⭐️¿Qué es la “identidad digital” de una persona?

Es el rastro que cada usuario de Internet deja en la red como resultado de su interrelación con otros usuarios o con la generación de contenidos.

⭐️¿ Cuáles son los riesgos principales de tener nuestra Wi-Fi desprotegida?

Tener la WiFi abierta implica tener nuestra conexión a Internet compartida, además de otros riesgos como la reducción del ancho de banda: Dependiendo del número de dispositivos intrusos y del uso que hagan de la red, pueden llegar a impedir la conexión de nuestros equipos, el robo de la información transmitida. Una configuración inadecuada de nuestra red inalámbrica puede permitir a un atacante robar la información que transmitimos, la conexión directa con nuestros dispositivos. Un intruso con los conocimientos suficientes, ayudado por un problema de seguridad o una instalación sin la seguridad apropiada, podría acceder a los equipos conectados a la red. Esto implicaría darle acceso a toda nuestra información y la responsabilidad ante acciones ilícitas. Cuando contratamos una conexión a Internet con un proveedor de servicios, ésta queda asociada a nosotros, asignándole una dirección IP que nos identifica dentro de Internet. Cualquier acción realizada desde esa dirección IP lleva a la persona que contrata el servicio: nosotros.  
Si un usuario no autorizado comete acciones ilegales mediante nuestra conexión WiFi, puede acarrearnos problemas muy serios.

⭐️¿Cuáles son los fraudes más habituales en internet?

1. Las subastas: Algunos mercados virtuales ofrecen una amplia selección de productos a precios muy bajos. Una vez que el consumidor ha enviado el dinero puede ocurrir que reciban algo con menor valor de lo que creían, o peor todavía, que no reciban nada.  
2. Acceso a servicios de Internet: El consumidor recibe una oferta de servicios gratuitos. La aceptación lleva implícita el compromiso de contrato a largo plazo con altas penalizaciones en caso de cancelación.  
3. Las tarjetas de crédito: En algunos sitios de Internet, especialmente para adultos, se pide el número de la tarjeta de crédito con la excusa de comprobar que el usuario es mayor de 18 años. El verdadero objetivo es cobrar cargos no solicitados.  
4. Llamadas internacionales: En algunas páginas, por lo general de material para adultos, se ofrece acceso gratuito a cambio de descargar un programa que en realidad desvía el módem a un número internacional o a un 906. La factura se incrementa notablemente en beneficio del propietario de la página.  
5. Servicios gratuitos: Se ofrece una página personalizada y gratuita durante un período de 30 días. Los consumidores descubren que se les ha cargado facturas a pesar de no haber pedido una prórroga en el servicio.  
6. Ventas piramidales: Consiste en ofrecer a los usuarios falsas promesas de ganar dinero de manera fácil sólo por vender determinados productos a nuevos compradores que éstos deben buscar.  
7. Viajes y vacaciones: Determinadas páginas de Internet ofrecen destinos maravillosos de vacaciones a precios de ganga, que a menudo encubren una realidad completamente diferente o inexistente.  
8. Oportunidades de negocio: Convertirse en jefe de uno mismo y ganar mucho dinero es el sueño de cualquiera. En la Red abundan las ofertas para ganar fortunas invirtiendo en una aparente oportunidad de negocio que acaba convirtiéndose en una estafa.  
9. Inversiones: Las promesas de inversiones que rápidamente se convierten en grandes beneficios no suelen cumplirse y comportan grandes riesgos para los usuarios. Como norma general, no es recomendable fiarse de las páginas que garantizan inversiones con seguridad del 100%.  
10. Productos y servicios milagro: Algunas páginas de Internet ofrecen productos y servicios que aseguran curar todo tipo de dolencias. Hay quienes ponen todas sus esperanzas en estas ofertas que normalmente están lejos de ofrecer garantías de curación.

⭐️ ¿Cuáles son las recomendaciones básicas de seguridad relativas al sistema operativo?  
Sin duda, unas de las recomendaciones básicas al hablar de seguridad, es la de usar contraseñas robustas y no repetirlas. Pero es complicado recordarlas toda.Una solución simple es usar un gestor de contraseñas.