Unidad 2.- Internet, seguridad y responsabilidad.

2.1: - Internet, definiciones.

Internet es una red de millones de ordenadores y dispositivos conectados entre sí mediante conexiones alámbricas o inalámbricas. Comparten información y archivos en todo el mundo.

Si queremos usar Internet con nuestra computadora o dispositivo electrónico, necesitamos:

- Un navegador del programa que nos muestra los contenidos de una página web.
- Un buscador: un programa en un servidor que nos ayuda a encontrar la información que buscamos en Internet.
- Servidor: un ordenador especial donde podemos almacenar una página web para que todos puedan acceder a ella las 24 horas del día.

La dirección de un sitio web se llama URL (uniform resource locator) y es única para cada sitio web.

2.2.- Conexiones a Internet.

Para conectar nuestro ordenador a Internet, necesitamos:

- Un ISP, un proveedor de Internet, generalmente una compañía de telecomunicaciones. Tenemos que pagar una tarifa y nos asignan una dirección IP, que es la identificación de nuestra computadora.
- Una línea telefónica: una línea ADSL o de fibra óptica de alta velocidad o móvil 4G.
- Un router o enrutador, que conecta nuestras computadoras o dispositivos a la línea telefónica.
- Un protocolo de comunicaciones instalado en nuestro ordenador. Este es un programa que maneja la comunicación a través de la red. Este programa se llama protocolo TCP / IP.
- Un servidor DNS, que traduce el número de dirección IP de una página web en palabras, más fácil de recordar.

2.3.- Amenazas y riesgos de Internet

Cuando usamos Internet, existen algunos riesgos, para la máquina o para las personas, que debemos aprender a protegernos a nosotros y a nuestro ordenador contra ellos.

Amenazas

- Pérdida de privacidad y daños a nuestra imagen o identidad.
- Robo de identidad.
- Cyberbulling: bullying que tiene lugar utilizando tecnología electrónica. Los ejemplos de acoso cibernético incluyen rumores enviados por correo electrónico o publicados en redes sociales, y fotos, videos, sitios web o perfiles falsos embarazosos.
- Phishing: una página web fraudulenta o falsa que intenta obtener tus contraseñas, información bancaria, etc.
- Virus y troyanos: programas que infectan nuestro ordenador para dañarlo o tomar el control de el.
- Spyware: malware que intenta obtener datos de los usuarios.
- Hackers: programadores que saben cómo encontrar agujeros de seguridad en tu computadora para causar daños u obtener dinero.

Soluciones

• Antivirus: un programa que protege nuestro ordenador de virus y troyanos. Debe estar actualizado.
• Firewall: un sistema de defensa que controla la información a través de los puertos de nuestra computadora.
• Contraseñas: deben ser seguras, no las digas a otras personas ni facilite su descubrimiento, como tu fecha de nacimiento.
• Criptografía: su información a través de Internet debe estar encriptada para que otras personas no puedan leerla.
• Sentido común, nuestra actitud es la mejor protección.

2.4.- Responsabilidad digital.

Como hemos visto, nuestra actitud es nuestra mejor protección, debemos ser responsables digitales. Y también hay algunas leyes que nos protegen:
• Ley de Protección de Datos.
• Leyes del derecho a la intimidad y al honor personal.

Aquí hay algunas pautas que debes tener en cuenta cuando estés en la red:

a) No pidas ni des tus datos o información sobre ti.
b) No hables con extraños.
c) Coloque una pegatina en su cámara web, puede funcionar de forma remota.
d) Piensa antes de subir fotos o videos tuyos o de otras personas.
e) Manten actualizado tu antivirus y tu sistema operativo.
f) Asegúrate de tener la edad mínima requerida para ingresar o unirse a un sitio web.
g) Infórmate sobre los sitios web, lee los términos de uso antes de hacer clic en Aceptar.
h) Informa a sus padres si recibe algo inusual o desagradable.