En la actualidad usamos Internet a diario, ya sea para buscar información, ver lo que han hecho nuestros amigos en las redes sociales o incluso para aprender cosas nuevas. Pero como en la vida misma, hay personas por Internet que no tienen buenas intenciones y que buscan su propio beneficio a costa de los demás, llegando en ocasiones a hacer mucho daño. En este nivel, aprenderás a evitar estar al alcance de estas personas y a **navegar de forma segura por Internet**. ¡A por ello!

El principal método que tienen los ciberdelincuentes para conseguir de nosotros lo que quieren es el engaño. Existen muchas formas en las que pueden engañarnos, pero todas tienen en común que intentan imitar algo real y de confianza para nosotros. Te dejo aquí algunas **medidas de seguridad que deberías seguir**:

1. **Si te quieres conectar a una red Wifi estando fuera de casa, intenta que no sea a alguna pública o gratuita**. Por lo general, estas redes no son seguras y todo el tráfico de información es transparente para cualquiera que mire**. Es preferible usar los datos móviles**, ya sean tuyos o compartidos con alguien de confianza. Pero en caso de que no tengas datos móviles disponibles y tampoco haya redes seguras a las que conectarse, sigue las siguientes recomendaciones para navegar por Internet lo más seguro posible.

2. **Comprueba que la red es oficial**. Muchos ciberdelincuentes crean redes falsas con un nombre similar al oficial con el objetivo de que caigas en la trampa. Si te encuentras en esta situación, **pregunta a alguien que sepa cuál es la original o simplemente ignora ambas redes** por si las moscas.

3. **Si te conectas a una red Wifi pública, no compartas información**. ¿Qué quiere decir esto? Evita entrar en sitios donde tengas que introducir un nombre de usuario y una contraseña. Es más, tampoco envíes ningún correo. Haciendo esto, nos protegemos de las personas que estén monitorizando la red.

4. **Debemos asegurarnos de que nuestros dispositivos estén actualizados con la última versión disponible**. De este modo, evitaremos que los ciberdelincuentes se aprovechen de vulnerabilidades o fallos que tengan los sistemas de nuestros dispositivos.

5. También **es importante que nuestros navegadores estén actualizados**, aunque la forma de hacerlo varía dependiendo del navegador. Te sugerimos que busques en Internet una guía para seguir paso a paso cómo actualizar el navegador que uses más a menudo.

6. Si navegamos por Internet y entramos a alguna página, **tenemos que asegurarnos de que sea una web con HTTPS y con un certificado de seguridad**. Para comprobarlo, basta con **mirar la dirección o URL de la página** a la que queremos entrar. Si empieza con "https", significa que, en principio, es segura. En algunos dispositivos, también se puede ver un candado cerrado al lado de la dirección de la página. Este es otro indicador de que se trata de una página segura. Entrando en estas páginas, nos aseguramos de que **la comunicación está cifrada** y minimizamos los riesgos.

7. **Otra forma de navegación segura es usando la navegación privada, también conocida como modo "incógnito"**. Este modo permite que podamos entrar en páginas web **sin que se almacene en el navegador información sobre las mismas**, como puede ser en el historial o con las "cookies" que emplean algunas páginas web. Un ciberdelincuente podría emplear ese registro de qué páginas hemos visitado para obtener información importante para nosotros. Para evitar que pase esto**, es recomendable eliminar el historial y las "cookies" cada cierto tiempo**.

8. Hay navegadores web que disponen de extensiones, que son un tipo de programa que permite personalizar el navegador. Algunas de estas extensiones permiten eliminar los anuncios y la publicidad que salen en las páginas web, borrar automáticamente las "cookies" e incluso ayudar a detectar páginas maliciosas. Son bastante útiles, pero **recomendamos tener cuidado y no descargar cualquier extensión sin buscar información sobre ella**, ya que las extensiones requieren que les des ciertos permisos. Los ciberdelincuentes se aprovechan de nuestra pereza para leer e incluyen permisos excesivos en sus extensiones falsas para robarnos información y conseguir acceso a nuestros dispositivos.

Ya hemos hablado de entrar en páginas cuya dirección empiece por "https", pero si no nos fijamos y entramos en un sitio falso, **debemos prestar atención a ciertos detalles**:

1. **Si miramos la dirección de la página web y vemos que no coincide con el nombre de la web original, la empresa o el programa que queramos descargar, debemos desconfiar**. Lo mejor sería abandonar la página web y buscar otras alternativas.

2. **Presta atención a los detalles estéticos**. Por lo general, **las webs falsas no están cuidadas** y pueden tener textos traducidos automáticamente, imágenes de baja calidad o tienen el aspecto de ser una web hecha muy deprisa, sin cuidar los detalles del sitio (cosa que no sucede con las páginas oficiales).

3. **Si comprobamos los anuncios que tiene la página web, podemos también averiguar si es segura o no**. las páginas falsas suelen tener muchos anuncios, siendo muchos de ellos peligrosos, que impiden disfrutar tranquilamente de la navegación por Internet o que buscan que hagamos clic por todos los medios posibles.

4. **Si la página web a la que queremos entrar es fiable, podemos encontrar información sobre el propietario o del desarrollador en Internet**. De esta forma podemos comprobar qué tan seguro es entrar en dicha web.

Ahora deberías poder manejarte sin problemas por Internet, evitando las trampas y engaños de los ciberdelincuentes. Pero antes de navegar como loco por Internet, deberías poner a prueba todo lo que has aprendido en este nivel para asegurarte de que no se te olvida nada. ¡Veamos si estás listo para ver a través del engaño de los ciberdelincuentes!