Vocabulary: -

1.Introduction to Ethics.
- Definition of Ethics
- Computer Ethics
- Ethical rules

2. Ethics Philosophical Issues.
- Ethics Theories
- Utilitarianism Theory
- Right Theory
- Justice Theory
- Egoism Theory

3.Intellectual Property Rights.
- Software ownership rights
- Software Ownership Terms
- Software licenses
- types of software licenses

4.Computer Crimes.
- Definition of crime:
- Computer role in crime
- How fraudsters steal passwords
- The concept of informatics crime
- Definition of Computer Crime
- Computer crimes by type are classified
- Means of crime
- Computer Protection
- Tags that may indicate that your device is compromised
- What should you do if something weird happens while you're online
- Some types of hack files

5.Information Privacy
- Definition of Privacy
- Confidentiality
- Types of privacy
- Why the Internet is different from other means in relation to privacy
- Modern technologies and their impact on information privacy
- Protection of information privacy
- The most important elements to be taken to provide protection for any information .
- Attacks and risks related to information protection operations

6. The Concept of plagiarism

1.Introduction to Ethics

It is common knowledge that, throughout the ages, every profession or work practiced by man has its ethics values which must be adhered to. In this age we often hear about the ethics of the use of knowledge or the so-called (ethics of the profession) and through the label we can conclude that any profession practiced by man has ethics and rules must be adhered to, and from the importance of many universities and scientific institutes began to teach ethics as part of every specialty, for example, the Faculty of medicine is studying the ethics of the medical profession and the Faculty of Education teaches teaching ethics, etc.

In the last century, the life of nations has begun to change because of the emergence of a new science and a new era, the era of information technology, the age of computers. This science has provided a great service to mankind and has provided a better and easier life in most areas of life and at all levels, between individuals through communication, sending messages, etc., or in the conduct of business as information systems that conduct the work of different companies and organizations. The computer has provided us with a lot of services to talk about. We will mention, for example, the possibility of storing our own files and folders and doing our various work.

After the development of the Internet, we can communicate faster and send different data, Our business from and to anywhere in the world.

If everything we have said so far is beautiful and wonderful as long as we can do everything we need by computer what's the problem?
The truth that was absent from our minds in the past period is that with all of the services we have obtained from the development of information technology there is a very serious problem accompanied by this development, how do we not hear the crimes of a number called "computer crimes" occurring in the world by criminals of the type (The criminals of the computer)

This has been hacked his device and tampering with its contents and to see the privacy of his program was stolen and selling, and this institution has been hacked the of their database and knowledge of secrets and the destruction of their database and a country has been revealed secrets, and in this bank has been stolen a number of customer balances and many examples cannot be limited.

Here are questions that are starting to arise:

- How do we protect our files stored in the computer from spies and intruders?
- How do we protect our money, actions and ideas from thieves?
- Are there laws that protect our private data scattered everywhere?
- If these laws exist, are they capable of doing so?

- Are protection programs sufficient to protect the rights and privacy of individuals, institutions and countries?
- What is the best way to protect the rights and privacy of individuals, institutions and countries ?

Objective of the study : teaching our students and anyone who uses any kind of modern technical devices of all kinds (computers, mobile phones, etc.) in general, and who deals with the computer in particular whether he is a regular user of the computer or specializes in it, the ethics of this profession and the positive effects it leaves commitment to this ethics.

Definition of Ethics:

It is a set of common rules, principles and values to deal with people in a particular society.

Computer Ethics: is a new branch of ethics that is growing and changing rapidly as computer technology also grows and develops. The term "computer ethics" is open to interpretations both broad and narrow.

On the one hand, for example, computer ethics might be understood very narrowly as the efforts of professional philosophers to apply traditional ethical theories like utilitarianism, Kantianism or virtue ethics to issues regarding the use of computer technology. On the other hand, it is possible to construe computer ethics in a very broad way to include, as well, standards of professional practice codes of conduct, aspects of computer law, public policy, corporate ethics--even certain topics in the sociology and psychology of computing.

Ethical rules: -

1. Commitment to honesty in all their dealings, even with themselves.
2. Dedication in performing all kinds of work.
3. Not to spy and attack the privacy and rights of others.
4. Do not tamper with and steal the rights of others.

Today we are completely opposite in everything, is not it?

Yes, this is clear through our dealings with ourselves and with others as follows:

1. Many of us make lying a fundamental principle in all his dealings with others, but even lie to himself.
2. Many of us do not work and do not learn with sincerity, but they feel this heavy burden on them do not know when they get rid of it.
3. Spying and assaulting each other on some.
4. Some enjoy reading about the privacy of others, violating their sanctities, distorting their reputation, etc.

