Cómo usar Internet con seguridad y evitar ponerte en peligro

Consejos para usar Internet de forma prudente y segura

Si quieres navegar seguro en Internet hay una serie de reglas o consejos que es conveniente seguir para no llevarnos sorpresas desagradables. Según los expertos estas son las principales prácticas de seguridad que hay que cumplir si queremos usar Internet de forma segura.

1. Instala un antivirus y mantenlo actualizado

Cada día se descubren nuevas vulnerabilidades y formas diferentes de comprometer tu información privada o asaltar tu cuenta corriente.

2. Actualiza las versiones

No ignores las actualizaciones de seguridad ya que solucionan posibles intrusiones de virus mediante parches que protegen tu ordenador.

3. Realiza copias de seguridad periódicamente

Haz copias de seguridad que te permitan recuperar toda la información en caso de perderla o sufrir un ataque informático.

4. No uses la misma contraseña para todo

A pesar de que es muy cómodo es mejor que no uses la misma contraseña para todo ya que si un hacker la consigue te podría robar todas tus cuentas. Utiliza siempre contraseñas seguras.

Es recomendable que contenga al menos ocho caracteres conteniendo números, letras mayúsculas y minúsculas, y diferentes símbolos, como puntos o guiones. Tambiés es aconsejables cambiar las contraseñas con frecuencia

5. Cuidado con los archivos adjuntos

Antes de abrir los adjuntos que llegan al correo es importante comprobar si el remitente es fiable, y por supuesto nunca abras un archivo adjunto que no sabes quién lo envía. Podrían contener malware, incluso los ficheros aparentemente inofensivos podrían poner en riesgo tu seguridad.

6. Ojo con los enlaces que abres

Cuidado con los enlaces que abres, sobre todo las urls acortadas con bit.ly o goo.gl. Siempre debes fijarte hacia donde redirigen ya que podrían tratarse de páginas falsas que escondan phishing o incluso contengan malware. Si tu navegador te avisa de que esa web no es segura no lo ignores.

7. Las WiFis públicas pueden suponer un riesgo

Intenta ser cauteloso con el contenido que compartes a través de WiFis públicas.

Las redes wifi desconocidas pueden ser utilizadas para robar la información privada del dispositivo que se esté utilizando, evita siempre utilizar contraseñas o datos financieros a través de ellas y trata de acceder sólo a páginas que utilicen **protocolo seguro (https)**.

8. Comprar online con seguridad

Realiza con precaución las compras por Internet. Antes de realizar una compra comprueba si el sitio es fiable y observa si cuenta con el sello de Confianza Online, si el sitio es fiable su url tiene que usar el **protocolo https** o la tecnología **SSL (*Secure Sockets Layer*)** que permite cifrar la información de la tarjeta de crédito que se envía en internet .

Por otro lado es aconsejable que controles las operaciones y trámites bancarios, una vez has realizado la compra. Recuerda llevarlas a cabo siempre desde redes privadas y gestiónalas directamente desde la web oficial del banco.

9. Descarga de Apps

Evita la descarga de aplicaciones fuera de Google Play o Apple Store y antes de hacerlo es recomendable leer los comentarios

de los usuarios y observar el número de descargas que lleva la aplicación. Otro punto importante es comprobar los permisos que la aplicación solicita durante su instalación, generalmente se pueden limitar.

10. Redes sociales

Cuidado con la información que publicas en las redes sociales. Algunas aplicaciones permiten el registro con la cuenta de otro servicio como Facebook, Twitter, Google… así que piénsatelo antes de enviar o publicar información ya que podría hacerse pública.

Decir cuando nos vamos de vacaciones, compartir el sitio en el que nos encontramos o simplemente con quien estamos podría ser peligrosa si acabara en malas manos.

Lee las condiciones de uso del servicio y trata de limitar la información que recopilarán. Es importante comprobar que información compartirán y en caso de vincular ambas cuentas debemos limitar al máximo la información compartida.

11. La cámara y el micrófono de tu ordenador

En su día fue muy comentada una foto de Mark Zuckerberg en la que se puede ver su ordenador con la cámara y el micrófono tapados con un poco de cinta adhesiva.

Para muchos esta precaución puede parecer excesiva, pero hay programas que permiten hackear el acceso a las cámaras y micrófonos de nuestros ordenadores y teléfonos y monitorear a los usuarios de forma remota sin que seamos conscientes, de forma que nuestra vida privada puede quedar expuesta al alcance de cualquiera.

Fuente: euroresidententes.com