	Words		Definitions
1	log in	a	certain to remain safe and unthreatened.
2	username	b	a mark or character used as a conventional representation of an object, function, or process, e.g.
3	server	c	an identification used by a person with access to a computer, network, or online service
4	account	d	a password or code used when logging in.
5	secure	e	being the only one of its kind; unlike anything else
6	unique	f	the continued possession, use, or control of something.
7	symbol	g	go through the procedures to begin use of a computer, database, or system
8	retention	h	a computer or computer program which manages access to a centralized resource or service in a network.

9	login	i	a system of words, letters, figures, or symbols used to represent others, especially for the purposes of secrecy
10	code	j	an arrangement in which a person uses the Internet or e-mail services of a particular company

1	2	3	4	5	6	7	8	9	10

T.5.1 Listen and check.

T.5.2 Listen and match the following phrase.

1.payment	a. access
2. social	b. websites
3. gains	c. networking
4. online	d. cracker
5. dangerous	e. attack
6. good	f. services
7. personal	g. password
8. password	h. characters
9. combination of	i. shopping
10. dictionary	j.information

1	2	3	4	5	6	7	8	9	10

T. 5. 3 Listen again and complete the sentences.

Passwords are the digital keys to our networks of friends, our work colleagues, and even our banking and payment 1_______________. We want to keep our passwords private to protect our personal lives, and that includes our financial information. While some 2________________ may want to hack into our social networking or email accounts, most want the financial gain that hacking bank accounts can bring.

The most important two passwords are those for your email and social network accounts. If someone gains 3__________ to your email account, they could use the "forgot your password?" link on other websites you use, like online shopping or banking sites. If a hacker gets into your social 4___________, they have the ability to scam your friends by sending out links to dangerous websites or posting fraudulent messages asking for money. The bottom line is that a good password is all that may stand between you and a cybercriminal.

How is it done?

There are many ways that 5____________ can crack your password outside of phishing attempts and spyware. One method is by attempting to log on to your account and guessing your password based off of personal information gained from your security questions. This is why it is extremely important not to include any personal information in your 6______________.

5.Read the text and choose the best title.

1. What is a social engineering attack?
2. What is phishing?
3. How to avoid getting hooked?

To launch a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about a company (your financial institution) or its computer systems. The attacker can look like anyone, and could fool you by saying they're a repairman, or a new intern or employee, and they could actually have identification that says they work for your institution. They'll try to gain your confidence, by asking questions, they may be able to piece together enough information to infiltrate your institution's network. If an attacker is not able to gather enough information from one source, they will try to contact another person in the institution and give the information gleaned from the first person they talked to (you) to add to their credibility and story.

Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

-Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

-Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

-Don't send sensitive information over the Internet before checking a web site's security. Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g.,.com vs. .net).(https://securitytrails.com/blog/social-engineering-attacks)

6.Read the text and define whether the statements are True or False.

1. To launch a social engineering attack, an attacker doesn't use human interaction to obtain or compromise information about a company or its computer systems.

2. The attacker could lie you by saying they're a repairman, or a new intern or employee, and they could actually have identification that says they work for your institution.

3. Phishing is a form of social networking.

4. When users respond with the requested information, attackers don’t use it to gain access to the accounts.

5. If an unfamiliar person claims to be from a legitimate organization, try to verify his or her identity directly with the company.

6. You should pay attention to the URL of a web site.

7.Dos and Don’ts

In order to avoid being a victim of these kinds of hacks, here given a collection of Do’s and Don’ts on how to choose a secure user password. A secure password is one a hacker can't easily guess or crack using software tools and one that is unique and complex. Write Do or Don’ts in each blank.

1._____ use Two-Factor Authentication (2FA) whenever possible. 2FA adds another layer of security to any account you may be logging into. When using 2FA, you can choose two of three types of identification to provide:

1. A password or pin number.
2. A tangible item such as the last 4 digits of a credit card in your possession or a mobile device that a code can be sent to.
3. A part of you such as a fingerprint or voiceprint.

2._____use a combination of uppercase and lowercase letters, symbols and numbers.

3._____ use commonly used passwords such as 123456, the word "password," “qwerty”, “111111”, or a word like, “monkey”.

4._____ make sure your user passwords are at least eight characters long. The more characters and symbols your passwords contain, the more difficult they are to guess.

5._____use a solitary word in any language. Hackers have dictionary-based systems to crack these types of passwords. If you insist on using a word, misspell it as much as possible, or insert numbers for letters. For example, if you want to use the phrase "I love chocolate" you can change it to @1L0v3CH0c0L4t3!

6._____ use a derivative of your name, the name of a family member or the name of a pet. In addition to names, do not use phone numbers, addresses, birthdays or Social Security numbers.

7._____use the same password across multiple websites. If remembering multiple passwords is an issue, you can use a password manager such as Norton Identity Safe to securely store your passwords.

8.______ use abbreviated phrases for passwords. You can choose a phrase such as "I want to go to England." You can convert this phrase to an abbreviation by using the first letters of each word and changing the word "to" to a number "2." This will result in the following basic password phrase: *iw2g2e*. Make it even more complex by adding punctuation, spaces or symbols: *%iw2g2e!@*

9.______ write your passwords down, share them with anyone or let anyone see you log into devices or websites.

10.______ change your passwords regularly.

11.______log out of websites and devices when you are finished using them.

12.______ answer "yes" when prompted to save your password to a particular computer's browser. Instead, rely on a strong password committed to memory or stored in a dependable password management program. Norton Security stores your passwords securely and fills them in online in encrypted form.

If all of this is too much for you, you can simplify this process by using the Norton Identity Safe Password Generator. It will allow you to customize your password by length, and gives you the choice of including letters, numbers, mixed case and punctuation.

This may seem like a long, complicated process to go through just to log into a website, however, it is not as complicated as a cybercriminal gaining access to your passwords and stealing your identity. Just remember that a bit of legwork now can protect you from extremely compromising situations in the long run.

EnglishGrammar

Comparative and Superlative Adjectives			
		Comparative	**Superlative**
Short adjectives	Cheap Small *big	Cheaper Smaller Bigger	Cheapest Smallest Biggest
Adjectives that end in-y	Funn**y** Earl**y** Heav**y**	Funn**ier** Earl**ier** Heav**ier**	Funn**iest** Earl**iest** Heav**iest**
Adjectives with two syllables or more	Careful Boring Expensive Interesting	**More** careful **More** boring **More** expensive **More** interesting	**Most** careful **Most** boring **Most** expensive **Most** interesting
Irregular adjectives	Far Good Bad	Further Better Worse	Furthest Best Worst
*For short adjectives with one vowel + one consonant, double the consonant:			
Hot/hotter/hottest/		*fat/fatter/fattest.*	
*2. **Than** is often used after a comparative adjective.*			
*I'm **younger than** Nilufar.*			
*Nilufar's **more intelligent than** Nargiza.*			
*3. **Much** can come before the comparative to give emphasis.*			
*She's **much nicer than** her sister.*			
*Is Tokyo **much more modern than** London?*			
*4. **The** is used because superlative adjectives.*			
*He's **the funniest** boy in the class.*			
*Which is **the tallest** building in the world?*			

Use

1. Comparatives compare one thing, person or action with another.

She's ***taller*** *than me. / London's* ***more expensive*** *than Rome.*
2.We use superlatives to compare somebody or something with the whole group.
She's the ***tallest*** *in the class. / It's the* ***most expensive*** *hotel in the world.*
3. As … as shows that something is the same or equal.
Olim's ***as tall as*** *Hamid. / I'm* ***as worried as*** *you are*.
4. Not as … as shows that something isn't the same or equal.
She's isn't ***as tall as*** *her mother. / He* ***isn't*** *nearly* ***as clever as*** *me!*

Grammar exercise 1. Fill in the comparative or superlative degrees of the adjectives.

1. In fact, if you conduct a risk-based analysis, you will quickly determine that password expiration does far _____than good and actually increases your risk exposure.(harmful)
2. Also, the greatest risk to your password is no _____ cracking, but password harvesting. (long)
3. They're_____ likely to buy into the program, rendering adverse results.(little)
4. Long passphrases are ____to remember AND to type.(easy)
5. Hands down, this is one of______, most effective ways to secure any authentication requirements.(simple)
6. If you really just can't let the password expiration go gracefully, consider a policy where the _____the password is, the ____frequently people have to change it.(long, little)
7. In this day and age, changing passwords every 90 days gives you the illusion of _____ security while inflicting needless pain, cost, and ultimately additional risk to your organization. (strong)
8. Current research strongly indicates that mandated password changes do ______than good. (harmful)
9. They drive users to choose _____passwords, re-use passwords, or update old passwords in ways that are easily guessed by hackers.(weak)

10. When the user's password expires, they'll get a notification that appears in the ______ right corner of their screen.(low)

Grammar exercise 2. Find the incorrect form of the adjectives:

1. In addition, if an employee used a mobile device to access Office 365, you can wipe it to ensure the password is no longest stored and recycled from there.
2. By monitoring the modifications that are made it is more easier to track potential security problems.
3. Both NIST and Microsoft guidance highlight a need to move away from traditionally accepted strong password the better practices
4. Ensuring that users create strong passwords could allow administrators to implement more little frequent password expiration dates.
5. Users must understand what constitutes a more stronger password.
6. Because frequent password expiration dates have been industry standard, moving away from that the better practice might seem unnerving.
7. Instead, we suggest using an MFA system to gooder ensure security because it requires several separate pieces of evidence to confirm a user's identity instead of just two.
8. To prevent this, the specific minimum age should be set from three to seven days, making sure that users are more little prone to switch back to an old password.
9. For even more greater security, you could set the minimum password length to 14 characters.
10. Passphrases are easier to remember and type but much hardest to crack due to length.

T. 5.4 Listen and check.

Grammar exercise 3. Complete the Table:

Combination of words	Comparative	Superlative
Reliable password		
Simple composition		
		The most secure password
	Better dictionary	
Long password		
	More popular tag	
		The most finite length
	Weaker tag-rules	
Available hashs		
		The least significant

WRITING an application letter.

Answer the questions below.

What does a job application mean?

What is the real purpose of a job application?

What information is required on a job application?

What is a Job Application Letter?

A letter of application, also known as a cover letter, is a document sent with your resume to provide additional information about your skills and experience to an employer. The letter of application is intended to provide detailed information on why you are are a qualified candidate for the job.

As with all cover letters, the body of this job application letter is divided into three sections:

The introduction, which should include why the applicant is writing.

The body, which discusses relevant qualifications.

The close, which thanks the reader and provides contact information and follow-up details.

Your signature to end the letter.

Applying for a job

8.Look at the job advertisement for a computer programmer at Uz.Daily Telegraph. Write an application letter to the director of the company.

COMPUTER PROGRAMMER

We are looking for a bright, competent computer programmer with at least three years' experience in programming and layout. Strong communication skills are essential and experience of coder, C++ and JAVA is an advantage. Ability to work in a team and to tight deadlines is vital. Send your CV and an application letter to Temur Rashidov, Director of the Uz.Daily Telegraph, Navai Street 80. Tashkent.

Follow these steps:

Dear Mr/Mrs

I am writing to apply for the position of…

Education and experience

Personal skills

I have knowledge of (foreign languages)/I can…

Reasons why you are applying for this job

I look forward to…

Yours faithfully/sincerely

LESSON 5. PASSWORD RETENTION AND PASSWORD ATTACKS

REVISE AND CHECK

CAN YOU:

…speak about various attacks on password?

What is password protection?

What is password guessing attack?

How do hackers guess your password?

How do hackers get personal information?

…write an application letter?

…give definition of:

log in_______________________

username___________________

server______________________

account_____________________

secure______________________

unique______________________

symbol_____________________

retention____________________

login_______________________

code________________________

…do these tests.

1. System hacking involves password hacking as one of the major hacking methodologies.

A. False B. True

2. In ________________ attacks an attacker do not contact with authorizing party for stealing password.

A. active online C. offline

B. non-electronic D. passive online

3. Passwords need to be kept encrypted to protect from such offline attacks.

A. False B. True

4.In ________________ attacks an attacker do not contact with authorizing party for stealing password.

A. active online C. non-electronic

B. offline D. passive online

LESSON 6. ENCRYPT FILES AND DISKS

1.Work in pairs and discuss these questions.

1.What does hardware encryption mean?

2.What is data encryption software?

3.What is the difference between hardware and software encryption? Look at the table and discuss it with your partner.

Hardware vs. Software Encryption

	Dell Hard Drive Encryption	Software Encryption
Computer Memory Resources Consumption	No	Yes
CPU Cycles Consumption	No	Yes
Encryption Key Access	No	Yes
Encryption Key Generation Risk	No	Yes
Turn Off Possibility	No	Yes
Decryption need for OS Maintenance	No	Sometimes
IT Deployement and Management	Easy	Moderate to Difficult
Secure and instant Erase	Yes	No
Recovery password	Yes	Sometimes
Windows Password Synchronization	Yes	Sometimes
Compliance Certification	NSA approved	FIPS 140-2
Remote Management	Yes	Yes
Specific Drive need	Yes	No
Non-Microsoft OS support	No	Sometimes

https://www.slideshare.net/

2.Complete the table looking at the Information given above.

	pros	cons
Software Encryption	______________ ______________ ______________	______________ ______________ ______________
Hardware Encryption	______________ ______________ ______________	______________ ______________ ______________

T. 6.1 Listen and complete the sentences.

Full disk encryption, also known as whole disk 1)______________, protects data that's at rest on a computer or phone, as opposed to email and instant messaging data that's in transit across a network. When done effectively, it prevents any 2)____________ person, including phone and computer makers themselves, from accessing data stored on a disk. This means that if you leave your 3)____________ or phone behind in that a driver's car, or some shifty 4)_____________ tries to access your computer at an airport or other border crossing or when you lose it, they won't be able to get at your data without your help—even if they remove the hard drive and place it in another machine.

Full disk encryption comes built into all major commercial 5)_____________ systems; a user simply has to opt to use it and choose a strong password or phrase. To access a system 6)_____________ with full disk encryption, the user is prompted, after turning on the device but before it boots up fully, to enter that password or phrase. When entered, that password unlocks an encryption key in the system, which in turn unlocks the system, and gives you 7)_____________ to it and your files. Some full disk encryption systems require two-factor authentication, prompting the user to enter not only a password but to slip a smart card into a reader connected to the computer, or enter a number generated randomly by a 8)____________ token.

T.6.2 Listen again and answer the questions.

1. How do you understand “whole disk encryption”?

2.Why do we need full disk encryption?

3.What do full disk encryption systems require?

4.What does full disk encryption protect against?

5.Read the text and find the meaning of these words. If necessary use a dictionary.

1. Encryption- _________________________

2. Storage- ____________________________

3. Decoder- ___________________________

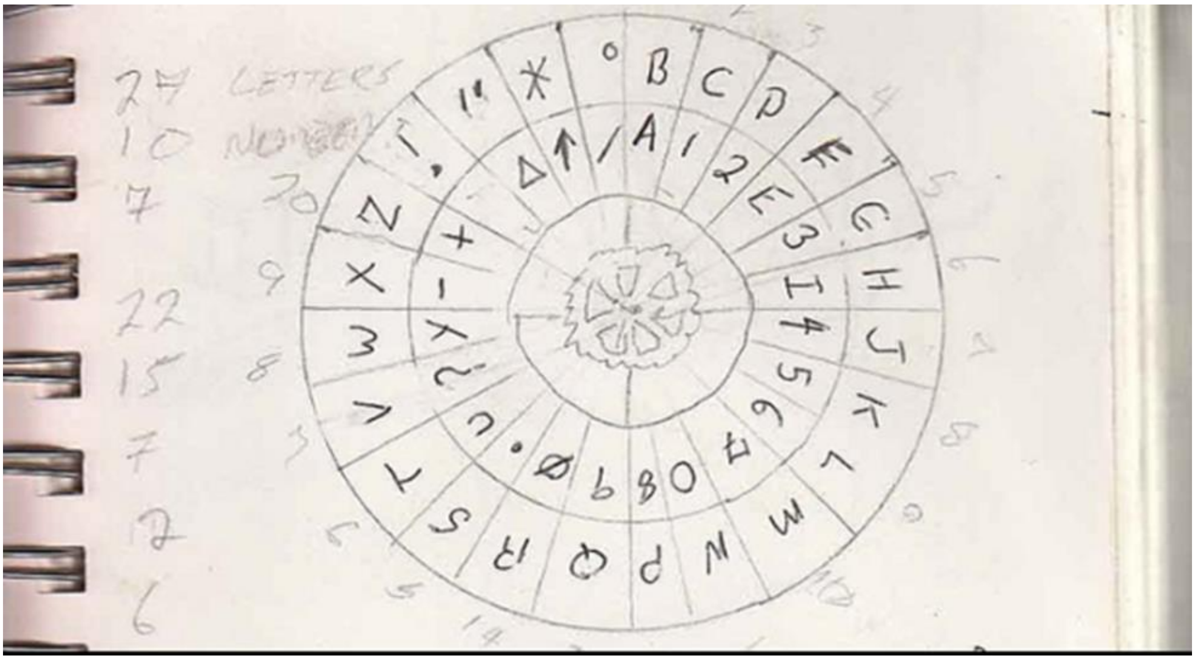
4. Gibberish-___________________________

5. Cipher- _____________________________

6. Retrieve- ___________________________

What Is Encryption?

Encryption is a method of protecting data from people you don’t want to see it. For example, when you use your credit card on Amazon, your computer encrypts that information so that others can’t steal your personal data as its being transferred. Similarly, if you have a file on your computer you want to keep secret only for yourself, you can encrypt it so that no one can open that file without the password. It’s great for everything from sending sensitive information to securing your email, keeping your cloud storage safe, and even hiding your entire operating system. Encryption, at its core, is similar to those decoder rings you played with when you were younger. You have a message, you encode it using a secret cipher, and only other people with the cipher can read it. Anyone else just sees gibberish. Obviously, this is an incredibly simplified explanation. The encryption in your computer is far more complex—and there are different types of encryption that use multiple “decoder rings”—but that’s the general idea.



Should I Encrypt My Files?

First of all, a short answer: yes. Things can get stolen even if you don’t share your computer. All someone needs is a few minutes in front of the keyboard to retrieve anything they want. A login password won’t protect you, either—breaking into a password-protected computer is insanely easy.

Encrypting a select group of files—like the ones that contain personal information—keeps them safe without any extra complications. However, if someone had access to your computer, they could still break into it and view any non-encrypted files, access your browser, install malware, and so on.

Encrypting your entire drive makes it difficult for anyone to access any of your data or even boot up your computer without your password. However, if you experience any corruption on your drive, it’s much less likely that you’ll be able to retrieve that data.

Process and Types of Encryption

To encrypt a file or other information stored in a computer means to convert it into a secret code so that it can't be used or understood until it is decoded or decrypted. You might want to encrypt a file if it contained a secret formula for a new invention, or some financial plans that your competitors would love to know about in advance. When you encrypt something, the computer will ask you to set up a password. After that, no one will be able to make sense of the information unless they have the same password. (https://searchsecurity.techtarget.com/definition/encryption)

6.Read the text and decide whether the statements are True or False.

1. Encryption is a method of protecting data from people you want to see it.
2. The encryption in your computer is complicated—and there are different types of encryption.
3. Everyone wants a few minutes in front of the keyboard to retrieve anything they want.
4. However, if someone had access to your computer, they couldn’t break into it.
5. Encrypting your entire drive makes it easy for anyone to access any of your data.

6.When you encrypt something, you need to set up a password.

EnglishGrammar

<table>
<tr><th colspan="7">Future Simple (Will+infinitive without to)</th></tr>
<tr><th colspan="3">Positive and negative</th><th colspan="4">Questions</th></tr>
<tr><td rowspan="2">I/He/she/
it/you/we/
they</td><td rowspan="2">'ll(will)
won't</td><td rowspan="2">come
help you
invite Umid</td><td colspan="2" rowspan="2">Will</td><td rowspan="2">you</td><td>help me?</td></tr>
<tr><td>Yes, I will.
No, I won't.</td></tr>
<tr><td rowspan="3"></td><td rowspan="3"></td><td rowspan="3"></td><td rowspan="3">What time</td><td rowspan="3">will</td><td>I</td><td rowspan="3">be back?</td></tr>
<tr><td>he/she/it</td></tr>
<tr><td>you
we
they</td></tr>
<tr><td colspan="7">Will is used:</td></tr>
<tr><td colspan="7">1. to express a future intention made at the moment of speaking.</td></tr>
<tr><td colspan="7">a. It's Malika's birthday. Is it? I'll buy her some flowers.</td></tr>
<tr><td colspan="7">b. I'll give you my phone number.</td></tr>
<tr><td colspan="7">c. Do you want the blue or the red pen? I'll take the red one.</td></tr>
<tr><td colspan="7">2. to express an offer.</td></tr>
<tr><td colspan="7">I'll carry your suitcase. We'll do the washing-up.</td></tr>
<tr><td colspan="7">3. to express a future fact. The speaker thinks it is sure to happen in the future.</td></tr>
<tr><td colspan="7">I'll come next week. It will be a nice day tomorrow.
This use is called the pure future. The speaker is talking about the future without expressing an intention, plan or personal opinion.</td></tr>
</table>

Grammar exercise 1. Choose the correct form of the tense.

1. Truly secure encryption **will be / had been** complex enough that a third party is highly unlikely to decrypt the cipher text.
2. This means that you **needed to / will need to** archive de-activated keys and use them only for decryption.

3. An algorithm **will use / used** the key in order to alter the data in a predictable way.
4. Even though the encrypted data **will appear / appears** random, it can be turned back into plaintext by using the key again.
5. A website served over HTTPS instead of HTTP **had / will have** a URL that begins with https:// instead of http://.
6. A website that implements HTTPS **will have / has** an SSL certificate installed on its origin server.
7. At the beginning of the encryption process, the sender must decide what cipher **will best disguise / best disguised** the meaning of the message and what variable to use as a key to make the encoded message unique.
8. If the hardware test fails, the system reboots, and encryption **will not be / had not been** enforced.
9. As a result, quantum-encoded data cannot be copied because any attempt to access the encoded data **changed / will change** the data.
10. Likewise, any attempt to copy or access the data **will cause / caused** a change in the data, thus notifying the authorized parties to the encryption that an attack has occurred.

