

# Module 2

---

INFORMATION TECHNOLOGIES IN DAILY LIFE

# Information Technology

---

- Set of tools, processes, and methodologies (such as coding/programming, data communications, data conversion, storage and retrieval, systems analysis and design, systems control) and associated equipment employed to collect, process, and present information.
- In broad terms, IT also includes office automation, multimedia, and telecommunications.



# E-Commerce

---

- Electronic commerce (ecommerce) is a type of business model, or segment of a larger business model, that enables a firm or individual to conduct business over an electronic network, typically the internet.
- Electronic commerce operates in all four of the major market segments: business to business, business to consumer, consumer to consumer and consumer to business.



# E-Commerce Types

---

- **Firm-Firm (Business to Business - B2B):** Companies ordering the supplier in electronic form, providing the invoices and paying the costs are evaluated in this section. According to 1999 data; commercial transactions in the Firm-Firm category constitute 90% of the e-Commerce turnover.
- **Company-Customer (Business to Consumer - B2C):** As a result of rapid developments in WWW technology, the virtual store applications were released with the sale of many products to consumers.
- **Firm-Government (Business to Government - B2G):** Commercial transactions between companies and public institutions, which includes the publication of public tenders on the Internet and the companies' offer. In order to support the spread of e-commerce, the public tax payments and customs procedures are also performed in the virtual world.

# E-Commerce Types

---

- **Consumer to Government - C2G:** It is the e-commerce between the consumer and the public administration. This category involves driving license, passport applications, social security premiums and tax payments with related apps. The transition to the Electronic Government is aimed.
- **Consumer to Consumer - C2C:** Electronic commerce takes between consumer and consumer. Coming together through reliable websites, you can process the process of buying and selling products with different payment types. The best example in the world is Ebay.com. In Turkey, gittigidiyor.com is the example web site.
- **Business to Employee (B2E):** It is a e-commerce type where companies offer special opportunities to their employees and sell only to their employees.

# E-Banking

---

- Online banking, also known as internet banking, e-banking or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website.
- The customer visits the financial institution's secure website, and enters the online banking facility using the customer number and credentials previously set up.



# E-Banking

---

- The types of financial transactions which a customer may transact through online banking are determined by the financial institution, but usually includes obtaining account balances, a list of the recent transactions, electronic bill payments and funds transfers between a customer's or another's accounts.
- Some banks also enable customers to download transactions directly into the customer's accounting software. The facility may also enable the customer to order a cheque book, statements, report loss of credit cards, stop payment on a cheque, advise change of address and other routine actions.



# E-Government

- The use of or application of information technologies (such as Internet and intranet systems) to government activities and processes in order to facilitate the flow of information from government to its citizens, from citizens to government and within government.
- Services offered to the citizens through the e-Government Portal may be grouped as follows;
  - Information services
  - e-Services
  - Payment transactions
  - Shortcuts to agencies and organizations
  - Information updates and announcements
  - Messages to citizens from agencies





# E-Learning

---

- E-learning is electronic learning, and refers employing Information and communication technologies to deliver part, or all of a course of a school, part of business training or a complete distance learning course.
- **Advantages of e-Learning for Society**
  - It provides equal opportunities for individuals that have no chance to attend formal education
  - It is cost effective since it removes costs of travel, accommodation, and printed materials
  - It eliminates geographical and regional barriers since it is independent from time and place
  - It provides instructional facilities for the ones who are required to work in a job



# Telework

---

- Telework means the use of information technology (IT) and telecommunications to replace work-related travel.
- Teleworking allows employees work at home or at a local telework center one or more days per week using communication tools, such as such as phone, fax, modem, Internet teleconferencing, e-mail or IM, to perform work duties from a remote location.



# Advantages of Teleworking

---

- Teleworking frees up the time each day spent travelling to work.
- Saves the cost of using a car or public transport to travel to work.
- Provides an opportunity for flexible working around carer responsibilities.
- Reduced costs from not having to provide office space for the teleworker.
- Teleworkers can be more productive because they do not suffer the interruptions to their work that they would in an office.
- Improved motivation with reduced levels of stress and absence due to illness.
- An employer might be able to retain an employee by allowing them to work part time from home when their personal circumstances change.

