Ciudad de México, a 10 de agosto de 2026

BOLETÍN 31/2026

LLAMA C5 A PREVENIR EL CLICKFIX

El Centro de Comando, Control, Cómputo, Comunicaciones y Contacto Ciudadano (C5) de la Ciudad de México exhortó a la ciudadanía a conocer y prevenir el ClickFix, una técnica de fraude con sitios web falsos para engañar mediante supuestas alertas de seguridad enviadas a los dispositivos.

Los ciberdelincuentes manipulan a las personas para que copien y peguen comandos en herramientas del sistema como PowerShell, Windows Terminal o la ventana Ejecutar (Win+R). De esta forma, logran instalar un software malicioso (malware) que les permite tomar el control del equipo y acceder a datos personas o información confidencial.

“Estos ataques representan un desafío constante por el uso de técnicas más sofisticadas para acceder a dispositivos y datos personales. Para fortalecer la ciberseguridad es recomendable evitar sitios sospechosos, mantener actualizados los equipos y proteger las cuentas con contraseñas seguras y verificación en dos pasos”, destacó Salvador Guerrero Chiprés, Coordinador General del C5.

El organismo recomendó no ejecutar comandos solicitados en páginas web, evitar la descarga de archivos desconocidos y no ingresar datos personales en sitios sospechosos.

En caso de haber lanzado o ejecutado el comando se aconseja desconectar de inmediato el equipo de la red de internet, cambiar contraseñas desde otro dispositivo seguro, realizar un análisis completo con el antivirus y solicitar apoyo técnico especializado.

Para reportar fraudes, extorsiones o robo de identidad, el C5 opera 24/7 la Línea Antiextorsión 55 5533 5533, así como el 089 para denuncias anónimas.

–o0o–