Grammar exercise 2. Complete the sentences in Future simple tense with the verbs in brackets.

1. Even the slightest change to the message can be detected because it _______ (make) a big change to the resulting hash.
2. _______ the industry ever _______ (reach) a point where all encryption algorithms can be broken by brute force and rendered useless or uneconomic?
3. The bad guys _______ (figure out) how to create a Trojan that steals CPU cycles from all over the world to break encryption.
4. Meanwhile the good guys _______ (find) a way to add another 64 bits, making the decrypt cycles take exponentially longer for brute force -- and on and on it _______ (go).

5. I believe this _______ (happen) if a workable large-scale quantum computer can be developed.
6. The more effective the encryption becomes, the harder the criminals' endeavor on breaking/stealing passwords ________ (be).
7. People like to be helping and preying on that ("Social Engineering") _______ (continue) to be a bigger threat than these sorts of technical discussions.
8. Those trying to decrypt a message ______ (study) the frequency of letters or groups of letters in a cipher text.
9. When you encrypt something, the computer _______ (ask) you to set up a password.
10. After that, no one _______ (be) able to make sense of the information unless they have the same password.

T.6.3 Listen and check.

Grammar exercise 3. Fill in the gaps with the correct tenses.

1. If someone knows the secret key and can figure out the algorithm, communications ________.
   a. insecure
   b. will be insecure
   c. unsecured
   d. will secure
2. A successful approach __________ on the sensitivity and risk level of your organization's information and its data storage methods.
   a. depends
   b. depended
   c. will depend
   d. depending
3. If the encryption algorithm should fall into the interceptor's hands, future messages can still be kept secret because the interceptor ______the key value.

a. do not know
b. did not know
c. have not known
d. will not know

4. The interceptor should not be able to predict what changing one character in the plaintext _________ the cipher text.
    a. did to
    b. done to
    c. will do to
    d. does to
5. An algorithm providing good confusion _________ functional relationship between the plaintext key pair and the cipher text.
    a. will have a complex
    b. had a complex
    c. has a complex
    d. have a complex
6. If we observe the table carefully, we will realize that it contains only 48 bit positions.
    a. will realize that
    b. are realizing that
    c. have realizing that
    d. realized that
7. When you change one bit of the plaintext, you _________ spanning all of the 128 bits of the cipher text block.
    a. see its effect
    b. saw its effect
    c. will see its effect
    d. had seen its effect
8. Plain text encrypted and then encrypted again __________ to the same plain text.

a. leads back

b. leading back

c. lead back to

d. will lead back

9. Once the data has been decrypted by the old key, it __________ by the new key.

a. is encrypted

b. was encrypted

c. been encrypted

d. will be encrypted

WRITING a complaint letter.

Complaint letter is a letter you write to complain about something. It could be something you have purchased or a bad service that you have received, or an accident that happened to you. You must describe it and demand appropriate actions from relevant people. There are three paragraphs in this type of letter:

Paragraph 1 The reason for your complaining about and what happened.

Paragraph 2 What did you do to resolve the situation and how do you feel about the problem.

Paragraph 3 Write what you would like to do and what will you do if they don't do what you want.

7.Sort out expressions in the box into three columns.

<table>
<tr><td colspan="3">The ideal solution would be, I am writing to complain about, I regret to inform you that your service wasn't good, I am writing in regard to, You can imagine how unhappy I was to discover, I hope you can settle this matter by, I would like to draw your attention to, I insist on getting a refund of…</td></tr>
<tr><th>Paragraph 1</th><th>Paragraph 2</th><th>Paragraph 3</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

TASK.

Write a letter of complaint to the manager of an online shopping site about a product that you bought and aren't happy with. In your letter:

- give Information about your order.
- explain about the problem with the product.
- say what you want the manager to do about it.

Dear Sir/Madam,

I am writing to express my dissatisfaction with ________________________

____

____

____

____

____

You can't imagine how unhappy I was to discover________________________

____

____

____

____

____

____

____

I hope you can settle this matter by …(doing something)___________________

____

____

____

____

____

Yours sincerely/ faithfully

LESSON 6. ENCRYPT FILES AND DISKS ***REVISE AND CHECK***

CAN YOU:

…give definition of:

Encryption_______________

Decryption_______________

Storage_________________

Decoder_________________

Gibberish_______________

Cipher__________________

Retrieve________________

File____________________

…say what is the difference between hardware and software encryption?

Is full disk encryption necessary?

What does drive encryption do?

Can encrypted data be recovered?

…write a complaint letter?

…do these tests

1.What is encryption?

A. The process of converting data that has been converted into an unreadable form of text back to its original form

B. The process of verifying the identity of a user who logs on to a system, or the integrity of transmitted data

C. The process of providing proof that a transaction occurred between identified parties

D. The process of converting data into an unreadable form of text

2. What is the term for a password-protected, encrypted data file that can be used to authenticate a program?

A. Cookie C. Encryption key

B. Digital signature D. Digital certificate

3.Which of the following is unlikely to damage or delete data?

A. System crash C. Archiving

B. Virus

LESSON 7. NETWORK SECURITY VULNERABILITIES AND THREATS

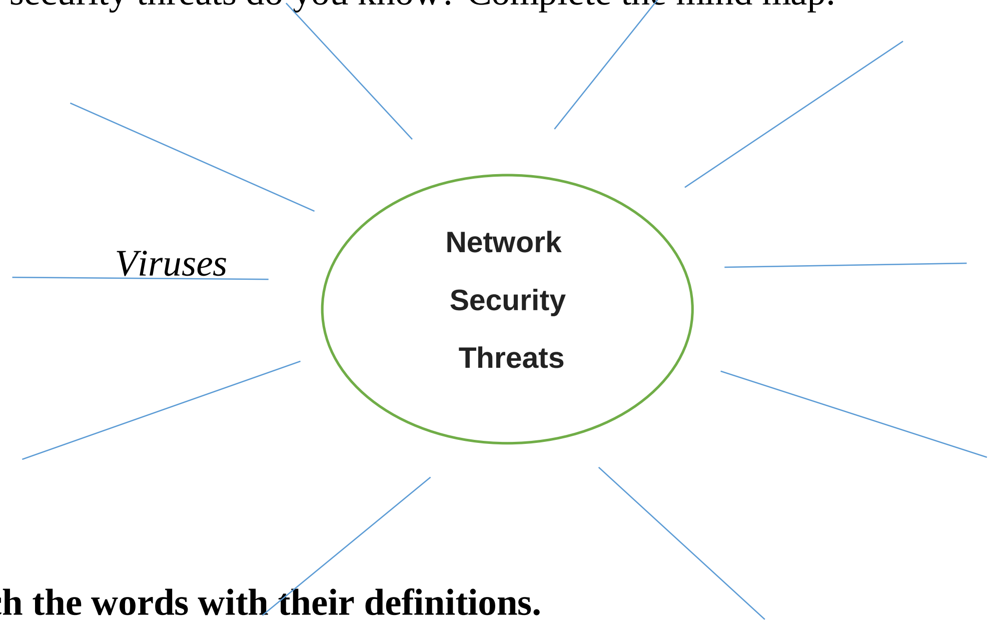
1.Work in pairs and discuss these questions.

1.What are security threats and vulnerabilities?

2.What are the types of network security?

3.What are the 4 main types of vulnerability?

4.What security threats do you know? Complete the mind map.



2.Match the words with their definitions.

	Words		Definitions
1	cloud	a	A set of programs that tell a computer to perform a task.
2	software	b	A malicious application or script that can be used to take advantage of a computer's vulnerability.
3	domain	c	a statement of an intention to inflict pain, injury, damage
4	Virtual Private Network(VPN)	d	A technology that allows us to access our files,services through the internet from anywhere in the world.
5	exploit	e	A type of malware aimed to corrupt, erase or modify information on a computer
6	firewall	f	A group of computers, printers and devices that are interconnected and governed as a whole

7	worm	g	a weakness which can be exploited by an attacker, to perform unauthorized actions within a computer system
8	virus	h	A tool that allows the user to remain anonymous while using the internet by masking the location and encrypting traffic
9	vulnerability	i	A piece of malware that can replicate itself in order to spread the infection to other connected computers.
10	threat	j	A defensive technology designed to keep the bad guys out

1	2	3	4	5	6	7	8	9	10

T. 7.1 Listen and check.

T. 7.2 Listen and match the following phrases.

1. stuff is on your — a. awareness
2 it all suddenly — b. wrong hands
3. ended up in the — c. issues
4. raise — d. computer
5. security — e. working day
6. the next — f. disappeared
7. key to — g. sense measures
8 information protection — h. more secure
9. a high — i. survival
10. keep their info — j. their data
11. common — k. agency
12. backing up — l. priority

1	2	3	4	5	6	7	8	9	10	11	12

T. 7.3 Listen again and put the words into the gaps in the text.

raise	happen	actively	hold	wrong	seriously	holding
encourage	suggests	priority	stressed	reform		
survival	aware	common	crucial			

We all need to take Computer Security Day seriously. Imagine how much important stuff is on your computer. Imagine if it all suddenly disappeared. What would 1____________ if your passwords ended up in the wrong hands? The Association for Computer Security Day started this event in 1988.

It hoped to 2____________ awareness of the importance of security issues. It also wanted to encourage people to think more about their computers and information. Officially, CSD is on November the 30th. However, if this is a weekend, many companies and organizations 3____________ their events on the next working day.

More than 50 countries 4____________ participate in this day, distributing posters and holding workshops. Information is key to 5____________ and success in today's connected world. A top information protection agency stressed: "Information is among a business's greatest assets…It is 6____________ to make information security a high 7____________ and to make employees ____________ of the important role they play in strengthening the organization's security." The Association for Computer Security Day website 8 ____________ over 50 ways for companies to keep their info more secure. These include practical things, like installing smoke alarms in computer rooms, to 9 ____________ sense measures, such as staff regularly changing their passwords and backing up their data. One interesting idea is to: “Declare an amnesty day for computer security violators who wish to 10 ____________.”

5.CHOOSE THE CORRECT WORD Delete the wrong word in each of the pairs.

We all need to take Computer Security Day **serious / seriously**. Imagine how much important stuff/ staff is on your computer. Imagine if it all suddenly disappeared. What would happen if your passwords ended up / down in the wrong hands? The Association for Computer Security Day started this event in 1988.

It hoped to **rise / raise** awareness of the **important / importance** of security issues. It also wanted to encourage people **at / to** think more about their computers and information. Officially, CSD is on November the 30th. However, if this is a weekend, many companies and organizations hold their events on the **after / next** working day. More than 50 countries actively participate in this day, **distributing / distribute** posters and holding workshops. Information is key to survive / survival and success in today’s connected world. A top information protection agency **stressful / stressed:** “Information is **between / among** a business’s greatest assets…It is crucial to make information security a high priority and to make employees aware of the important **roll / role** they play in strengthening the organization’s security.” The Association for Computer Security Day website suggests over 50 ways **for / by** companies to keep their info more **security / secure**.

These include practical things, like installing smoke alarms in computer rooms, to common **sense / senses** measures, such as staff regularly changing their passwords and backing **down / up** their data. One interesting idea is to: “Declare an amnesty day for computer security violators who wish to reform.”

6.Read the text discuss the difference between passive and active threats.

Network Security Threats

Network security threats fall into two categories:

1. Passive threats

(a) Release of message contents

(b) Traffic analysis

2. Active threats

(a) Masquerade

(b) Replay

(c) Modification of message contents

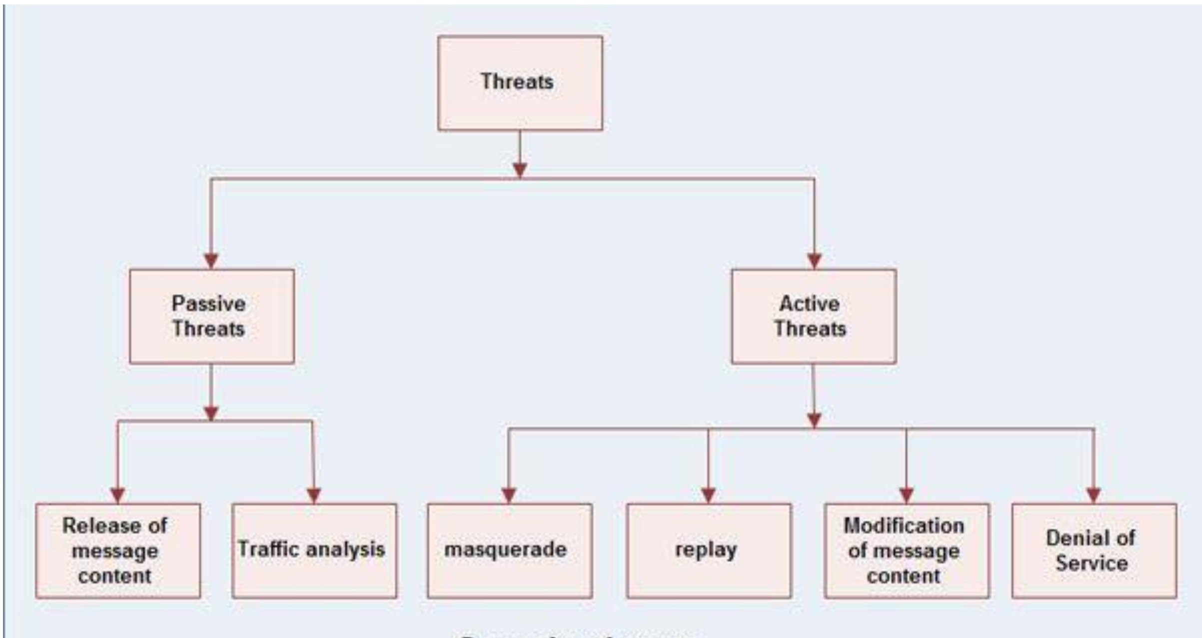
(d) Denial of service

• Passive threats, sometimes referred to as eavesdropping dropping, involve attempts by an attacker to obtain information relating to communication.

(a) Release of message contents

• A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information.

• We would like to prevent the opponent from learning the content of these transmissions.



Security threats

(b) Traffic analysis

• It is a kind of attack done on encrypted messages.

• The opponent might be able to observe the pattern of such encrypted message.

• The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged .

• **Active threats** involve some modification of the data stream or the creation of a false stream.

(a) Masquerade

• It takes place when one entity pretends to be a different entity.

• A masquerade attack usually includes one of the other forms of active attack.

• For *e.g.* authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

(b) Replay

• It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

(c) Modification of message

• It means that some position of a message is altered, or that messages are delayed or rendered, to produce an unauthorized effect.

(d) Denial of service (DOS)

• A denial of service attack takes place when the availability to a resource is intentionally blocked or degraded by an attacker.

• In this way the normal use or management of communication facilities is inhibited.

• This attack may have a specific target. For *e.g.* an entity may suppress all messages directed to a particular destination.

• Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance. (www.theamegroup.com › network-security-threats)

7.Read the text and define whether the statements are TRUE or FALSE.

1. Passive threats, sometimes referred to as eavesdropping dropping, involve attempts by an attacker to get information relating to communication.________

2. A telephone conversation, an e-mail message and a transferred file doesn't contain sensitive or confidential information.__________

3. The opponent can't determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged .________

4. A masquerade attack usually includes two of the other forms of active attack.____

5. A denial of service attack takes place when the availability to a resource is intentionally unblocked or degraded by an attacker.__________

6. Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.___________

EnglishGrammar

<table>
<tr><th colspan="6">Past Simple</th></tr>
<tr><th colspan="6">Positive</th></tr>
<tr><td colspan="2">I
He/she/it
You
We
They</td><td colspan="2">finished
arrived
went</td><td colspan="2">yesterday</td></tr>
<tr><td colspan="3">Question</td><td colspan="3">Short answer</td></tr>
<tr><td colspan="3">Did you go to work yesterday?</td><td colspan="3">Yes, I did.</td></tr>
<tr><td colspan="3">Did it rain last night?</td><td colspan="3">No, it didn't.</td></tr>
<tr><td colspan="6">The negative of the Past Simple is formed with didn't</td></tr>
<tr><td colspan="2">I
He/she/it
You</td><td colspan="2">didn't arrive</td><td colspan="2">yesterday</td></tr>
</table>

We They			
The question in the Past Simple is formed with *did.*			
When	did	she/you/they/etc.	arrive?

Grammar exercise 1. Complete the sentences with the suitable verbs in the Past tense.

become	receive	kick off	
offer	hold	be	aim

The semi-final of the contest "Cyber Security Challenge Uzbekistan" 1……….. at the Palace of youth creativity.

From 18 may to 10 June, the six regions of the country – Samarkand, Fergana, Bukhara, Navoi, Khorezm and Kashkadarya 2……… master classes and pre-selection of participants. Besides, an online testing was carried out on the official website of the project and they 3……… the participants tasks in five competition areas: steganography, cryptography, web vulnerability, vulnerability of operating systems, and software vulnerability. Contestants, who according to the final results have scored the maximum number of points 4……….. semi-finalists and 5……….. the permit for cyber-quest.

The contest "Cyber Security Challenge Uzbekistan" 6……… the country's first open contest in the field of cybersecurity. It 7……….. at increasing the intellectual potential of youth interested in the field of safe information technologies.

Grammar exercise 2. Fill in the gaps with the correct form of the verbs (Past Simple Tense).

1. The history of cyber security ______________(begin) with a research project.
2. A man named Bob Thomas ____________(realize) that it was possible for a computer program to move across a network, leaving a small trail wherever it went.
3. He ____________ (name) the program Creeper
4. A man named Ray Tomlinson _______(see) this idea and ________ (like) it.

5. Then he ________(write) another program—Reaper, the first antivirus software—which would chase Creeper and delete it.
6. The practice of computer security revolving around governance risk and compliance (GRC) therefore ___________ (evolve)separately from the history of computer security software.
7. Network breaches and malware _________ (exist) and were used for malicious ends during the early history of computers, however.
8. At this point in the history of cyber security, computer viruses_________ (begin) to become less of an academic prank, and more of a serious threat.
9. Increasing network connectivity _________ (mean) that viruses like the Morris worm nearly ________ (wipe) out the early internet, which________ (begin) to spur the creation of the first antivirus software.
10. He _________ (write) a program designed to propagate across networks, infiltrate Unix terminals using a known bug, and then copy itself.

WRITING an e-mail.

Discuss these questions.

1. What is email simple words?
2. How do you write an email?
3. What is the format of an email address?

Email stands for electronic mail. It is the easiest and the cheapest way of communication. Emails are of three types:

- **Informal email** (An email written for any friends, family members or relatives).

-**Semi-Formal email** (An email written for any teammates or colleague).

-**Formal email** (An email written for business communication or professional, for any government department, school authority, company or any officers).

The email writing format is the same for each of the categories. Though the choice of words and language differ depending upon the type of email. One can use friendly and casual language in informal emails. The language used in formal emails should be professional, clear, and formal. The email writing format is:

From: Sender’s email id

To: Recipient’s email id

Subject: Title or the reason of writing mail

Salutations: Words like Dear, Respected, Hi etc.

Main body: The main content of the mail

1.Introduction

2.Matter in detail

3.Conclusion

Closing: Ending statement

Attachments: Attached files with emails

Signature line: Sender’s name, signature and other details of contact

Write an email to the course enrollment “Future with computers” which is organized by the authority of Computer Engineering faculty of TUIT.

-Give personal information.

-Ask about starting date/time/fees/course duration.

-What courses are you aimed to attend/requirements.

-Qualification and certification etc.

LESSON 7. NETWORK SECURITY VULNERABILITIES AND THREATS

CAN YOU: ***REVISE AND CHECK***

…count network security threats?

…tell about network security vulnerabilities?

What are the 4 main types of vulnerability?

What are the types of network security?

…write an e-mail?

…give definition of:

Cloud____________________

Software____________________

Domain____________________

Virtual Private Network(VPN)__

Exploit____________________

Firewall____________________

Worm____________________

Virus____________________

Vulnerability________________

Threat____________________

…do these tests

1.A strong password is better with;

A. A simple password based on interests.

B. A password no one would relate to you but you can remember.

C. A complicated password you may forget.

D. A combination of letters, numbers & special characters

2. Which of the following are consider physical security risks?

A. password cracking C. phishing

B. cooking D. Hardware theft

3.Longer passwords are more difficult to brute force.

A. False B. True

4.Choosing the right privacy setting on Facebook can help protect your personal info?

A. False B. True

LESSON 8. WIRELESS NETWORK SECURITY

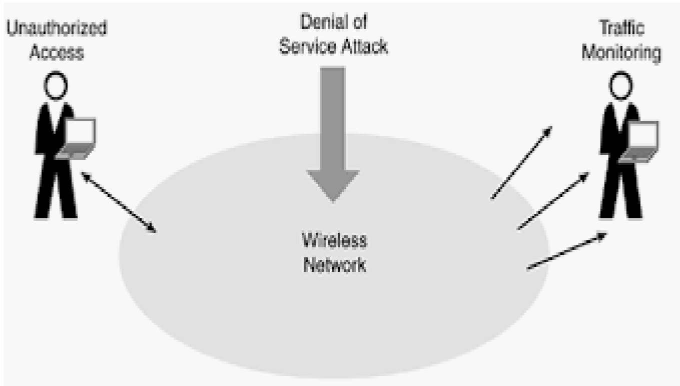
1.In pairs discuss these questions.

1.Why is wireless network security important?

2.What is the best security mode for WiFi?

3.Can router be hacked?

4.Can you see who is using your WiFi?



2. Learn the glossary of common wireless network abbreviations.

1	**IP** - Internet Protocol: technology that supports voice, data and video transmission via IP-based local area networks, wide area networks, and the Internet.
2	**DSL** - Digital Subscriber Lines: various technology protocols for high-speed data, voice and video transmission
3	**DNS** - Domain Name System (or Service, or Server): a program that translates domain names to IP addresses
4	**Wi-Fi** - Wireless Fidelity: a term developed by the Wi-Fi Alliance commonly used to describe any type of 802.11 standard wireless network.
5	**WPA** - Wi-Fi Protected Access: a Wi-Fi security standard that provides a high level of wireless network security.
6	**WEP** - Wired Equivalent Privacy: basic wireless security provided by Wi-Fi.

