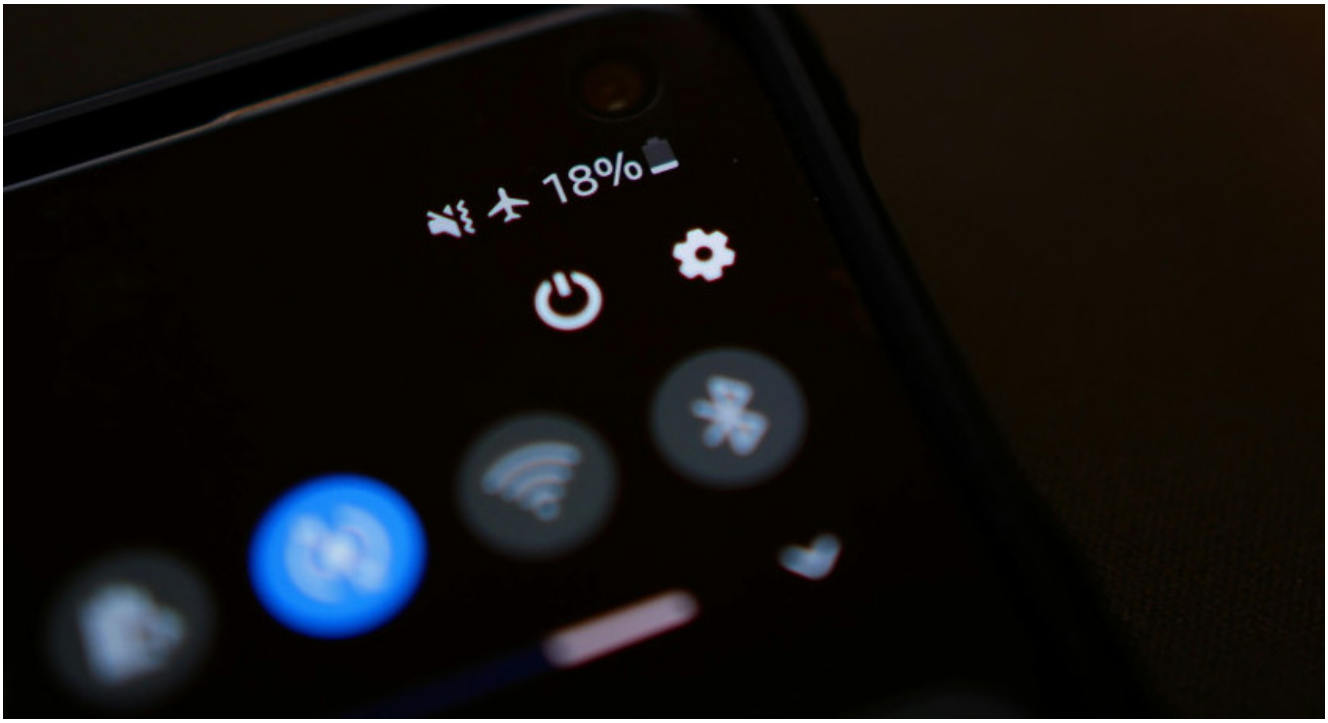
Cuidado con el «bluebugging», la nueva modalidad de robo de información a través de Bluetooth

12/10/2024



El robo de información es un delito que cada vez crece más como consecuencia de las nuevas modalidades de estafa implementadas por los ciberdelincuentes. Un ejemplo de ello es el bluebugging, una novedosa pero preocupante forma de ataque cibernético que le permite a los delincuentes acceder y controlar los dispositivos de manera no autorizada a través de la señal de Bluetooth.

Esta tecnología inalámbrica da lugar al *bluebugging*, una **técnica de hackeo que aprovecha los puntos débiles de esta función**, representando una verdadera amenaza para los teléfonos inteligentes. Esto se debe a que la nueva modalidad de robo permite que **un hacker se conecte a un dispositivo con el Bluetooth en modo abierto y así poder tomar el control**

total del dispositivo.

 *Desactivar el Bluetooth ayuda a prevenir estos delitos. Foto: Unsplash*

Dentro de las consecuencias de esta técnica de hackeo se encuentran **la escucha de llamadas y conversaciones** sin que la víctima tenga conocimiento, **el acceso a los mensajes**, ya sean de texto o los que se encuentran dentro de las apps de mensajería. Esto puede llevar a que se hagan pasar por la víctima y llevar adelante estafas virtuales, sin mencionar el **robo de datos personales e información sensible**, como fotos y contactos.

Sin embargo, la efectividad del *bluebugging* es bastante limitada, ya que **solo pueden hacerlo con dispositivos que se encuentren dentro de los 15 metros de distancia y con el Bluetooth activado**, aunque pueden ampliar el rango utilizando antenas direccionales.

 *El bluebugging es una nueva modalidad de robo de información. Fuente: Pexels.*

¿Cómo protegerse del bluebugging?

Para evitar ser víctima del *bluebugging*, se deben tomar una serie de medidas de prevención al usar la tecnología Bluetooth de los teléfonos inteligentes, como:

- **Desactivar el Bluetooth cuando no se lo esté usando:** esto evitará que se establezcan conexiones no deseadas.
- **Mantener los dispositivos actualizados:** tener instaladas las últimas actualizaciones de seguridad es de gran ayuda para proteger los dispositivos de vulnerabilidades conocidas.

Ciberseguridad. Foto: Unsplash

- **Configurar el dispositivo como «no descubrible»:** esto hará que el dispositivo no sea tan fácil de encontrar para los atacantes.
- **Desconfiar de las solicitudes de conexión desconocidas:** no se deben aceptar conexiones de dispositivos que no sean conocidas.

Esta técnica de robo de información es diferente al *bluehacking* y al *bluesnarfing*, dado que **la primera se trata de enviar mensajes no deseados a otros dispositivos** Bluetooth sin acceder a los datos, mientras que **la segunda permite que el atacante pueda descargar información** sensible del teléfono sin autorización del dueño, pero sin tener control total del dispositivo.

Fuente: Canal 26