2. Ethics Philosophical Issues

Ethics Theories

The subject of work ethic is one of the most complex issues. Individuals with differing views tend to hold divergent views. There are important differences between them about the components of ethical behavior, how decisions must be made or the work done ethically. The field has four theories to describe the ethical frameworks used:

1.Utilitarianism Theory

According to the view of utilitarian theory, the decision should be based on what is good for the largest number of people. In order to apply this theory, all people affected by the decision should be studied and then the solution that satisfies most of them is chosen. The utilitarian theory demands that the effects of the act be tested on the persons affected, including the person who already exists. From an ethical point of view if its aggregate net benefit exceeds the aggregate net benefits of any other act. The theory of utilitarianism determines whether the act is right or wrong by assessing its consequences.

2.Right Theory

The authors of this theory believe that everyone has fundamental rights that should be respected and protected, such as the freedom to express opinion, privacy, equality, education, etc. So people look from an ethical point of view when looking at their health, which should not threaten unfamiliar products. , And they have the right not to be deceived or overlooked

3.Justice Theory

The basis for this theory is that all people are treated fairly when making decisions. Justice here includes two types: distributive justice and procedural fairness.

Distributive Justice seeks the fairness of rewards, punishments, and results in the Organization, as it ascertains whether employees have received rewards commensurate with their performance or that there are no too many or too many rewards have been given to the employees. Procedural justice includes justice and regularity in the application of rules and procedures

4.Egoism Theory

People who base their ethic decisions on this theory believe that personal interest should be maximized as long as it does not harm others. This theory is derived from the principles of capitalism and evaluation according to this theory is based on the pursuit of positive things desired by the person and avoid the negative painful, and although ethical selfishness seeks self-interest, but some selfish people consider the interests of others as a way to reach their ends, Others care about the interests of others because they do not want to

3.Intellectual Property Rights

What Is Intellectual Property?

The term IP is used to describe the unique creation of the human mind which has commercial value. Examples of intellectual property include poems, photographs, songs, plays, books, paintings, sculptures, films, logos, designs, perfumes, recipes and computer programs.

Comments:

1. John Locke holds that when people remove something from Nature through their own labor, they have mixed their labor with it, and therefore they have a property right in that object.

2.If more than two people create the identical intellectual property, there is only one instance of that property, not two, meaning both people cannot claim full rights to that property. Copying an intellectual property is different from stealing a physical property. Perfect copies can be made of objects embodying an intellectual property. When this happens, the original owner has lost exclusive control over use of the property, even though he or she still has the original article.

3.An individual or firm in the United States may protect intellectual property through trade secrets, trademarks, service marks, patents, and copyrights.

4.A trademark is a word, symbol, picture, sound, color, or smell used to identify a product. It is good when a company's trademark becomes well known to the public. Examples of trademarks are Kleenex, McDonald's Golden Arches, and Advil. Your college or university's logo is most likely trademarked. A trade secret is a piece of intellectual property that is kept confidential. Examples of trade secrets are formulas, processes, proprietary designs, strategic plans, and customer lists. The information loses much or all of its value if it becomes public knowledge.

5.The advantage of a trade secret is that it does not expire. The disadvantage of a trade secret is that a company cannot prevent another company from attempting to reverse engineer the formula or process. The advantage of a patent is that the government gives the patent owner the exclusive right to the intellectual property. The disadvantage of a patent is that this right expires after 20 years.

6.Digital rights management refers to any of a variety of actions owners of intellectual property stored in digital form may take to protect their rights. Examples of digital rights management include encryption, digital watermarking, and making CDs copy- proof.

Patents are considered an unreliable way of protecting intellectual property rights in software because the Patent Office has given out many bad software patents than cannot hold up in court. This has happened because for decades the Patent Office did not give out patents on software. During this time a lot of “prior art” was being developed. Now, when a company applies for a software patent, the Patent Office may not be aware of some of the prior art. It may issue a patent even though the algorithm is not novel. Such a patent has little value. The existence of bad patents in software reduces the value of software patents in general

Software ownership rights

First: What is software: We can divide the software into two parts

1. General programs: which are loaded on computers to start work on them.• The operating system software through which the computer works (windows).

• Software to create, design and open files, images and video on various computers.

2. Special programs: programs that are created in particular by a special request to serve a specific person or entity.

•These programs serve people, companies, institutions and governmental and private bodies.

• Examples of these accounting programs, information systems software, websites and many more.

.

•Second: What rights should be maintained for this software?

If you think a little bit, we will find that each product is created by a particular person or institution and the examples are many and we will mention, for example:

1.The rights of ownership of food products The producer has the full right to its product and no other party has the right to use or imitate the product unless it is authorized by it

2. Copyright and printing The author of the book and the author of the book have the full right in this book and no other party may use or imitate it except with the official permission of them.