# Disadvantages of Teleworking

---

- Increased costs from providing computer equipment and telecommunication links for teleworkers.
- More difficult to manage teleworkers and monitor their performance.
- Increased risk to the security of the information that is used by teleworkers.
- Some types of work are unsuitable for teleworking.
  
- A teleworker may feel isolated because they miss the social interaction from their colleagues at work.
- May be unable to work effectively because of distractions in the home environment.
- May not have the space at home to provide a suitable environment for teleworking.

# E-mail

---

- Short for electronic mail, e-mail or email is information stored on a computer that is exchanged between two users over telecommunications.
- More plainly, e-mail is a message that may contain text, files, images, or other attachments sent through a network to a specified individual or group of individuals.



# E-Mail Usage

---

**From:** Includes the e-mail address of the person who sent the e-mail (and First Name, Last Name, even if not required).

**To (To):** It contains the e-mail addresses of the people we will send the e-mail to. If sent to more than one person addresses are written with a comma or a space between them.

**Subject:** The e-mail content is written briefly. (Such as Hello, Important, Announcement etc.).

**Cc (Carbon Copy):** Send a copy of the e-mail to another person or persons (usually via e-mail content).

**Bcc (Blind Carbon Copy) (Hidden):** With a difference, it functions the same as Cc. People who have received the e-mail they cannot see the information.

**Attachment (Attachment File):** Any file can be sent with e-mails, if desired, by attaching it to the end of the mail.

# Instant Messaging

---

- Instant messaging, often shortened to simply "IM" or "IMing," is the exchange of text messages through a software application in real-time.
- Generally included in the IM software is the ability to easily see whether a chosen friend, co-worker or "buddy" is online and connected through the selected service.
- Instant messaging differs from ordinary e-mail in the immediacy of the message exchange and also makes a continued exchange simpler than sending e-mail back and forth.
- Most exchanges are text-only, though popular services, such as AOL, MSN Messenger, Yahoo! Messenger and Apple's iChat now allow voice messaging, file sharing and even video chat when both users have cameras.



# Voice over Internet Protocol

- Voice over Internet Protocol (Voice over IP, VoIP and IP telephony) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.
- The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN).





# Real Simple Syndication (RSS)

---

- Real Simple Syndication (RSS) is the term used to refer the collection of Web feed formats that provide updated or shared information in a standardized way. The information could be website or blog entries, news headlines, or audio or video files. RSS documents usually contain complete or summarized text, metadata, and author and publishing information.
- RSS feeds benefit both publishers and subscribers because they syndicate work automatically in a format that can be easily accessed and viewed by different applications.



# Blogs

---

- A blog (or **weblog**) is an online journal that is frequently updated and intended for general public viewing. Posts are displayed in reverse chronological order.
- Blogs often provide commentary or news on a particular subject, such as food, politics, or local news; some function as more personal online diaries.
- A typical blog combines text, images, and links to other blogs, web pages, and other media related to its topic.
- Most blogs are primarily textual although some focus on photographs (photoblog), videos (vlog), or audio (podcasting), and are part of a wider network of social media.

# Online Communication

---

There are numerous ways people communicate with each other over the Internet, including e-mail, instant messaging (IM), feedback on blogs, contact forms on websites, industry forums, chat rooms and social networking sites.



# Publishing Content Online

---

Contents can be published online in different ways such as in blogs (text, photo, audio, video, etc.), in Youtube (video), in Jalbum (photos)



# How to be Safe in Internet

---

- Choose strong passwords. Use different passwords for different accounts and change them every few months.
- Do not give out personal details to strangers, both online and offline.
- Don't fall prey to scams. This includes phishing scams and online scams.
- Use an anti-virus program, an anti-spyware program, and a firewall.
- Secure your wireless router with a unique name and password.
- Download files from trusted sources. Don't open or download anything from un-trusted sources.



# Tips for Computer Users

---

## ➤ **Tips for Computer Users**

- Repetitive and prolonged use of a computer keyboard and/or mouse can lead to muscle aches and discomfort. Posture and positioning are important.  
Try to incorporate the following tips into your work style to avoid problems.
- **Maintain Good Posture When Working**
- Sit all the way back in the chair against the backrest.
- Keep your knees equal to, or lower, than your hips with your feet supported.
- Keep your elbows in a slightly open angle (100° to 110°) with your wrists in a straight position. The keyboard tilt can help you attain the correct arm position. A negative tilt (front of keyboard higher than back) helps when working in upright sitting positions. If you recline, a positive tilt (front of the keyboard lower than the back) might be necessary.