7	**URL** - Uniform Resource Locator: also referred to as a Web address, since it identifies the location of a file or resource on the Web.
8	**SSL** - Secure Sockets Layer: a commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions.
9	**WAN**-Wide area network
10	**LAN**-Local area network

T. 8.1 Listen and check your pronunciation.

T. 8.2 Listen and choose the best answer.

1.Wireless networks offer great potential for exploitation for ______ reasons.

a) 3 b) 4 c) 2

2. Unlike traditional _____________in which communications travel along a shielded copper wire pair or optical cable,…………….

a) wireless networks b) wired networks c) wide networks

3. Additional wireless access security challenges come through the use of wireless-enabled ____________by employees, …………..

a) network b) devices c) wireless

4. To ensure effective, automated wireless ___________ protection, companies and government organizations should implement a complete wireless security solution…………

a) threat b) attack c) hack

5. ……… in the most secure, easy-to-use and cost-effective ________ available.

a) many b)money c) manner

T.8.3 Listen and fill in the gaps.

The importance of wireless security

Wireless networks offer great potential for exploitation for two reasons; they use the 1___________ for communication, and wireless-enabled laptops are ubiquitous. To make the most of their security planning, enterprises need to focus on threats that pose the greatest risk. Wireless networks are 2___________ in a myriad of ways, some of the most likely problems being rogue access points and employee use of mobile devices without 3__________ security precautions, but malicious hacking attempts and denial-of-service attacks are certainly possible as well. Unlike 4___________ wired networks in which communications travel along a shielded copper wire pair or optical cable, wireless radio frequency signals literally traverse the open air. As a result, RF 5_________ are completely exposed to anybody within range and subject to fluctuating environmental factors that can degrade performance and make management an administrative nightmare. Whether authorized or not, wireless 6__________ points and their users are subject to malicious activity and employee misuse.

5.Read and answer the questions.

1.What are the four major threats to the security of wireless networks?

2.What are the risks of wireless networks?

3.Is wireless network secure?

4.How do you secure a wireless device?

Why Is Wireless Network Security A Concern?

Have you noticed while you're using your home wireless network how many neighbors have wireless networks too?

If you look at the list of wireless networks available to connect to, there's usually quite a few. So if you can see them and they can see you too, how do you protect your wireless network? And what if you're a business with a wireless network - if you have customer data, like credit card numbers on your servers, how do you protect it?

Wireless network access points (which connect your wireless device to the network) typically have an effective range of around 150 feet. So unless you build a home or office with spy-proof, high-tech walls and windows, people outside your building can intercept your wireless network signal. If they can intercept your signal, they can potentially log onto your network and gain access to your devices and data.

Securing your wireless network is vital to protecting your data. The first thing you can do to protect your wireless network is to assign a strong password to the access point. The password for your wireless network is also known as the **network security key**. When you do the initial setup on the wireless access point (if it's one you bought yourself), one of the first questions you're asked during the process is what kind of wireless security do you want to use. The most common today is **WPA2 (Wi-Fi Protected Access 2)**. WPA2 controls the **authentication process** (verifying the identity of both parties before the session begins), and your password is the cornerstone of this sequence.

Access points will broadcast a **SSID (Service Set Identifier)**, a name given to the access point by the end user (or sometimes by the Internet service provider). If you're using an access point or router that was provided by the Internet service provider (ISP), in addition to setting the SSID the ISP, you may also have to set up a default network security key.

Setting up a wireless router includes choosing a strong password. When you log onto a wireless network with the proper password through WPA2 security, the data flowing back and forth is also protected via **encryption**, meaning the data is encoded so no one can use or understand it without the proper key. The combination of the password and the encryption is the heart of your network defenses.

(https://study.com/academy/lesson/wireless-network-security-issues-solutions.

6.Read the text and decide whether the statements are True or False.

1.When you use your home wireless network nobody can see it._______

2. Wireless network access points typically have an effective range of around 150 km._______

3. The first thing you can do to protect your wireless network is to assign a strong password to the access point._______

4. WPA2 controls the authentication process and your password isn't the cornerstone of this sequence._______

5. A wireless router should have a strong password._______

6. The combination of the password and the encryption is the heart of your network defenses.________

EnglishGrammar

Present Perfect Tense		
Have/has + -ed (past participle)		
The past participle of regular verbs ends in-ed. There are many common irregular verbs		
Positive and negative		
I/You/We/They	've (have) haven't	won a competition
He/she/it	's(has) hasn't	
Question		
Have	I/You/We/They	been to the United States?
Has	He/she/it	
Short answer		
Have you been to Las Vegas?	***Yes, I have/No, haven't***	
Has she ever written a novel?	***Yes, she has/No, she hasn't***	
1. The Present Perfect expresses an action or state which began in the past and continues to the present.		
I've known *Jasur for six years.*		

How long ***have*** *you* ***worked*** *for the London Gazette?*
The time expressions for and since are common with this use. We use for with a period of time and since with a point in time.
We've lived here ***for*** *three years.(a period of time)*
They've lived here ***since*** *2010. (a point in time)*
2.In many languages,this use is expressed by a present tense. But in English, we say:
Rashid ***has been*** *a teacher* ***for*** *ten years.* NOT (Rashid is a teacher for ten years.)
3. The Present Perfect connects the present and the past. It expresses experiences in life before now.
I've ***met*** *a lot of famous people. (before now)*
She ***has won*** *a lot of awards. (in her life)*
I've ***travelled*** *a lot in Africa. (in my life)*
She's ***written*** *three books. (up to now)*
The action can continue to the present, and probably into the future.
He's ***made*** *six TV programmes. (So far. He'll probably make more.)*
Ever and never are common with this use.
Have you ***ever*** *been to Africa?*
I've ***never*** *played poker.*
4. The Present Perfect expresses a past action with results in the presents. It is often a recent past action.
I've lost *my wallet. (I haven't got it now)*
*The taxi****'s arrived****. (it's outside the door now)*
Has *the postman* ***been****? (Is there a parcel for me?)*
The adverbs just, already, and yet are common with this use. Yet is used in questions and negatives.
She's ***just*** *had some good news.*
I've ***already*** *had breakfast.*
Has the postman been ***yet?***
It's 11.00 and she hasn't got up ***yet.***

Grammar exercise 1. Use the correct tense form to complete the text.

Wireless networks and security might be considered an oxymoron. Indeed, it is hard to believe in security when it is so easy to access communication media such as wireless radio media. However, the research community in industry and academia 1____ *(for many years extend)* wired security mechanisms or developed new security mechanisms and security protocols to sustain this marriage between wireless/mobile networks and security. Wireless and mobile communication networks 2____ (*have*) tremendous success in today's communication market both in general or professional usage. In fact, obtaining communication services anytime, anywhere and on the move 3____ (*be*) an essential need expressed by connected people. This becomes true thanks to the evolution of communication technologies from wired to wireless and mobile technologies, but also the miniaturization of terminals. Offering services to users on the move 4____ (*significantly improve*) productivity for professionals and flexibility for general users.

Several security mechanisms 5____ (*develop*) such as authentication, encryption and access control others in order to offer secure communications over the network. According to the network environment, some security mechanisms are more mature than others due to the early stages of certain networking technologies such as wireless networks, ad hoc or sensor networks. However, even with maturity, and even if they 6__________ *(be already implemented)* in marketed products, some security mechanisms still need some improvement. It is also important to consider the limited resources of mobile terminals and radio resources to adapt the wired network's security mechanisms to a wireless context.

Grammar exercise 2. Put the verbs in brackets in the correct present perfect forms.

1. We ____ (*put*) all our records on computer
2. Wireless technologies ____ (*become*) increasingly popular in our everyday business and personal lives.
3. The standard is used in designing and implementing cryptographic modules that federal departments and agencies operate or ____ (*operate*) for them.

4. The mobile phone, for instance, ____ (*increase)* functionality that now allows it to serve as a PDA as well as a phone.
5. Because of these fundamental benefits, the WLAN market ____ (*increase*) steadily over the past several years and WLANs are still gaining in popularity.
6. Vendors generally try to correct known software (and hardware) security vulnerabilities when they ____ (*identify*).
7. Vendors ____ (*start*) applying the fix to new wireless products and have developed software patches for many existing products.
8. An intrusion detection system (IDS) is an effective tool for determining whether unauthorized users are attempting to access, ____ (*already access*), or have compromised the network.
9. Network-based IDS sensors that ____ (*place*) on the wired network behind the wireless access point will not detect attacks directed from one wireless client to another wireless client (i.e., peer to peer) on the same subnet.
10. Because the agent resides on the component itself, the host-based system is able to examine the data after it ___ (*decrypt*).

Time words

- Since is usually used with Perfect tenses to express a starting point. The Perfect tense is used in the main clause.

He has been here since July. I've known him since we were at school.

- For is used to express the duration of an action.

She has been in Lisbon for ten days. She had been working there for two years before she applied for a new post.

- Already is used with Perfect tenses in mid - or end - position in statements and questions.

She had already dressed when Tohir arrived. Has she cooked dinner already?

- Yet is used with Perfect tenses in negative sentences after a contracted auxiliary or at the end of the sentence.

She hasn't yet passed her exams. She hasn't passed her exams yet.

- In questions yet only comes at the end.

Has he come yet?

- Still is used in statements and questions after the auxiliary or before the main verb.

I can still walk long distances. Can she still play the piano well?

Grammar exercise 3. Underline the correct item.

1. **Since/For** the 1970s, two cryptography families emerged.
2. A series of algorithms named SHA-256, SHA-224 and SHA-512 have been invented by the NSA (National Security Agency) **since/for** 2000.
3. As has **already/yet** been noticed, the watermarking paradigm covers heterogeneous applications, very often with contradictory aims and challenges.
4. Watermarking has **yet/already** proved its efficiency in this respect [COX 02].
5. **Yet/Still**, several breaches have been identified. The underlying A3 or A8 cipher may be independently and arbitrarily chosen by GSM operators.
6. This prevents unknown attacks or attacks for which evidence has not **still/yet** been defined from being detected.
7. SS methods have **yet/already** been used in telecommunication applications.
8. Some handheld devices **still/already** use voice authentication for authenticating users to the device or to network resources.
9. **Still/Yet** another solution is to use APs with integrated firewalls.
10. Password protection is **still/already** included with most handheld devices.

T.8.4 Listen and check.

WRITING a summary

Answer these questions.

1.How do you summarize a text?

2.What should be included in a summary?

3.How do you start a summary?

Summary Writing Format

-When writing a summary, remember that it should be in the form of a paragraph.

-A summary begins with an introductory sentence that states the text's title, author and main point of the text as you see it.

-A summary is written in your own words.

-A summary contains only the ideas of the original text. Do not insert any of your own opinions, interpretations, deductions or comments into a summary.

-Identify in order the significant sub-claims the author uses to defend the main point.

-Copy word-for-word three separate passages from the essay that you think support and/or defend the main point of the essay as you see it.

-Cite each passage by first signaling the work and the author, put "quotation marks" around the passage you chose, and put the number of the paragraph where the passages can be found immediately after the passage.

-Write a last sentence that "wraps" up your summary; often a simple rephrasing of the main point.

Task. Summarize the text "Advantages and disadvantages of wireless network". Follow these steps:

1. Read the text.
2. Underline the relevant information in each paragraph.
3. Make points about the main points. Leave out details such as examples.
5. Write the final version of your summary. Don't forget to check the spelling and grammar.

Advantages and disadvantages of wireless network

There are many advantages associated with installing a wireless network compared to a wired network such as mobility, cost-effectiveness and adaptability.

Wireless Networking is relatively cheaper than wired Networks since they require no cables between the computers as well as lower long term costs due to less maintenance since there is less equipment. The reduction of cables also reduces the trip hazard caused by cables running along the floor in most homes. Most wireless network equipment is plug-and-play, which helps reduce the total cost such as vendor installation and eliminates redundancy is case of a system crash.

Wireless Networking is also very mobile and versatile; it is adaptable to most situations and requirements. Wireless networks can easily be set up and dissembled, which is perfect for many people who are on temporary worksites/homes or leased space. It can also provide networking in places where regular wire cannot reach such as the backyard in a home situation. Access points can be used to boost the wireless signal range if required. Since portable workstations such as laptops have become popular, wireless networks can provide quick and easy access to the internet and workspaces for students and teachers in universities etc. It is also extremely easy to add other components onto this type of network such as easy installation of VoIP and printers etc without the need to configure ones computer.

Since wireless networking is a relatively new and contingent form of networking, it is filled with it own hazards and problems such as unreliability and security.

Wireless networks have limited bandwidth, hence they cannot support Video Teleconferencing(VTC). It is also limited in its expandability due to the lack of available wireless spectrum for it to occupy. Wireless Network can also be a security risk if not installed and maintained properly. Wireless networks don't require any physical components to connect up to it such as wires, only a wireless adapter is required which significantly increases the accessibility of the network to potential hackers. This scenario is worsened if the network doesn't contain a password since it can then be accessed by anyone with ease.

Wireless networks also have an increased chance of jamming and interference due to external factors such as fog and dust storms or when a flying object such as an aero plane passes over the field. When too many people in the same area use wireless networks, the band of air that they transmit signals on can become overloaded.

Write at least 100 words.

LESSON 8. WIRELESS NETWORK SECURITY

REVISE AND CHECK

CAN YOU:

...understand these abbreviations:

IP____________________

DSL__________________

DNS__________________

Wi-Fi_________________

WPA_________________

WEP_________________

URL__________________

SSL__________________

WAN_________________

LAN__________________

…speak about WiFi?

Why do we need wireless network security?

What are the three main types of wireless encryption?

How do I secure a network connection?

…**summarize** the given text

...do these tests.

1.Which of the following is NOT a component of a Wi-Fi network?

A. A wireless client C. An access point

B. A wireless LAN controller D. A Bluetooth controller

2.The Wi-Fi brand was created by which organization?

A. ISO C. IEEE

B. Cisco D. Wi-Fi Alliance

3.Wireless networks are flexible because:

A. You can connect a limitless number of computers to one router.

B. You don't need any special hardware other than the router.

C. You can use many computers at a time.

D. You don't need wires to connect your computer to the router.

LESSON 9. RECOVERY AND BACKUP OF DATA

1.Work in pairs and discuss these questions.

1. What is data backup and recovery?

2. How is data recovered?

3. Why is data recovery important?.

4.What are the types of backup?

2.Match the backup and recovery glossary with the definitions.

	Glossary		Definitions
1.	**Backup**	**a.**	Data that has to be kept by a business for regulatory compliance or data that is not being used, but still kept on a storage device.
2.	**Archive data**	**b.**	The process of moving unused data to a storage device.
3.	**Data restore**	**c.**	A system that enables the recovery of data stored on computers which is typically automated, eliminating the need for manual backups.

4.	**Disaster recovery**	**d.**	A log that keeps track of events that happen during the backup process
5.	**Cloud backup**	**e.**	The process of copying files from a backup to the original location.
6.	**Data center**	**f.**	The process of testing the backup and recovery tools a business has in place, before they are necessary.
7.	**Automatic backup**	**g.**	The onsite and offsite storage of data copies.
8.	**Backup log**	**h.**	The process of backing up your data in the cloud as opposed to on-prem or in a data center.
9.	**Backup and recovery testing**	**i.**	A group of networked computers used for storage, processing and distributing data.
10.	**Data archiving**	**j.**	The method your organization will use to get your business back up and running after a disaster.

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

T.9.1 Listen and check.

T.9.2 You are going to listen about four phases of date recovery. Listen and write the key words for each phase of date recovery.

	Key words
Phase 1	______________________ ______________________
Phase 2	______________________ ______________________
Phase 3	______________________ ______________________
Phase 4	______________________ ______________________

T.9.3 Listen again and complete the sentences.

1. The hard drive is ____________ in order to get it running in some form, or at least in a state suitable for reading the data from it.

2. If the spindle motor is bad the ____________ and heads should be moved to a new drive.

3. The longer a ______________ is used, the more likely further data loss is to occur.

4. After the drive has been cloned to a new drive, it is suitable to attempt the retrieval of ______________.

5. Data damage can be caused when, for example, a ____________ is written to a sector on the drive that has been damaged.

6. Corrupted documents can be recovered by several _____________ methods or by manually reconstructing the document using a hex editor.

5.Work in three groups. Jigsaw reading and speaking.

1.Group A Read about **Importance of Backup and Recovery**

2.Group B Read about **Data backup methods**

3.Group C Read about **Data recovery methods**

Importance of Backup and Recovery

The purpose of the backup is to create a copy of data that can be recovered in the event of a primary data failure. Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data. Backup copies allow data to be restored from an earlier point in time to help the business recover from an unplanned event.

Storing the copy of the data on separate medium is critical to protect against primary data loss or corruption. This additional medium can be as simple as an external drive or USB stick, or something more substantial, such as a disk storage system, cloud storage container, or tape drive. The alternate medium can be in the same location as the primary data or at a remote location. For best results, backup copies are made on a consistent, regular basis to minimize the amount data lost between backups.

The more time passes between backup copies, the more potential for data loss when recovering from a backup. Retaining multiple copies of data provides the insurance and flexibility to restore to a point in time not affected by data corruption or malicious attacks.

Data backup methods

- Disks or tape backup. These are the oldest of the backup methods we're discussing. Traditional tape backups have their benefits (fairly inexpensive), but also have their drawbacks (slower backup and recovery times, and management of physical tapes). With tape, you're sequentially backing up your data on a physical device. Hard disks offer a faster backup and recovery process than tape and include additional benefits such as deduplication and data compression.
- Hybrid cloud backup. With a hybrid cloud backup solution, you're essentially backing up data on a local device and in a secure offsite data center for redundancy. You always have a secure local copy of your data, but you also have it stored offsite. Also, your machines are backed up to the local device first, so you don't have to worry about the replication to the cloud affecting the performance of machines or your Internet connection. The best practice, in this case, would be to back up from the local device to a secure offsite data center after business hours (automatically of course).
- Direct-to-cloud backup. With direct-to-cloud backups, you send your data directly to the cloud, bypassing the need for a local device. In this case, you're backing up your data in a remote data center, without the local copy in your office. Depending on your Internet speeds and specs of your machines, these backups could take much longer. Direct-to-cloud backups may make sense for SaaS data because you're essentially doing a backup of data that already lives in the cloud!

Data recovery methods

- Recover from your local device. This only works if you have a device locally (like in the hybrid cloud backup method mentioned above). Some solutions actually allow you to spin up a virtual machine right from the device, so your business operations (applications, settings, files, folders) can all run from the device. This may be a great option if you’ve experienced server failure, or a machine has had a security compromise. And because you’re recovering from your local device, it happens quickly.

- Recover from the cloud. Other solutions require you to download your backed up data from the cloud. This involves transferring gigabytes or even terabytes of data over your Internet connection (in most cases) which could result in hours or even days of downtime. If this is the route you take, it’s imperative you find a solution that can recover from the cloud in a few minutes.
- Recover right in the cloud. If your local device is damaged, some providers can spin up a virtual machine for you right in the cloud, also known as “disaster recovery as a service”. In other words, you can continue to run these important applications right from the cloud!

These are just a few of the ways businesses back up and recover data. There are advantages to each backup method, but finding a solution that offers you the combination of fast, reliable backups and robust recovery solutions can determine how quickly and easily your business can recover. (https://www.netapp.com/us/info/what-is-backup-and-recovery)

Share the information from A/B/C articles. Complete the chart.

	Know	Want to know	Have known
Importance of Backup and Recovery			
Data backup methods			
Data recovery methods			

6.Read the text again and decide whether the statements are True or False.

1. The purpose of the backup is to create a copy of data that can not be recovered in the event of a primary data failure. _______

2. Keeping the copy of the data on separate medium is critical to protect against primary data loss or corruption. __________

3. Floppy disks offer a faster backup and recovery process than tape and include additional benefits such as deduplication and data compression. _________

4. With direct-to-cloud backups, you receive your data directly to the cloud, bypassing the need for a local device. _________

5. If your local device is damaged, some providers can not spin up a virtual machine for you right in the cloud, also known as "disaster recovery as a service"._________

6. Reliable backups and robust recovery solutions can determine how quickly and easily your business can recover. __________

EnglishGrammar

Modal verbs: can, must, may			
These are modal auxiliary verbs.			
Can will	Could would	must	should
They have certain things in common:			
1. *They go with another verb and add meaning.*			
*He **can** play the guitar.*			
*I **must** wash my hair.*			
2. There is no 's in the third person singular. The form is the same for all persons.			
*She **can dance** very well.*			
*He **should try** harder.*			
*It **will rain** soon*			
*We **must hurry**.*			
4. There is no don't/doesn't in the negative.			
*I wouldn**'t** like to be a teacher.*			
They ca**n't** speak French.			
Note			
will not = won't			

*It **won't** rain tomorrow*		
Most modal verbs refer to the present and future. Only can has a Past tense form, could.		
*I **could** swim when I was three.*		
Form		
must + infinitive without *to*		
The Forms of *must* are the same for all persons		
Positive and negative		
I You/We/They He/She	must mustn't	try harder. steal.
Note		
Questions with ***must*** are possible, but ***have t***o is more common. What time do we have to leave?		
Use		
1. Must expresses strong obligation. Generally, this obligation comes From 'inside' the speaker.		
*I **must** have a shower.* (I think this is necessary.) *We **must** get a new car.*		
2. You must … can express a strong suggestion.		
You must *see the Monet exhibition. It's wonderful.* ***You must*** *give me a call when you're next in town.*		

Grammar exercise 1. Complete the sentences with the given modal verbs.

can, should, must, may, need

1. Without data backup and a disaster recovery plan, you … be unable to retrieve data that was lost.
2. Cloud-based backup options have recently gained popularity due to the fact that cloud-based options … replicate data in real-time.