3. The person or producer of the software shall have the full right to protect their programs. No person or any other entity shall have the right to use, sell or market these programs without the authorization of the producer, and upon the acquisition of any software that must be paid and registered according to certain conditions.

Software Ownership Terms:

1. Copy the programming disks to be used as backup copies when the original disks are damaged only.

2. Not using the software in a computer network without the consent of the producer according to the conditions of the license.

3. Protecting this code from viruses that is caused by sharing or lending.

4. Not to commit piracy to illegally copy programs and then sell and distribute them.

5. These terms apply to commercial and free software.

Software licenses

What do software licenses mean?

Software Licenses: is to obtain a license to use such software and not to acquire its own rights and this license has terms that should be respected and adhered to. These terms are called terms of use and are usually written on the external enclosure, documenting the software or appear on the screen at the start of the download.

Types of software licenses

- What are the types of software licenses?

There are two types of software licenses:

1. Single Use License: This license means the download and use of this software on one computer only by the purchaser of this software.

2. Multiple use license: Here you can download and use this software on several devices whose number is determined in the license.

4.Computer Crimes

Definition of crime:

A person may infringe upon the property and privacy of others regardless of the means used, the purpose and the motivation behind it.

Comments:

1.Is an illegal activity directed to copy, change, or delete information stored inside the computer that is turned on its way.

2. Any unlawful or unauthorized conduct with respect to the transmission of data.

3. It is a pattern of crimes known in the Penal Code as long as associated with information technology.

4. The crime in which computer data and information programs play a major role.

Computer role in crime:

The computer plays three roles in the field of committing crimes:

First: The computer may be a target of the crime, as in the case of unauthorized access to the system.

Viruses to destroy data and stored files or in case of seizure of data stored or transmitted across systems.

Second: The computer may be a tool of crime, as in the case of computer exploitation to seize money by making illegal transfers or using technology in counterfeiting, counterfeiting or seizure of funds by credit card numbers.

Third: The computer may be the environment of crime, as in the storage of programs in its system or if used to publish illegal material, and the computer can play the three roles with fraud and steal passwords:

Many problems can occur if someone steals the password, and those who steal the password can do many things of which:

1. Your credit card may be used to purchase goods in thousands of dollars online.

2. Someone may enter private areas on the websites you have registered with.

3. Someone may see your email and send threatening messages via your email.

4. Someone may use your account to launch fraud attacks around the world and people may think you are the actor.

How fraudsters steal passwords:

There are many ways to steal your password:

1. One of the simplest methods used by fraudsters to steal your password is to call you claiming they are computer security experts and ask for your password.

2. Also common are guessing, such as the first letters of their names or the date of birth of a relative.

3. The last means is to probe any discovery attempt and fraudsters check the information that is displayed over the Internet and enable them to know and use the password.

The concept of informatics crime :

Is the use of modern technical devices of all kinds or one of its components or programs in the implementation of suspicious and unethical work does not satisfy the community and contrary to the principles and rules of public ethics.

Definition of Computer Crime

Is the use of the computer or one of its accessories in carrying out suspicious actions to achieve unethical and immoral goals that affect the rights of individuals and communities and are contrary to the general principles and rules of ethics.

Computer crimes by type are classified as follows:

• **Infiltration and espionage:** There is a class of people infected with the love of espionage and knowledge of the privacy of others, and has evolved the operations of espionage in terms of methods used over time,

from eavesdropping in the past and the use of audio devices later to connect to the computer at the present time, where These patients penetrate the organs of others and see their privacy.

As the computer became the repository where most files are saved, such as images, documents of the work, financial accounts, etc. and the entry of the criminal to the device has broken all secrets.

• **Destruction** : Here the victim's device is broken in order to tamper with or destroy and destroy its own files, such as deleting them or transferring them to other places. Such crimes are committed in the rights of individuals, organizations and institutions.

• **Fraud and change:** This includes Some persons falsify documents or documents of their own or other persons for a purpose. Such as forging a certificate for a job and many others and this work does not require penetrating other people's devices.

• The offender breaches another person's device and changes the documents, dates, and names in the device.

• To falsify images and change people in a particular picture to achieve despicable goals such as defaming people.

• **Deception and deceit:** The deception and delinquency is unacceptable in law and custom, which caused the spread of these days is the development of technology and software that used the bad use by the weak souls and is through:

• Use professional software to obtain improved images other than real pictures or hide defects and shows only the pros.

