# tellows

# II Magazine Oficial

## ¿Estás cansado de llamadas dudosas y molestas?

Cada vez más los consumidores son víctimas de spam o fraudes telefónicos, o simplemente son provocados frecuentemente por llamadas no deseadas. Los estafadores usan varios trucos para sacar dinero de nuestros bolsillos. ¡Con esta revista, ya no serás víctima de tales trucos!

## Tipos de estafa Visión General

Información sobre cómo funciona la estafa, informes basados en la experiencia real y consejos sobre cómo protegerse de la estafa.

## Legal Básico

Información acerca del marco legal actual sobre fraude telefónico y las autoridades y reguladores involucrados.

## Solución

Métodos de protección en la lucha contra las llamadas molestas y el fraude telefónico.

## Más...

Estadística, Experiencia de usuarios, información sobre como aprendieron los estafadores tu número de teléfono,
¡y mucho más!

# Indice

## 1. En portada



## 2. ¿Por qué recibo estas llamadas?



## 3. ¿Qué tipo de fraudes existen?



## 4. Información legal



## 5. ¿Cómo puedo protegerme?



## 6. Imprenta

# ¿Qué es tellows magazine?

Todos hemos tenido que lidiar con ello alguna vez. Tu teléfono suena de forma descontrolada, bombardeado con llamadas molestas y no hay manera de saber quién está llamando. ¿Como demonios se puede saber con certeza la fiabilidad de un número cuando no lo tienes registrado?. La verdad es que puede haber un buen número de posibilidades; Será un vendedor de tele marketing o, aún peor, un contestador automático por tonos? ¿O simplemente un@ conocid@ con un nuevo número? En ese caso, ¿Deberías responder a la llamada o ignorarla?


En respuesta a este problema universal, tellows.es funciona como una base de datos online de números de teléfono asociados con actividades fraudulentas como spam y scam. Proporcionamos una plataforma en línea donde los usuarios pueden compartir sus experiencias con llamadas fraudulentas y alertar números responsables de llamadas no deseadas.

Por su parte, el tellows magazine tiene como objetivo principal concienciar a los consumidores sobre este tema y protegerlos sobre posibles casos de llamadas molestas y/o fraudulentas. Informaciones recientes por parte de los consumidores sirven de ejemplo para saber cómo tellows funciona en más de 50 países con más de 75.000 números de teléfono en su base de datos a nivel mundial. Por otra parte, y como muchos consumidores no están familiarizados con sus derechos y protección legal ante casos de abuso y fraude, el magazine de tellows proporciona una rápida perspectiva del marco legal y agencias tanto públicas y privadas que tratan con este tipo de denuncias. La aplicación de tellows para tu smartphone, que te ayudará a lidiar con las llamadas molestas, también será presentada en este magazine.

¡El equipo tellows te ayuda a luchar contra el acoso telefónico y las llamadas fraudulentas!

# Las estadísticas dicen...

1. La preocupación por la seguridad aumenta

La seguridad en telefonía móvil, así como la magnitud del las consecuencias de fraude a través de estos dispositivos, es creciente. Si bien disponemos de datos de la industria de telefonía móvil exclusivamente, éstos sirven de referencia para ver que, efectivamente, los fraudes también se hacen un lugar en estos dispositivos. No obstante, se encuentran con un usuario más precavido, informado y preparado.

Según el informe digital sobre Internet y redes sociales en el mundo 2018 de Hootsuite, la plataforma de administración de redes sociales, en el caso de España el uso de la telefonía móvil se ha incrementado en un 5%, teniendo en cuenta que un 96% de ciudadanos tiene un teléfono móvil y de ellos, un 87% son smartphones. Además, 35,8 millones de usuarios se conectan a Internet mediante su teléfono móvil.

Gráfico 1: Usuarios que disponen de teléfono móvil


Fuente: Hootsuite

Por otro lado, según datos del Instituto Nacional de Ciberseguridad (INCIBE), sólo en 2017, España registró más de 123.000 ataques cibernéticos, un 7% más que en 2016, el cual es una cifra récord que cada año va en aumento, si se tiene en cuenta que en 2014 fueron 18.000. La mayoría de estos ataques (116.642) han afectado principalmente a empresas y ciudadanos. Hasta mediados de 2018, el INCIBE ha respondido a más de 13.300 incidentes cibernéticos y ha explicado que los ciberataques se están incrementando especialmente por el aumento de dispositivos móviles conectados a internet y por la expansión del cibercrimen, que genera grandes beneficios a sus autores.