3. Recovering data quickly … be costly without an effective plan in place.
4. Most companies see a backup solution as enough. As long as they have easy and reliable access to data in the event of a disaster, everything … be alright.
5. Here’s why you … have both if you want to protect your pertinent data.
6. By preparing and planning for data loss, you … act quickly without sacrificing budget and productivity related to the loss.
7. Recovery … be required due to physical damage to the storage devices or logical damage to the file system that prevents it from being mounted by the host operating system (OS).
8. The data stored in them ….. not be accessed in a normal way.
9. You ….. to keep your essential files in a second storage environment so that you have access to them if the worst-case scenario were to happen.
10. Few basic computer skill is all you ….. to be able to recover almost anything you’ve lost or deleted permanently.

T.9.4 Listen and check.

Grammar exercise 2. Choose the best answer.

1. Recovery of lost data _______ be performed on the verity of storage media’s including a hard disk drive, solid state drive, USB, laptop or desktop internal hard drive, Flash drive, Memory or SD cards

a) can b) could c) must d) would

2. They carries set of electronic equipment which may abruptly fail, become damaged or simply stops working and all the stored data ______ be compromised.

a) can b) need to c) may d) would

3. Data recovery will look for the desired files around the storage area of aforementioned storage devices and recover them successfully even if the drive stops working or ______ be normally accessed.

a) would b) couldn’t c) can’t d) might

4. In logical failure or damages, you’ll not ______ access the drive

a) must b) be able to c) may d) should

5. You … seek for the alternatives of data recovery like recovery programs or dedicated data recovery experts which ______ guide you well on easily restoring your data from inaccessible storage device.

a) must, can b) should, must c) would, can d) can, can

6. The backup drive itself ______ become corrupt or damaged.

a) should b) must c) can d) may

7. You ______ avoid employing unwanted attempts to get back your data from non-working or physically failed storage devices.

a) should b) can c) must d) shouldn't

8. The user ______ try to put the failed storage device into the freezer to make it accessible one more time so that they can retrieve important files

a) must b) may c) could d) is able to

9. You ______ not be able to access the recovered files sometimes even if the recovery program states that the files have been recovered successfully.

a) must b) should c) ought to d) may

10. Simply deleted or formatted files ______ still be recovered as long as it's not been overwritten or malfunctioned by virus/Trojan programs.

a) can b) must c) should d) might

WRITING a composition.

Discuss these questions.

1.What is a composition in writing?

2.How do you write a composition?

3.How many paragraphs are in a composition?

How To Write A Whole Composition

The following is a general structure to follow for many kinds of writing. Adapt it to specialized assignments as appropriate.

I. Introduction

The introduction is intended to draw the reader into the body of material to follow. It should begin with a general statement or question, sometimes called the "thesis statement” or “thesis question,” followed by a quick narrowing down to the main theme to be developed in the body. Set the stage quickly, give appropriate background, then move right into a transition sentence that will set up the reader for the body.

II. Main (body) part

The body of a written piece is where you elaborate, defend, and expand the thesis introduced in the introduction. The body should support your main contention with supporting evidence and possible objections. A good body presents both sides of a case, pro and con. As you make your case, save your best argument for last. When presenting contrary views, be sure to set forth the strongest arguments so you can avoid being charged with erecting a “straw man.” The body includes three components:

Elaboration: Spell out the details by defining, or by clarifying and adding relevant, pertinent information.

Illustration: Paint a verbal picture that helps make or clarify your point(s). Well illustrated pieces are easier to read and follow than abstract ones.

Argumentation: Give the reasons, justifications, and rationales for the position or view you have taken in the introduction. Draw inferences for the reader and explain the significance or assertions or claims being made.

When moving from one sub-point or argument to another, use connecting or transitional words and phrases that enable your reader to easily follow the flow of your thinking. The following is a partial list of logical connectors that you can use:

exceptions – *but, alas, however, etc.*

illustrations – *for instance, for example, etc*.

conclusions – *thus, so, therefore, consequently, etc.*

comparisons – *similarly, by contrast, etc.*

qualifications – *yet, still, etc.*

additions – *moreover, furthermore, etc.*

III. Conclusion

Make your final appeal to the reader, a finishing, all-encompassing statement that wraps up your presentation in a powerful or even dramatic fashion. Normally a single paragraph, brief and concise, will suffice. The purpose of the conclusion is to leave the reader with an idea or thought that captures the essence of the body while provoking further reflection and consideration.

Task. Write a composition about your native town describing the culture and practices . What changes would you like to bring about in the town.

Read your composition to the class.

LESSON 9. RECOVERY AND BACKUP OF DATA

REVISE AND CHECK

CAN YOU:

…answer what is data backup and recovery?

How does data backup work?

What are the methods of backup?

What are the benefits of backing up data?

…explain modal verbs

…give definition of:

Backup______________________

Archive data__________________

Data restore___________________

Disaster recovery_______________

Cloud backup__________________

Data center____________________

Automatic backup______________

Backup log____________________

Backup and recovery testing______

Data archiving_________________

…do these tests

1.You should backup your data before...

A. a user uses it daily

B. anyone can browse the internet

C. turning off your computer

D. installing anything new

2.Information that is backed up is static which means...

A. if you change the file, it will also change the backup

B. if you change the file, nothing happens,

C. if you change the file, the file is lost

D. if you change the file, you will have to re-backup

3.A network-based data backup is stored...

A. off site

B. on USB

C. on DVDs

D. in file servers

LESSON 10. INFORMATION SECURITY POLICY AND ITS MANAGEMENT

1.Work in pairs and discuss these questions.

1.What is an information security policy?

2.What are the 3 principles of information security?

3.What are the types of security policies?

4.Why do we need security policies?

2.Work with a partner. Look at the puzzle and find the words related to “Information security policy” given in the picture.

F	H	R	A	V	F	A	U	D	I	T	G	G	P	E
Q	A	S	D	F	G	H	J	K	L	E	H	A	R	W
W	R	E	C	O	V	E	R	Y	D	E	N	S	E	Q
E	N	M	K	H	G	F	D	S	A	F	R	D	V	D
R	B	L	L	M	M	N	C	A	U	V	I	F	E	V
T	Y	K	P	A	S	S	X	Z	D	B	S	G	N	M
U	V	H	P	N	E	K	L	N	I	P	K	B	T	B
I	C	F	B	A	C	K	U	P	T	O	I	B	I	V
O	X	D	O	G	U	D	F	G	O	H	N	H	O	C
P	L	A	N	E	R	V	L	S	R	T	T	L	N	X
A	Z	S	O	M	I	B	K	A	S	H	H	O	L	Z
S	L	S	I	E	T	N	V	H	J	G	R	I	K	L
D	K	Q	U	N	Y	J	U	G	D	L	E	U	J	H
F	J	E	Y	T	P	O	L	I	C	Y	A	Y	F	G
G	H	R	T	B	N	M	C	Z	X	T	T	T	D	S
M	E	A	S	U	R	E	S	Q	W	W	E	R	S	A

1____________________ 4____________________

2____________________ 5____________________

3____________________ 6____________________

7____________________ 8____________________

T.10.1 Listen and match the following phrases.

1. strategic a. citizens
2. effective b. purposes
3. illegal c. tasks
4. national d. policy
5. freedom of e. system
6. state f. space
7. information g. threats
8. security h. interests
9. existing i. actions
10. destructive j. measures

1	2	3	4	5	6	7	8	9	10

T.10.2 Listen again and complete the sentences with ONE or TWO words.

According to the ministry, the draft concept identifies the main threats to information security, which should be highlighted in development of effective measures on countering and 1)__________________. Special importance in the project is given to counteracting a new trend of using opportunities of the 2)_________________ for various illegal purposes.

The concept will lay the basic directions for ensuring 3)_________________, as well as national interests in the information space, based on principles of protecting the legitimate rights and freedom of citizens when using the Internet.
The concept will become an important coordinating document, which will determine the 4)______________ of the state policy in the field of information security. It will stimulate formation of safe environment for 5)_____________ interaction and sustainable functioning of information, communication and 6)_______________ systems in the national information space, their safe use in the interests of the individual, society and the state.

5.Read the text and find the words with the following definitions.

1. __________- the basic physical and organizational structures and facilities
2. __________- gather together or acquire an increasing number or quantity of
3. __________ - too long, slow, or dull; tiresome or monotonous
4. __________- the state of being able to see or be seen
5. __________- acting or done in the same way over time, especially so as to be fair or accurate
6. __________- the state of being whole and undivided.
7. __________- certain to remain safe and unthreatened
8. __________- he action of remedying something, in particular of reversing or stopping environmental damage

Why is network security policy management necessary?

Businesses must protect people, physical assets, and data that travels across and lives within their networks. Administrators do this by setting security policies that describe in detail parameters such as who or what is allowed to access which resources.

The job gets more challenging as networks become more complex. Companies with large infrastructures accumulate vast libraries of security policies across a vast array of security products. As organizations add more people and more devices, they seek ways to automate tedious and repetitive tasks, simplify operations, and identify inconsistencies that could leave them vulnerable to attack. Network security policy management helps them gain visibility across their distributed environment, and then organize and standardize these policies to improve business security.

How does network security policy management improve business security?

Security policies govern the integrity and safety of the network. They provide rules for accessing the network, connecting to the Internet, adding or modifying devices or services, and more. However, rules are only effective when they are implemented. Network security policy management helps organizations stay compliant and secure by ensuring that their policies are simplified, consistent, and enforced.

How is network security policy management implemented?

Network security policy management tools and solutions are available. Businesses use them to automate administrative tasks, which can improve accuracy and save time. The solutions can make management processes less tedious and time consuming, and can free up personnel for higher-value projects.

These solutions also help IT teams avoid misconfigurations that can cause vulnerabilities in their networks. And if problems arise, network security policy management solutions can ease troubleshooting and remediation. (https://www.cisco.com/c/en/us/products/security)

6.Read and define whether the statements are True or False.

1. Businesses must save people, physical assets, and data that travels across and lives within their networks.
2. The job gets more challenging as networks become more simple.
3. Network security policy management doesn't help them gain visibility across their distributed environment.
4. Security policies govern the integrity and safety of the network.
5. Businesses use them to automate administrative tasks, which can enhance accuracy and save time.
6. The solutions can not make management processes less tedious and time consuming, and can free up personnel for higher-value projects.

EnglishGrammar

Verb patterns
Here are four verb patterns.
1. Verb + *to* + infinitive
*They **want** to **buy** a new car.* *I'd **like** to **go** abroad.*
2. Verb + .. ing

We ***love going*** *to parties. I* ***enjoy travelling*** *abroad.*
3. Verb + -*ing* or + *to* + infinitive with no change in meaning.
It ***started to rain/raining.*** *I* ***continued to work/working*** *in the library.*
4. Verb + preposition + -*ing*
*We****'re thinking of moving*** *house.* *I* ***love dancing*** *= This is one of my hobbies.*
like doing **and** ***would like to do***
1. *Like doing* and *love doing* express a general enjoyment. *I* ***like working*** *as a teacher. = I am a teacher and I enjoy it.* *I* ***love dancing****. = This is one of my hobbies.*
2. *Would like to do* and *would love to* do express a preference now or at a specific time. *I'****d like to be*** *a teacher. = When I grow up, I want to be a teacher.* *Thanks, I****'d love to dance****. = At a party, I'm pleased you asked me*

Question	**Short answer**
Would you like to dance? *Would you like to come for a walk?*	*Yes, I would./Yes, I'd love to.* *Yes, I would./No, thank you*
Note: No, I wouldn't is not common because it is impolite.	

Grammar exercise 1. Choose the best answer.

1.Organizations large and small must…………… a comprehensive security program to cover both challenges.

a) Creating b) to create c) create d) creates

2.If you would like…………more about how Linford and Company can assist your organization in defining security policies or other services such as FedRAMP, HITRUST, SOC 1 or SOC 2 audits, contact with administration.

a) learning b) to learn c) learn d) learns

3.While entire books have been published regarding how to write effective security policies, below are a few principles to keep in mind when you're ready to start …….. out (or reviewing existing) security policies.

A) to tap b) tap c) tapping d) taps

4…………your security policy truly effective, update it in response to changes in your company, new threats, conclusions drawn from previous breaches, and other changes to your security posture.

a) making b) to make c) make d) makes

5.SPs should …………… all data, programs, systems, facilities, infrastructure, users, third-parties and fourth-parties of an organization.

a) addressing b) to address c) address d) addresses

6.Keeping SOC and CSIRT separate, however, may ……….. an organization clearly define the responsibilities of a partner.

a) to help b) help c) helping d) helps

7.An organization must first ………… its security strategy and then provide a suitable infrastructure for the SOC team to work with.

a) defining b) to define c) define d) defines

8.Organizations will ………… and grow over a period of time; hence, an information security policy should have room for the required version updates.

a) changing b) to change c) changes d) change

9.SIEM systems created correlation rules to group similar events into alerts, this helped teams ………… the tens of thousands of events isolated daily.

a) deal with b) to deal with c) dealing with d) deals with

10.Organizations need ……… solutions that not only group alerts but automatically investigate and validate them.

a) develop b) developing c) to develop d) develops

Grammar exercise 2. Put in the correct form.

1. It is good practice to have employees acknowledge receipt of and agree ______ by them on a yearly basis as well. (abide)
2. **2.** Modern security operations center technology allows the SOC team _______and deal with threats quickly and efficiently.(find)

3. An information security policy (ISP) is a set of rules, policies and procedures designed ____________ all users and networks within an organization meet minimum IT security and data protection security requirements.(ensure)
4. Some industry experts argue that keeping SOC teams and CSIRT teams separate lets them ____________on their core objectives, namely detection vs. response. (concentrate)
5. Training should be conducted ___________ employees of security requirements, including data protection, data classification, access control and general cyber threats. (inform)
6. Up Guard Breach Sight can help combat__________ data breaches and data leaks, avoiding regulatory fines and protecting your customer's trust through cyber security ratings and continuous exposure detection. (prevent)
7. Then, to address what actions are employees allowed __________ while using company resources (namely Internet, email, mobile devices, and wireless networks), you'll want to _____document your Acceptable Use Policy. (take)
8. USERIDs Request Procedures This section outlines in detail the steps required ___________ access to the system or, change access or suspend/delete access. (request)
9. One positive feature of this framework is that it attempts________ the "maturity" of processes and security controls. (characterize)
10. Importantly, because spatiotemporal measurements are somewhat intuitive, the metrics derived from these measurements could also help______ common language between executive management, security personnel, and information technologists. (establish)

T.10.3 Listen and check.

WRITING a film review.

1.What is a film review definition?

2.What should a film review include?

3.How do you structure a review?

A movie review is basically a report on a movie. This has been generally written by experts or critiques after watching a film. A film review includes a lot of things. Different people watch a movie from different perspectives and create different kinds of opinions.

How to write a film review

Title: The simplest solution is to take the title of the film. Puns and allusions are more sophisticated and entertaining.

Introduction: You can start off with information about the film (e.g.financial aspects, awards, reviews) and/or the director (e.g. awards, former movies). Also quotes and/or anecdotes may catch the reader's attention. You can also describe what you expected from the film.

Main part: Provide a brief summary of the plot. Make sure that your summary makes sense to a reader who does not know the movie. Do not refer to specific scenes. Is the plot interesting, believable or rather predictable?

Present the **main actors** and **their characters** and say something about their performance. If you like you may give reasons why you identify with a certain character. Are the actors believable and sympathetic?

State your **opinion** of the movie and give reasons for it. What are its strengths and weaknesses? Support your opinion with specific scenes. Is the **soundtrack** appropriate?

You can relate the film to other well-known examples of its **genre** (thriller, comedy, drama etc.) and/or **theme.** What is unique about your film? Does it have a specific message? If so, do you agree with this message? In which respect is your film superior/inferior?

You can place the film in its cultural context or describe/speculate on the director's **intention and message.**

Conclusion: Either recommend the film or advise against seeing it. Is this only a film for women, men, teenagers? Take care that your final judgement is logically developed from what you have written before (above).

TASK. ***Write about a film you enjoyed or a film that you didn't like. It could be a recent film or a film that you watched a long time ago. (It should be about 180 words).***

Here's how to organize your movie review:

Introduction (with title, release date, background information)__________________

____

____

Summary of the story____

____

____

____

Analysis of the plot elements (rising action, climax)___________________________

____

____

____

Creative elements (dialogues, characters, use of colors, camera techniques, mood, tone, symbols, costumes or anything that contributes or takes away from the overall plot)____

____

____

Opinion (supported with examples and facts from the story)_____________________

____

____

Conclusion (announcing whether the filmmaker was successful in his/her purpose, re-state your evidence, explain how the motion picture was helpful for providing a deeper understand of course topic)____

LESSON 10. INFORMATION SECURITY POLICY AND ITS MANAGEMENT

CAN YOU: ***REVISE AND CHECK***

…give definition of:

Security____________________

Risk_______________________

Audit______________________

Management________________

Accumulate_________________

Challenge___________________

Integrity____________________

Safety______________________

…speak about information security policy?

What should be in an information security policy?

Why do you need an information security policy?

…write a film review

…do these tests

1.Why is it important to have a good understanding of Information Security policies and procedures?

A. Helps protect individuals from being victims of security incidents.

B. Provides an understanding of steps to follow in the event of a security incident

C. Helps to understand levels of responsibility

D. All of the above

2.What should everyone know about information security?

A. Computer security is part of everyone's job

B. Verify everything! Verify who the person is on the phone. Verify that the website is real. Verify that the visitor belongs where you find them.

C. Report anything suspicious to your system administrator

D. Do not ignore unusual computer functioning. It might be a sign of malware.

LESSON 11. RISK MANAGEMENT

1.Work in pairs and answer the questions.

1.What is risk management in simple words?

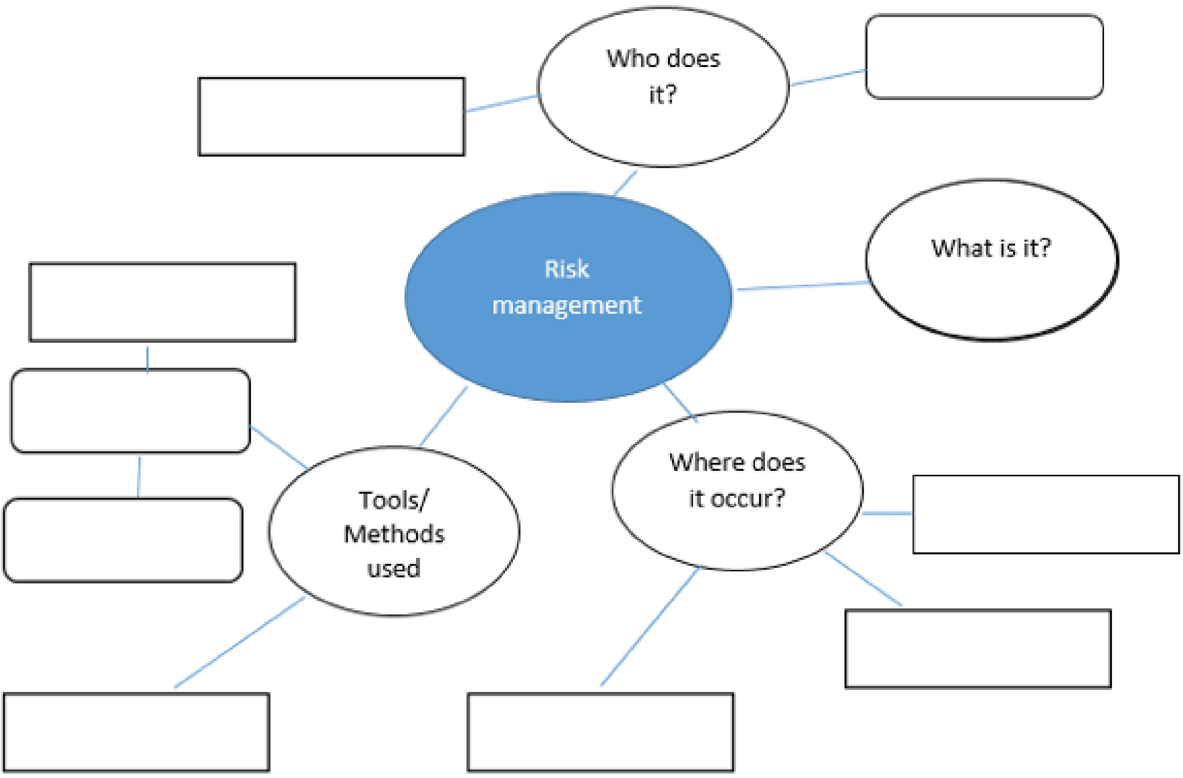
2.What is the main goal of risk management?

3. Why is it important to manage risks?

4.What are the risks of using technology?

5.With your partner read the definition of the risk management and try to complete the mind map.

Risk management is the process of identifying, assessing and controlling threats to an organization's capital and earnings. These threats, or risks, could stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents and natural disasters.



Write your definition for "Risk management".

T.11.1 Listen and write 5 steps of risk management process.

1.____________________________

2.____________________________

3.____________________________

4.____________________________

5.____________________________

T.11.2 Listen again and complete the sentences with the words given in the box.

acceptable	management	potential
monitor	objectives	prevention

1. The Company identifies and defines ________________risks that may negatively influence a specific company process or project.

2. The goal of the analysis is to further understand each specific instance of risk, and how it could influence the company's projects and _________________.

3. The company can then make decisions on whether the risk is ______________and whether the company is willing to take it on based on its risk appetite.

4. These plans include risk mitigation processes, risk _____________tactics and contingency plans in the event the risk comes to fruition.

5. Part of the mitigation plan includes following up on both the risks and the overall plan to continuously ____________ and track new and existing risks.

6. The overall risk____________ process should also be reviewed and updated accordingly.

4.Group work. According to the following ideas conduct the SWOT analysis. SWOT is the method of strategic plan giving structural description and solution for the very problem of any situation. SWOT analysis strategic planning method is to identify the factors of internal and external environment of the object (the object, organization, etc.) and their division into four categories: Strengths, Weaknesses, Opportunities and Threats.

Information technology (IT) risk management

Information technology (IT) plays a critical role in many businesses.

IT **risk management** is the application of the principles of **risk management** to an IT organization in order to manage the **risks** associated with the field. IT **risk management** aims to manage the **risks** that come with the ownership, involvement, operation, influence, adoption and use of IT as part of a larger enterprise.