• One of the manifestations of deception is the reincarnation of a personality other than the basic personality, such as claimed to be the official, or that he is from the public tribe, or that he is a female opposite, but there are some programs helped to that, including changing the voice, from male to female and vice versa with the possibility of improvement and work effects It's happening a lot on the Internet.

Means of crime

Cybercrime of different types, objectives, motives and methods of implementation are done in the following main ways:

1. Email: where email is used to send viruses and horses Trojan or send links to suspicious sites or is also used to send rumors and lies and others.

2.Computer and its pursuits and programs: The computer is the first means of information crimes, and the variety of programs and professionalism, which is easy to use and spread by some people, which began to increase day by day.

3. Mobile phone and its programs and accessories: The mobile phone, especially the advanced, which has become close to the characteristics of computers are easier to transmit news, photos and clips of Bluetooth on a large scale.

4. Local and international networks: Companies, institutions and others are considered as an environment for transmitting rumors, in the absence of regulations that prevent this. And even if they are not implemented and strictly, the Internet, the Internet is more severe and is a space open to everyone to spread what appeared to him.

Computer Protection

One of the causes of cybercrime may be due to the lack or lack of adequate protection from viruses penetrating the device. This course provides an appropriate environment for hackers and makes it easier for them to find ports through which to carry out hacking operations.

Therefore, we will determine several tasks to be done by the user to protect his device and data as much as possible from penetration and espionage and not being exposed to any computer crime and this is a cycle to reduce these crimes and these tasks as follows:

1. Install antivirus and update it constantly.

2. Install one of the programs to check the device and Registry and do a periodic check to make sure that the device is free of hacking files.

3. Do not receive files except from people who are trustworthy.

4. Increase the caution of the files that come by e-mail especially if the file type exe or dll. I sent a message from an unknown destination so do not open it.
5. Make the password long and contain numbers, letters and symbols so it is difficult for the hacker to break it and change it periodically.

6. Inspect the device, especially the registry periodically, to ensure that there are no hacking files such as Trojans . It is a server that allows the hacker to control the whole of your device, and is planted by your device through the hacker and send it to you through your e-mail, for example, or through instant chat programs such as ICQ.

or through a floppy disk or you are planting it in your device by mistake because of tampering with the hacking programs. You disassemble Trojans in your system, instead of sending it to the device to be hacked,

so I advise you not to download these programs permanently and to make sure whether your device is Trojans or not, there are several methods such as searching the log file registry For windows, and for the importance of registry and to avoid accidentally deleting files, we will look for Trojans in a secure way using software

that is the best C Cleaner which is usually available with some modern systems such as windows vista or any other program which is many and if you do not have it, download it immediately.

Tags that may indicate that your device is compromised:

There are no specific things you get when a person's device is hacked and may not feel anything at all but there are some strange things that might happen like:

1. Open and close programs suddenly.
2. Run the CD Without a user command.
3. The appearance of any other strange signs.

What should you do if something weird happens while you're online?

1. Disconnect the Internet immediately and restart the device.
2. Search for suspicious files inside the device by a program or manually
3. Delete foreign files immediately.

Some types of hack files

There are many types of spyware and is still developing unfortunately, and with the passage of days we are surprised by the emergence of many of them, which are used by the owners of the sick souls and here we will mention
some of them and identify them and methods of discovery and how to deal with them and disposal so that we can address them and not give them the opportunity to penetrate our devices control and spy and tampering with our files.

1.Back orifice

One of the hacking programs that are used is that this file opens a background window to the hacker in your device by one of the ports and usually it is Port 3317 This file is hidden in the Registry.

Disposal method:
1. Either by searching by a program
2. By manually searching the manual

The file extension is: EXE
Its easiest way to identify it is because the server's name is
variable is the file name and the spacing between them is a distance ..
As follows : "server .exe"
clear the entire file ..
.Back orifice

2. File Reg edit

One of the most popular hacking programs, it is easy to spread the server file.
Uses Patch
Server and hiding in Registry.
Method of disposal
1. Turn off the device.
2. Turn it back on Safe mode
2. Head to Registry Look for the following file:
c: \ windows \ patch.exe
3. When you find it, delete it and then restart the device.

3.File name:. Net Bus 2000

Net Bus 200 uses the normal server "server.exe" but the name can be changed and it registers itself but in another registry area.

Disposal method:
Search for the file .. If found :
1. Turn off the device.
2. Restart it in safe mode.
3. Delete the file and then restart the device.

4. File:HKEY_LOCAL_USER \ SOFTWARE \ MICROSOFTE \ WINDOWS \ CURREN T VERSION \ RUN
- Heack'a Tack 'a
SERVICES \ Key: UMG32.EXE 4
The name of Server
Server.exe

of a dangerous program because it uses a protocol
FTP It is difficult for many programs to detect and detect spyware scanners.
Disposal of the file:
Server.exe

The file or server is hiding in a file Registry, Move to a file
Registry , As we have explained and when you reach
: Run or Run once
Search for the file if you are infected with the file you will find it in a file Registry
With the certainty that many are infected with this file and scan the file immediately ..