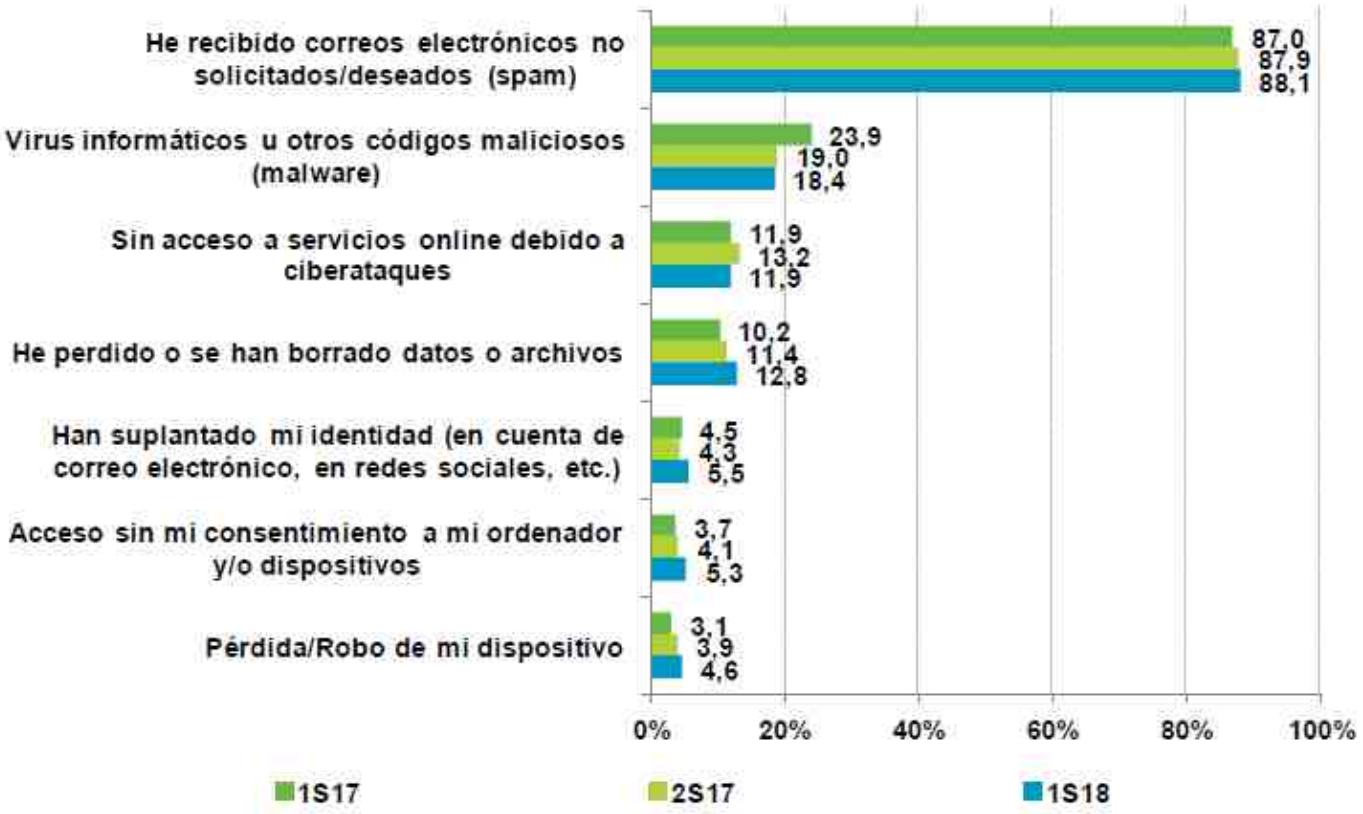
# Las estadísticas dicen...

Las principales tipologías de ciberataques o incidentes se corresponden con las infecciones por códigos informáticos maliciosos o "malware", intentos de intrusión o accesos no autorizados a redes y sistemas, fraude electrónico, uso de correo spam malicioso u otros ataques relacionados con las denegaciones de servicio publicados en Internet.

