# Por qué no usar estaciones gratuitas de carga para celulares

11/04/2023

La sede de Denver (Estados Unidos) de la Oficina Federal de Investigaciones (**FBI**) emitió una alerta en la que recomienda no utilizar ninguna estación de **carga gratuita** para la batería de dispositivos como celulares inteligentes debido a la presencia de posibles **virus** que puedan ser instalados en estos módulos y que se difunden cada vez que un **teléfono** es conectado.

Según el comunicado de la institución de **seguridad** norteamericana, los lugares más comunes en los que se han reportado estas actividades son **aeropuertos**, hoteles y centros comerciales. Entre los virus que se pueden encontrar en este tipo de escenarios, se han hayado rastros de **programas** maliciosos de vigilancia creados por **piratas informáticos**.

El FBI indica que una forma para evitar que ser una víctima de este tipo de **ciberataques** es “llevar cargador propio,

cable **USB** y utilice una toma de corriente en su lugar”. De esta manera, el dispositivo podrá cargar directamente con electricidad en lugar de hacerlo por medio de un puerto USB que transfiere **datos**.

La información brindada por el FBI fue corroborada por la **Comisión Federal de Comunicaciones** (FCC) de Estados Unidos, que también publicó en su p**ágina web** que los malware instalados en los módulos de carga llegan ahí por medio de los puertos USB que la componen. Una vez que se ha “sembrado” el malware, solo queda esperar que se conecten los celulares para iniciar la infección. Esta práctica se conoce como “**juice jacking**”.

Los cargadores portátil solares son otra alternativa en caso de que sea necesario cargar un celular en la calle.

Con este método de ciberataque “silencioso”, los **delincuentes** buscan que los usuarios no se den cuenta que sus celulares han sido infectados con un virus que es capaz de

adquirir datos personales, así como **contraseñas**, números de tarjetas de crédito, cuentas de **banco**, perfiles de redes sociales, entre otros, que pueden usar para venderlos a otros o para realizar nuevos ataques cibernéticos usando otras modalidades como el **phishing** o el **secuestro de datos**.

Solo en caso de que sea inevitable utilizar una estación de carga que podría estar infectada, también es posible que los celulares, al menos los que tienen el sistema operativo Android, muestren un menú de opciones entre los que se puede elegir el tipo de uso que se le desea dar al puerto USB.

Las posibilidades son: “Transferir fotos”, “Transferir archivos” y “**Solo carga**”. Para evitar ser víctimas de los ciberdelincuentes se debe seleccionar esta última opción para que solo se proceda a hacer un intercambio de energía entre el módulo y el celular en lugar de un traspaso de datos que vulnera la seguridad del dispositivo,


Adaptador USB Data Blocker. (Xataka)

Por otro lado, en el caso de que aparezca un mensaje adicional en el que se pregunta si el usuario confía en el dispositivo al que se conecta el celular (en este caso el **módulo de carga**), siempre es preferible pulsar la opción “No”, pues no se sabe quiénes han podido utilizar la estación previamente o si su seguridad se ha visto comprometida.

Otra de las alternativas disponibles, aunque requiere de realizar una **inversión**, es adquirir un cargador portátil de cualquier marca y precio. De esta forma se puede garantizar

que no ha sido infectado con un virus (pues solo servirá para cargar un dispositivo o varios del mismo dueño) y también se añadirá una carga adicional de forma rápida y segura para el **celular**.

En ese sentido, los “Data Blocker” también pueden ser útiles. Son adaptadores **USB** que ofrecen una protección adicional en caso de que se decida utilizar una estación de carga gratuita en espacios públicos.

Fuente: Infobae