

No...¡TE PROMETO QUE NO ES MICROSOFT!



Proyecto P-
45 "Audaz"



Buenas a todos ciber-navegantes. En esta entrega me gustaría hablaros de una estafa que ataca sobre todo a particulares, especialmente a personas que no tienen conocimientos técnicos: **El timo del falso servicio técnico**,

Popularmente es mal llamado "Timo de Microsoft" (aunque la empresa se está llevando aquí unas culpas que para nada tiene! 😞)

En este timo, básicamente un supuesto empleado **de una empresa muy conocida** (*Microsoft, Apple, HP...*) entra en contacto contigo de alguna forma para **solucionarte un supuesto problema** que tienes y, a consecuencia de esto, instala programas no autorizados en tu equipo y/o te roba dinero usando diferentes tácticas.

Las variantes del timo

Pero antes de entrar en harina, tengo que decirte que **hay dos variantes principales**: la que conoce menos gente y la que sale en las noticias cada poco 😊

La variante que conoce menos gente puedes verla en esta imagen de un artículo de [ElHacker.Net](#) (que te recomiendo consultar porque te habla más en detalle de este timo)

Advertencia !!!

Tiene un virus y su unidad de disco duro se eliminará si cierra esta página.

Por favor llame con urgencia al soporte técnico de Microsoft, al número gratuito 900 649 653 para detener el proceso de borrado de datos.

[Ignorar Ahora](#) [Chatea Ahora](#)

Figura 1. Estás navegando tan tranquilamente y de repente te sale esto en tu navegador 😊. ¡Es un intento de estafa!

Tú estás navegando tranquilamente por una página web y **un anuncio en ella**, pagado por un delincuente, **te dice que tienes un virus o un problema de seguridad** muy grave. Y lo hace lanzándote un aviso como si fuera una ventana de estas que aparecen de repente, imitando el aspecto de *Windows* y con otros elementos que mejoran la credibilidad del engaño. En ese aviso

se incluye un teléfono para que seas tú el que llame al supuesto servicio técnico, no te llaman ellos. Una vez haces la llamada, **el modus operandi es el mismo que en la otra variante**.

🔍 **Sí, en esta variante no solo te roban, sino que encima tú pagas la llamada** (*¡no siempre te dan un nº 900 gratuito!*). Quizá por eso sea menos popular 😊

La variante que sale en las noticias es esa en la que te llaman a tu casa contándote la historia de que son personal técnico de Microsoft (o de quien sea), que **han detectado un virus** o un fallo de seguridad en el equipo, y que tienes que seguir unas instrucciones para librarte de él, etc.

Además, en estas llamadas el delincuente **intenta convencer por todos los medios** a la víctima de que tiene un verdadero problema, qué es necesario que lo solucione lo antes posible (la prisa para que te precipites es la gran aliada del delincuente 😞), y llega incluso a **ponerse agresivo para coaccionarle**.

🔍 **Todo lo que sea necesario con tal de que la víctima se ponga nerviosa y que haga lo que el delincuente quiere sin pensar. Por ejemplo, si les dices que no tienes ordenador lo intentan con tu teléfono o tu tablet con excusas cada vez más surrealistas...**

¿Qué pretenden realmente con esas instrucciones que te dan?

Lo que buscan es **que instales un programa**, que puede ser bien *malware* o bien uno legal, para **controlar tu equipo remotamente**. Que esto último de usar un programa legal no te extrañe, porque existen programas legítimos que le dan a alguien externo el control total de tu equipo, y que se usan principalmente para resolver problemas técnicos remotamente.

🔍 **Es decir, ¡para lo que ellos dicen qué te van a hacer!. Otra vez convierten una funcionalidad legítima (asistir a alguien en apuros tomando control de su máquina para solucionar problemas) en algo para cometer un fraude**

Además, es bastante común usar un programa legal, para que así el antivirus que puedes tener instalado no “cante” las intenciones del delincuente o bloquee el programa. Normalmente, para que el delincuente se pueda conectar a tu equipo **va a necesitar un código** que el programa que has instalado para controlar tu máquina te da, y que te aparecerá en tu pantalla. Lógicamente, te va a convencer **para que se lo des** en la llamada. En cuanto lo hagas, el delincuente tendrá el control total de tu equipo 😞.

🔍 **Hazte a la idea de que es como si lo hubieras sentado en tu silla, con tu pantalla desbloqueada y tu teclado. Por supuesto, el delincuente en ningún momento te dirá que es esto lo que va a pasar...**

¿Qué hacen una vez consiguen instalar lo que quieren?