La banca española es uno de los sectores más amenazados por los fraudes de suplantación de identidad, una práctica conocida como "phishing" y con la que los ciberatacantes pretenden robar datos personales de los clientes. Esta estafa consiste en el envío de miles de "emails", aunque también se producen por mensajes y llamadas telefónicas, que redirigen al destinatario a una web engañosa, con la imagen e incluso el dominio de la entidad, para que introduzca los datos y las claves personales de su cuenta bancaria.

Según el informe del "Estudio sobre la Ciberseguridad y Confianza de los hogares españoles", elaborado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de Red.es en cooperación con INCIBE, las mayores incidencias de seguridad percibidas por los españoles son las campañas de spam ocupando el primer lugar (88,1% de las declaraciones), seguido por las incidencias de virus y malware.

GRÁFICO 2: EVOLUCIÓN DE LA CLASIFICACIÓN DE LAS INCIDENCIAS DE SEGURIDAD (%)

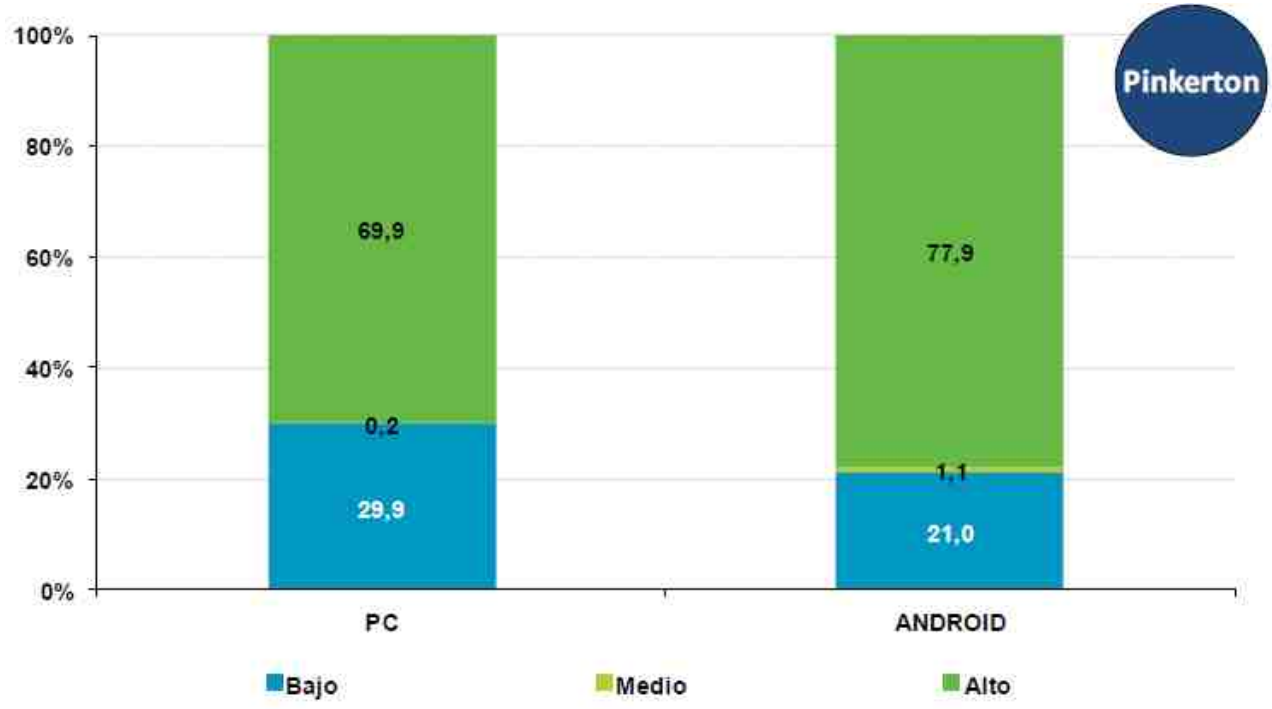



*Base: usuarios que han sufrido alguna incidencia de seguridad*
*Fuente: Panel hogares, ONTSI*

# Las estadísticas dicen...

Además, casi el 70% de los ordenadores y el 78% de los dispositivos Android infectados con malware se encuentran en un nivel de riesgo alto, lo cual incrementa la probabilidad de que los incidentes de seguridad relacionados con malware logren sus objetivos y tengan consecuencias negativas para los usuarios, tales como robo de información, impacto económico, pérdida de datos, etc.

