

Estafas telefónicas: ¡No caigas en la trampa!

Publicado el [El Informatico](#) - 8 de noviembre de 2021 -



En España tenemos una pandemia de estafadores telefónicos que nos llaman todos los días a cualquier hora del día con la única finalidad de engañarnos para que nos cambiemos de compañía telefónica sin nuestro consentimiento o incluso engañarnos para hacer que contratemos algún tipo de servicio o producto fraudulento. Que ésta práctica siga en marcha después de tantos años tiene dos factores culpables: la dejadez por parte de los políticos que imponen medidas inútiles para “frenar” ésta práctica, y por otro lado el hecho de que aún hay mucha gente que pica con éstas estafas. Si la gente no picara, estos estafadores se verían forzados a dejar de realizar ésta práctica.

En éste artículo te cuento cómo identificar rápidamente una estafa telefónica, y como evitar caer en ellas.

“Le llamo del departamento de mejora de calidad para clientes de <Compañía telefónica>”

Recibo una llamada en mi teléfono fijo. Descuelgo, pero al otro lado nadie responde. Hay un silencio, hasta que pasados unos segundos el silencio se rompe. Alguien al otro lado de la línea, responde:

-“Buenos días. ¿Hablo con <titular de la línea>?”

-“¿Con quien hablo?”

-“Mi nombre es <nombre falso> y le llamo del departamento de mejora de calidad para clientes de <compañía telefónica>. Le llamo para ofrecerle una rebaja en su factura telefónica.”

¿Departamento de “mejora de calidad”? Suena demasiado raro. Está claro que mencionan el nombre de mi compañía telefónica, pero no han mencionado que realmente pertenezcan a dicha compañía. Así que la pregunto...

-“¿A qué compañía pertenece su departamento?”

-“Le hablo del departamento de mejora de calidad para clientes de <compañía telefónica>”

Otra vez me responde lo mismo, pero evita mencionar a qué compañía pertenece ese departamento.

-“Eso ya me lo ha dicho, le estoy preguntando que a qué compañía pertenece ese departamento.”

Al preguntar otra vez, empieza a hablarme con un tono más cabreado.

-“Usted no me está entendiendo. Le estoy diciendo que le llamo desde el departamento de mejora de calidad para clientes de <compañía telefónica>”

Al ver que me estaba subiendo el tono y repitiendo otra vez lo mismo, decidí hacer yo lo mismo y subir un poco el tono, haciendo la pregunta más directa.

-“Usted es quien no me está entendiendo a mí. No le estoy preguntando a qué departamento pertenece, le estoy preguntando que a qué empresa pertenece ese departamento. ¿Para quién trabaja?”

Tan pronto subí el tono, la mujer se dio por vencido y, con un tono más deprimido, decidió decir la verdad.

-“MásMóvil”

Evidentemente no pertenecía a mi compañía telefónica, sino que llamaba evitando mencionar a MásMóvil y forzando de alguna manera el nombre de mi compañía telefónica para intentar ganarse mi confianza. Algo que evidentemente no “coló”. La idea es la de ofrecerte una “rebaja” en tu factura telefónica que se traduce en un cambio de compañía, engañándote para que les des tu falso consentimiento.

Un abuso de un vacío legal y de la dejadez de nuestros políticos

El tipo de prácticas mencionado en mi caso no es totalmente ilegal, es un “vacío legal” donde la empresa queda impune siempre y cuando la víctima de su consentimiento expreso. Ésto se traduce a responder “Sí” a una serie de preguntas que el estafador te hará durante la llamada, así como facilitarle tus datos. Evidentemente el estafador te hará creer que te están ofreciendo una rebaja en tu factura, pero no es así. Lo que te estará ofreciendo es, en realidad, un cambio de compañía. Lo que además puede incurrir en costes adicionales si estás bajo un contrato.

En ocasiones los estafadores realizarán las llamadas desde otro país ajeno. Aunque la policía puede detectar el origen de las llamadas sin problemas, en la mayoría de los casos requiere de acciones coordinadas con la policía del país de origen de la llamada, que puede resultar muy complicado dependiendo de las leyes y de la forma en la que actúe la justicia del lugar (Si la hay). A veces pueden llamar de forma directa, pero muchas veces llaman a través de otro número de teléfono que pertenezca al país de destino, motivo por el cuál hay una pequeña demora en la línea (ese silencio que detallé en mi ejemplo), o incluso que no haya conexión (descuelgas y nadie responde hasta que se corta la llamada).