5. File Master -Explorer32 "C / WINDOWS \ Expl32.exe 5
Paradise
Is one of the most dangerous and prevalent programs and is called the leader of hacking programs.
How to get rid of the file:
Turn Registry
Then look for the file extension:
"C: \ windows \ nameofthe.exe"
When you find this file in Registry clear it immediately.

6. File ICQ Trojan :This file creates a hole for the hacker inside the device, which is one of the types of deceptive files, where it occupies the original file location and change the name as follows: ICQ.exe This is a hacking file ,ICQ2.exe   This is the original file.

How to get rid of the file: Go to the file ICQ
If you are infected with this file you will find two files as follows:
ICQ.exe This is a hacking file
ICQ2.exe This is the original file.
Delete the file ICQ.exe   And then change the name of the second file ICQ.exe to ICQ2.exe

5.Information Privacy

Definition of Privacy: Means keeping personal data from unauthorized use such as adding delete and modify.

Confidentiality: Means keeping personal data from being stolen. Using different methods such as encryption and passwords.

Types of privacy:

1. Privacy of information such as identity card.

2. Bodily privacy such as genetic testing.

3. Privacy of communications such as e-mail and voice mail.

4. Regional Privacy Prevent access to sensitive places such as ministries or companies without inspection.

The use of computers and the Internet has led to a reduction in privacy, where information can be accessed quickly and easily.

There is a kind of information called, especially since it relates to the same person and belongs to its entity as a human being such as name, address, phone number and other information, it is information that takes the form of data that binds to any identifiable natural person or identifiable. This type of information has become very important today in the contemporary philosophy of informatics, especially since the idea of the digital world, can not evolve and keep pace with human concerns only using information.

From here emerged what is known as informational privacy.
The principle of informational privacy, which is the right of a person to control the information that concerns him, is considered an old principle.
Therefore, we can say that the privacy of information is the protection of data, there is a general synonym between the term privacy of information and data protection, not between privacy and data protection,

In view of the rapid development «IT revolution» As well as the global and decentralized typists of the network Internet, making dealing with the phenomenon of privacy violation is very complex,

Perhaps these violations may reach the limit of infiltration into our personal files, and perhaps surveillance through the cameras installed in our computers without us feel it, Although its capacity varies due to the protection and encryption systems that programmers are constantly developing, but it remains possible, The idea of privacy and its association with information technology is the first issue of computer law in general from a historical point of view.

The academic legal studies that concern the privacy and human rights in the light of technical developments are limited in general. It can be said that the end of the sixties and seventies witnessed the launch of such studies, In which the concept of information privacy was first and foremost conceived as a concept independent of the rest of the concepts of privacy, specifically physical intervention and control issues, and was credited with drawing attention to the concept of information privacy.

Why the Internet is different from other means in relation to privacy: -

The development of a system to protect privacy in the internet environment must take into account the nature of the specific threats to which it is exposed privacy in the scope of the use of internet operations, the internet creates a series of new challenges in the face of plans consumer protection and protection of privacy. These challenges are as follows:

1.The Internet increases the amount of data collected, processed and stored

The Internet has seen a growing trend towards data collection in the real world as it becomes easier in the internet environment in terms of accessibility, more convenient for tabulation due to computing techniques, and becomes easier to exchange in the light of the means of exchanging information in all its forms made available by the Internet and the software of navigation.

2.The Internet has facilitated the globalization of information and communications

In the Internet environment, information and communication flows across boundaries without regard to geography and sovereignty. Individuals give their information to internal and external entities and possibly to unknown entities. This raises the risk of misuse of this data, especially in countries where there is no legal protection for personal data.

3.The challenge of loss of centralization and mechanisms of control and control

The adoption of a national law or the development of an appropriate national strategy for the protection of a human rights may be effective due to the element of control and sovereignty and the ability to control and prevent or perpetrate aggression, which also allows compensation and prosecution of violators, but how is the situation under the Internet owned by each person and which are not owned by anyone, and where there is no central authority or sovereign authority that provides protection or provides the opportunity and mechanism for legal protection when an attack occurs.

Modern technologies and their impact on information privacy

The risks of modern technologies are increasing in terms of privacy protection, such as video surveillance cameras, identity cards, electronic databases, personal databases, means of intercepting and controlling mail and communications, and controlling the work environment.

