"Estaba en mi ordenador trabajando en mi tesis, al mismo tiempo que navegaba por Internet buscando información en diversas fuentes. De pronto, una ventana apareció por pantalla indicando que mi ordenador estaba infectado, que no lo apagara y que llamara al número de soporte técnico que allí aparecía.

Tras hablar con el supuesto técnico, me explicó cómo instalar un programa para que él pudiese conectarse a mi ordenador y desinfectarlo de forma remota."

¿Cómo nos afectaría?

Los ciberdelincuentes podrían pedirnos dinero por hacer una **falsa reparación** del dispositivo o, incluso, **instalarnos programas maliciosos en él** para robar información privada y **realizar acciones maliciosas o ilegales desde él.**

Recomendaciones "Buenas prácticas del cibernauta"

Restablecer el dispositivo

Si hemos concedido acceso a los estafadores, consideremos la posibilidad de restablecer el dispositivo.

Actualizaciones de seguridad

Aplicar todas las actualizaciones de seguridad en cuanto estén disponibles.

Desinstalar las Apps

Desinstalar lo antesposible las aplicaciones que los estafadores te hayan pedido instalar.

Instalar Apps originales

Instalar aplicaciones originales, solo desde las páginas webs oficiales.

Descarga Disponible Google play

Descarga Disponible App Store

Cambiar las credenciales

Cambiar las claves de acceso a nuestras aplicaciones y servicios.

Reportar el incidente

Si nos mintieron diciendo que eran el asistente oficial de un software, podremos reportarlo al proveedor original.

Llamar a nuestro Banco

Llamar a nuestro banco para cancelar los pagos al soporte técnico falso.

Enlaces relacionados

- ¿Microsoft te ha llamado sin haberlo solicitado?
- Mensajes fraudulentos, invitan llamar a un falso soporte técnico.
- Llamadas desde el falso soporte técnico.
- Servicio técnico falso, pero estafa real.