Microsoft Security

5 señales reveladoras de una estafa de soporte técnico

En una estafa de soporte técnico, los delincuentes te engañan para que creas que necesitas una reparación de tu software o dispositivo. Algunos estafadores pueden intentar cobrar una cuota para "solucionar" el problema inexistente, mientras que otros intentarán robar tus datos personales o financieros o incluso intentar acceder a tu red para instalar ransomware.

No te conviertas en la siguiente víctima de una estafa de soporte técnico. Aquí tienes cinco señales reveladoras de estafas de soporte técnico, junto con información útil sobre qué hacer si eres objeto de un ataque:

1 Si te sucede esto...

Recibes una llamada inesperada de alguien que dice ser del servicio de soporte técnico (¡Cuidado! Algunos estafadores tienen herramientas para generar identificadores de autor de la llamada falsos).

Recuerda

Microsoft nunca realiza llamadas telefónicas no solicitadas. No te llamaremos para ofrecerte soporte técnico si no te pones en contacto con nosotros primero.

2 Si te sucede esto...

Recibes un mensaje de error en el que se te pide que llames a un número urgentemente.

Recuerda

Los mensajes de error de Microsoft nunca incluyen números de teléfono. El navegador Microsoft Edge bloquea sitios de estafas de soporte conocidos mediante Microsoft Defender SmartScreen.

3 Si te sucede esto...

Tu contacto de soporte técnico te pide que les pagues para solucionar tus "problemas" con criptomonedas o tarjetas regalo.

Recuerda

Los técnicos de soporte legítimos te indicarán las posibles tarifas antes de prestar el servicio. Y si se requiere un pago, nunca será con tarjetas regalo ni criptomonedas como Bitcoin.

4 Si te sucede esto...

El técnico de soporte te pide que descargues el software desde un correo electrónico o un sitio web de terceros.

Recuerda

Siempre debes poder descargar software desde un sitio web oficial o una tienda de aplicaciones. Todo el software de Microsoft se puede descargar desde nuestro sitio web oficial o los sitios web oficiales de nuestros partners.

5 Si te sucede esto...

El soporte técnico te pide una contraseña u otros datos confidenciales y privados.

Recuerda

El soporte técnico de Microsoft nunca te pide la contraseña, el número de seguridad social ni otros datos personales.

Qué hacer si crees que estás en medio de un intento de estafa de soporte técnico

- Desinstala las aplicaciones que los estafadores te hayan pedido que instales.
- Realiza un análisis completo con Windows Security para eliminar cualquier malware.
- Si has dado acceso a los estafadores a tu ordenador, reinicia tu dispositivo.
- Cambia tus contraseñas.
- Si ya has pagado, llama a tu proveedor de tarjetas de crédito lo antes posible.
- Denuncia la estafa en www.microsoft.com/reportascam.
- Informa de sitios web no seguros en Microsoft Edge en Configuración y más > Ayuda y comentarios > Notificar un sitio web no seguro.

Explora más temas de concienciación sobre ciberseguridad y oportunidades de formación en https://aka.ms/cybersecurity-awareness.

Microsoft Security