GRÁFICO 3: NIVEL DE RIESGO EN EL ORDENADOR DEL HOGAR Y EN DISPOSITIVOS ANDROID (%)



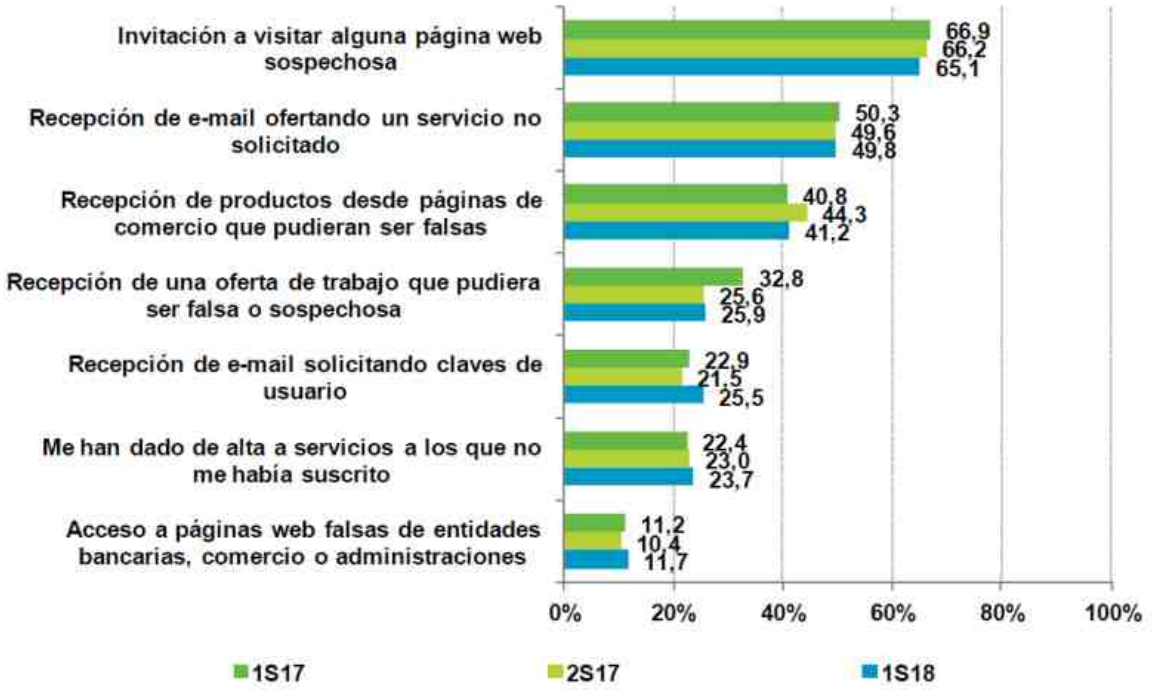

*Base: PCs y dispositivos Android que alojan malware*
*Fuente: Panel hogares, ONTSI*

De este modo hay evidencia que las invitaciones a visitar alguna página web sospechosa (65,1%) continúan constituyendo el tipo de manifestación de fraude online más frecuentemente acontecido. La recepción de e-mails ofertando servicios no solicitados (49,8%) es la segunda forma más común. Prácticamente todos estos tipos de fraude online son enviados al usuario a través de correo electrónico no solicitado o spam (GRAFICO 2), o de las redes sociales.

También resulta habitual que los fraudes online se presenten ante el usuario simulando ser inocuas encuestas o concursos que, suplantando la identidad de alguna entidad o marca bien conocida, ofrecen premios, cupones descuento, cheques regalo, o cualquier otro tipo de gancho para lograr que un usuario incauto proporcione información personal y, sin percatarse, acepte recibir promociones, servicios no solicitados y publicidad no deseada (nuevamente spam), el alta en servicios de SMS Premium, instalar algún tipo de programa o aplicación no segura –y potencialmente maliciosa–, etc.