Una vez llegados a este punto, lo que te puede pasar es muy variado:

- **Te pueden robar tus datos personales**, cuentas bancarias, claves, etc. con la intención de sacar dinero de tus cuentas o suscribirse a servicios que luego tu pagues.
 - Otra opción es **usar tus datos personales** (Ej.: robarte copias de tu DNI que tengas en tu PC) para hacerse pasar por ti y **cometer más delitos en tu nombre**.

- **Pueden robarte información y extorsionarte** con ella, porque si encuentran que hay algo, vamos a decir, “sensible” te van a pedir dinero para no publicarlo en internet...
- Otra posibilidad es que finjan el engaño hasta el final y **no hagan nada en ese momento** porque necesitarían tu intervención personal y puede levantar sospechas. El problema es que luego van a **llamarte suplantando** a tu banco, compañía de luz, gas, etc. y usarán esos datos que te han robado para hacerte creer que son ellos. En ese momento es cuando ejecutan la estafa.
- Otra opción, también tristemente popular, es que te **instalen un ransomware**, cifren todos tus archivos, y te pidan dinero por volver a recuperarlos.
- Finalmente, se ha dado el caso de variantes donde el técnico **finge arreglarle algo** y luego te pide que le hagas un pago por la factura de los servicios que te ha prestado, con lo cual el delincuente obtendrá dinero a cambio de nada.

 **En esta última, además podría “dejarte de recuerdo” cualquiera de las opciones anteriores...** 😞

¿Y qué podemos hacer?

Bueno, y después de esta “galería del terror” acerca de este timo con tantas variantes, os preguntareis **¿Qué podemos hacer si nos llaman, Redondo?** pues mirad, en realidad es sencillo: si alguien te llama diciendo que es de un soporte técnico de cualquier empresa (da igual la que sea) **cuelga inmediatamente**. Yo te prometo que ninguna empresa te va a llamar motu proprio para decirte algo así, a no ser que se lo pidas tú primero.

Si por desgracia ya has sido víctima (tú, o alguno de tus familiares que no sabe que esto puede ocurrir), el mejor consejo que te puedo dar es que **contactes con el INCIBE** (<https://www.incibe.es/linea-de-ayuda-en-ciberseguridad>), expliques tu caso y sigas los consejos que te den sus expertos.



Figura 2. El 017 es un servicio público, está para ayudarte y tiene varias formas de poder contactar con él. ¡Úsalo si lo necesitas!

 **El problema es que son tantas las cosas que pueden hacer en tu equipo y tantas variantes que no hay una receta general que puedas hacer tú mismo...**

Finalmente, me gustaría también recordarte que **existen aparatos para falsificar los números de teléfono que te llaman**. Por tanto, aunque el número de teléfono “te suene”, si te pide algo

como que instales un programa **no le hagas caso**. **Cuelga**. No te fíes del número de teléfono y, si te quedan dudas, llama tú a quien dice ser con el nº de teléfono que usas siempre.

Y recuerda, esto solo funciona si se entera la gente, así que por favor, como te digo siempre **no se te olvide contar este estafa a tus amigos, conocidos o familiares**, ya que por desgracia va por oleadas. Si transmites este mensaje, entre tú y yo conseguiremos que los delincuentes lo pasen un poco peor. **¡Que corra la voz!**

¡Y esto es todo! Muchas gracias y... ¡nos vemos en la próxima entrega!

Y recuerda amigo/a, ¡NINGUNA compañía legítima te va a llamar para ofrecerte asistencia gratuita, siempre es una estafa!



¿Quieres escuchar como hablo de esta estafa en menos de 5 minutos?



- [Escúchalo en IVOOX](#)
- [Escúchalo en Amazon Podcast](#)

¿Quieres leer alguna noticia relacionada?



- [Protéjase de las estafas del soporte técnico](#)
- [Vuelve la llamada de Microsoft, el fraude telefónico que busca acceder a nuestro ordenador \(9/10/2021\)](#)
- [Estafa del falso soporte técnico de Microsoft \(15/02/2022\)](#)
- [Atención estafa: esto es lo que tienes que hacer si recibes la llamada del último timo de moda, el de Microsoft \(11/09/2022\)](#)

Este documento usa material generado con IA²

¹ Audio emitido en "Más de Uno". 95.2 Onda Cero Oviedo (<https://www.ondacero.es/emisoras/asturias/oviedo/directo/>) el 31/10/2022

² Las imágenes del texto del documento han sido generadas con la IA Bing Chat