# Tips for Computer Users

---

## ➤ **Avoid Overreaching**

- Keep the mouse and keyboard within close reach.
- Center the most frequently used section of the keyboard directly in front of you.
- Center the monitor in front of you at arm's length distance and position the top of the monitor 2" to 3" above seated eye level. You should be able to view the screen without turning or tilting your head up or down.
- Place source documents on a document folder positioned between your monitor and keyboard. If there is not enough space, place documents on an elevated surface close to your screen.

# Tips for Computer Users

---

## ➤ Use Good Typing Technique

- Float your arms above the keyboard and keep your wrist straight when keying.
- If you use a palmrest, use it to support your palms when pausing, not while keying.
- Hit the keyboard keys with light force. The average user keys four times harder than necessary.
- Keep your wrists straight and hands relaxed when using your pointer.
- Don't hold the pointer with a tight grip or extend fingers above the activation buttons.
- Avoid moving the pointer with your thumb or wrist. Movement should originate at your shoulder and elbow.



# Tips for Computer Users

---

## ➤ **Limit Repetitive Motions**

- Reduce keystrokes with macros and software programs such as voice recognition. Reduce pointing device movement with scroll locks and keystroke combinations.

## ➤ **Customize Your Computer Settings**

- The screen font, contrast, pointer size, speed, and color can be adjusted to maximize comfort and efficiency.

## ➤ **Reduce Glare and Eye Fatigue**

- Place your monitor away from bright lights and windows. Use an optical glass glare filter when necessary.
- Take eye breaks and intermittently refocus on distant objects. Try palming your eyes in your hands to reduce eye fatigue.

# Tips for Computer Users

---

## ➤ **Take Breaks**

- Take 1 or 2 minute breaks every 20-30 minutes, and 5 minute breaks every hour.
- Take eye breaks and intermittently refocus on distant objects. Try palming your eyes in your hands to reduce eye fatigue.

## ➤ **Wrist Splints**

- Non-precipitous medication or wrist splints can often be more harmful than helpful. If you begin to develop symptoms, seek help.
- Early intervention can prevent future problems.

## ➤ **Wellness**

- Stay in shape by stretching and exercising regularly. Stretches and exercises can be found on our website.

# Importance of Recycling

---

- Increasing costs on computer supplies can help professionals replace and recycle print cartridges. As a result of these efforts, economic savings and significant scientific developments have been achieved aimed at reducing environmental damage.
- Refill cartridge use is the result of these developments. After the printer cartridges are used up, they are not discarded but filled.
- Black cartridges covering 3 to 7 color cartridges offer 2 to 4 refills.
- The cartridge is both economical and minimizes the damage to the environment. Cartridge refill machines are used for this purpose.
- The use of electronic texts reduces the need for printed documents, thus it is the most important factor to reduce it.

# Energy-saving

---

- Computers are the devices that generate the fastest electrical charge in the world. In the coming years this amount will gradually will increase.
- However, most of the energy used by computers is turned on when the computer is not in use is wasted.
- Computers should be switched off, where applicable, plug must be disconnected.
- In this way, unnecessary energy consumption of computers in standby mode will be prevented.



# Username and Password Usage

---

- Identity testing in terms of network security means that the recipient is sure that the sender is who he claims.
- In addition, entering a password while using a computer program can also be used as part of an identity test.
- When logging in to the computer, the purpose of using the user name and password is to have a predefined identity.
- This proof is a password, the use of a smart card, a one-time password, a numeric signature information can also be in the form of determining a biometric feature.



# Password Protection Policies

---

- Passwords should not be used for too long and should be changed periodically.
- It should never be shared with others.
- If a user ID tries to log into the system with the wrong password many times, this password will be guessed.
- An empty password should never be used. Password must be at least 8 characters, including letters, numbers, other special characters such as (%!,?, =).
- Password should not be a known or predictable Word (surname, pet name, city name) or words found in dictionaries.



# Data Security

---

- Although data security has many dimensions, the basic function is to make a system backup and regularly to carry out.
- Although this is a difficult process, one day the computer system can be disabled for some reason.
- Loss of data or corruption reveals the importance of the issue.