# Las estadísticas dicen...

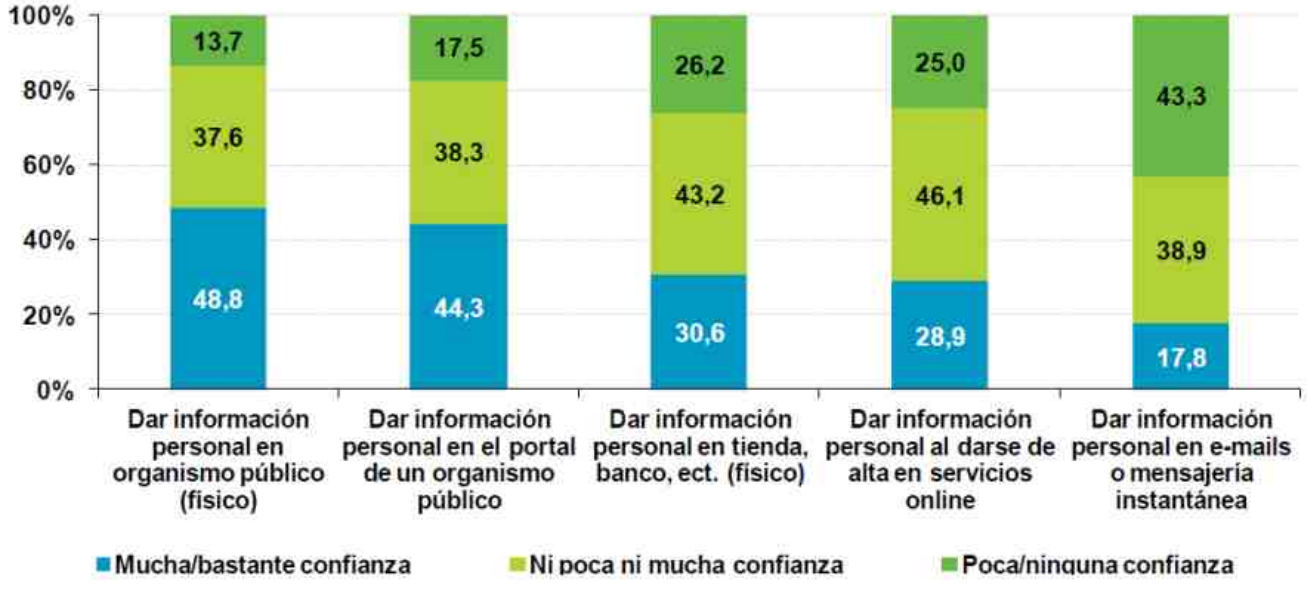
GRÁFICO 4: EVOLUCIÓN DE LA MANIFESTACIÓN DE LOS INTENTOS DE FRAUDE ONLINE (%)




*Base: Usuarios que han sufrido un intento de fraude*
*Fuente: Panel hogares, ONTSI*

Son numerosas las campañas de scam, phishing o cualquier otro tipo de fraude que intente recopilar información personal y/o privada del receptor, sin embargo se observa un importante rechazo por parte de un 43,3% de los internautas españoles que desconfían ante solicitudes de información personal o privada a través del correo electrónico o mensajería instantánea.Sin embargo, este rechazo disminuye hasta un 25% en el caso de que dicha información se solicite durante el registro o alta de un servicio web. Es importante puntualizar que muchos de los scam o fraudes comentados anteriormente se pueden presentar en forma de –falsa– promoción de alta en un servicio online con el único objetivo de obtener la información del usuario.

GRÁFICO 5: NIVEL DE CONFIANZA EN FACILITAR DATOS PERSONALES (%)