If you own or manage a business that makes use of IT, it is important to identify risks to your IT systems and data, to reduce or manage those risks, and to develop a response plan in the event of an IT crisis. Business owners have legal obligations in relation to privacy, electronic transactions, and staff training that influence IT risk management strategies.

IT risks include hardware and software failure, human error, spam, viruses and malicious attacks, as well as natural disasters such as fires, cyclones or floods.

You can manage IT risks by completing a business risk assessment. Having a business continuity plan can help your business recover from an IT incident. This guide helps you understand IT risks and provides information about ways to prepare for and respond to IT incidents.

Strengths	Weaknesses
1.Identification of risks 2.______________________________ 3.______________________________	1.______________________________ 2.______________________________ 3.______________________________
Opportunities	Threats
1.______________________________ 2.______________________________ 3.______________________________	1. hardware/software failure 2.______________________________ 3.______________________________

Suggestions____

____

5.Read the text and find the definition of these words.

1. eliminate___________________________________
2. excessive___________________________________
3. asset______________________________________
4. identify____________________________________
5. measure___________________________________
6. reimburse__________________________________

Threat Identification

The first thing to realize is that there is no way to eliminate every threat that may affect your business. There is no such thing as absolute security. To make a facility absolutely secure would be excessive in price, and it would be so secure that no one would be able to enter and do any work. The goal is to manage risks, so that the problems resulting from them will be minimized.

The other important issue to remember is that some threats will be excessive in cost to prevent. For example, there are a number of threats that can impact a server. Viruses, hackers, fire, vibrations, and other risks are only a few. To protect the server, it is possible to install security software (such as anti-virus software and firewalls) and make the room fireproof, earthquake proof, and secure from any number of threats. The cost of doing so, however, will eventually become more expensive than the value of the asset. It would be wiser to back up the data, install a firewall and anti-virus software, and run the risk that other threats will not happen. The rule of thumb is to decide which risks are acceptable.

After calculating the loss that may be experienced from a threat, you will need to find cost-effective measures of protecting yourself. To do this, you will need to identify which threats will be dealt with and how. Decisions will need to be made by management as to how to proceed, based on the data you've collected on risks. In most cases, this will involve devising methods of protecting the asset from threats. This may involve installing security software, implementing policies and procedures, or adding additional security measures to protect the asset.

Another option is to transfer the potential loss associated with a threat to another party. Insurance policies can be taken out insuring the asset, so that if any loss occurs the company can be reimbursed through the policy. Leasing equipment or services through another company can also transfer the risk. If a problem occurs, the leasing company will be responsible for fixing or replacing the assets involved. (https://www.sciencedirect.com/topics/computer-science/threat-identification)

Read the text again and define whether the statements are True or False.

1. The first thing to realize is that there is no way to eliminate every threat that may not affect your business.
2. The goal is to manage risks, so that the problems resulting from them won't be minimized.
3. The other essential issue to remember is that some threats will be excessive in cost to prevent.
4. It would be wiser to back up the data, install a firewall and anti-virus software, and run the risk that other threats will not occur.
5. Leasing equipment or services through another company can not transfer the risk.
6. If a problem happens, the leasing company will be responsible for fixing or replacing the assets involved.

EnglishGrammar

VOICE IN ENGLISH	
ACTIVE	**PASSIVE**
In the active voice, the subject and verb relationship is straightforward: the subject is a do-er. *Our plant in Ohangaron manufacture Artel TV sets.*	The passive voice is used to express what is done to someone or something or to place focus on the object rather than the subject. *Artel TV sets are manufactured in our plant in Ohangaron. (here focus is on Artel TV sets)*
FORMATION	

TENSE	ACTIVE Subject+Verb+object	PASSIVE Object + to be + past participle
Present Simple	We send letters every day. Farida doesn’t clean her room in the morning. Do people all over the world speak English?	Letters are sent every day. The room is not cleaned in the morning. (by Fraida, if you want to show a doer of an action.) Is English spoken all over the world?
Present Continuous	We are sending letters now. Farida is still cleaning her room. Are people all over the world still speaking English?	Letters are being sent now. The room is still being cleaned. Is English still being spoken all over the world?
Past Simple	We sent letters yesterday. Farida didn’t clean her room last week. Did people all over the world speak English 50 years ago?	Letters were sent yesterday. The room wasn’t cleaned last week. Was English spoken all over the world 50 years ago?
Present Perfect	We have just sent letters. Farida hasn’t cleaned her room yet. Have people all over the world speak English for 50 years?	Letters have been just sent. The room hasn’t been cleaned yet. Has English been spoken all over the world for 50 years?
Future Simple	We’ll send letters next week. Farida won’t clean her room tomorrow. Will people all over the world speak English after 50 years?	Letters will be sent next week. The room won’t be cleaned tomorrow. Will English be spoken all over the world after 50 years?

Modals	We must send letters immediately. Farida should clean her room every day. Can people all over the world speak English after 50 years?	Letters must be sent immediately. The room should be cleaned every day. Can English be spoken all over the world after 50 years?

Grammar exercise 1.Fill in the gaps with the correct passive form.

1. Once you've identified the risks that can pose a probable threat to your company, and determined how much loss……………………..(can expect) from an incident.
2. By the time we arrived the thief .... (catch) by the police.
3. The goal is to manage risks, so that the problems resulting from them ………………..(will minimize).
4. Insurance policies can be taken out insuring the asset, so that if any loss occurs the company ………………….(can reimburse) through the policy.
5. It's important to remember that the risk environment is always changing, so this step …………………(should revisite) regularly.
6. Once all reasonable potential solutions …………(list), pick the one that is most likely to achieve desired outcomes.

T.11.3 Listen and check.

Grammar exercise 2. Choose the correct word or words to complete each sentences.

1. Command injection __________ on the software code when system commands are used predominantly.

a.is being achieved c.had been achieved

b.can be achieved d.were being achieved

2. New system commands ________ to existing commands by the malicious attack.

a.appended c.have been appended

b.were being appended d.are appended

3. Software systems __________ to steal information, monitor content, introduce vulnerabilities and damage the behavior of software.

a.attacked c.will attack

b.can be attacked d.was attacked

4. The only way to avoid such attacks is to practice good programming techniques. System-level security _______ using better firewalls.

a.provided c.can be provided

b.was provided d.have been provided

5. The term _______ means taking care of a user's name as well as the identity hidden or veiled using a variety of applications.

a.pseudonymus c.homonymous

b.eponymous d.anonymous

6. In integrity, making sure the data ________ by an unauthorized entity.

a.have not been modified c.be modified

b.has not been modified d.is being modified

7. Data Leakage __ by using tools, software, and strategies known as DLP tools.

a.have been prevented c.can be prevented

b.prevented d.prevent

8. An OSI model is a reference model for how applications ______ over a network.

a.have communicated c.are communicated

b.communicate d.have been communicated

9. In confidentiality, the information ________ just in case someone uses hacking to access the data.

a.strongly encrypt c.have been strongly encrypted

b.should be strongly encrypted d.have strongly encrypted

10. In integrity, if an authorized system is trying to modify the data and the modification was not successful, then the data _________ back.

a.reversed c.has been reversed

b.have been reversed d.should be reversed

WRITING an opinion essay.

1.What types of essays do you know?

2.What is an opinion essay?

3.What are the steps in writing an opinion essay?

4.How do you start your introduction?

5.How do you start your first paragraph?

6.How do you conclude an essay?

An opinion essay is a formal piece of writing which requires your opinion on a topic. Your opinion should be stated clearly. Throughout the essay you will give various arguments/reasons/viewpoints on the topic and these will be supported by evidence and/or examples. You could also include an opposing viewpoint in a paragraph.

Organizing an essay into clear paragraphs.

Introduction: Introduce the topic and give your opinion. Say whether you agree or disagree with the statement.

Body: 2 or 3 paragraphs. For each paragraph give a reason to support your opinion.

Conclusion: Summarize your ideas and repeat your opinion using different words

TASK.Write an essay on the following topic: *Nowadays many universities offer their courses on the Internet so that people can study online. Is this a positive or negative development?*

Introduction____

____

Body(paragraph 1)____

____

Body(paragraph 2)____

Conclusion____

____

____

____

____

LESSON 11. RISK MANAGEMENT

<u>REVISE AND CHECK</u>

CAN YOU:

…**explain** risk management in simple words?

What are the five steps in risk management process?

Why is risk management important?

…**write** an opinion essay

…give definition of:

Eliminate________________

Excessive________________

Asset____________________

Identify_________________

Measure_________________

Reimburse_______________

Responsible______________

Insurance________________

…do these tests

1.Which of these is not a source of risk?

A. Political Risk

B. Technology Risk

C. Environmental Risk

D. Functional Risk

2.Which of the following statements best describes risk?

A. Uncertainty when looking at the past

B. Certainly of not suffering harm or loss

C. Clarity in future decisions

D. Uncertainty when looking to the future

3.Which factor is not normally considered in risk control?

A. Effort

B. Cost

C. Time

D. Quality

LESSON 12. CYBER CRIME

1.Work in pairs and discuss.

1.What are the most harmful Internet activities from the social point of view?

2.What is Cybercrime?

3.What types of cybercrime do you know?

4.What do you understand in these pictures.

2.Match the words with their definitions.

	Words		Definitions
1	malware	a	criminal activities carried out by means of computers or the Internet.
2	cybercrime	b	wrongful or criminal deception intended to result in financial or personal gain
3	hacker	c	a malware computer program that replicates itself in order to spread to other computers
4	illegal	d	a person who commits fraud, especially in business dealings
5	fraud	e	imitate fraudulently
6	worm	f	a person who uses computers to gain unauthorized access to data
7	piracy	g	the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals

			to reveal personal information, such as passwords and credit card numbers.
8	counterfeit	h	contrary to or forbidden by law, especially criminal law
9	fraudster	i	software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
10	phishing	j	the unauthorized use or reproduction of another's work.

1	2	3	4	5	6	7	8	9	10

T.12.1 Listen and check.

T. 12.2 You are going to listen to a radio program. According to Inspector Azimov , what is "Cyber crime"?

Cyber crime is____

____

____

____

____

T.12.3 Listen to the radio program again and choose the best answer.

1. Cybercrime has grown in importance as the computer has become …………… to commerce, entertainment, and government.

a) social

b) central c) science

2.New technologies create new ……………… opportunities.

a) different

b) crucial

c) criminal

3. Cybercrime represents an extension of existing criminal …………….. alongside some novel illegal activities.

a) behavior

b) actions

c) activities

4. Cybercrime highlights the centrality of ………………….. computers in our life.

a) working

b) networked

c) worked

5.Read the text and answer the questions.

1. What was the first cybercrime related to?
2. What was developed in the 90's?
3. How did effect social media on cyber crime?

How Cyber Crime Has Evolved

The history and evolution of cybercrime are easy to track and coincide with the evolution of the Internet itself. The first crimes were of course simple hacks to steak information from local networks but as the Internet became more established so too did the attacks. While cyber crime existed before this, the first major wave of cyber crime came with the proliferation of email during the late 80's. It allowed for a host of scams and/or malware to be delivered to your inbox.

The next wave in the cyber crime history timeline came in the 90's with the advancement of web browsers. At the time there were a multitude to choose from, many more than today, and most were vulnerable to viruses. Viruses were delivered through Internet connections whenever questionable websites were visited. Some caused your computer to run slow, others may have caused annoying pop-up advertising to crowd your screen or redirect you to the illegal sites.

Cyber crime really began to take off in the early 2,000's when social media came to life. The surge of people putting all the information they could into a profile database created a flood of personal information and the rise of ID theft. Thieves used the information in a number of ways including accessing bank accounts, setting up credit cards or other financial fraud.

The latest wave is the establishment of a global criminal industry totaling nearly a half-trillion dollars annually. These criminals operate in gangs, use well-

established methods and target anything and everyone with a presence on the web.
(https://www.le-vpn.com/history-cyber-crime-origin-evolution)

6.Read the text and define whether the statements are True or False.

1. The evolution of cybercrime are related to the evolution of the Internet itself.
2. While cyber crime existed before this, the first major wave of cyber crime came with the proliferation of email during the late 90's.
3. The next wave in the cyber crime history timeline came in the 80's with the advancement of web browsers.
4. Viruses were delivered via Internet connections whenever questionable websites were visited.
5. Cyber crime really start to take off in the early 2,000's when social media came to life.
6. The latest wave is the establishment of a global criminal industry totaling nearly a half-billion dollars annually.

7.Choose the best answer.

1.The word "cyber" is related to ____.

a)computers

b)money

c)crime

2.What does it mean to "remain vigilant for fraud"?

a)to watch out for any kind of illegal cheating or deception

b)to watch out for anyone named Ford

c)to watch out for anything that relates to drugs

d)to watch out for spyware and error messages

3.What is a "heist"?

a) a murder c) a robbery

b) a rape d) a movie

4.**Data theft is when stored information is stolen or accessed.**

a)true b)false

8.Using these words make at least 5 sentences about Cyber crime.

blackmail, identity theft, piracy, money laundering, counterfeiting, internet, attack, spam, fraud database, digital crime

1.____

2.____

3.____

4.____

5.____

EnglishGrammar

Relative clause		
relative pronoun	**use**	**example**
who	subject or object pronoun for people	I told you about the woman *who* lives next door.
which	subject or object pronoun for animals and things	Do you see the cat *which* is lying on the roof?
which	referring to a whole sentence	He couldn't read, *which* surprised me.
whose	possession for people animals and things	Do you know the boy *whose* mother is a nurse?
whom	object pronoun for people, especially in non-defining relative clauses (in defining relative clauses we colloquially prefer *who*)	I was invited by the professor *whom* I met at the conference.
that	subject or object pronoun for people, animals and things in defining relative clauses (*who* or *which* are also possible)	I don't like the table *that* stands in the kitchen.

Defining Relative Clauses
Defining relative clauses (also called identifying relative clauses or restrictive relative clauses) give detailed information defining a general term or expression. Defining relative clauses are not put in commas. *Do you know the girl* ***who*** *is talking to Tohir?* Defining relative clauses are often used in definitions. *A seaman is someone* ***who*** *works on a ship.* Object pronouns in defining relative clauses can be dropped. (Sentences with a relative clause without the relative pronoun are called Contact Clauses.) *The boy* ***(who/whom)*** *we met yesterday is very nice.*
Non-Defining Relative Clauses
Non-defining relative clauses give additional information on something, but do not define it. Non-defining relative clauses are put in commas. *Do you know the girl,* ***who*** *is talking to Tom?* *The book,* ***which*** *I hadn't read, was still on the shelf.*

Grammar exercise 1. Choose the correct relative pronoun (who, which, whose).

1. I talked to the girl **………** car had broken down in front of the shop.
2. Mr Richards, **………** is a taxi driver, lives on the corner.
3. I live in a house in Norwich **…………** is in East Anglia.
4. This is the girl **………** comes from Spain.
5. That's Makhmud, the boy **……….** has just arrived at the airport.
6. Thank you very much for your e-mail **……….** was very interesting.
7. The man, **……….** father is a professor, forgot his umbrella.
8. The children **………** shouted in the street are not from our school.
9. The car, **……..** driver is a young man, is from Ireland.
10. What did you do with the money …….. your mother lent you?

T.12.4 Listen check.

Grammar exercise 2. Make one new sentence from each pair of sentences. Begin as shown, and use the word given in capitals.

1.Madina is a friend. I went on holiday with her. WHO

Madina is the friend who I went on holiday with.

2.This is Mr Xodjayev. His son Baxtiyor plays in our team. WHOSE

This is Mr Xodjayev ....

3.Her book was published last year. It became a best seller. WHICH

Her book ....

4.This is the bank. We borrowed the money from it. WHICH

This is the bank from ....

5.I told you about a person. She is at the door. WHO

The person ....

6.Murod's car had broken down. He had to take a bus. WHOSE

Murod, ...

Grammar exercise 3. Complete the sentences using relative clauses. Use *who* and *which.*

1.A Scot is a person *who* lives in Scotland.

2.Nessie is a monster (live in Loch Ness)________________________________

3.A fridge is a thing (keep food cool) ____________________________________

4.A DJ is someone (play music in a disco) ________________________________

5.A bee is an insect (make honey) ______________________________________

6.A lemon is a fruit (be yellow and sour) _________________________________

7.A watch is a thing (tell the time) ______________________________________

8.A ferry is a ship (carry people across the water) _________________________

9.A shop assistant is someone (work in a shop) ___________________________

10.A key is a thing (can open and lock doors)______________________________

9.CHOOSE THE CORRECT WORD.

Where does cybercrime come from?

Cybercrime, like other crime, is the work of criminals but it is practiced by those who have ***technological/technology*** skills and use the internet to achieve their nefarious ends. Cybercriminals ***employ/employs*** their diverse skill set to access bank accounts, steal identities, blackmail, defraud, stalk, and harass or use a compromised computer as part of a sophisticated botnet to stage DDoS attacks on large institutions.

How do you recognize cybercrime?

Recognizing a cybercrime depends on the crime being committed. Malware ***surreptitiously/surreptitious*** downloaded to your computer might slow it down and prompt it to give you error messages. Phishing attacks, meanwhile, usually involves ***receiving/recieve*** emails from unknown sources trying to trick you into giving up your passwords or personal ***date/data***. Keyloggers leave their own telltale signs, like strange icons, or duplicating your messages. On the other hand, you may never suspect your computer has been enslaved to a botnet.

How do you stop cybercrime?

Resolving cybercrime is a job for the police, ***nationality/national*** cyber security departments, and commercial cyber security firms. On a personal level, however, you can put an end to cybercrime by removing the most common methods of committing these types of crimes: malware. Comprised of viruses, spyware, and ransomware, using a powerful antivirus to ***scan/scanning*** your system and removing dangerous files not only keeps you safe, it ***keep/keeps*** cyber-criminals from making money, which is typically their primary motivation.

Protect yourself from cybercrime

Protecting yourself against cybercrime can be ***time-consumer/time-consuming***, but always worth it. Practicing safe browsing, such as avoiding strange downloads and untrusted sites, is a common-sense solution to cybercrime. Being careful with your login details and personal information can also keep you a step ahead of cybercriminals. But the best thing you can do to protect yourself is to use a powerful antivirus ***program/programs***.

9.Look at the diagram. Write a report describing the process shown.

Useful tips!

1) Look carefully at the diagram and make sure you understand what it is about.

2) Use your answer sheet to make notes on, but remember to cross them out when you have finished your answer.

3) Begin your answer by writing a summary sentence to introduce what the diagram is about.

4) Note that the passive is often used in this task.

LESSON 12. CYBER CRIME

REVISE AND CHECK

CAN YOU:

…give definition of:

Malware____________________

Cybercrime__________________

Hacker______________________

Illegal______________________

Fraud_______________________

Worm_______________________

Piracy______________________

Counterfeit__________________

Fraudster___________________

Phishing____________________

…**speak** about Cyber crime?

What types of cybercrime do you know?

What are the reasons for cyber crime?

How does cybercrime affect society?

…describe a diagram

…do these tests

1.The attempt to obtain sensitive information such as username, password, and credit card details:

A. DDos

B. Firewall

C. Computer virus

D. Phishing scam

2.The word "cyber" is related to ____.

A. crime

B. money

C. people

D. computers

12. To protect a computer from virus, you should install -------- in your computer.

A. backup wizard

B. disk defragmenter

C. disk cleanup

D. antivirus

4.Common cases of cybercrime include fraud, misuse of devices, hacking, identity theft, and cyberstalking.

A. False

B. True

SELF - STUDY MATERIALS AND TASKS

Self – Study № 1.

WORD BUILDING IN ENGLISH

In English new words can be created from existing words in three main ways.

I. Affixation – adding a suffix or prefix.

Suffixes are added to the end of an existing word and used to form different parts of speech. Ex: To inform (verb)-infor**mation** (noun); To animate – anima**tion;** To erase – eras**able** (adjective)

SUFFIXES THAT MAKE NOUNS	
–er /- or: a person who does something	programmer, adviser / advisor, teacher, learner
–ian	optician, mathematician
–ment: result of action	improvement, advancement
–ism: name of system or belief	realism, optimism
–ist: the person who believes in the system	realist, optimist
–ion	confusion, apparition
–ness	happiness
–ship	leadership
–ence / ance	permanence, appearance
–acy	lunacy
–age	marriage
–ity	annuity
–y	photography
–cy	fluency
SUFFIXES THAT MAKE VERBS	
–ify	falsify, modify
–ise	modernise
SUFFIXES THAT MAKE ADJECTIVES	
–ic	idiotic, periodic
–ful	awful, wonderful
–able / ible	comfortable, terrible
–proof / resistant	waterproof, childproof, fireproof
–free	alcohol free beer, nuclear free zone
–less without	hopeless, childless

Prefixes are added to the beginning of an existing word in order to create a new word with a different meaning. Ex: Volatile – **non** - volatile, date – **up**date, formal – **in**formal

COMMON PREFIXES WITH THEIR MEANINGS AND SOME EXAMPLES	
anti (= against)	antivirus, anti-social
auto (self)	autobiography, automobile
bi (= two)	binary
co (= with)	cooperate, coordinate
contra (= against)	contradict, contravene
de (= remove)	deregulate, deselect
dis (= not)	disappear
il (= not)	illegal
im (= not)	immaterial, immature
inter (= between)	international, interface
mis(= badly/wrongly)	misinform, misbehave, misunderstand
multi (= many)	Multimedia, multinational
non (= opposite)	non-linear
out (= more than)	outperform, outdone
over (= too much)	oversleep, overwork
post (= after)	postpone, postnatal
pre (= before)	predict
re (= again)	rewrite, relive
sub (= under)	submarine
super (= higher/improved)	supermarket
trans (= across)	transfer
uni (= one)	uniform
under (= not enough)	underpaid, underfed

II.Conversion – converting words into other parts of speech

Example: *Network (noun) – to network (verb); access – to access; google – to google; host – to host*

III.Compounding - linking together two or more bases to create a new word.

Example: Multi +media – multimedia, Firefox, QuickTime, Open office and so on.

Read the article and give your opinion on it.

By Richard Gray 24th March 2020

Some people hope that outbreaks of the new coronavirus will wane as temperatures rise, but pandemics often don't behave in the same way as seasonal outbreaks. BBC Future looks at what we know.