# Consequences of Not Backing Up Data

---

- Energy Loss
- Hardware Loss
- Software Loss
- Loss of User Preferences
- Loss of Data





# Firewall

---

- Firewalls are hardware or software used to control IP traffic between two networks.
- Firewalls are solutions that separate private parts of a system from public parts, allowing users to take advantage of the system only at the level of their assigned rights.
- A firewall can be installed on a specific computer to control it, or it can be installed to control a computer network.
- Firewalls are systems that protect computers and networks from outside threats using a method similar to filtering.
- Thanks to a small database they are in, they have a set of rules and do not allow data traffic that does not comply with the rules.

# Prevention of Data Theft

---

- Data theft is increasingly common today. Credit card information, identification numbers, financial records and ATM passwords are the most stolen data.
- These data are classified into 3 main types: Identity theft, corporate data theft, and stolen laptops data theft.
- In order to be protected from data theft, first of all, it should be ensured that the line and equipment used to connect to the Internet are secure, and applications and sites that require using personal data from public points should not be accessed.



# Identity Theft

---

- Identity theft is a special form of data theft.
- Usually stolen personal information consists of the person's full name, residence or official address, date of birth, social security number, e-mail addresses and passwords, telephone numbers, family members information, credit card numbers and bank account information.
- The thief tends to use stolen personal information to gain access to the victim's bank accounts or other confidential information.
- Stolen personal information can also be used forged or sold to third parties for profit.



# Precautions To Protect From Data Theft

---

- **Physical Security:** The computer and its accessories can be secured by connecting with a physical immovable chain such as a Kensington lock.
- **Biometric Security:** Although it is mandatory to use security passwords, it is more effective to use biometric identifiers because passwords are easily broken.
- **Concealing:** A flat carrying case or backpack should be used to reduce the risk of laptop theft.
- **BIOS Password Protection:** Any operating system will not work unless the BIOS password is entered. This method is not insurmountable, but will still prevent most data theft.

# Precautions To Protect From Data Theft

---

- **Using Complex Passwords:** It becomes difficult to crack complex passwords consisting of different numbers and letter combinations and capital letters and symbols.
- **Disk Encryption:** Encrypting all data on the hard drive is an important form of data protection. Full disk encryption protects all data running on the computer and is easy to use.
- **Using a Hard Disk Password Security Lock:** With a password security lock, it is almost impossible to access a hard disk. It is not possible for anyone to access the drive without entering the correct password.
- **Using Password Protection for Your Files:** Operating systems and many free software provide secure usage password for the protection of important files and folders. Using it reduces the chance of attacking your computer.

# Computer Viruses

---

- Computer viruses are software programs designed to interfere with the operation of the computer, to save, corrupt or delete data, or to cause slowdowns or other problems by spreading themselves over the Internet to other computers.
- They are added to computer programs involuntarily and they never do the main functions that the programs should do, restrict them or make wrong operations.



# Computer Viruses

---

- A number of anti-virus software have been developed to protect against viruses. It is possible to obtain these softwares easily. However, it would be a great mistake to trust anti-virus programs completely against viruses. Because anti-virus programs will only contain information about the viruses that were up to that time. In other words, this program will not play a protective role against a virus that is written only a short time after you install your anti-virus program and can enter your machine.
- The best way to protect your computer from viruses and to reduce the loss of information and time, as well as the anti-virus programs you will use, is to first learn the ways viruses enter your computer and take some general protection measures accordingly.

# Ways for the Virus to Enter the Computer

---

- From floppy disks, removable disks and sticks that we are not sure are clean.
- From the CDs and DVDs we use to install a program,
- From an infected computer that we are connected to from network neighbors (in cases where network sharing is open),
- From e-mails and files we have received via e-mail,
- From various interview programs and files received through them
- From the posts we make on social networks.
- Often times, even browsing through unreliable web pages can cause malicious program particles to settle, which will endanger the security of our computer.



# Precautions To Be Taken Against The Virus

---

- A good anti-virus program should be installed and updated regularly.
- Every random memory stick should not be used on the computer we are using.
- CDs and DVDs from unreliable people who do not know for sure that they will work for us should not be used and programs should not be installed.
- The network should never give full sharing to its neighbors. If sharing is required, sharing must be given based on password. It should be removed when the job is done.
- It should not transfer data from computers that you are not sure of the reliability of viruses and trojans during sharing.
- Should not open e-mails from people we do not know if necessary, If there is a file attachment, care should be taken.