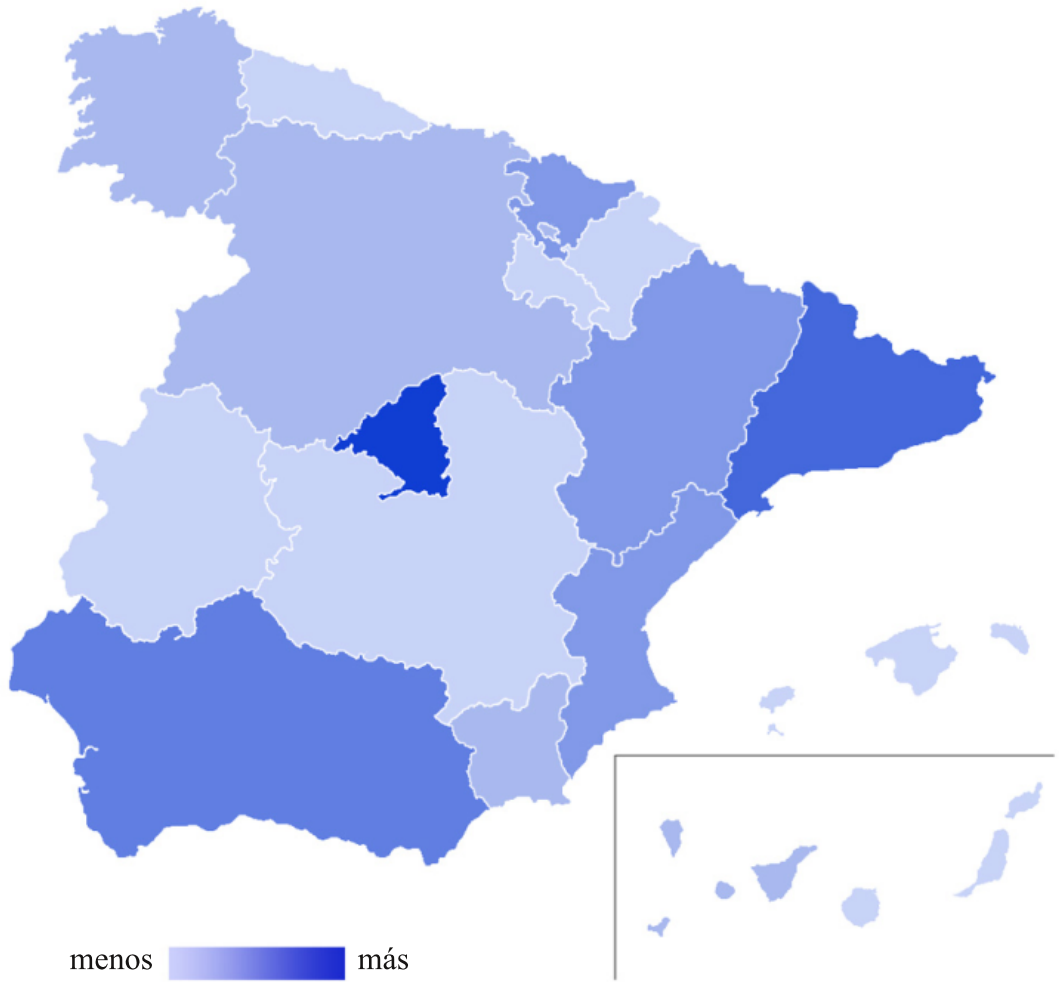



*Base: total usuarios*
*Fuente: Panel hogares, ONTSI*

# ¿Quién es el más perjudicado en España?

El presente mapa destaca las provincias más perjudicadas por las llamadas de tipo scam y spam.

Frecuencia de búsquedas de números por Comunidad Autónoma




Fuente: elaboración propia

En base a los datos facilitados en el 2018 por la web principal de tellows España, se aprecia claramente que las regiones que sufren mayor concentración de llamadas molestas corresponden a Madrid y Cataluña. Siguen, Andalucía, País Vasco, Aragón y Valencia. El resto de Comunidades Autónomas parecen tener un muy ligero o cuasi inexistente índice de búsquedas.

# ¿Cómo saben mi número?

Muy a menudo nos preguntamos de donde obtuvo nuestra información la persona que llama. Aquí ponemos algunos comentarios de ejemplo:

| | | |
|---|---|---|
| *(Estefanía): ¡Me gustaría saber de donde sacaron mi número de teléfono si no está en el directorio telefónico!* | *(Juan): ¿Cómo es que sabían mi número? ¿Es que hay algún proveedor de servicios telefónicos que vende nuestros contactos?* | *(Carla): ¿Qué quieren de mi? ¡Sólo di mi número de teléfono a unos pocos contactos!* |

*Comentarios directos de los usuarios de tellows*

Los principales recursos de los que disponen los defraudadores son, en primer lugar, las páginas amarillas y directorios de búsqueda directa. También intentan elegir nombres antiguos para poder cerciorarse de que los objetivos a los que intentan estafar tienen una cierta edad y sin acceso a la red. Aunque parezca mentira, los números de teléfonos en los periódicos oficiales también son objeto de abuso. Disfrazados de falsas “recompensas por fidelidad”, los defraudadores engañan con aparentes ofertas de todo tipo.

