Los tres botones que se deben desactivar antes de salir de casa para evitar ciberataques

Muchas personas suelen salir de casa sin prestar atención a ciertos ajustes de seguridad en sus dispositivos móviles, lo que podría poner en riesgo su información personal. Especialistas en ciberseguridad advierten que mantener algunas funciones activas, como el **WiFi, el Bluetooth o el GPS**, mientras se transita por la calle o se utiliza el transporte público, aumenta considerablemente el riesgo de sufrir **ciberataques**.

Aunque acciones cotidianas como la conectividad a internet o la geolocalización parecen inofensivas, pueden dejar expuestos datos sensibles sin que el usuario lo advierta. Los expertos aseguran que malas prácticas simples, como olvidar desactivar estas funciones antes de salir, pueden resultar en filtraciones de datos bancarios, apropiación de cuentas personales, rastreo no autorizado y explotación de información en tiempo real, según refiere Infobae.

WiFi: un riesgo inadvertido en espacios públicos

La opción de mantener el WiFi activado se elige frecuentemente por conveniencia y para ahorrar en el consumo de datos. Sin embargo, los especialistas en ciberseguridad recomiendan **deshabilitar esta función antes de salir del hogar**. Los teléfonos con WiFi encendido buscan automáticamente redes públicas disponibles para conectarse sin que el usuario tenga conocimiento previo, lo que representa un riesgo significativo.

ESET, una de las principales firmas de ciberseguridad, advierte sobre los peligros de los ataques «Man in the Middle», donde **ciberdelincuentes interceptan la comunicación entre el dispositivo del usuario y una red WiFi pública**. Este tipo de ataque permite a los hackers acceder a información sensible como **contraseñas de redes sociales, cuentas bancarias, archivos personales y credenciales digitales**.

GPS: un peligro de geolocalización en espacios públicos

El botón de ubicación o GPS, utilizado a diario para aplicaciones de navegación, redes sociales y servicios meteorológicos, también representa un punto vulnerable si se mantiene activo en lugares públicos. El Instituto Nacional de

Ciberseguridad de España (Incibe) señala que, cuando el GPS está encendido, el teléfono transmite información constante sobre la ubicación del usuario, lo que puede ser interceptado por terceros.

Esta geolocalización, si es capturada por ciberdelincuentes, puede ser utilizada para **realizar ingeniería social, identificar rutinas diarias o conocer los lugares más frecuentados**. Estos datos permiten desde fraudes personalizados hasta robos de identidad, facilitando ataques dirigidos basados en patrones de comportamiento del usuario.

Bluetooth: un riesgo silencioso de conexión

El Bluetooth, que facilita la conexión de dispositivos como audífonos o computadoras, también puede convertirse en una puerta abierta a ataques cibernéticos. Mantenerlo activado permite a los ciberdelincuentes emplear técnicas como el Bluesnarfing, mediante las cuales acceden a dispositivos cercanos sin el consentimiento del usuario. Esta práctica puede derivar en el robo de archivos, la instalación de software malicioso o el envío de mensajes de spam.

Muchos usuarios desconocen estos riesgos y continúan utilizando el Bluetooth de manera permanente. Los expertos recomiendan **activarlo solo cuando sea estrictamente necesario** y apagarlo inmediatamente después de finalizar la conexión.

Estrategias de seguridad adicionales

El apagado de WiFi, GPS y Bluetooth es solo una de las medidas sugeridas por los expertos. También se destaca la importancia de mantener los dispositivos actualizados, ya que las nuevas versiones del sistema operativo incluyen parches de seguridad que corrigen vulnerabilidades conocidas. Además, se recomienda reiniciar el teléfono al menos una vez a la semana, lo que corta procesos en segundo plano y mejora la seguridad del dispositivo.

Para reforzar aún más la protección, los especialistas sugieren activar la autenticación multifactor en cuentas personales y bancarias. Esta capa adicional de seguridad reduce considerablemente el riesgo de acceso no autorizado, incluso si una contraseña es obtenida por un tercero.

Aplicar estas recomendaciones, junto con la desactivación de las funciones de conectividad antes de salir de casa, contribuye a reducir la exposición a ciberataques y refuerza la seguridad personal en el entorno digital.

Con información de VF