Many infectious diseases wax and wane with the seasons. Flu typically arrives with the colder winter months, as does the norovirus vomiting bug. Others, such as typhoid, tend to peak during the summer. Measles cases drop during the summer in temperate climates, while in tropical regions they peak in the dry season.

Perhaps unsurprisingly, many people are now asking whether we can expect similar seasonality with Covid-19. Since it first emerged in China around mid-December, the virus has spread quickly, with the number of cases now rising most sharply in Europe and the US.

Many of the largest outbreaks have been in regions where the weather is cooler, leading to speculation that the disease might begin to tail off with the arrival of summer. Many experts, however, have already cautioned against banking too much on the virus dying down over the summer.

A study conducted 10 years ago by Kate Templeton, from the Centre for Infectious Diseases at the University of Edinburgh, UK, found that three coronaviruses – all obtained from patients with respiratory tract infections at hospitals and GP surgeries in Edinburgh – showed "marked winter seasonality". These viruses seemed to cause infections mainly between December and April – a similar pattern to that seen with influenza. A fourth coronavirus, which was mainly found in patients with reduced immune systems, was far more sporadic.

There are some early hints that Covid-19 may also vary with the seasons. The spread of outbreaks of the new disease around the world seems to suggest it has a preference for cool and dry conditions, although it is worth noting that the virus has appeared in countries with a wide range of climates, including hot humid ones.

An unpublished analysis comparing the weather in 500 locations around the world where there have been Covid-19 cases seems to suggest a link between the spread of the virus and temperature, wind speed and relative humidity. Another unpublished study has also shown higher temperatures are linked to lower incidence of Covid-19, but notes that temperature alone cannot account for the global variation in incidence.

Further as-yet-unpublished research predicts that temperate warm and cold climates are the most vulnerable to the current Covid-19 outbreak, followed by arid regions. Tropical parts of the world are likely to be least affected, the researchers say.

https://www.bbc.com/future/article/20200323-coronavirus-will-hot-weather-kill-covid-19

How did COVID-19 affect your life? Share your experience.

Self – Study № 2.

FUTURE TENSES

There are a number of different ways of referring to the future in English. It is important to remember that we are expressing more than simply the time of the action or event. Obviously, any "future" tense will always refer to a **time "later than now"**, but it may also express our **attitude to the future event**.

FUTURE CONTINUOUS			
Form The future continuous is made up of two elements: **the simple future of the verb "to be" + the present participle (base+ing)**			
Subject		**simple future of the verb "to be"**	**present participle**
you		will be	watching
Examples:			
Affirmative	**Negative**	**Interrogative**	**Negative Interrogative**
I will be staying.	I won't be staying.	Will I be staying?	Won't I be staying?
Functions			

1. The future continuous refers to an unfinished action or event that will be in progress at a time later than now. The future continuous is used for quite a few different purposes.

Examples:

This time next week ***I will be sun-bathing*** *in Bali.*
By Christmas ***I will be skiing*** *like a pro.*
Just think, next Monday ***you will be working*** *in your new job.*

2. The future continuous can be used for predicting or guessing about future events.

Examples:

He'll be coming to the meeting, I expect.
I guess you'll be feeling thirsty after working in the sun.
You'll be missing the sunshine once you're back in England.

Time Expressions we use with future continuous:

Tomorrow, tonight, next week/month, etc., in two/three, etc. days, the day after tomorrow, soon, in a week/ month, etc.

FUTURE PERFECT

Form

The future perfect is composed of two elements:
the simple future of the verb "to have" (will have) + the past participle of the main verb

Subject	+ will have	+ past participle of the main verb
He	will have	finished

Function

The future perfect tense refers to a completed action in the future. When we use this tense we are projecting ourselves forward into the future and looking back at an action that will be completed sometime later than now. It is most often used with a time expression.

Examples

I will have been here for six months on June 23rd.
By the time you read this I will have left.
Will you have eaten when I pick you up?

Time Expressions we use with future perfect:

By, by the time, before, until/till, by(then), etc.

FUTURE PERFECT CONTINUOUS

<table>
<tr><td colspan="5"></td></tr>
<tr><td colspan="5">Form
The future perfect continuous is composed of two elements:
the future perfect of the verb "to be" (will have been) + the present participle of the main verb (base + ing)</td></tr>
<tr><td colspan="2">Subject</td><td>+ will have been</td><td colspan="2">+ present participle</td></tr>
<tr><td colspan="2">He</td><td>will have been</td><td colspan="2">playing</td></tr>
<tr><td colspan="5">Examples:</td></tr>
<tr><td>Affirmative</td><td>Negative</td><td>Interrogative</td><td colspan="2">Negative Interrogative</td></tr>
<tr><td>I will have been living</td><td>I won't have been living</td><td>Will I have been living?</td><td colspan="2">Won't I have been living?</td></tr>
<tr><td colspan="5">Function</td></tr>
<tr><td colspan="5">Like the future perfect simple, this form is used to project ourselves forward in time and to look back. It refers to events or actions that are currently unfinished but will be finished at some future time. It is most often used with a time expression.</td></tr>
<tr><td colspan="5">Examples</td></tr>
<tr><td colspan="5">When I finish this course, I will have been learning English for twenty years.
Next year I will have been working here for four years.
When I come at 6:00, will you have been practicing long?</td></tr>
</table>

Grammar Practice.

1. Put the verbs into the correct form (future I progressive).

1. At midnight we (sleep)_____________.
2. This time next week we (sit) _____________ at the beach.
3. At nine I (watch) ____________the news.
4. Tonight we (cram up)____________ for our English test.
5. They (dance)___________ all night.
6. He (not / play)_____________ all afternoon.
7. I (not / work)_______________ all day.
8. (eat / you)____________ at six?
9. (drive / she)______________ to London?
10. (fight / they)_____________ again?

2. Fill in the gaps with the words at the very end of the sentences in **Future Perfect Tense**.

1. When you arrive I probably ___________ the job. **start**

2.They____________ dinner by the time we get there. **have**

3. A few centuries from now wars, I hope, **_________ a** thing of the past. **become**

4. In a year's time he **___________ to** some more serious sort of job. **take**

5. You **__________ a** lot of your work by the end of this month. **do**

6. By November all the leaves **____________. fall**

7. If he doesn't hurry,they____________ before he comes. **leave**

8. I am sure that tomorrow you ______________ all these rules. **forget**

9. Be quick! The child **____________ before** you rescue it. **drown**

10. She **___________ old** before she learns the use of prepositions. **Grow**

Read the text and answer the questions.

1. How is the education system in UK?
2. What are the main parts of the UK education system?
3. What subjects are taught in the UK secondary schools?

The UK education system

The British education system may seem bewildering at first glance, but it is based on long-lived traditions and follows a strict code of rules. Education principles differ slightly in the four countries which constitute the UK, so we will provide you with the basic information on school institutions.

Primary education in the UK

In England and Wales, the law states that all children aged five to sixteen must receive full-time education. In Northern Ireland, the compulsory age for starting school is four. For children under age of five, publicly-funded nurseries and pre-schools are available for a limited number of hours each week.

Children leave primary school at the age of eleven, moving on to secondary school. Parents can choose to educate their children at state or private schools. All children in the UK between the ages of five and sixteen are entitled to a free place at a state school, in contrast with the private education sector, where taxes are quite expensive.

In the UK there are four main types of state schools. First is the community school, which is run by the local authority and has strong links with the local community, sometimes offering use of their facilities and providing services like childcare and adult learning classes.

There are also foundation and trust schools. Foundation schools are run by their own governing body, which employs the staff and sets the admissions criteria; while a trust school is a type of foundation school which forms a charitable trust with an outside partner. Voluntary-aided schools are mainly religious or 'faith' schools, although anyone can apply for a place. As with foundation schools, the governing body employs the staff and sets the admission criteria. Voluntary-controlled schools are similar to voluntary-aided schools, but are run by the local authority.

Secondary education in the UK

At the age of eleven, children start their secondary-school education. From the age of eleven to fourteen, students in British state and private schools study a broad range of 10-15 subjects. Among them are: English, Maths, Science, Design and Technology, Information and Communication Technology (ICT), History, Geography, Modern Foreign Languages, Art and Design, Music, Citizenship, Physical Education. Careers education and guidance, and Religious education may also be included in the education curriculum.

Secondary school graduation covers the period from age fourteen to fifteen. After this two-year period, students take GCSE (General Certificate of Secondary Education) state examinations. The GCSE is a single-subject examination, set and marked by independent examination boards. Students usually take up to ten (there is no upper or lower limit) GCSE examinations in different subjects, including mathematics and English language. After this examination, students may choose to either leave school or continue with their education. They may continue at vocational or technical colleges, or pursue higher education in a university.

University preparation in the UK

At the age of sixteen, following two years of study, students may take A-Levels (Advanced Level examinations) required for university entrance in the UK. Over these two years following secondary school education, students specialize in three or four subjects that are usually relevant to the degree subject they wish to follow at university. At the end of the first year, students take AS level examinations. They continue with three or four of these subjects in the second year and convert them into full A level qualifications at the end of the year. A-Levels are state examinations and are recognized by all UK universities, and by institutions worldwide.

Schools in the UK do not generally rank pupils within their year; currently, the principal standards are the GCSE, SCE and AS and A-Level examination results.

https://www.expatica.com/uk/education/

What differences between the UK and Uzbekistan education system? Tell the class.

Self – Study № 3.

<table>
<tr><th colspan="4">TYPES OF CONDITIONALS
A conditional sentence is a sentence containing the word if.</th></tr>
<tr><th>Type</th><th>Usage</th><th>Used verb form</th><th>Example</th></tr>
<tr><td colspan="4">“Zero” conditional – present real, used to talk about habits, scientific facts, general truths, instructions and rules.
if + present simple... present simple
If you do not brush your teeth, you get cavities.</td></tr>
<tr><td colspan="4">The first conditional – future real, used to talk about things which might happen in the future. <u>If + present simple, ...will + infinitive</u>
If you set a goal, you will ultimately achieve it.</td></tr>
<tr><td colspan="4">The second conditional - future unreal, used to talk about things in the future that are probably not going to be true. <u>If + past simple, ... would + infinitive</u>
If I were you, I would help Madinah as she is in trouble.</td></tr>
<tr><td colspan="4">The third conditional - past unreal, used to describe a situation that didn't happen.
<u>if + past perfect, ... would + have + past participle</u></td></tr>
</table>

If you had worked hard you would have entered the University
Mixed conditional refers to unreal past condition and its probable result in the present. if + past perfect … would + infinitive *If I had won the lottery, I would be rich.*
Wish sentences are used to talk about something that we would like to be different in the present or the future. It's used for things which are impossible or very unlikely.

Grammar Practice.

1.Real:first conditional. Underline the most suitable verb forms in each sentence.

1.If the machine stops / will stop, you press / will press this button.

2.I can’t understand what he sees in her! If anyone treats / will treat / treated me like that, I am / will be / would be extremely angry!

3.If you help / helped me with this exercise, I will / wo uld do the same for you one day.

4.According to the timetable, if the train leaves / left on time, we will / would arrive at 5.30.

5.If it is / will be fine tomorrow, we go / will go to the coast.

6.If we find /found a taxi, we will get / would get there before the play starts.

7.Its quite simple really. If you take / will take / took these tablets every day, then you lose / will lose / lost / would lose weight.

8.I don’t like this flat. I think I am /1 will be / Id be happier if I live / will live / would live / lived in a house in the country.

9.I don’t know how to play baseball, but I’m sure that if I will do / did, I play / will play / would play a lot better than anyone in this awful team!

10.If I phone / will phone / phoned you tonight, are you / will you be / would you be in?

2.Unreal/imaginary situations: second conditional. (See grammar reference). Put each verb in brackets into a suitable verb form.

1.Why didn't you phone?. If I (know) had known you were coming, I (meet) .... you at the airport.

2.It's a pity you missed the party. If you (come) ...., you (meet) .... my friends from Samarkand.

3.If I (have) .... my phone here with me, I (be able) .... to call a taxi now, but I left it at home.

4.If you (not help) .... me, I (not pass) .... the exam.

5.It's a beautiful house, and I (buy) .... it if I (have) .... the money, but I can't afford it.

6.I can't imagine what I (do) .... with the money if I (win) .... the lottery.

7.If Mansur (train) .... harder, he (be) .... a good runner.

8.If Nodira (listen) .... to her mother, she (not marry) .... Nozim in the first place.

3.Wishes and related forms. Underline the most suitable verb form in each sentence.

1.Sorry to ask you, but I'd rather you pay /paid me in advance.

2.Imagine you live / lived in New York. How would you feel?

3.If only I have / had / would have a screwdriver with me.

4.If you want to catch the last train, it's time you leave / left.

5.I'd rather you don't / didn't tell anyone about our conversation.

6.I feel really tired. If only I didn't stay up / hadn't stayed up so late last night.

7.If you don't mind, I'd sooner you practiced / had practiced / would practice your violin somewhere else.

8.It's high time you learn / learned to look after yourself.

9.Anora thinks that everyone likes her. If only she knows / knew what people say behind her back!

10.I'd rather we stay / stayed at home this Navruz for a change.

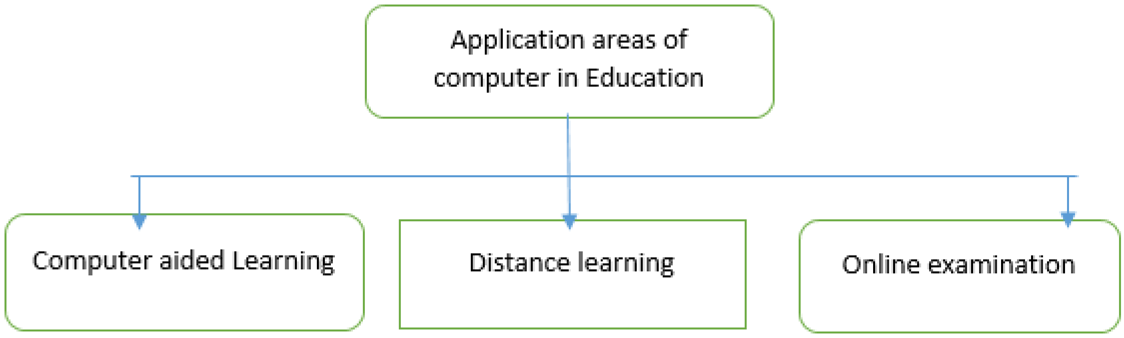
Read the text and find the synonyms of the words or give the definition to them.

Words	Synonyms/Definition
1. evaluate (v)	
2. different (adj)	
3. important (adj)	
4. campus (n)	
5. enhance (v)	
6. impact (v)	

ROLE OF COMPUTER AND INFORMATION TECHNOLOGY(IT) IN EDUCATION

By Dr.Neetu Dabas

In earlier days, computers were used in the classroom to teach the basic skills and provide the knowledge of computer as per the curriculum. For example, word processor was used to improve the writing skills of the students. Moreover, students were evaluated on the basis of standardized test scores or other traditional measures to assess the student's achievement. Computer and its technology has been performed various roles such as tutor, surrogate teacher etc.in different field of education. It changed dramatically in the nature of way of teaching has been used in classrooms. Its technology has proved very successful in education management applications like planning, data analysis etc. According to J. T. Fout ,the first computer was introduced into the field of education as students and teachers learning program". Thereafter, learning process was improved by software sophistication and instruction design and it is still in progress. According to Y.Bo , computer technology should be used to reform the teaching methods and curriculum program and the author also present a report on the usage of computer in the field of education. According to Li. Yumei, computer can be used in education by three different ways such as "As a teacher", "As a learner", and "As an assistant" and author also describe each role in detail. Broadly, one can consider the following roles of education where computer has been effectively used as shown in Figure below.



1. Distance Learning

Computer has become an important part of every walk of life such as on campus, at home and in office. Computer and related technologies have been used in distance learning through various ways such as Teleconferencing, video-conferencing, audio graphics, Teletext, video text, multimedia and hypermedia, e books, online database, online discussion, on-demand call in course etc. Virtual classrooms play an important role in distance learning. Students can raise their doubts and teachers can provide the solutions without going to one's place. The following are the different benefits of using technology in distance learning:-

• Cost effective

• Independent of time and place

• Quality education through results access from mass product of course material

• Simultaneously a lot of students can be benefitted

2. On-Line examination and monitoring

Online examination and monitoring system have completely changed due to the development of modern education technology. These systems ensure about the fairness and impartiality in the examination.Various researchers have been developing online examination system based on web. Today, various exams like GRE, GMAT, SAT, CCNA, MCSE and much more have been conducting computers in all over the world. There are following benefits of using the online examination and monitoring systems:-

• Security

• Fairness and impartiality

• Save time and cost

3. Computer-Aided Learning

Today, computers have improved the quality of teaching and enhance the learning process with the help of various tools such as multimedia projector, PowerPoint presentations etc. Traditional methods of teaching can be monotonous, boring and students start getting frustrated. But information technology make learning process more interested through games, animated graphics etc. There are the following benefits of computer-aided learning:-

• Interest and motivation

• Individualization

• Compatible learning style

• Optimal use of learning time

• Immediate feedback

• Error analysis

• Repetitive practice

• Pre-determined to process syllabus

Computer and its related technology have completely revolutionized our lives. Now, information technology is important in every walk in life. Undoubtedly, computer and information technology great impact in our education system. Various technologies have been used to improve the teaching and learning process. Information technology makes our education system interested and effective. Students can learn better without getting bored and frustrated.

http://www.ijetjournal.org

Read the text again retell it.

Self – Study № 4.

COMPOUND AND COMPLEX SENTENCES

A compound sentence joins two or more independent clauses with a coordinator such *as for, and, or but, or a semi-colon.*

Independent clauses are two phrases that can stand alone as a complete thought. They're not dependent upon one another to express a complete thought, but they tie together similar ideas.

Here are a few examples:

Alex likes to fish *and*	***he is going fishing on Friday***.
an independent clause	an independent clause
I am very smart, *but*	***I do not enjoy school.***
an independent clause	an independent clause

A complex sentence contains at least one independent clause and at least one dependent clause. Dependent clauses can refer to the subject (who, which) the sequence/time (since, while), or the causal elements (because, if) of the independent clause.

The following words act as conjunctions in complex sentences.

after	before	though
although	how	unless
as soon as	if	until
as long as	in order to	when
as though	once	whether
because	since	while

If a sentence begins with a dependent clause, note the comma after this clause. If, on the other hand, the sentence begins with an independent clause, there is not a comma separating the two clauses.

Here are a few examples:

Although she completed her literature review,	***she still needed to work on her methods section.***

a dependent clause	an independent clause
Note the comma in this sentence because it begins with a dependent clause.	
They studied APA rules for many hours	***as they were so interesting*.**
an independent clause	a dependent clause
Note that there is no comma in this sentence because it begins with an independent clause.	
See: **If the flight is on time,** Bobur will get home tonight. Bobur will get home tonight ø **if the flight is on time.**	

Grammar Practice.

1.State which of the following sentences are compound and which are complex?

1. The house was destroyed in the fire, but the whole family was saved.
2. Walking through the wood, he saw a fox that was following him.
3. If I do not get this job, I will start a business.
4. He said that he was so disappointed that he would not try again.
5. The men who rule the world with their pens are mightier than those who rule the world with their swords.
6. The evil that men do lives after them.
7. All that glitters is not gold.
8. Neither the color nor the design of this cloth appeals to me.

2.Combine the following sets into compound or complex sentences using one of the conjunctions from the box given above.

1. I want to travel. I need to earn money.
2. I want to learn. I should practice.
3. You might like this book. You might not.
4. I wish you would call. I miss you.
5. I don't like artichokes. I don't like Brussels sprouts.
6. I studied hard. I was uncertain about my score.
7. Make a schedule. Send me the details.

8. It was so hot outside. Summer came early.

9. Do you want to go to the park? Do you want to go to a movie?

10. I prepared for the presentation. I forgot my USB at home.

Different topics for speaking in English classes.

Friends

- How many real good friends do you have?
- Friends are important for everyone - What do think about it?
- What is more important - the appearance or the character of a person?

Home town

- What would you show a guest in your hometown?
- Tell something about the history of your hometown.
- How can young people spend their free time in your hometown?

Environment

- What do you do to protect the environment?
- Tell something about the dangers of the nature.
- What do you prefer - living in a city or in the country?

Work

- What work do/did you do?
- How do/did you like the work?
- What is your dream job?

Television

- How often do you watch TV?
- What television programs are popular in your country?
- What do you think will be the future of television?
- What is your opinion on television?

Problems

- How do you deal with your problems?
- What problems do you come across in your work or life?
- Do you feel that problems are opportunities? Why or why not?
- What was the last problem you solved and how did you do it?

GLOSSARY

Word/Term	Definition
Access control	Controlling who has access to a computer or online service and the information it stores.
Asset	Something of value to a person, business or organization.
Authentication	The process to verify that someone is who they claim to be when they try to access a computer or online service.
Backing up	To make a copy of data stored on a computer or server to lessen the potential impact of failure or loss.
Bring your own device (BYOD)	The authorised use of personally owned mobile devices such as smartphones or tablets in the workplace.
Broadband	High-speed data transmission system where the communications circuit is shared between multiple users.
Business continuity management	Preparing for and maintaining continued business operations following disruption or crisis.
Certification	Declaration that specified requirements have been met.
Certification body	An independent organization that provides certification services.
Chargeback	A payment card transaction where the supplier initially receives payment but the transaction is later rejected by the cardholder or the card issuing company. The supplier's account is then debited with the disputed amount.

Cloud computing	Delivery of storage or computing services from remote servers online (ie via the internet).
Common text	A structure and series of requirements defined by the International Organization for Standardization, that are being incorporated in all management system International Standards as they are revised.
Data server	A computer or program that provides other computers with access to shared files over a network.
Declaration of conformity	Confirmation issued by the supplier of a product that specified requirements have been met.
DMZ	Segment of a network where servers accessed by less trusted users are isolated. The name is derived from the term “demilitarised zone”.
Encryption	The transformation of data to hide its information content.
Ethernet	Communications architecture for wired local area networks based upon IEEE 802.3 standards.
Firewall	Hardware or software designed to prevent unauthorised access to a computer or network from another computer or network.
Gap analysis	The comparison of actual performance against expected or required performance.
Hacker	Someone who violates computer security for malicious reasons, kudos or personal gain.

