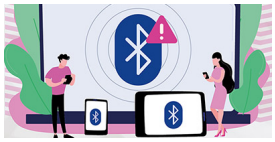

El Bluetooth es una tecnología de conexión inalámbrica ampliamente utilizada en diversos dispositivos tecnológicos y, por consiguiente, también explotada por ciberdelincuentes para llevar a cabo sus ataques.

El término “bluesnarfing" surge de la combinación de "Bluetooth" y "snarf" y se refiere a una técnica cibercriminal que implica el acceso no autorizado a dispositivos mediante tecnología Bluetooth. Aunque afecta principalmente a teléfonos móviles, también puede comprometer la seguridad de otros dispositivos como tablets, ordenadores portátiles y relojes inteligentes.

Su principal objetivo es robar información almacenada en el dispositivo vulnerado, sin conocimiento ni consentimiento de la víctima; como, por ejemplo:

- contactos
- mensajes y llamadas
- archivos multimedia
- contraseñas
- datos bancarios y/o financieros

¿Cómo ocurre?

1. Un dispositivo se encuentra con Bluetooth activo.
2. Un atacante cercano al dispositivo aprovecha vulnerabilidades de seguridad en la conexión Bluetooth.
3. Accede sin autorización y, sin ser detectado, obtiene datos almacenados en el dispositivo.
4. Copia los datos comprometidos para posibles usos ilícitos (como, por ejemplo: fraude, suplantación de identidad digital, venta ilegal.

Es fundamental tener en cuenta que:

- Cualquier dispositivo con Bluetooth puede ser vulnerable, no solo teléfonos móviles.
- El atacante debe encontrarse físicamente cerca.
- No siempre se requiere autorización para emparejamiento debido al uso de programas que permiten una conexión directa.

Bluesnarfing vs. Bluejacking
Ambos usan tecnología Bluetooth sin autorización, pero el Bluejacking se enfoca en enviar mensajes o datos no autorizados, sin acceder para robar información confidencial.

Bluesnarfing vs. Bluesniffing
El Bluesniffing se centra en la detección pasiva de dispositivos Bluetooth cercanos mientras que el Bluesnarfing es un ataque activo.

Es importante destacar que el bluesnarfing es una práctica ilegal que infringe la privacidad de las personas. La clave radica en tomar conciencia sobre los riesgos asociados a la conectividad inalámbrica y prevenir este tipo de ataque.

¿Cómo protegernos?

- Desactivar el Bluetooth cuando no se utiliza.
- Configurar adecuadamente sus opciones de seguridad.
- Ponerlo en modo "no visible"/"no detectable".
- Cambiar la contraseña predeterminada y usar claves robustas.
- Evitar conexiones con dispositivos y redes desconocidas o no confiables.
- Mantener actualizado el firmware y software de seguridad a la última versión disponible.

DUDAS O CONSULTAS
Escribir a ciberseguridad@ba-csirt.gob.ar