Por otra parte, las apuestas o loterías son otra modalidad popular de fraude. Los participantes son engañados con falsas probabilidades de dinero fácil a cambio de sus datos. Algunos call-centers intentan diferentes técnicas y combinaciones llamando aleatoriamente, igual que con el envío automático de SMS o mensajería instantánea.

En la era de Internet, es aún más fácil espiar y obtener información de direcciones, números de teléfono o información confidenciales como contraseñas personales. Por la red también circulan programas capaces de rastrear estos directorios o anuncios clasificados. Con este panorama, las redes sociales no son sino una plataforma adicional para los defraudadores.

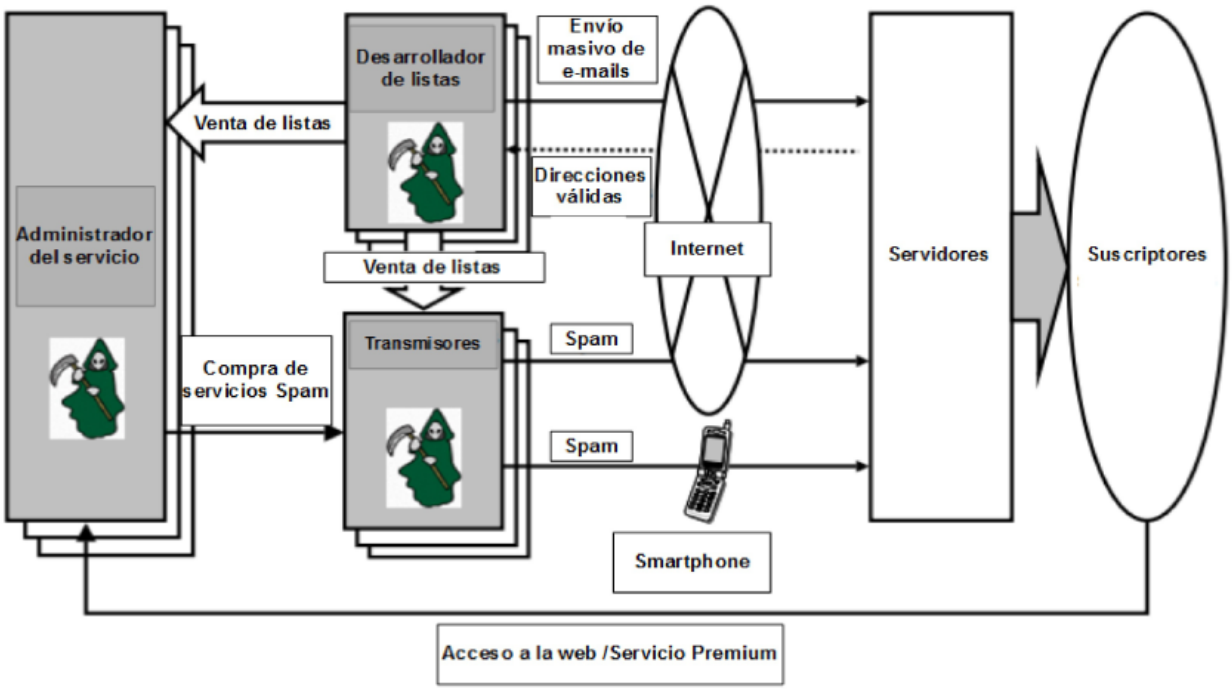
# La venta de bases de datos

Uno de los mayores problemas en el negocio del fraude es sin duda la compra-venta de bases de datos. Muchas compañías basan un gran volumen de sus beneficios en el negocio que deriva directamente de la recolección, venta y reventa de bases de datos, con un precio mayor contra más detalladas son.

Como ejemplo práctico, podríamos mencionar casos de usuarios que han pedido presupuesto para contratar una nueva póliza de seguros a través de Internet, proporcionando su número particular de teléfono, y a los pocos días han sido contactados de forma masiva por vendedores de pólizas de seguros.