The breach of privacy on the Internet can be done by three basic entities: Internet Service Provider and Sites visited by the browser, as well as Internet hackers, (Hackers) Individuals or security and intelligence agencies.

That the Internet Service Provider can monitor everything you do on the Internet (place and time of access to the network, sites visited, words searched, messages, emails exchanged etc.), from Internet Protocol the user's Internet number and other devices through Packet, Proxy,Sniffer : It is a software capable of analyzing every movement on the web. ,
The websites visited by the browser are able to determine the movement of the browser, through the introduction of small files known as«Cookies» on the hard disk in the computer. In addition to the

E-forums and social networking sites, most notably Twitter and Facebook, contain gaps that allow hackers to see the details of personal details of their subscribers,

although these sites are constantly working to devise ways to protect privacy. It represents the biggest challenge facing individuals, businesses and websites, and it seems, Hacking is a breakthrough it is like an open war, not a fixed base, but only for each side to benefit from the gaps of the other. It is usually done through complex programs and different forms, which may reach to the extent of monitoring our personal movements, by penetrating laptops, and watching us inside our homes

In the digital world and the world of global information networks, the user leaves many traces and connotations related to him in digital records about the site he visited, the time he spent on the network, the things he searched for, the materials he downloaded, the means he sent, the services and the goods he ordered and bought. Personality, life, hobbies and user tendencies on the web are automated records with personal content related to the individual. Surfing and browsing through the Internet leaves the site with a large amount of information, although part of this information is needed to allow access to the Internet and browsing, and once access to the site page, certain information

available from the customer which is known as header information
Which he provides the computer used for the server computer hosting the websites, and this information may include:

1. The IP address of the customer or entity that registered the domain through the system of names of organizations and their location.

2. Basic information about the browser, operating system and physical system equipment used by the customer.
3. Time and date of site visit.

4. Internet sites and the address of the previous pages visited by the user before entering the page throughout the visit.

5. It may also include the search engine information used by the user to access the page, depending on the type of browser the user's email address may appear.

6. Depending on the operation of the user, special commands about the management of the handling of the network may show information about the time spent on each page and the statement of information sent and received.
Many, if not all, interactive sites, specifically business and e-commerce websites, require the user to submit and fill out a form that includes different information, whether in signing up for certain services, registering or joining discussion groups, or even posting or posting a message.

This information includes the user's name, address, work, home, phone and fax numbers, e-mail address, age, gender, marital status, place of residence, monthly or annual income,

Selling and buying online and the locations where payments are made, they require the credit card number, type and date of expiry.

Despite the great benefits of information technology and global information networks, they have also created a practical plan that represents the possibility of collecting, storing, communicating and accessing information, and making it available online for use by various business sectors and mobile devices without the knowledge or knowledge of the owner of the information.

Says Jerry Byrne and Deirdre Mulligan imagine you are going in one store, the markets among the many stores do not know which one, you put on your back a signal to show every shop I visited and what I did and what I bought, that is something similar to what can happen in the internet environment when individuals use websites, they expect a bit more hidden in their activity than they expect in the real physical world. In the latter, their presence can be seen and watched by others. Unless a person discloses data, he thinks no one will know who he is or what he is doing. Internet across server systems and network management systems
You make a great deal of information when you pause in the network space.

These data may be caught and identified by the employees of the establishment, for example - by the employer when using the network or their subscriptions bound to it, and may be collected by the sites visited the same,
and as we said, the collection of different information and behaviors may provide the clearest picture of a person did not reveal any from the details of what it contained.
There are no legal provisions in Iraq to protect individual privacy or to protect individuals from automated processing of data, so the whole matter is not yet organized and there is no clear official or legal position on it.

Protection of information privacy

For privacy, according to its historical development, there are three main stations: First:- Recognition of privacy as a right to protect the individual from physical abuse of their lives and property, which is known as physical privacy. And Second: - The implication of privacy to protect the values and moral elements of the person, which is known as moral privacy. The Third:- is privacy as a general right whose scope extends to protect the person from all aspects of attacks and interference in his life, regardless of its appearance or nature. In the latter sense, a new concept of privacy has been created, The privacy of information or the right of individuals to control information and private data in the face of the challenges of the digital age

The right to privacy and protection of data developed in the 1960s and 1970s as a result of the impact of information technology and the potential control powers of computer systems that required the development of certain rules governing the collection and processing of private data. In this field it is important to note that the first legislative process in the field of data protection was 1970