Hard disk	The permanent storage medium within a computer used to store programs and data.
Identification	The process of recognising a particular user of a computer or online service.
Infrastructure-as-a-service (IaaS)	Provision of computing infrastructure (such as server or storage capacity) as a remotely provided service accessed online (ie via the internet).
Inspection certificate	A declaration issued by an interested party that specified requirements have been met.
Instant messaging	Chat conversations between two or more people via typing on computers or portable devices.
Internet service provider (ISP)	Company that provides access to the internet and related services.
Intrusion detection system (IDS)	Program or device used to detect that an attacker is or has attempted unauthorized access to computer resources.
Intrusion prevention system (IPS)	Intrusion detection system that also blocks unauthorized access when detected.
'Just in time' manufacturing	Manufacturing to meet an immediate requirement, not in surplus or in advance of need.
Keyboard logger	A virus or physical device that logs keystrokes to secretly capture private information such as passwords or credit card details.

Leased circuit	Communications link between two locations used exclusively by one organization. In modern communications, dedicated bandwidth on a shared link reserved for that user.
Local area network (LAN)	Communications network linking multiple computers within a defined location such as an office building.
Macro virus	Malware (ie malicious software) that uses the macro capabilities of common applications such as spreadsheets and word processors to infect data.
Malware	Software intended to infiltrate and damage or disable computers. Shortened form of malicious software.
Management system	A set of processes used by an organization to meet policies and objectives for that organization.
Network firewall	Device that controls traffic to and from a network.
Outsourcing	Obtaining services by using someone else's resources.
Passing off	Making false representation that goods or services are those of another business.
Password	A secret series of characters used to authenticate a person's identity.
Personal firewall	Software running on a PC that controls network traffic to and from that computer.
Personal information	Personal data relating to an identifiable living individual.

Phishing	Method used by criminals to try to obtain financial or other confidential information (including user names and passwords) from internet users, usually by sending an email that looks as though it has been sent by a legitimate organization (often a bank). The email usually contains a link to a fake website that looks authentic.
Platform-as-a-service (PaaS)	The provision of remote infrastructure allowing the development and deployment of new software applications over the internet.
Portable device	A small, easily transportable computing device such as a smartphone, laptop or tablet computer.
Proxy server	Server that acts as an intermediary between users and others servers, validating user requests.
Restore	The recovery of data following computer failure or loss.
Risk	Something that could cause an organization not to meet one of its objectives.
Risk assessment	The process of identifying, analyzing and evaluating risk.
Router	Device that directs messages within or between networks.
Screen scraper	A virus or physical device that logs information sent to a visual display to capture private or personal information.
Security control	Something that modifies or reduces one or more security risks.

Security information event management (SIEM)	Process in which network information is aggregated, sorted and correlated to detect suspicious activities.
Security perimeter	A well-defined boundary within which security controls are enforced.
Server	Computer that provides data or services to other computers over a network.
Smartphone	A mobile phone built on a mobile computing platform that offers more advanced computing ability and connectivity than a standard mobile phone.
Software-as-a-service (SaaS)	The delivery of software applications remotely by a provider over the internet; perhaps through a web interface.
Spyware	Malware that passes information about a computer user's activities to an external party.
Supply chain	A set of organizations with linked resources and processes involved in the production of a product.
Tablet	An ultra-portable, touch screen computer that shares much of the functionality and operating system of smartphones, but generally has greater computing power.
Threat	Something that could cause harm to a system or organization.
Threat actor	A person who performs a cyber attack or causes an accident.

Two-factor authentication	Obtaining evidence of identity by two independent means, such as knowing a password and successfully completing a smartcard transaction.
Username	The short name, usually meaningful in some way, associated with a particular computer user.
User account	The record of a user kept by a computer to control their access to files and programs.
Virtual private network (VPN)	Link(s) between computers or local area networks across different locations using a wide area network that cannot access or be accessed by other users of the wide area network.
Virus	Malware that is loaded onto a computer and then run without the user's knowledge or knowledge of its full effects.
Vulnerability	A flaw or weakness that can be used to attack a system or organization.
Wide area network (WAN)	Communications network linking computers or local area networks across different locations.
Wi-Fi	Wireless local area network based uponIEEE 802.11standards.
Worm	Malware that replicates itself so it can spread to infiltrate other computers.

TAPESCRIPTS

LESSON 1 Cybersecurity

T.1.1 1. patch- An update or change or an operating system or application **2. cyberattack-** an attempt by hackers to damage or destroy a computer network or system **3.password-** a string of characters that allows access to a computer system or service **4. malicious**- characterized by malice; intending or intended to do harm **5.domain-** an area of territory owned or controlled by a particular ruler or government **6.bug-** an error, flaw or fault in a computer program or system that causes it to produce an incorrect or unexpected result **7.cybersecurity-** the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. **8.Spyware-** software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive **9.security control-** Anything used as part of a security response strategy which addresses a threat in order to reduce risk.**10.privacy-** the state of being free from public attention

T.1.2 Today, people use the Internet to advertise and sell products in various forms, communicate with their customers and retailers, and perform financial transactions. Due to this, hackers and cybercriminals use the internet as a tool to spread malware and carry out cyber attacks.

Cybersecurity aims to protect the computers, networks, and software programs from such cyber attacks. Most of these digital attacks are aimed at accessing, altering, or deleting sensitive information; extorting money from victims; or interrupting normal business operations.

Cyber Security is classified into the following types:

1.Information Security

Information security aims to protect the users' private information from unauthorized access, identity theft. It protects the privacy of data and hardware that handle, store and transmit that data. Examples of Information security include User Authentication and Cryptography.

2.Network Security

Network security aims to protect the usability, integrity, and safety of a network, associated components, and data shared over the network. When a network is secured, potential threats gets blocked from entering or spreading on that network. Examples of Network Security includes Antivirus and Antispyware programs, Firewall that block unauthorized access to a network.

3.Application Security

Application security aims to protect software applications from vulnerabilities that occur due to the flaws in application design, development, installation, upgrade or maintenance phases.

T.1.4 1.Cyber security **protects** the integrity of a computer's internet-connected systems, hardware, software and data from cyber attacks.

2.Cybersecurity **is** the practice of protecting systems, networks, and programs from digital attacks.

3.Cyber security **refers** to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals.

4.Spyware is a program running in the background that **monitors** the user's computer activities.

5.Anti-Virus Software that **attempts** to identify and eliminate computer viruses and other malicious software by:

6.Every one **uses** electronic communications in some manner; whether it be to check a bank account on a mobile phone, to make reservations at a restaurant, or just browsing social media sites.

7.Personal Use of Cyber Security On personal computers cyber security **includes** the encryption of information.

8.Commercial use of Cyber Security Companies and corporations **rely** on different aspects of cyber security in order to protect the shipments of their products ,and more importantly, the financial information of their customers.

9.Network penetration **is** a very important aspect of infrastructure integrity.

10.Cyber security **makes** use of security standards which **help** organizations in following best security practices and techniques to be used in order to minimize the number of successful cyber attacks.

LESSON 2 Cryptography

T.2.1 **1.A-label-**The ASCII compatible encoded (ACE) representation of an internationalized (unicode) domain name. A-labels begin with the prefix xn--. **2.Authentication-**The process of verifying that a message was created by a specific individual (or program). Like encryption, authentication can be either symmetric or asymmetric. Authentication is necessary for effective encryption. **3.Bytes-like-**A bytes-like object contains binary data and supports the buffer protocol. This includes bytes, byte array, and memory view objects. **4.Cipher –** A cipher is an algorithm, which changes the normal order and arrangement of letters within a message. **5.Cryptography** – Cryptography is the study of hiding the meaning of a message by changing the content of the message using rules. It involves ciphers and codes. **6.Decryption-**The process of converting cipher text to plaintext. **7.Encryption-**The process of converting plaintext to cipher text. **8.Key -**Secret data is encoded with a function using this key. Sometimes multiple keys are used. These must be kept secret, if a key is exposed to an attacker, any data encrypted with it will be exposed. **9.Nonce-**A nonce is a number used once. Nonce is used in many cryptographic protocols. Generally, a nonce does not have to be secret or unpredictable, but it must be unique. A nonce is often a random or pseudo-random number .**10.Plaintext-** User-readable data you care about.

T.2.2 Cryptography, the use of codes and ciphers to protect secrets, began thousands of years ago. Until recent decades, it has been the story of what might be called classic cryptography — that is, of methods of encryption that use pen and paper, or perhaps simple mechanical aids.

Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.

Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored. Cryptography also aids in nonrepudiation. This means that the sender and the delivery of a message can be verified.

T. 2.4 1.Jamila *is working* in the garden. 2. I *am reading* Oliver Twist at the moment. 3. He *is watching* TV now. 4. Who *is playing* the violin? 5. Don't make noise. The baby *is sleeping*. 6. I *am waiting* in the park now. 7. Karim and Saida *are cooking* in the kitchen. 8. He *is making* pizza at the moment. 9. Mother *is knitting* a sweater.10. Sevara and her friend *are coming* over for lunch.

LESSON 3 Symmetric and asymmetric cryptosystems

T. 3.1 1.decipher- convert (a text written in code, or a coded signal) into normal language.**2.symmetric-** made up of exactly similar parts facing each other or around an axis **3.asymmetric-** not symmetrical; lacking symmetry; disproportioned **4.recipient-** a person or thing that receives or is awarded something **5.algorithm-** a process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer **6.secret key-** the piece of information or parameter that is used to encrypt and decrypt messages in a symmetric encryption **7.cryptosystem-** a suite of cryptographic algorithms needed to implement a particular security service, most commonly for achieving confidentiality **8.technique-** a way of carrying out a particular task, especially the execution or performance of an artistic work or a scientific procedure **9.decrypt-** make (a coded or unclear message) intelligible **10.encrypt-** convert (information or data) into a code, especially to prevent unauthorized access.

T.3.2 A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system.

Types of Cryptosystems

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system −

Symmetric Key Encryption

Asymmetric Key Encryption

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key.

Symmetric Key Encryption

The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption.

The study of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems. Prior to 1970, all cryptosystems employed symmetric key encryption. Even today, its relevance is very high and it is being used extensively in many cryptosystems. It is very unlikely that this encryption will fade away, as it has certain advantages over asymmetric key encryption.

Asymmetric Key Encryption

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible. Asymmetric Key Encryption was invented in the 20th century to come over the necessity of pre-shared secret key between communicating people.

T.3.4 1.Authentication is **a** common technique for masking contents of messages or other information traffic so that opponents cannot extract the information from the message.2.Replay an attacker performs **a** capture of **a** data unit and its subsequent retransmission to produce an unauthorized effect. 3.Feistel is **the** block cipher structure in DES.4.**The** greatest common divisor of two integers is the largest positive integer that exactly divides both integers. 5.**The** distribution of bits in a random number sequence should be uniform therefore the frequency of occurrence of ones and zeros should be approximately equal. 6.Miller–Rabin algorithm is typically used to test **a** large number for primality.

LESSON 4. Authentication

T.4.1 1.verification- the state of being verified **2.certification** a certified statement **3.corroboration-** evidence which confirms or supports a statement, theory, or finding; confirmation **4.authorize-** give official permission for or approval to (an undertaking or agent) **5.validation-** the action of checking or proving the validity or accuracy of something **6.verify-** make sure or demonstrate that (something) is true, accurate, or justified **7.credential-** a qualification, achievement, quality, or aspect of a person's background, especially when used to indicate their suitability for something **8.testimony-** a formal written or spoken statement, especially one given in a court of law

9.validate- check or prove the validity or accuracy of **10.declaration-** a formal or explicit statement or announcement

T.4.2 User authentication occurs within most human-to-computer interactions outside of guest accounts, automatically logged-in accounts and kiosk computer systems. Generally, a user has to choose a username or user ID and provide a valid password to begin using a system. User authentication authorizes human-to-machine interactions in operating systems and applications, as well as both wired and wireless networks to enable access to networked and internet-connected systems, applications and resources.

Many companies use authentication to validate users who log into their websites. Without the right security measures, user data, such as credit and debit card numbers, as well as Social Security numbers, could get into the hands of cybercriminals.

Organizations also use authentication to control which users have access to corporate networks and resources, as well as to identify and control which machines and servers have access. Companies also use authentication to enable remote employees to securely access their applications and networks. For enterprises and other large organizations, authentication may be accomplished using a single sign-on (SSO) system, which grants access to multiple systems with a single set of login credentials.

T.4.4 1.Organizations also use authentication to control which users **have** access to corporate networks and resources.2.An old security adage **has** it that authentication factors can be "something you know, something you have or something you are."3.This approach to authentication **has** several drawbacks, particularly for resources deployed across different systems. 4.Now that you **have** routes and views setup for the included authentication controllers. 5.Many smartphones **have** a fingerprint sensor that allows you to unlock your phone. 6.Some facilities **have** retinal scanners, which require an eye scan to allow authorized individuals to access secure areas.

LESSON 5. Password retention and password attacks

T.5.1 1.log in- go through the procedures to begin use of a computer, database, or system **2.username-** an identification used by a person with access to a computer, network, or online service **3.server-** a computer or computer program which manages access to a centralized resource or service in a network. **4.account-** an arrangement in which a person uses the Internet or e-mail services of a particular company **5.secure-** certain to remain safe and unthreatened. **6.unique-** being the only one of its kind; unlike anything else **7.symbol-** a mark or character used as a conventional representation of an object, function, or process, e.g. **8.retention-** the continued possession, use, or control of something **9.login-** a password or code used when logging in **10.code-** a system of words, letters, figures, or symbols used to represent others, especially for the purposes of secrecy.

T.5.2 Passwords are the digital keys to our networks of friends, our work colleagues, and even our banking and payment services. We want to keep our passwords private to protect our personal lives, and that includes our financial information. While some cybercriminals may want to hack into our social networking or email accounts, most want the financial gain that hacking bank accounts can bring.

The most important two passwords are those for your email and social network accounts. If someone gains access to your email account, they could use the "forgot your password?" link on other websites you use, like online shopping or banking sites. If a hacker gets into your social network, they have the ability to scam your friends by sending out links to dangerous websites or posting fraudulent messages asking for money. The bottom line is that a good password is all that may stand between you and a cybercriminal.

How is it done?

There are many ways that hackers can crack your password outside of phishing attempts and spyware. One method is by attempting to log on to your account and guessing your password based off of personal information gained from your security questions. This is why it is extremely important not to include any personal information in your passwords.

Another way that hackers can attempt to gain access to your password is via a password cracker. A password cracker uses brute force by using multiple combinations of characters repeatedly until it gains access to the account.

The shorter and less complex your password is, the quicker it can be for the program to come up with the correct combination of characters. The longer and more complex your password is, the less likely the attacker will use the brute force method, because of the lengthy amount of time it will take for the program to figure it out. Instead, they'll use a method called a dictionary attack, where the program will cycle through a predefined list of common words that are used in passwords.

T.5.4 1.In addition, if an employee used a mobile device to access Office 365, you can wipe it to ensure the password is no **longer** stored and recycled from there. 2.By monitoring the modifications that are made it is **easier** to track potential security problems. 3.Both NIST and Microsoft guidance highlight a need to move away from traditionally accepted strong password the **best** practices. 4.Ensuring that users create strong passwords could allow administrators to implement more **less** frequent password expiration dates. 5.Users must understand what constitutes a **stronger** password 6.Because frequent password expiration dates have been industry standard, moving away from that the **best** practice might seem unnerving 7.Instead, we suggest using an MFA system to **better** ensure security because it requires several separate pieces of evidence to confirm a user's identity instead of just two. 8.To prevent this, the specific minimum age should be set from three to seven days, making sure that users are more **less** prone to switch back to an old password 9.For even more greater security, you could set the minimum password length to 14 characters.10.Passphrases are easier to remember and type but much **harder** to crack due to length.

LESSON 6. Encrypt files and disks

T.6.1 Full disk encryption, also known as whole disk encryption, protects data that's at rest on a computer or phone, as opposed to email and instant messaging data that's in transit across a network. When done effectively, it prevents any unauthorized person, including phone and computer makers themselves, from accessing data stored on a disk. This means that if you leave your laptop or phone behind in that a driver's car, or some shifty agent tries to access your computer at an airport or other border crossing or when you lose it, they won't be able to get at your data without your help—even if they remove the hard drive and place it in another machine.

Full disk encryption comes built into all major commercial operating systems; a user simply has to opt to use it and choose a strong password or phrase. To access a system locked with full disk encryption, the user is prompted, after turning on the device but before it boots up fully, to enter that password or phrase. When entered, that password unlocks an encryption key in the system, which in turn unlocks the system, and gives you access to it and your files. Some full disk encryption systems require two-factor authentication, prompting the user to enter not only a password but to slip a smart card into a reader connected to the computer, or enter a number generated randomly by a security token.

T.6.3 1.Even the slightest change to the message can be detected because it will make a big change to the resulting hash. 2.Will the industry ever reach a point where all encryption algorithms can be broken by brute force and rendered useless or uneconomic? 3.The bad guys will figure out how to create a Trojan that steals CPU cycles from all over the world to break encryption. 4.Meanwhile the good guys will find a way to add another 64 bits, making the decrypt cycles take exponentially longer for brute force -- and on and on it will go. 5.I believe this will happen if a workable large-scale quantum computer can be developed.
6.The more effective the encryption becomes, the harder the criminals' endeavor on breaking/stealing passwords will be. 7.People like to be helping and preying on that ("Social Engineering") will continue to be a bigger threat than these sorts of technical discussions. 8.Those trying to decrypt a message will study the frequency of letters or groups of letters in a cipher text. 9.When you encrypt something, the computer will ask you to set up a password. 10.After that, no one will be able to make sense of the information unless they have the same password.

LESSON 7. Network security vulnerabilities and threats

T.7.1 1.cloud- A technology that allows us to access our files,services through the internet from anywhere in the world.**2.software-** A set of programs that tell a computer to perform a task. **3.domain-** A group of computers, printers and devices that are interconnected and governed as a whole**4.Virtual Private Network(VPN)-** A tool that allows the user to remain anonymous while using the internet by masking the location and encrypting traffic**5.exploit-** A malicious application or script that can be used to take advantage of a computer’s vulnerability.**6.firewall-** A defensive technology designed to keep the bad guys out **7.worm-** A piece of malware that can replicate itself in order to spread the infection to other connected computers **8.virus-** A type of malware aimed to corrupt, erase or modify information on a computer **9.vulnerability-** a weakness which can be exploited by an attacker, to perform unauthorized actions within a computer system **10.threat-** a statement of an intention to inflict pain, injury, damage

T.7.2 We all need to take Computer Security Day seriously. Imagine how much important stuff is on your computer. Imagine if it all suddenly disappeared. What would happen if your passwords ended up in the wrong hands? The Association for Computer Security Day started this event in 1988. It hoped to raise awareness of the importance of security issues. It also wanted to encourage people to think more about their computers and information. Officially, CSD is on November the 30th. However, if this is a weekend, many companies and organizations hold their events on the next working day. More than 50 countries actively participate in this day, distributing posters and holding workshops. Information is key to survival and success in today's connected world. A top information protection agency stressed: "Information is among a business's greatest assets…It is crucial to make information security a high priority and to make employees aware of the important role they play in strengthening the organization's security." The Association for Computer Security Day website suggests over 50 ways for companies to keep their info more secure. These include practical things, like installing smoke alarms in computer rooms, to common sense measures, such as staff regularly changing their passwords and backing up their data. One interesting idea is to: "Declare an amnesty day for computer security violators who wish to reform."

LESSON 8. Wireless network security

T.8.1 1.IP - Internet Protocol: technology that supports voice, data and video transmission via IP-based local area networks, wide area networks, and the Internet. **2.DSL** - Digital Subscriber Lines: various technology protocols for high-speed data, voice and video transmission **3.DNS** - Domain Name System (or Service, or Server): a program that translates domain names to IP addresses **4.Wi-Fi** - Wireless Fidelity: a term developed by the Wi-Fi Alliance commonly used to describe any type of 802.11 standard wireless network. **5.WPA** - Wi-Fi Protected Access: a Wi-Fi security standard that provides a high level of wireless network security.**6.WEP** - Wired Equivalent Privacy: basic wireless security provided by Wi-Fi.**7.URL** - Uniform Resource Locator: also referred to as a Web address, since it identifies the location of a file or resource on the Web. **8.SSL** - Secure Sockets Layer: a commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. **9.WAN**-Wide area network**10.LAN-**Local area network.

T.8.2 Wireless networks offer great potential for exploitation for two reasons; they use the airwaves for communication, and wireless-enabled laptops are ubiquitous. To make the most of their security planning, enterprises need to focus on threats that pose the greatest risk. Wireless networks are vulnerable in a myriad of ways, some of the most likely problems being rogue access points (APs) and employee use of mobile devices without appropriate security precautions, but malicious hacking attempts and denial-of-service (DoS) attacks are certainly possible as well.

Unlike traditional wired networks in which communications travel along a shielded copper wire pair or optical cable, wireless radio frequency (RF) signals literally traverse the open air. As a result, RF signals are completely exposed to anybody within range and subject to fluctuating environmental factors that can degrade performance and make management an administrative nightmare. Whether authorized or not, wireless access points and their users are subject to malicious activity and employee misuse.

Additional wireless access security challenges come through the use of wireless-enabled devices by employees, the growing amount of confidential data residing on those devices, and the ease with which end users can engage in risky wireless behavior.

To ensure effective, automated wireless threat protection, companies and government organizations should implement a complete wireless security solution covering assets across the enterprise that enables them to discover vulnerabilities, assess threats, prevent attacks, and ensure ongoing compliance - in the most secure, easy-to-use and cost-effective manner available.

