Plaza del Mercado, 6 **45200 Illescas (Toledo)**
Teléfono: 925 51 13 96 **Fax: 925 53 20 77**

La AGENCIA ESPAÑOLA DE PROTECCIÓN de DATOS elabora un decálogo con consejos prácticos de privacidad y seguridad en dispositivos conectados

Uno de los ejes principales de actuación de la Agencia Española de Protección de Datos (AEPD) es apostar de forma decidida por la prevención para que los ciudadanos sean más conscientes de los derechos que les asisten; por tanto, la Agencia ha elaborado un listado de 10 claves imprescindibles en materia de privacidad y seguridad a tener en cuenta si te regalan o vas a regalar un dispositivo conectado.

1. Tu cuerpo dice más de lo que crees. La tecnología 'vestible' (pulseras, relojes, podómetros, etc.) incorpora sensores que registran y pueden transferir información sobre hábitos y costumbres del usuario, tanto al fabricante como a terceros. Si los utilizas para monitorizar tu actividad física, es recomendable comprobar quién está recogiendo los datos que aportas, para qué los va a utilizar y si los va a ceder a otros. Si vas a subir estos datos a una red social intenta dar la menor información personal posible al registrarte y elimina o limita el acceso a tu ubicación siempre que puedas, ya que a partir de este dato se puede inferir mucha más información sobre ti de la que imaginas.

2. Una ventana indiscreta. Buena parte de los dispositivos incorporan cámaras que aportan funcionalidades añadidas. Desconéctala o tápala con una cinta adhesiva si no la estás utilizando para evitar que un extraño pueda verte si se hace con el control del dispositivo sin que te des cuenta. Por otro lado, si te han regalado un dron, además de la normativa aeronáutica, ten en cuenta que si difundes por internet imágenes en las que se pueda identificar a las personas que aparecen en ellas, necesitarás tener su permiso o consentimiento.

3. Dispositivos vulnerables. Bloquea la pantalla de inicio y utiliza un código de desbloqueo lo más largo posible. Además, actualiza el software de tus dispositivos siempre que sea posible para evitar que sean vulnerables ante un posible hackeo y valora instalar algún programa que te proteja ante el software malicioso. Desactiva el bluetooth si no vas a utilizarlo y la conexión automática a wifis abiertas, ya que pueden ser una puerta de entrada para posible ataques.

4. Protege tus datos ante pérdidas o robos. Localiza en las opciones de configuración del terminal la forma en la que podrías acceder a distancia a su contenido para eliminarlo y piensa si te interesa utilizar una aplicación para realizar el borrado remoto. Valora si además quieres bloquear algunas aplicaciones que contengan información sensible y, en cualquier caso, realiza copias de seguridad con frecuencia.

5. Apps: no aceptes sin leer. Antes de instalar una aplicación, consulta su política de privacidad para comprobar quién va a recoger qué datos sobre ti y qué va a hacer con ellos. Valora también los comentarios de otros usuarios, ya que en ocasiones pueden aportarte información útil. Además, comprueba periódicamente las apps instaladas y qué permisos les has concedido, y elimina aquellas que ya no utilices.

6. La ubicación no siempre es necesaria. Configura tu dispositivo móvil para que las apps te pidan permiso para acceder a tu ubicación y comprueba si tus redes sociales difunden tu posición. Activa la geolocalización manualmente sólo cuando la necesites.

7. Juguetes conectados. Comprueba en primer lugar si pueden captar la voz o la imagen de los menores, entre otros datos, mientras juegan con ellos y dónde se almacenan. Revisa la política de privacidad para consultar qué permisos estás concediendo y a quién sobre esos datos. Si te piden que registres el juguete online para obtener funciones adicionales, averigua cual será el destino de la información personal facilitada y para qué se utilizará.

8. Demasiadas contraseñas. Las contraseñas deben ser robustas y es necesario utilizar una diferente para cada servicio. ¿Cómo recordarlas todas? Es recomendable utilizar un gestor de contraseñas que las almacene cifradas en el dispositivo y que, para acceder a ellas, utilices lo que se conoce como una contraseña maestra. En cualquier caso, evita tener las contraseñas almacenadas en tu correo electrónico o en un documento sin seguridad.

9. Menores: edúcales. El diálogo y la supervisión son las mejores herramientas cuando los menores entran en contacto con la tecnología. Es recomendable acordar con ellos para qué van a utilizar los dispositivos y valorar si se quieren instalar herramientas de control parental. Es aconsejable que si los padres quieren instalar un software de localización en el dispositivo para conocer la ubicación del menor, lo hablen previamente con él.

10. ¿Sabes dónde compras? Asegúrate en primer lugar de que la dirección web de la página es en la que realmente quieres comprar y, antes de facilitar tu información, comprueba quién y para qué la utilizará, revisando especialmente si la política de privacidad identifica al responsable y si muestra su domicilio social. Presta especial atención a las casillas que te piden permiso para utilizar tu información para enviarte publicidad y no las marques si no te interesa, ya que no es obligatorio. Sospecha de las páginas que ofrecen precios excesivamente bajos y si te surgen dudas busca una alternativa que te aporte más confianza y seguridad.

Se puede ampliar información sobre estos consejos, así como encontrar recomendaciones adicionales en la 'Guía de privacidad y seguridad en internet' realizada por la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad (INCIBE), que incluye 18 fichas con consejos prácticos para reducir los riesgos en un mundo hiperconectado.