

# Expertos alertan de los peligros del wifi gratis de hoteles, bares o cafeterías

El Colegio de Ingenieros de Informática elabora un decálogo con consejos para utilizar internet con seguridad

■ DANIEL GUINDO

**VALENCIA.** «Habrá problemas gravísimos si no se aumentan y mejoran los controles en internet». En el Colegio Oficial de Ingenieros en Informática de la Comunidad Valenciana lo tienen claro: la red puede llegar a ser, «potencialmente, muchísimo más peligrosa de lo que la gente cree».

Por ello, y con motivo del Día de Internet, que se celebra hoy, esta institución ha elaborado un decálogo para el internauta valenciano en el que proporcionan algunos consejos prácticos para utilizar internet con seguridad.

En este documento, estos expertos alertan de varios peligros como, por ejemplo, la utilización de redes wifi gratuitas de establecimientos públicos como cafeterías, restaurantes, hoteles, aeropuertos o bibliotecas, entre otros. «Estas redes son como una sala sin paredes, no sabes quién puede estar escuchando», explica la guía.

Al respecto, el presidente del colegio, Juan Pablo Peñarrubia, aconseja a los internautas que únicamente usen estas redes gratuitas para navegar por páginas seguras, mientras que, bajo ningún concepto, se lleven a cabo gestiones como proporcionar claves o datos personales importantes, especialmente para transacciones bancarias o pagos con número de tarjeta de crédito.

En relación a los teléfonos móviles, y más concretamente a los smartphones, estos expertos aconsejan que, únicamente, se descarguen apps de los sitios oficiales. De lo contrario, advierten que «pueden tener programas ocultos que enviarán nuestros datos privados a sitios incontrolados»; como la información de la agenda personal y de contactos o, por ejemplo, la ubicación del usuario.

Junto con esta práctica, pueden resultar especialmente peligrosos también ciertos errores graves que

se cometen normalmente a través de distintas redes sociales, como colgar imágenes del interior del domicilio particular o anunciar periodos vacacionales. «Pueden controlar dónde estamos por el móvil y conocer si hay una ventana por donde entrar a nuestra casa. Los usuarios de la red deben ser mucho más conscientes del peligro que corren si no adoptan las medidas de seguridad necesarias», destaca Peñarrubia.

Una práctica muy habitual a la hora de instalar programas en ordenadores y dispositivos móviles es la de «aceptar, aceptar, aceptar», es decir, «instalarlo sin leer los cuadros de diálogo que aparecen», apunta. Sin embargo, esto facilita la inclusión en los dispositivos de distintos virus espías, que pueden llegar a robar claves o cualquier otro dato personal del usuario.

La guía elaborada por los informáticos valencianos proporciona también pequeños trucos como, por ejemplo, pulsar las teclas <Alt> y <F4> para cerrar páginas que se abren espontáneamente, evitando clicar sobre ellas con el ratón; o introducir las claves bancarias con el ratón directamente en pantalla, en lugar de con el teclado físico. De esta forma «prevenimos el robo de claves si el ordenador estuviera infectado por un programa espía». También aconsejan no descargar contenidos gratuitos a cambio de rellenar un formulario con los datos personales, puesto que «puede que aceptes que se los vendan a terceros».

---

**Advierten de que las apps no oficiales «pueden tener programas que espíen nuestros datos»**

---

**El Colegio de Informáticos reclama más y mejores controles de internet para evitar graves problemas**