Bloquear el número de teléfono no es efectivo, pues los estafadores utilizan múltiples líneas telefónicas para evitar que puedas bloquearles la llamada. Por éste mismo motivo, aunque las compañías telefónicas bloqueen una línea determinada, los estafadores podrán saltarse el bloqueo usando otra línea.

Si tu número de teléfono está registrado en la denominada Lista Robinson, sólo podrán llamarte empresas a las que les hayas dado tu consentimiento expreso para llamarte. Esta lista es una lista telefónica que indica que los números registrados **no deben recibir llamadas de ninguna empresa que no tenga una relación con los dueños de éstos números de teléfono**. Es decir, que si una empresa como MásMóvil te llama a tu teléfono sin tú tener ningún servicio suyo contratado con ellos (o que no tenga tu consentimiento), y tu número de teléfono está registrada en ésta lista, **tienes derecho a denunciar a la empresa**.

La Lista Robinson es gratuita, e inscribirse es muy sencillo. Sólo tienes que facilitar tu nombre, número de teléfono asociado y tu correo. Pero como todo, que te dejen en paz no va a ser tan sencillo. Muchas empresas intentarán ganarse tu consentimiento para seguir llamándote o mandándote publicidad sin que te enteres, muchos estafadores recurren a otras estrategias para aprovecharse de vacíos legales, y por otro lado **muy poca gente denuncia**. Hay empresas que incluso se pasan éstas normas por el forro y se toman las multas como si fuesen un pago por la publicidad.

No sólo empresas, incluso me han llamado de partidos políticos durante la pasada campaña electoral con mensajes grabados estando mi número en esa lista.

Los estafadores y sus tácticas

Las llamadas para ofrecerte falsas “rebajas” (o **a veces también vienen a avisarte de una falsa “subida” o “modificación” en tu próxima factura, bajo el falso pretexto de pertenecer al área de facturación de tu actual compañía**), ya sea de compañías de teléfono, luz, gas, seguros, etc, son las más comunes. Pero lamentablemente, no son las únicas.

En ocasiones puedes recibir una llamada de un técnico en “ciberseguridad” (o seguridad informática o similar) **de Microsoft, o incluso de Windows, para avisarte de que tienes tu “línea” infectada por un virus**. Algo que cualquiera que entienda un mínimo va a identificar como un engaño de manera inmediata, pero que a la persona que no tiene ni idea de informática podría tomárselo como una amenaza muy seria. **Todo con la finalidad de ofrecerte un falso servicio de reparación por un “módico” precio**. Normalmente **éste servicio lo prestan a través de TeamViewer o algún servicio similar**. Evidentemente debes desconfiar de cualquiera que te diga que te llama de una compañía informática, ya que en el supuesto caso de que pudieras tener un malware que afectara de algún modo al tráfico saliente de tu red, sería tu propio ISP (compañía telefónica) quien te avisara, normalmente por correo electrónico. En cualquier caso, eso es algo muy raro.

Otras tácticas que usan es la de **hacerse pasar por tu banco** con la finalidad de, evidentemente, sacarte tu dinero. Generalmente **te avisaran de un fraude o similar en tu cuenta bancaria y te pedirán que realices una serie de acciones para subsanar el problema, bajo la amenaza de que si no lo haces podría incurrir en sanciones económicas o incluso penales**. Lo normal es que te pidan que entres en algún tipo de portal bancario falso y que desde ahí realices dichas acciones.

Si recibes alguna llamada de éste tipo, diles que **hablarás tú mismo con la compañía**. Cuelga, y si dudas de que pudiera haber algún problema con tu cuenta, **llama al servicio de atención al cliente de tu banco**. O incluso acude en persona a cualquiera de sus oficinas para tratar el tema.