T.8.4 1.**Since** the 1970s, two cryptography families emerged. 2.A series of algorithms named SHA-256, SHA-224 and SHA-512 have been invented by the NSA (National Security Agency) **since** 2000. 3.As has **already** been noticed, the watermarking paradigm covers heterogeneous applications, very often with contradictory aims and challenges. 4.Watermarking has **already** proved its efficiency in this respect [COX 02]. 5.**Yet**, several breaches have been identified. The underlying A3 or A8 cipher may be independently and arbitrarily chosen by GSM operators. 6.This prevents unknown attacks or attacks for which evidence has not **yet** been defined from being detected. 7.SS methods have **already** been used in telecommunication applications. 8.Some handheld devices **already** use voice authentication for authenticating users to the device or to network resources. 9.**Still** another solution is to use APs with integrated firewalls. 10.Password protection is **already** included with most handheld devices.

LESSON 9. Recovery and backup of data

T.9.1 **1.Back up-** The onsite and offsite storage of data copies **2.Archive data-** Data that has to be kept by a business for regulatory compliance or data that is not being used, but still kept on a storage device **3.Data restore-** The process of copying files from a backup to the original location **4.Disaster recovery-** The method your organization will use to get your business back up and running after a disaster. **5.Cloud backup-** The process of backing up your data in the cloud as opposed to on-prem or in a data center. **6.Data**

center- A group of networked computers used for storage, processing and distributing data **7.Automatic backup-** A system that enables the recovery of data stored on computers which is typically automated, eliminating the need for manual backups **8.Backup log-** A log that keeps track of events that happen during the backup process **9.Backup and recovery testing-** The process of testing the backup and recovery tools a business has in place, before they are necessary **10.Data archiving-** The process of moving unused data to a storage device.

T.9.2 Usually, there are four phases when it comes to successful data recovery, though that can vary depending on the type of data corruption and recovery required.

Phase 1. Repair the hard disk drive

The hard drive is repaired in order to get it running in some form, or at least in a state suitable for reading the data from it. For example, if heads are bad they need to be changed; if the PCB is faulty then it needs to be fixed or replaced; if the spindle motor is bad the platters and heads should be moved to a new drive.

Phase 2. Image the drive to a new drive or a disk image file

When a hard disk drive fails, the importance of getting the data off the drive is the top priority. The longer a faulty drive is used, the more likely further data loss is to occur. Creating an image of the drive will ensure that there is a secondary copy of the data on another device, on which it is safe to perform testing and recovery procedures without harming the source.

Phase 3. Logical recovery of files, partition, MBR and file system structures

After the drive has been cloned to a new drive, it is suitable to attempt the retrieval of lost data. If the drive has failed logically, there are a number of reasons for that. Using the clone it may be possible to repair the partition table or master boot record (MBR) in order to read the file system's data structure and retrieve stored data.

Phase 4. Repair damaged files that were retrieved

Data damage can be caused when, for example, a file is written to a sector on the drive that has been damaged. This is the most common cause in a failing drive, meaning that data needs to be reconstructed to become readable. Corrupted documents can be recovered by several software methods or by manually reconstructing the document using a hex editor.

T.9.4 1.Without data backup and a disaster recovery plan, you **might** be unable to retrieve data that was lost. 2.Cloud-based backup options have recently gained popularity due to the fact that cloud-based options **can** replicate data in real-time. 3.Recovering data quickly **can** be costly without an effective plan in place. 4.Most companies see a backup solution as enough. As long as they have easy and reliable access to data in the event of a disaster, everything **should** be alright. 5.Here's why you **should** have both if you want to protect your pertinent data. 6.By preparing and planning for data loss, you **can** act quickly without sacrificing budget and productivity related to the loss. 7.Recovery **must** be required due to physical damage to the storage devices or logical damage to the file system that prevents it from being mounted by the host operating system (OS). 8.The data stored in them **can** not be accessed in a normal way. 9.You **need** to keep your essential files in a second storage environment so that you have access to them if the worst-case scenario were to happen. 10.Few basic computer skill is all you **need** to be able to recover almost anything you've lost or deleted permanently.

LESSON 10. Information security policy and its management

T. 10.1 Ministry for Development of Information Technologies and Communications of Uzbekistan together with other relevant ministries and departments of the country is developing the information security concept of the Republic of Uzbekistan, which will define strategic tasks and conceptual areas in the sphere of countering cyber threats.

According to the ministry, the draft concept identifies the main threats to information security, which should be highlighted in development of effective measures on countering and preventing cybercrime. Special importance in the project is given to counteracting a new trend of using opportunities of the information space for various illegal purposes.

The concept will lay the basic directions for ensuring information security, as well as national interests in the information space, based on principles of protecting the legitimate rights and freedom of citizens when using the Internet.

The concept will become an important coordinating document, which will determine the strategic tasks of the state policy in the field of information security. It will stimulate formation of safe environment for information interaction and sustainable functioning of information, communication and technological systems in the national information space, their safe use in the interests of the individual, society and the state. To this end, development and improvement of the national information security system will be carried out, which should be aimed not only at counteracting existing threats, but also at reducing the risk of using ICT in order to carry out hostile and destructive actions against the country.

T.10.3 1.It is good practice to have employees acknowledge receipt of and agree to abide by them on a yearly basis as well. 2.Modern security operations center technology allows the SOC team to find and deal with threats quickly and efficiently. 3.An information security policy (ISP) is a set of rules, policies and procedures designed to ensure all users and networks within an organization meet minimum IT security and data protection security requirements. 4.Some industry experts argue that keeping SOC teams and CSIRT teams separate lets them concentrate on their core objectives, namely detection vs. response. 5.Training should be conducted to inform employees of security requirements, including data protection, data classification, access control and general cyber threats. 6.Up Guard Breach Sight can help combat prevent data breaches and data leaks, avoiding regulatory fines and protecting your customer's trust through cyber security ratings and continuous exposure detection.

7.Then, to address what actions are employees allowed to take while using company resources (namely Internet, email, mobile devices, and wireless networks), you'll want to document your Acceptable Use Policy. 8.USERIDs Request Procedures This section outlines in detail the steps required to request access to the system or, change access or suspend/delete access. 9.One positive feature of this framework is that it attempts to characterize the "maturity" of processes and security controls. 10.Importantly, because spatiotemporal measurements are somewhat intuitive, the metrics derived from these measurements could also help to establish common language between executive management, security personnel, and information technologists.

LESSON 11. Risk Management

T.11.1 All risk management plans follow the same steps that combine to make up the overall risk management process:

1. Risk identification: The Company identifies and defines potential risks that may negatively influence a specific company process or project.

2. Risk analysis: Once specific types of risk are identified, the company then determines the odds of it occurring, as well as its consequences. The goal of the analysis is to further understand each specific instance of risk, and how it could influence the company's projects and objectives.

3. Risk assessment and evaluation: The risk is then further evaluated after determining the risk's overall likelihood of occurrence combined with its overall consequence. The company can then make decisions on whether the risk is acceptable and whether the company is willing to take it on based on its risk appetite.

4. Risk mitigation: During this step, companies assess their highest-ranked risks and develop a plan to alleviate them using specific risk controls. These plans include risk mitigation processes, risk prevention tactics and contingency plans in the event the risk comes to fruition.

5. Risk monitoring: Part of the mitigation plan includes following up on both the risks and the overall plan

to continuously monitor and track new and existing risks. The overall risk management process should also be reviewed and updated accordingly.

T.11.3 1.Once you've identified the risks that can pose a probable threat to your company, and determined how much loss **can be expected** from an incident. 2.By the time we arrived the thief **had been caught** by the police. 3.The goal is to manage risks, so that the problems resulting from them **will be minimized.** 4.Insurance policies can be taken out insuring the asset, so that if any loss occurs the company **can be reimbursed** through the policy. 5.It's important to remember that the risk environment is always changing, so this step **should be revisited** regularly. 6.Once all reasonable potential solutions **are listed**, pick the one that is most likely to achieve desired outcomes.

LESSON 12. Cyber crime

T.12.1 1.malware- software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system **2.cybercrime-** criminal activities carried out by means of computers or the Internet. **3.hacker-** a person who uses computers to gain unauthorized access to data **4.illegal-** contrary to or forbidden by law, especially criminal law **5.fraud-** wrongful or criminal deception intended to result in financial or personal gain **6.worm-** a malware computer program that replicates itself in order to spread to other computers **7.piracy-** the unauthorized use or reproduction of another's work. **8.counterfeit-** imitate fraudulently **9.fraudster-** a person who commits fraud, especially in business dealings **10.phishing-** the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals

T.12.2 Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.

By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another.

New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy. All those activities existed before the "cyber" prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behaviour alongside some novel illegal activities.

Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our life, as well as the fragility of such seemingly solid facts as individual identity.

T.12.4 1.I talked to the girl **whose** car had broken down in front of the shop. 2.Mr Richards, **who** is a taxi driver, lives on the corner. 3.I live in a house in Norwich **which** is in East Anglia. 4.This is the girl **who** comes from Spain. 5.That's Makhmud, the boy **who** has just arrived at the airport. 6.Thank you very much for your e-mail **which** was very interesting. 7.The man, **whose** father is a professor, forgot his umbrella. 8.The children **who** shouted in the street are not from our school. 9.The car, **whose** driver is a young man, is from Ireland. 10.What did you do with the money **which** your mother lent you?

ANSWER KEY

LESSON 1.Cybersecurity

1	2	3	4	5	6	7	8	9	10
c	e	a	f	i	g	d	j	h	b

4. Listening

1.F 2.T 3.T 4.T 5.T 6.F

8.Reading.

1.A 2. B 3.E 4. A 5. A 6. A 7.C 8.C

9.Do's and Don'ts.

1.Do 2.Don't 3. Don't 4. Don't 5. Don't 6. Don't 7. Don't 8. Don't 9. Do 10. Do 11.Don't 12.Do 13.Don't 14.Do

11.Crossword

1.Freeware 2.Encryption

3.Attachment 4.Crash

5.Firewall 6.FAQ

7.Pixel 8.Gegabyte

9.Backup 10.Bandwidth

11.Default 12.Bit

13.Megabyte 14.Bug

15.Cache 16.Cookie

17.Virus 18.Resolution

Grammar exercise: 1

1.d 2.c 3.a 4.a 5.c

Grammar exercise: 2

2.Matching

1.identity theft 2.authentication 3.integrity 4.Network Security 5.Antispyware 6.installation

7.Reading

protects, is, refers, monitors, attempts, uses, includes, rely, is, makes, help.

LESSON 2.Cryptography

3.Listening

1.a 2.a 3.c 4.b

4.Listening

1.protect secrets 2.classic cryptography 3.involves 4.converts 5.readable format 6.decrypt 7.integrity 8.delivery

5.Reading

1-f, 2-b, 3-d, 4-h, 5-a, 6-j, 7-c, 8-e

Grammar exercise 1.

1.b 2.b 3.a 4.a 5.a 6.b 7.b 8.a 9.a 10.b

Grammar exercise 2.

1.They are not reading.

2.I'm cooking tonight.

3.Is he seeing the doctor tomorrow?

4.Are you eating chocolate?

5.What are you doing?

6.Are we making a mistake?

7.You're coming tomorrow.

8.It's snowing.

9.Umid's sleeping at the moment.

10.He isn't dancing.

11.How are they getting here?

12.When is it starting?

13. I / not / speak Chinese at the moment

14.I'm staying with a friend for the weekend.

15. Are they coming to the party?

16. We aren't studying.

LESSON 3. Symmetric and asymmetric cryptosystems

2.Matching.

1	2	3	4	5	6	7	8	9	10
d	g	a	i	h	b	e	j	c	f

3.Listening

1.b 2.c 3.a 4.a

4.Listening

1. cipher system 2. decryption key 3. encryption key 4. Cryptography 5. cryptosystems 6. Plaintext

5.Reading.

1. information 2. algorithm 3. involve 4. message 5. internet 6. Communication

6.Reading

1.F 2.T 3.F 4.F 5.T 6.T

Grammar exercise 1.

1.a 2.a 3 . the 4. - 5.the 6.the 7. - 8.an 9.an 10.a

Grammar exercise 2.

1.a 2.b 3.b 4.a 5.c 6.a

Grammar exercise 3.

1.the 2.a 3. the 4.the 5.an 6. - 7.a 8.the 9.an 10. -

LESSON 4. Authentication

2.Matching

1	2	3	4	5	6	7	8	9	10
f	d	i	a	c	j	h	b	e	g

3.Listening

1.b 2.c 3.b. 4.a

4.Listening

1.password 2. applications 3.measures 4.resources 5. access 6. Credentials

6.Reading

1.T 2.F 3.T 4.F 5.F 6.T

7.Authentication quiz

1.a 2.d 3.a 4.d 5.a

Grammar exercise 1.

1.B 2.C 3.B 4.A 5.B 6.A 7.B 8.A 9.B 10.A

Grammar exercise 2.

1.have 2.has 3.has 4.have 5.have 6.have

LESSON 5. Password retention and password attacks.

2.Matching.

1	2	3	4	5	6	7	8	9	10
g	c	h	j	a	e	b	f	d	I

3.Listening.

1	2	3	4	5	6	7	8	9	10
F	c	a	I	b	g	j	d	h	e

4.Listening.

1. services 2.cybercriminals 3.access 4.network 5.hackers 6. passwords.

6.Reading. True or False.

1.F 2.T 3.F 4.F 5.T 6.T

7.Dos and Don'ts

1.Do 2.Do 3.Don't 4.Do 5.Don't 6.Don't 7. Don't 8.Do 9.Don't 10. Do 11.Do 12.Don't

Grammar exercise 1.

1.more harmful 2. Longer 3. less 4. easier 5. the simplest 6.longer,less 7.the strongest 8.more harmful 9.weaker 10. lower

Grammar exercise 2.

1.longer 2.easier 3.best 4.less 5.strong 6.best 7.better 8.less 9.greater 10.harder

Grammar exercise 3.

Combination of words	Comparative	Superlative
Reliable password	**More reliable password**	**The most reliable password**
Simple composition	**Simpler composition**	**The simplest composition**
Secure password	**More secure password**	The most secure password
Good dictionary	Better dictionary	**The best dictionary**
Long password	**Longer password**	**The longest password**
Popular tag	More popular tag	**The most popular tag**

LESSON 6. Encrypt files and disks

3.Listening.

1.encryption, 2. unauthorized 3.laptop 4.agent 5. operating 6. locked 7. access 8. security

6.Reading.

1.F 2.T 3.T 4.F 5.F 6.T

Grammar exercise 1.

1.will be 2.will need to 3.will use 4.will appear 5.will have 6.will have 7.will best disguise 8.will not be 9.will change 10.will cause

Grammar exercise 2.

1.will make 2.will … reach 3.will figure out 4.will find … will go 5.will happen 6.will be 7.will continue 8.will study 9.will ask 10.will be

Grammar exercise 3.

b. 2) c. 3) d. 4) c. 5) a. 6) a. 7) 8) d. 9) c. 10) d.

LESSON 7. Network security vulnerabilities and threats

2.Matching

1	2	3	4	5	6	7	8	9	10
d	a	f	h	b	j	i	e	g	c

3.Listening.

1	2	3	4	5	6	7	8	9	10	11	12
d	f	b	a	c	e	i	k	l	h	g	j

4.Listening.

1.seriously 2.raise 3.hold 4.actively 5.suevival 6.crucial 7.priority 8.suggests 9.common 10.reform

5.Choose the correct word.

seriously, raise, importance, to, next, distributing, stressed, among, role, for, secure, sense, up.

7.Reading.

1. T 2.F 3.F 4.F 5.F 6.T

Grammar exercise 1.

1.kicked off 2.held 3.offered 4.became 5.received 6.was 7.aimed

Grammar exercise 2.

1.began 2.realized 3.named 4. saw,liked 5.wrote 6.evolved 7.existed 8.began 9.meant, wiped, began 10. wrote

LESSON 8. Wireless network security

3.Listening

1.c 2.b 3.b 4.a 5.c

4.Listening

1.airwaves 2.vulnerable 3.appropriate 4.traditional 5.signals 6.access

6.Reading

1.F 2.F 3.T 4.F 5.T 6.T

Grammar exercise 1.

1.have for many years extended 2.have had

3.has been 4.has significantly improved

5.have developed 6.have been already implemented

Grammar exercise 2.

1.have put 2.have become

3.has been operated 4.has increased

5.has increased 6.have been identified

7.have started 8.have already accessed

9.have placed 10.has decrypted

Grammar exercise 3.

1.since 2.since 3.already

4.already 5.yet 6.yet 7.already

8.already 9.still 10.already

LESSON 9. Recovery and backup of data and information

2.Matching

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
g	**a**	**e**	**j**	**h**	**i**	**c**	**d**	**f**	**b**

4.Listening.

1.repaired 2.platters 3.faulty drive 4.lost data 5. file 6. software

6.Reading

1.F 2.T 3.F 4.F 5.F 6. T

Grammar exercise 1.

1. might 2. can 3. can 4. should 5. Should

6. can 7. must 8. can 9. need 10. need

Grammar exercise 2.

1. a 2. c 3. c 4. b 5. d 6. d 7. a 8. b 9. d 10. a

LESSON 10. Information security policy and its management

3.Listening.

1	2	3	4	5	6	7	8	9	10
c	j	b	h	a	d	f	e	g	i

4.Listening.

1. preventing cybercrime 2.information space 3. information security 4.strategic tasks 5. Information 6.technological

5.Reading.

1. infrastructure 2. accumulate 3. tedious 4. visibility 5. consistent 6. integrity 7. secure 8. Remediation

6.Reading.

1.T 2.F 3.F 4.T 5.T 6.F

Grammar exercise 1.

1. c 2.b 3. c 4.b 5. c 6.b
7. c 8.d 9. a 10.c

Grammar exercise 2.

1.to 2. to 3.to 4. - 5.to 6. -
7.to 8. to 9.to 10.to

LESSON 11. Risk management

3.Listening.

1. potential 2. objectives 3. acceptable 4. prevention 5.monitor 6. management

5.Reading.

1. completely remove or get rid of (something)

2. more than is necessary, normal, or desirable; immoderate

3. a useful or valuable thing or person

4. establish or indicate who or what (someone or something) is.

5. a plan or course of action taken to achieve a particular purpose

6. repay (a sum of money that has been spent or lost)

6.Reading

1.F 2.F 3.T 4.T 5.F 6.T

Grammar exercise 1.

1. can be expected 2. had been caught.
3. will be minimized 4. can be reimbursed
5. should be revisited 6. are listed

Grammar exercise 2.

1. b 2. d 3. b 4. c 5. d 6. b 7. c 8. b 9. b 10. d

LESSON 12.Cyber crime

2.Matching.

1	2	3	4	5	6	7	8	9	10
i	a	f	h	b	c	j	e	d	g

4.Listening.

1.b 2.c 3.a 4.b

6.Reading.

1. T 2.F 3.F 4.T 5.T 6. F

7.Choose the best answer.

1-a, 2-a, 3-c, 4-a

Grammar exercise 1.

1.whose 2.who 3.which 4.who 5.who 6.which 7.whose 8.who 9.whose 10. Which

Grammar exercise 2.

1.Madina is the friend who I went on holiday with.

2.This is Mr.Xodjayev, whose son Baxtiyor plays in our team.

3.Her book which was published last year, became a best seller.

4.This is the bank from which we borrowed the money.

5.The person who I told you about is at the door.

6. Murod, whose car had broken down, had to take a bus.

Complete the sentences using relative clauses. Use who and which.

Grammar exercise 3.

1.A Scot is a person *who lives in Scotland.*
2.Nessie is a monster *which lives in Loch Ness.*
3.A fridge is a thing *which keeps food cool.*
4.A DJ is someone *who plays music in a disco*.
5.A bee is an insect *which makes honey.*
6.A lemon is a fruit *which is yellow and sour*.
7.A watch is a thing *which tells the time.*
8.A ferry is a ship *which carries people across the water*.
9.A shop assistant is someone *who works in a shop*.
10.A key is a thing *which can open and lock doors*.

Ex.9. Choose the correct answer.

1.technological 2.employ 3. surreptitiously 4. receiving 5.data 6.national 7. scan 8.keeps 9. time-consuming 10.program

REFERENCES:

1.Mirziyoyev Sh.M. 2017. The Strategy of Action on Further Development of Uzbekistan for 2017-2021.

2.G. Bakieva, F. Rashidova and others. Scale up. 1,2,3, courses. Set of manuals for non philological higher educational establishments. Tashkent, 2015.

3.Santiago Remacho Esteras. Infotech English for Computer Users (4th ed.) CambridgeUniversity Press 2011.

5.Peter Master, “English Grammar and Technical Writing”, USA,2004

6.Michael Vince, “First Certificate Language Practice”.English grammar and vocabulary (4th ed.)Macmillan 2009.

7.Gert, Janet. "Selection for Preservation in the Digital Age." Library Resources & Technical Services,2000

8.Deborah Russell, G.T. Gangemi, Computer Security Basics, 2015.

9.Michael Black, Wendy Sharp, Cambridge objectives IELTS, 2011.

10.Els Van Geyte, reading for IELTS. Collins, 2011.

Password Security http://www.you tube.com/

What is network security www.paloaltonetwork.com

https://www.clickssl.net/blog/symmetric-encryption-vs-asymmetric-encryption
https://en.wikipedia.org/wiki/History_of_cryptography
https://en.wikipedia.org.Authentication
https://securitytrails.com/blog/social-engineering-attacks

www.theamegroup.com › network-security-threats

https://study.com/academy/lesson/wireless-network-security-issues-solutions.

https://searchsecurity.techtarget.com/definition/encryption

https://www.netapp.com/us/info/what-is-backup-and-recovery

www.en.wikipedia.org/wiki

www.breaking.news.com

www.britishcouncil.uz

www.flickr.com/photos

www.teachingenglish.org.uk/think/articles/listening

“ENGLISH IN CYBER SECURITY”
Course book for undergraduate students majoring in
5330300-Informartion security

Considered at the meeting of Foreign Languages
Department as if “______” June 2020. (Protocol№________)

Considered at the meeting of the faculty of Economics
and Management in ICT as if “_____” June 2020. (Protocol№ ______)

Considered at methodological board of TUIT as if
“______”June 2020. (Protocol№ ______)

Author: D.N. Abduvakhabova

Editor: Sh. Gulomov

Reviewers: (PhD) A.A.Sharipova

(PhD) N.A. Tukhtakhodjayeva