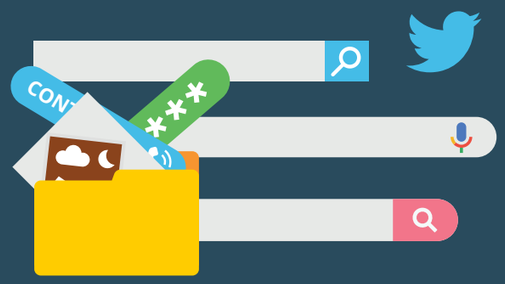
Navegar

POR INTERNET

Conectarnos a Internet se ha convertido **en una acción cotidiana** para cualquiera de nosotros.

Con **un solo clic** tenemos acceso a toda la información que queramos, **podemos estar en contacto con cualquier usuario y podemos efectuar compras online fácilmente.**

Pero **¿sabías que cada una de estas acciones deja un rastro de información?**



Cada vez que accedemos a Internet, se almacena mucha información sobre nosotros y nuestra actividad *online*.

Los ciberdelincuentes lo saben y llevan a cabo todo tipo de tácticas y ataques para hacerse con ella.

Por suerte, **existen medidas de protección** que podemos implantar para realizar una navegación segura.

TU AYUDA EN
CIBERSEGURIDAD

017

incibe_

@INCIBE @osiseguridad

incibe_ 017
INSTITUTO NACIONAL DE CIBERSEGURIDAD

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

www.incibe.es | www.osi.es

OSI Oficina de Seguridad del Internauta

Precauciones

EN NAVEGADORES WEBS

Debido a la cantidad de información que almacenan, son el objetivo de muchos ciberdelincuentes.
Para protegernos, debemos:

Actualizar a la última versión: para solucionar posibles vulnerabilidades.
Lo más sencillo es activar la actualización automática.

Instalar extensiones: nos ayudarán a filtrar conexiones inseguras, así como a disponer de un antivirus para el navegador.

No almacenar credenciales: así reduciremos el impacto en caso de ataque. En su lugar, utilicemos un gestor de contraseñas.

Eliminar cookies, caché e historial: conviene eliminarlos cada cierto tiempo desde la configuración del navegador.

Activar el modo incógnito. Para no dejar rastro de nuestra actividad online. Muy útil si tenemos que utilizar un dispositivo ajeno.

Precauciones

AL NAVEGAR POR PÁGINAS WEB

Al navegar por Internet debemos tener precauciones con las webs fraudulentas o la descarga de archivos maliciosos. Para ello, debemos:

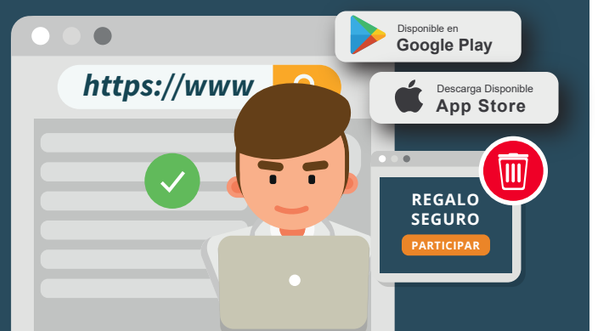
Confirmar que cuentan con certificado de seguridad. En la URL podremos comprobar que comienzan por *https* y cuentan con el candado.

Descargar aplicaciones desde el sitio oficial. Si no, corremos el riesgo de descargar *software* modificado o algún tipo de *malware*.

Ignorar los anuncios y *pop-ups*. Pueden ser enlaces a webs fraudulentas o contener *malware*.

Evitar ingresar información personal. A veces, los formularios de algunas webs piden datos demasiado sensibles. Del mismo modo, no es recomendable guardar nuestra información (datos bancarios o personales) en la web.

Utilizar el sentido común y no dejarnos llevar por promociones demasiado atractivas. Especialmente en épocas más consumistas, donde abundan los fraudes en compras online.



El router es la entrada desde Internet hacia nuestra red privada por lo que configurarlo debidamente nos protegerá de diversos tipos de ataque:

1. Modificar el nombre (SSID) de la red wifi y su clave. Evitaremos dar pistas al atacante sobre nuestro modelo y operador y utilizaremos una ***contraseña robusta.***

2. Modificar las credenciales de acceso a la configuración del router. Actualizándolas y utilizando una contraseña robusta, ***evitaremos que alguien sin permiso pueda modificar la configuración*** de nuestro router.

3. Elegir el mejor protocolo de cifrado. Existen varios tipos (WEP, WPA, WPA2), pero el más seguro, y que además está disponible en la mayoría de routers, es el ***WPA2-PSK.***

4. Desactivar WPS. Permite la conexión de dispositivos a nuestra red de una forma más sencilla, con un ***PIN de 8*** dígitos. Desactivarlo ***nos protege ante una puerta de acceso a los atacantes.***

5. Filtrado MAC. Permitiendo el acceso solo a ***dispositivos reconocidos.*** La dirección MAC funciona como un ***identificador único.***

6. Deshabilitar la administración remota. Así ***evitaremos que terceros puedan conectarse*** a nuestro router desde Internet.

7. Apagar el router. Si vamos a estar fuera de casa, es conveniente apagarlo para ***garantizar que no va a sufrir ataques.***

Precauciones

EN REDES WIFI PÚBLICAS

Los lugares públicos suelen disponer de redes wifi abiertas y gratuitas, pero pueden ser un peligro para nuestra seguridad y privacidad. Por ello, debemos:

Evitar las redes wifi públicas.

A no ser que sea imprescindible y evitando intercambiar información sensible o realizar compras, trataremos de ***priorizar el uso de datos móviles***.

Utilizar una VPN.

Nos permitirá ***cifrar la información*** que intercambiemos desde nuestro dispositivo.

Desactivar la conexión automática.

Así evitaremos conectarnos a una *red fraudulenta*.

Finalmente, **INCIBE** pone al servicio de los usuarios su **Línea de Ayuda en Ciberseguridad 017**, un teléfono gratuito y confidencial disponible todos los días del año al que puedes llamar en caso de duda.

017

incibe_