The most common concern for business owners in data privacy issues is the loss of customer confidence employees,

investors and trademarks, then comes the fear of loss of intellectual rights of products, research and studies, it is then comes the fear of manipulating the financial accounts of the facility. It is worth mentioning that 55% of the companies participating in the survey will increase the value of internal investment in data privacy issues in 2009 compared with the previous year, This increase is the use of new technologies and policies such as: network security (firewalls, anti-virus and virtual private networks VPN) Database monitoring tools, precautionary security (from tamper detection systems, vulnerability detection of applications and networks), and governance and risk applications and other systems and tools that help enterprises protect the privacy of their data. ,

Finally, the growing concern of people about preserving their privacy should be a reaction to the way enterprises use that information, not to information technology itself. "The technique is a double-edged sword and the user is the one who determines which thresholds are used.
To protect your privacy and privacy, please read our Privacy Policy

Before registering any data on your websites, be always careful when registering your privacy data.For example, (Address URL) Make sure that the site uses one of the encryption techniques, and you can tell from the URL that the address begins with https

Make sure the lock mark is on the corner of the screen. Read usage agreements before installing, Software. Periodically check the programs running on your device and use one of your ports to connect to the Internet by following the following command
(Netstat <- Run <- Start)
Or using a port control program such as the program Distroy Spybot Search and

Do not connect to the Internet using an unknown wireless network or it.
Change the default settings used by WPA2 Do not use a security protocol
Manufacturer, such as device name and passwords. Notify the competent authorities when you discover suspicious sites, and when your device is exposed to any security breach and leak information about you or your customers.

That the concept of information security has undergone several stages of development that led to the emergence of so-called information security, in the sixties computers were all that occupy the workers in the information departments, and their concern is how to implement programs and guidance and were not as busy with information security as they are concerned with the work of the devices and the concept of security revolves around to determine access or to view data by preventing outsiders from manipulating devices, the term computer security appears computer security

Which means protecting computers and databases, and as a result of the expanded use of computer security devices and its processing benefits for large volumes of data,

change interest to represent data control was accompanied by the use of data security passwords and protection. In the 1990s, the concept of data security, the simple secret of data access control, as well as the development of protection measures, was moved and the adoption of plans for additional copies of data and software away from the computer site, and in the eighties and nineties the importance of data usage has increased, and developments in the field of information technology have allowed more than one user to participate in the databases, all this led to the transition from the concept of data security to Information Security,

It has become necessary to maintain information, integrity, availability and degree of reliability appropriate security measures can contribute to ensuring desired results and reduce information penetration and manipulation.
Protecting the privacy of the internet user is part of the security on the internet, but security is not necessarily part of the protection of privacy. The concept of security on the net can be done through several steps and effective arrangements to protect your computer and your important information and protect privacy and your information is one of these steps what comes:-

First: Control the local participation files(LAN)because windows opens these files directly as a basic system, and these files are the biggest source of security threat to you because it allows anyone in the internet to access your device and share your files and information in the device.

Second: Protect your computer by preventing others from accessing it using a special device called Smart key .

Third: Avoid downloading any programs or files of a special operational nature from sources that are not certified.
Fourth: Avoid opening attached files in emails from unknown sources you have especially if they are of the type Com, and.bat, exe.

Fifth: If you have information that is very important or very special, use any program to encrypt your information and electronic messages.
sixth : Do not make any purchases from the Internet without making sure that you use a security server and that the lock mark is closed
in the browser as well as change : http: // to https.//

Seventh: Avoid agreeing to save username and password because if you agree, the process will make it easier for hackers to enter because they will find it stored and ready.

The most important elements to be taken to provide protection for any information are:
1. Confidentiality : It means ensuring that the information is not disclosed and not seen by persons who are not authorized to do so.

2.Integrity and content integrity(INTEGRITY): This means that the content of the information is correct and has not been modified or tampered with it. In particular, the content will not be destroyed, altered, or tampered at any stage of processing or exchange, either in the process of dealing with the information or through illegal interference.

3.Availability of information or service(AVAILABILITY): It is concerned with ensuring the continued operation of the information system and the continued ability to interact with information and provide service to informational sites, and that the user of the information will not be prevented from using it or entering it.
4. Not to deny the conduct associated with the information he has done (NON REPUDIATION)and is intended to ensure that the person who has acted on the information or its location is not denied, so that there is a capacity to prove that the action was done by someone at a certain time.

5. Not all information requires confidentiality and non-disclosure, not all information is equally important in terms of access to it or ensuring that it is not tampered with. Therefore, information security plans are based on the answer on a series of consecutive questions.

Attacks and risks related to information protection operations

If we want to describe the risks related to the protection operations themselves, we may be in fact facing all kinds of risks, and attacks, but from a narrow technical point of view, including five types of methods that relate to attacks targeting the system or strategy of entry,
Some of which are targeted to the system of data entry and processing, and some of them classified as an initial action to achieve unauthorized access to various types of networks, and we briefly refer to these methods and attacks with an explanation of the names of other activities and methods and attacks related to network penetration specifically and to identify the most important weaknesses:

Dat Diddling :This attack is aimed at altering data or creating data with fake data in the stages of entry or extraction, and in fact in dozens of patterns and technical methods.