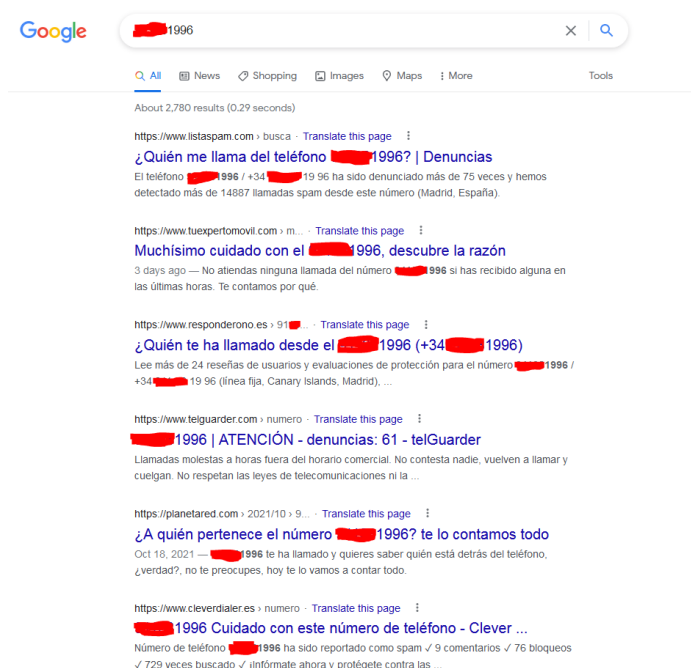
Similar a ésta táctica, **los estafadores podrían hacerse pasar por el ministerio de Hacienda o de la Seguridad Social para avisarte de algún impago o fraude en tu declaración de la renta o similar**. **Desconfía siempre de cualquier llamada o mensaje de éste tipo**, normalmente suelen mandarte una carta por correo certificado si tienes algún problema de verdad.

Cómo evitar éstas estafas

- Si recibes una llamada y tienes la certeza de que se trata de un fraude, **cuelga**

inmediatamente. A los estafadores les da absolutamente igual lo que les digas, es perder el tiempo y por mucho que les digas palabras “bonitas” no van a dejar de molestarte.

- Si no sabes exactamente de qué trata la llamada y quieres cerciorarte de que la llamada sea legítima o no, **pide siempre primero a quien esté al otro lado de la línea que se identifique con el nombre de la empresa para la que trabaja**, asumiendo que no lo haga al iniciar la conversación.
- Si el interlocutor no sabe con quien está hablando, o no conoce detalles que debería de conocer acerca de ti, **desconfía de forma inmediata y cuelga**. Por ejemplo, si preguntan por “el titular de la línea” sin mencionar tu nombre.
- **Nunca y bajo ningún concepto le des información personal o de tus contratos a la otra parte.** Ni tu nombre, ni tu relación con cualquier compañía que te mencionen (tengas o no tratos con dicha empresa), ni nada que les pueda dar ninguna información acerca de ti. Cuanto menos sepan de ti, mejor.
- **Evita responder con “Sí” o “No” a las preguntas que te hagan hasta que estés 100% seguro de que la llamada sea de alguien de confianza.** Si aún no estás seguro, diles que llamas tú a la empresa (Atención al cliente o a quien corresponda), cuelga y ponte en contacto tú mismo con la empresa.
- Si puedes, **graba todas las llamadas**. En el caso de que tengas que emprender acciones legales te ahorrarás un dolor de cabeza. Eso sí, si lo haces, **avisa al principio de la conversación de que estás grabando**. Lo normal es que cuelguen directamente cuando se lo digas.
- Si buscas el número de teléfono en Google, puedes identificar si se trata de una estafa o publicidad si el número aparece denunciado múltiples veces en las listas de spam. Si te llaman al fijo y tu teléfono lo soporta, puedes activar la detección de llamadas para saber quién te llama. Si tienes fibra óptica, algunos routers te pueden mostrar el registro de llamadas al fijo.



Búsqueda en Google de un número de teléfono usado para hacer publicidad



ANTERIOR

Jueves de buenas noticias

SIGUIENTE

El Metaverso: Nada nuevo en el horizonte

Buscar ...



Entradas Recientes

- [El Metaverso: Nada nuevo en el horizonte](#)
- [Estafas telefónicas: ¡No caigas en la trampa!](#)
- [Jueves de buenas noticias](#)
- [Facebook, una vez más, en problemas. Y es su propia culpa.](#)
- [Si usas Twitch, cambia tu contraseña de inmediato](#)
- [Diferencias entre Internet y La Web. ¿Qué es cada uno?](#)

Categorías

[Actualidad](#)[Android](#)[Básicos](#)[Ciberseguridad](#)[Criptografía](#)[Emulación / Virtualización](#)[FOSS](#)[Hacking](#)[Informática](#)[Internet](#)[Juegos](#)[Opinion](#)[Otros](#)[Personal](#)[Privacidad](#)[Programación](#)[Tecnología](#)[Time Machine](#)[Tutoriales](#)

RSS

[Suscribirse al feed RSS](#)

Inicio
Catálogo
Tutoriales
Política de privacidad
Política de Cookies
Acerca de mi
Acerca de ElInformati.co