# Precautions To Be Taken Against The Virus

---

- Should not open e-mails from people we do not know if necessary, If there is a file attachment, care should be taken.
- It should never transfer files from chat media and social networks from people we do not know or do not fully trust.
- The passwords of the programs we use on our computer should never be left saved. These programs should only be used by asking you for a password. In addition, these passwords should be changed at short intervals.
- Computers, which are very important for security, should not be connected to the network and internet unless necessary.

# What is Copyright?

---

- An act of copying computer software without the consent of the rights owner and without paying the copyright, such as using it without a license, or reproducing it more than allowed is called software copyright infringement.
- An international trend is emerging towards the patented protection of computer programs, algorithms, mathematical formulas, and to allow parallel import of intellectual property works in cases where there is no infringement of the right. As a result of this trend, the use of products produced in computer environment protection of copyright emerges as the main problem.



# How to Understand Licensed Software?

---

- If the software is purchased on materials distributed on compact discs or other portable media, a label is required. This is the Proof of License label. This label is located on an actual software copy and indicates that the software is a licensed copy.
- To be valid, the label must be on the software package or affixed on the back of portable devices (usually the operating system license).
- The separate purchase of the label is not considered a license proof and is invalid. To prove that you are a licensed user of the software, it is necessary to keep the labeled package.

# Product Identity Test (PID)

---

- PID is a unique identification number unique to each copy of a software system.
- During the software installation, it asks to enter product identifier information.



# End User Agreement (EULA)

---

- EULA may appear as an agreement protecting the user's rights.
- Basically, the EULA is a text that reminds you of the necessary legal obligations regarding the software you will use.
- The EULA is usually brought before you install the software and you will be asked to check a small box under the text to indicate your acceptance.
- Under the law, this is equivalent to signing under a piece of paper. Because it is not allowed to install the software without checking the small box that says "I accept".
- It basically contains clauses that protect the rights of the software company.

# Free Software and Types

---

**Public Domain Software:** The people who write these programs allow everyone to buy and use their programs for free. However, in some cases, this free use may be restricted.

**Free (Freeware) Software:** Free software can be used by the people who buy them without limitation. These software should not be sold to third parties for money. There is no license requirement.

**Shared (Shareware) Software:** Use in shareware, if you like it, send me a certain amount of money philosophy applies. However, there is no coercive mechanism here. In some cases, the shared program we use will not work when it expires.

**Open Source Software:** Open source software is software that is open to anyone who wants source code. The distinguishing feature of this type of software is that it gives the user the freedom to change the software.

# What is Data Protection?

---

- One of the most important issues in information security is to control who has access to resources and how, thus protecting data by preventing unauthorized modification and disclosure of information.
- Activities performed for this purpose are generally called access control.
- An example of an access control is when a user tries to access a directory on the network from his computer and encounters a screen asking him for a username and password.





# What is Access Control?

---

- Access control can be provided based on software and hardware.
- With the help of access control, how users and systems interact with other systems is determined. With access control controls, unauthorized access to resources is prevented and access of authorized users is restricted according to their authorization levels.
- Access control is carried out in 3 stages: 1. Identification, 2. Authentication and 3. Authorization.



# Identification

---

- A valuable resource should only be given access to those who have the right to access it.
- During the audit of this access authorization, two types of information are requested from users. The first information belongs to the user known to everyone and indicates the identity of the user, such as name and registration number. The second type of information is private information known only to the user. Programs and utilities are examples.



# Authentication

---

- It is the determination that a person is a person with a predefined identity. This proof appears in the form of a password, the use of a smart card, a one-time password, a digital signature information, and determining a biometric feature.
- The login password is the most common form of authentication. In addition to its ease of use, it should be used with caution as it is easy to get into the hands of others.



# Authorization

---

- It is the granting of access to system resources to users who have introduced themselves to the system with their identity and have been tested (that is, proved to be the person with the specified identity).
- When a user wants to access a file on a resource on the network after being authenticated, it is first tested whether that user is authorized to access this resource.
- If he has authority, he is allowed to access the resource. This means that a user does not have access to all resources after being authenticated. Access authorization / right is limited to the level of authorization given to it.

