Unit 2.- Internet, security and responsibility.

2.1:- Internet, definitions

Internet is a network of millions of computers and devices connected between them by means of re or wireless connections. They share information and files all over the world.

If we want to use internet with our computer or electronic device, we need:

- A browser the program that shows us the contents of a web page.
- A searching engine: a program in a server that helps us to find the information we are looking on the internet.
- Server: a special computer where we can store a web page in order to be accessible for everybody 24 hours each day.

The address of a web site is called URL (uniform resource locator), and it is unique for each web.

2.2.- Internet connections

For connecting our computer to the internet, we need:

- An ISP, an internet provider, usually a communication company. We have to pay a fee for it and they assign us an IP address, which is the identification of our computer.
- A telephone line: an ADSL or high speed optics fiber line.
- A router, that connect our computers or devices to the telephone line.
- A communication protocol installed in our computer. This is a program which handles the communication through the net. This program is called TCP/IP protocol.
- A DNS server, which translates the IP address number of a web page into words, more easy for us to remember.

2.3.- Internet threats and risks

When we are using internet, there are some risks, to the machine or to people, that we have to learn how to protect us and our computer against them.

Threats	Solutions
• Loss of privacy and damage to our image or identity • Identify theft. • Cyberbulling: bullying that takes place using electronic technology. Examples of cyberbullying include rumors sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles. • Phising: a fraud or false web page that tries to get your passwords, bank information, etc. • Viruses and trojans: programs that infect our computer to damage it or take the control of it. • Spyware: malware that tries to get data from users. • Hackers: programmers that know how to find security holes in your computer for causing damage or getting money.	• Common sense, our attitude is the best protection. • Antivirus: a program which protects our computer from viruses and trojans. It must be updated. • Firewall: a defense system that controls the information through the ports of our computer. • Passwords: do not say them to other people, or do not make it easy to discover, like your birth-date. • Cryptography: your information through the internet must be encrypted for making it impossible for other people to read it.

2.4.- Digital responsibility.

As we have seen, our attitude is our best protection, we must be digital responsible.
And there are also some laws that protect us:

- Ley de Protección de Datos.
- Leyes del derecho a la intimidad y al honor personales.

Here are some guidelines you must bear in mind when you are on the net:

a) Do not ask or give your data or information about you.
b) Do not talk to strangers.
c) Put a sticker on your webcam, it can remotely operated.
d) Think before you upload photos or videos of yourself or other people.
e) Keep your antivirus and operative system updated.
f) Make sure you are the minimum age required to enter or join a web site.
g) Inform yourself about sites, read the terms of use before clicking I agree.
h) Inform your parents if you receive something unusual or unpleasant.

USE COMMON SENSE.