Using an Internet

By

Ass. Lecturer Hania M.Salih A.Ridha

What is the Internet?

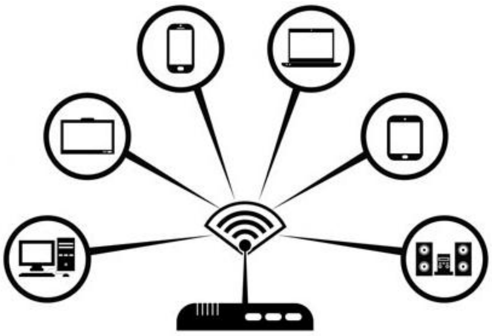
- The internet is a **telecommunications network** that uses telephone lines, cables, satellites and wireless connections to connect computers and other devices to the World Wide Web.
- It is a **network of networks** that consists of private, public, academic, business, and government networks of local to global scope.
- The Internet is a shortened of **interconnected network**

What is WWW?

The World Wide Web (WWW), commonly known as the Web, is an information space where documents and other web resources are identified by Uniform Resource Locators (URLs, such as https://www.uobasrah.edu.iq/), which may be interlinked by hypertext, and are accessible over the Internet. The resources of the WWW may be accessed by users by a software application called a web browser(such as Google, Google scholar, Yahoo, and ReaserchGate).

Ways to connect to the Internet

1.Connecting Using Wireless Broadband



Wireless broadband — or Wi-Fi — is a broadband connection to the internet that can be accessed without cables.

This is different from 3G or 4G mobile broadband, which uses mobile phone signals. With Wi-Fi, it's only the connection between your computer and the router that is wireless, not the actual broadband connection itself.

Mobile broadband: Another type of wireless broadband is mobile broadband, or 3G/4G broadband. It's a form of wireless broadband aimed for consumers who need a connection while they're on the move, allowing them to access the internet from wherever they are, even abroad.

The difference between 3G and 4G is pretty simple. The "**G**" is short for generation, so 3G and 4G represent the third and fourth generations of mobile broadband Internet. As a rule, provided that you're on the same carrier, a 4G connection will be faster than a 3G one, and more reliable access to rich online content.

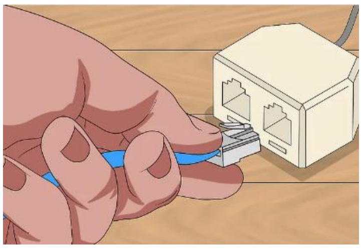
2.Connecting Using an Ethernet Cable

Many recent devices can connect directly to the router via an Ethernet cable. However, some aren't built to do that. Laptops, for example, often don't have components for using Ethernet.

Ethernet is more reliable than Wi-Fi, but that doesn't mean that things still can't go wrong.

3.Connecting a Computer Using Dial-Up

Dial-up internet requires the use of a phone line, and can only connect one person per phone at a time. With dial-up internet, you may be only limited to browsing websites that are mostly text and/or images without many features.



****

Note

Devices like smartphones, mobile tablets, iPods, handheld and gaming systems can usually only connect to Wi-Fi services, due to the portable nature of them. Therefore, you won't be able to connect a mobile device to Ethernet or to a dial-up network. Ethernet and dial-up connections are limited to computers and non-portable gaming devices

Purposes of using internet

1. **Electronic mail**.
2. **Research.**
3. **Downloading files**.
4. **Discussion groups**. These include public groups
5. **Interactive gaming**. Who hasn't tried to hunt down at least one game?
6. **Education and self-improvement.** On-line courses and workshops are found on internet.
7. **Electronic newspapers and magazines**. This category includes news, weather, and sports.
8. **Job-hunting**.
9. **Online shopping**.

Importance of internet in education

An importance of the internet as a learning tool is significant. The development of Internet technologies has raised the education level in all countries and it has changed the way students are being taught at Schools and Universities.

Internet applications respond to students and other people questions in real time. **Students are seeing Google as a new Teacher and the Internet as a school.** That's why it is important for teachers to use information technology in education.

How to protect your data on internet?

❖ How to protect your devices?

Antivirus software (abbreviated to AV software).

It is a computer program which protects your device from viruses that can destroy your data, slow down or crash your device, or allow spammers to send emails through your account. The Antivirus software was originally developed to detect and remove computer viruses.

❖ How to improve your internet privacy?

1. Check social privacy settings

If you have social accounts, those networks have a lot of information about you, and you might be surprised how much of it is visible to anybody on the Internet by default. That’s why we strongly recommend you check your privacy settings: It’s up to you to decide what info you want to share with complete strangers versus your friend or even nobody but you.

2. Don’t use online storage for private information

Don’t use online services for sharing information to store your private data. For example, Google Docs isn’t an ideal place to store a list of passwords, and Dropbox is not the best venue for your personal documents copies or photos.

3. Internet tracking

When you visit a website, your browser discloses a bunch of stuff about you and your surfing history. Marketers use that information to profile you and target you with ads.

4. Keep your main e-mail address and phone number private

Your reward for sharing your e-mail address and phone number? Tons of spam in your e-mail inbox and hundreds of robocalls on your phone. Even if you can’t avoid sharing this info with Internet services and online stores, don’t share it with random people on social networks. Create an additional e-mail account and purchase an additional SIM card to use for online shopping and other situations that require sharing your data with strangers.

5. Use messaging apps with end-to-end encryption

Most modern messaging apps use encryption, but in many cases it’s what they call encryption in transit — messages are decrypted on the provider’s side and stored on its servers. What if someone hacks those servers? Don’t take that risk chose end-to-end encryption that way, even the messaging service provider can’t see your conversations.

- Use a messaging app with end-to-end encryption for example, WhatsApp;
- Note that by default, Facebook Messenger, Telegram and Google Allo do not use end-to-end encryption.

6. Use secured passwords

Using weak passwords to protect your private information is as good as shouting that information to passersby. It’s nearly impossible to memorize long and unique passwords for all the services you use but try to:

- Use long (not less than 8 characters) passwords everywhere;
- Use a combination of letters, numbers and special symbols (@, #, %, &, *, !).
- Use a different password for each service.

7. Review permissions for mobile apps and browser extensions

Mobile apps prompt you to give them permissions to access contacts or files in device storage, and to use the camera, microphone, location, and so on. Some really cannot work without these permissions, but some use this information to profile you for marketing (and worse). Fortunately, it's relatively easy to control which apps are given which permissions. The same stands for browser extensions, which also have unfortunate spying tendencies.

- Review the permissions you give to mobile apps.
- Do not install browser extensions unless you really need them. Carefully check the permissions you give them

8. Secure your phone and computer with passwords or passcodes

Our computers and phones store a lot of data we'd rather keep private, so protect them with passwords. These passwords don't have to be complicated and unique, but they should keep random people out. On mobile devices, do a bit better: six-digit PINs or actual passwords rather than four digits and screen-lock patterns. For devices that support biometric authentication — whether fingerprint reading or face recognition — that's generally OK, but remember that these technologies have limitations.

- Use passwords or biometric authentication to set a lock for your phones, tablets, and computers.

9. Disable lock screen notifications

Protect your phone with a secure password, but leave notifications on the lock screen? Now any passerby can see your business. To keep that information from appearing on the locked screen, set up notifications correctly.

- Disable lock-screen notifications or hide sensitive information from the lock screen.

10. Stay private on Wi-Fi networks

Public Wi-Fi networks usually do not encrypt traffic, and that means anyone on the same network can try to snoop on your traffic. Avoid transmitting any sensitive data — logins, passwords, and credit card data over public Wi-Fi.

- Avoid using public Wi-Fi if possible.