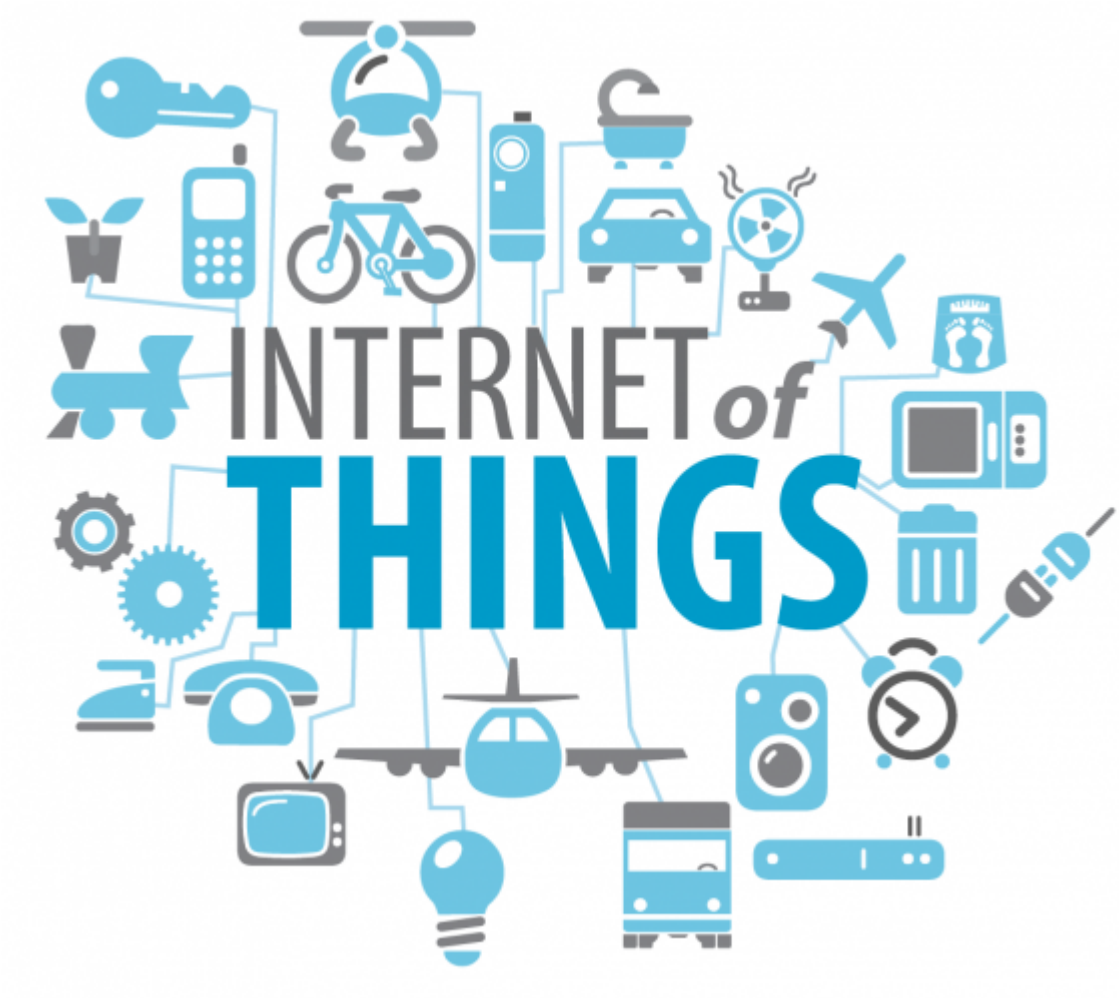
Objetos conectados muy inseguros, según ha comprobado Kaspersky

En 2015, **Kaspersky Lab analizó aleatoriamente 8 dispositivos IoT y la mitad no eran seguros**, dice su último informe, que recuerda que ahora, unos años despuñes, "la seguridad no ha mejorado" y es que su último estudio al respecto muestra que "el resultado sigue siendo idéntico". Concretamente, se cree que la mitad de los dispositivos pueden verse comprometidos debido a la falta de vigilancia del proveedor en la configuración de contraseñas.



Los dispositivos inteligentes conectados se consideran instrumentos que pueden hacer nuestras vidas más fáciles. Pero los expertos ven grandes fallas en cuanto a la seguridad. En los resultados del estudio publicados hoy, se ve que de 8 dispositivos IoT seleccionados al azar, **desde una plancha inteligente a un vehículo espía inteligente**, la mitad fueron hackeados gracias a la debilidad de las contraseñas (cargador inteligente, asistente personal doméstico, cafetera y cámara IP).

Dice el informe que "los dispositivos IOT tienen conectividad de red y están equipados con tecnología integrada que les permite interactuar entre sí o con el entorno. Debido a la gran cantidad y variedad de dispositivos disponibles, el IoT se ha convertido en un objetivo muy atractivo para los cibercriminales".

El problema de estas fallas de seguridad es que al hackear con éxito dispositivos IoT, los ciberdelincuentes pueden chantajear a las personas o espiarlas. Otros vectores puedes todavía ser

más peligrosos. Por ejemplo, l**os dispositivos domésticos pueden utilizarse para realizar actividades ilegales, o un cibercriminal que haya obtenido acceso a un dispositivo IoT podría llegar a chantajear y espiar a su propietario o extorsionarlo**.

Para su estudio, Kaspersky Lab analizó varios dispositivos inteligentes seleccionados al azar, entre los que se encontraban un cargador inteligente, un coche de juguete controlado desde una aplicación, un asistente personal (Smart home hub) – nodos que unen en un mismo lugar el intercambio de datos entre múltiples dispositivos inteligentes independientes –, una cafetera inteligente, un aspirador inteligente, una plancha inteligente, una cámara inteligente y un reloj inteligente. Los resultados han sido realmente preocupantes: **de los 8 dispositivos examinados sólo 1 llegó a satisfacer las exigencias de seguridad de los analistas**.

Además, la mitad de los dispositivos podrían verse comprometidos debido a la falta de vigilancia del proveedor en la configuración de contraseñas. Esto incluía tener una contraseña predeterminada y la imposibilidad de cambiarla, mientras que en algunos casos la contraseña incluso había sido unificada para todos los dispositivos durante su fabricación.