SEGURIDAD EN INTERNET

Paso 1. Seguridad en la conexión Wi-fi

PROTEGEMOS LA WIFI DE CASA

Muchos usuarios de Internet con conexión por Wi-fi que se dan cuenta con el paso del tiempo, de que la velocidad de su conexión es a veces más lenta de lo normal. ¿Es esto normal?

Sospecho que alguien utiliza mi conexión.

Hay una solución sencilla para saberlo:

1. Apaga todos los equipos que se conectan al router, si las luces siguen parpadeando... ¡Hay alguien que se está aprovechando de tu conexión!
2. Te aconsejamos una app para dispositivos Android que es capaz de revisar los dispositivos conectados a tu red: **Fing** (ten en cuenta al usarla que tu propio router aparecerá como uno de los conectados).

Qué más da si alguien utiliza mi conexión, ¿no?

Por muy generosos que seamos, no da lo mismo ya que:

1. Tendré menos ancho de banda
2. Pueden robar datos de mi red y dispositivos
3. Puedo ser acusado de realizar delitos asociados al uso de Internet.

¿Te parece importante? Pues vamos a ver en el punto siguiente como podemos poner soluciones.

Medidas de protección.

1. La configuración de fábrica del router no es segura. Una medida de protección básica es desactivar el WPS de nuestro router (en caso de estar activado). Si tu nivel de conocimientos informáticos no llega a este nivel pide ayuda a algún conocido que entienda o llama al servicio técnico de tu proveedor para que cambien la configuración.
2. Se recomienda no utilizar ninguna wifi sin clave.

Para más información:
Una wifi segura en sólo 7 pasos
https://www.osi.es/es/protege-tu-wifi

CONECTARSE A UNA WIFI FUERA DE CASA PUEDE TRAER VARIOS RIESGOS

Paso 2: El antivirus

EL ANTIVIRUS

¿Qué es?

El antivirus es un programa que ayuda a proteger tu ordenador contra la mayoría de los virus, worms, troyanos, etc. que podrían causarte daños importantes en tu ordenador y en los archivos guardados.

Algunos antivirus gratuitos

Avast
Microsoft Essentials
Panda free antivirus

Virus famosos/curiosos

1. **Tu ordenador se apagará en un minuto**. Este virus surgió en el año 2003. Al infectarse, el equipo se reiniciaba automáticamente.

2. **Virus de la policía**. Muchos se acuerdan de él porque pagaron 100€ en su intento por desinfectarse.

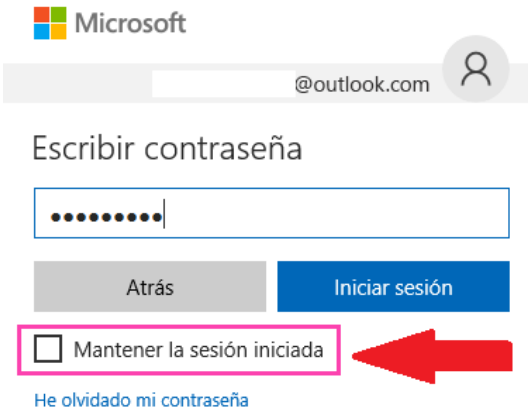
https://www.smythsys.es/

3. **Accesos directos en tu pen-drive**


https://www.marindelafuente.com.ar/

Paso 3: Prácticas adecuadas en la navegación.

BUENOS HÁBITOS



1. **<u>Cierra siempre tus sesiones.</u>** Cuando accedas a un servicio en Internet en el que nos tienes que identificar, como el correo electrónico, suele haber una casilla que dice: **"no cerrar sesión" o "recordar mis datos". <u>No marques esta casilla a no ser que navegues desde un ordenador de uso personal.</u>**
2. **<u>Navegación en sitios de confianza</u>**

http://www.tramitesaccesibles.aspaym.org/

3. **<u>Usa extensiones para aumentar la seguridad</u>**

Algunos ejemplos:

- **Adblock**. Bloquea la publicidad molesta. *Firefox y Chrome.*
- **Censureblock**. Bloquea páginas pornográficas. *Firefox.*
- **Url-filter**. Bloquea páginas. *Firefox.*

Paso 4: Contraseñas.

¿Qué son?

Son las llaves de acceso a muchos datos. Si es fuerte mantendrá a buen recaudo mi información más sensible, pero si no dejará nuestros datos al descubierto.

¿Tenemos una contraseña segura?

Es muy sencillo saberlo. Sólo tienes que hacer clic en el siguiente enlace:

https://www.internautas.org/compruebapassword.html

Los elementos de una contraseña segura

Si debes mejorar la fortaleza de tus contraseñas sigue los siguientes pasos:

1. **Usa frases.** Piensa en una frase que tenga algún significado para ti: ¡Tengo 2 hijos María y Juan!. Si tienen mayúsculas y números, mejor. Ahora, con la primera letra de cada palabra tienes: ¡T2hMyJ! Ésta sería una buena contraseña, ¿verdad? Recuerda que una contraseña segura debe tener letras mayúsculas y minúsculas, números y algún otro símbolo.
2. **Crea una contraseña sin vocales.** Busca palabras que tengan significado para ti, por ejemplo: mis 2 hijos María y Juan, ahora elimina las vocales: ms2hjsMrJn
3. **Guíate por el teclado**. Elige una sucesión de cifras que te resulte fácil de recordar. Por ejemplo: 856. Ahora busca cada uno de los números en el teclado y vuelve a introducirlo seguido por las letras que tiene justo debajo: 8ikm5tgb6yhn. Para complicarlo un poco más, cambia alguno de los caracteres por un símbolo, el que comparta tecla con una de las cifras, sin ir más lejos. 8(ikm5%tgb6&yhn

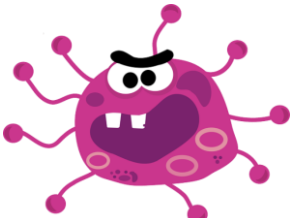
PUEDES COMBINAR ESTAS OPCIONES Y OBTENDRÁS CONTRASEÑAS MÁS FUERTES Y SEGURAS.

Recuerda los elementos de una contraseña segura:

Y sobre todo, nunca comuniques a nadie tu contraseña.

Paso 5: Malware.

¿Qué es?



http://navegaseguroporinternet.blogspot.com/

Es el conjunto de programas instalados sin el consentimiento del usuario que afectan al rendimiento del equipo. Dentro del malware están los virus, troyanos, spyware, etc.

Soluciones

Pero si a pesar de todas nuestras precauciones algún tipo de malware entre en mi ordenador, podemos instalar un software que limpie y proteja el equipo contra estas amenazas. Resultará imprescindible instalarlo si navego por páginas para adultos, foros de descarga o para compartir archivos, etc.

Paso 6: Los grupos de Whatsapp del centro.

Como alumno de un centro educativo la mayoría de nosotros somos añadidos al correspondiente grupo de Whatsapp en el que compartir información con los demás alumnos del grupo de clase...
Y aunque puede tener muchas funciones positivas, un mal uso del mismo puede ser perjudicial. Por eso te pedimos que hagas un buen uso del grupo Whatsapp de clase.

1. **Intercambia solamente información útil sobre el grupo clase.**
2. **Respeta la intimidad de los demás.** Una vez envías la foto o el texto ya no hay marcha atrás.
3. **Si en el grupo no se respetan los buenos usos quizá lo mejor sea no participar en él.**