Ip Spoofing : Convincing the Internet Protocol (disguise by exploiting the transport protocols) that the term does not mean concealment, it is a term for cheating, deception, imitations, simulation and cynicism,

But its common use now concerns internet viruses. We are talking here about a purely technical means. The attacker, by means of this method, falsifies the address attached to the packet of data transmitted so that it appears to the system as a valid address sent from within the network, so that the system allows the packet to pass as a legitimate packet .

Password Sniffing :Collecting Passwords the activities of abuse by using words and clipping the secret were often done in the past by guessing the passwords, taking advantage of the weakness of the words in general and the common choice of individuals for easy words related to their family environment or work environment or personal life,

The new software will be able to capture passwords while roaming in a part of the network or one of its components and monitor and follow the movement of communication on the network, so that the program originally collects the first 128 bytes or more - for example - from each network connection that is monitored and follow the movement of communication,

When the user prints the password or user name, the whole program collects and copies this information. In addition, some of these programs collect, re-analyze, and link information, and some hide the capture activity after performing the task.

Scanning and copying: A method used by the program (scanner) which is a program of possibilities based on the idea of changing structures or changing the probability of information, and uses the identification of the possibilities of password or phone number of the modem, and the simplest pattern when using the list of possibilities to change the phone number scans a list of large numbers to access To one that uses a modem to connect to the internet, or to scan many possibilities for a password to reach the right word that enables the hacker to enter the system.

Attempts to exploit additional advantages: The idea here relates to one of the strategic protection concerns. The knowledge that the user of the system - within the organization - has a specific scope of use and scope of authority for the system, but what happens in practice is that the advantages of use are increased without the risk assessment or without the knowledge of the person that in any case a hacker of the system will not only be able to destroy or tamper with the data of the user who entered the system through his subscription or via his own point of entry,

It will simply be able to destroy the various files of the system, not even connected to the entrances that entered it because it invested the additional benefits enjoyed by the user who was entered through the entrance,

and this alone gives us the perception of the importance of information security strategy and protection in the establishment, the identification of privileges and powers may prevent in fact to get mass destruction and makes breakthroughs ineffective, and will not allow conscious strategies to say that the Dole user has advantages not known about them but will not allow their existence originally.

THE CONCEPT OF PLAGIARISM

Scientific plagiarism is the use of ideas or words of another researcher without correct documentation. This is often due to a lack of awareness and research skills among researchers. Scientific plagiarism has become a threat to the academic community, especially in universities.

Including full scientific plagiarism, the theft of the scientific paper in full, 1.changing the name and address of the original researcher and the name and address of the fraudulent researcher.

2.Another type of scientific plagiarism is the literal transfer, in which the impersonator copies and pastes sections phrases from another search, without reference to the source or use of quotation marks.

3. Unethical co-operation in scientific research is also a type of scientific plagiarism, in which researchers use one of the specialized centers (in return for material) to complete parts of their research without mentioning it in published research (such as writing parts of the research, and others).

4.the misleading ratios of the list of authors is also a type of scientific plagiarism in which the researcher add the name of a researcher did not participate in the search or delete the researcher participated in
Search for authors list.

5.The cloning of research is to publish the same research in more than one scientific journal and this is also a kind of scientific plagiarism.
6.Repeated scientific plagiarism may also be done using data, tables, images or search methods from another search without attributing it to the original author.

7.Some may not realize that once he has changed some words from sentences in a search and reused them in his research with reference to the source he has fallen into a kind of scientific plagiarism with improper wording.

8. self-plagiarism is the researcher's use of parts of his previous research in his new research without reference to the appropriate reference on the grounds that he is the owner of the research.

9.The use of an incorrect source (hyphenated or incomplete) when writing the research is considered a kind of scientific plagiarism is called the invalid source.

10.Finally, the tenth type of plagiarism is obtaining information from a secondary source and attributing it to the original source without referring to the secondary source. This type is called secondary source plagiarism.

Universities have begun using plagiarism detection programs that detect plagiarism alone is not enough to detect all kinds of plagiarism but it works only On the detection of some types of text-based matching.

Increasing the awareness of researchers about the types of scientific research is the first way that universities should take this threat to the academic community by setting up workshops and seminars on scientific plagiarism and introducing a course for postgraduate students on scientific plagiarism and ways to avoid it. Appropriate legal legislation must also be enacted to address these crimes, which harm the reputation of universities.