Sumado a todos estos factores, y dada la gran variedad de posibilidades disponibles para las compañías para adquirir y vender datos de personas y empresas, es sumamente difícil prevenir totalmente las llamadas molestas. Debes ser muy cauteloso al proporcionar tus datos a suscripciones de Internet, newsletters, concursos y/o promociones online. A modo de referencia, el siguiente esquema muestra como funcionan estas empresas que actúan al límite y muchas veces al margen de la ley.

Funcionamiento de la industria de la compra-venta de bases de datos




Fuente: International Telecommunication Union (ITU)

# 2. ¿Por qué recibo estas llamadas?

A través de diferentes técnicas de captación de los datos, los desarrolladores de listas se encargan de recolectar información, que es vendida tanto a transmisores como administradores del propio servicio fraudulento. Los administradores compran/alquilan servicios Spam a los transmisores, que muchas veces son también víctimas colaterales de las acciones fraudulentas (por ejemplo individuales que buscan trabajo a distancia y flexible). A menudo el transmisor no es conocedor del mecanismo del fraude y en ocasiones no recibe pago alguno por sus servicios. Los servidores, a su vez, normalmente proveedores de telefonía, muchas veces no pueden controlar este tipo de estafas y se limitan a crear foros en Internet de ayuda, o bien informar en caso de que reciban alguna llamada peguntando por un número en concreto. Finalmente, una vez el usuario se convierte en suscriptor, la tarifa por el servicio es cargada y pasa a ser fuente esencial de ingresos del administrador para recuperar la inversión realizada.

Para más información, puedes ver artículo publicado en nuestro blog “Trampas al teléfono: Cuando presionar un botón te conlleva costos”.

Por último, nos gustaría aclarar que con el esquema presentado, no queremos generalizar incluyendo a las empresas que, de forma legal y profesional, se dedican a la recolección de datos para campañas de tele márqueting, ya sean éstas por teléfono, mensajería instantánea o cualquier otro medio. El objetivo del mismo es, como la mayoría del contenido de este magazine, informar al usuario de los riesgos que existen y el coste de proporcionar datos de carácter personal a terceros.

# La Comunidad de tellows habla...

Si preguntas a la persona que llama dónde y cómo encontró la información de tu número de teléfono, te encontrarás ante un caso claro de spam si la contestación se parece a una de la siguientes...

*(Antonia)*
*Pregunté como obtuvo mi información – su respuesta es; "en un directorio telefónico". ¿En serio, no me digas?*

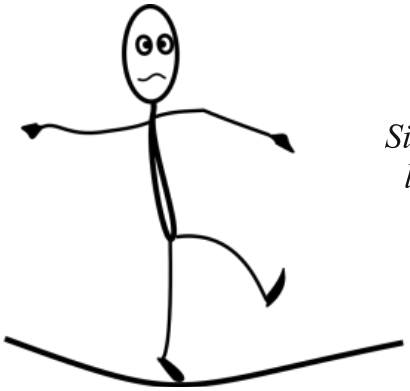
*(María)*
*¡¿No es esto denunciable?! ¡¿No va y me dice que su política de privacidad y secreto profesional le impide decirme de dónde ha sacado mis datos?!¡¿Es que somos tontos o qué?!*

*(Yolanda)*
*Pregunté a la operadora como había obtenido el número y cómo puede ser que yo estuviese e sus sistema. Me contestó que no podía decírmelo con exactitud?!!*

*(Jacob)*
*Al preguntarle cómo había obtenido mi número, tartamudeo diciendo que "nosotros tenemos nuestra propia base de datos". En ese momento colgué directamente.*

*(Carlos)*
*Se puso muy desagradable y defensivo al yo preguntarle cómo obtuvo mi número de teléfono y nombre...*

*(Lobezno)*
*He preguntado como han obtenido mi número y al respuesta ha sido que mi número ha sido generado aleatoriamente por un ordenador.. claro.*



*(Mario)*
*Simplemente me derivaron a otra línea cuando pregunté por mis datos, y seguido a eso me colgaron.*

*Comentarios directos de los usuarios de tellows*

**www.tellows.es/stats**

En la sección de estadísticas de la página de tellows de España, encontrarás un mapa que muestra la localización que ha estado utilizando el portal de tellows durante las últimas 24 horas. Es un mapa térmico que muestra el origen de las búsquedas.

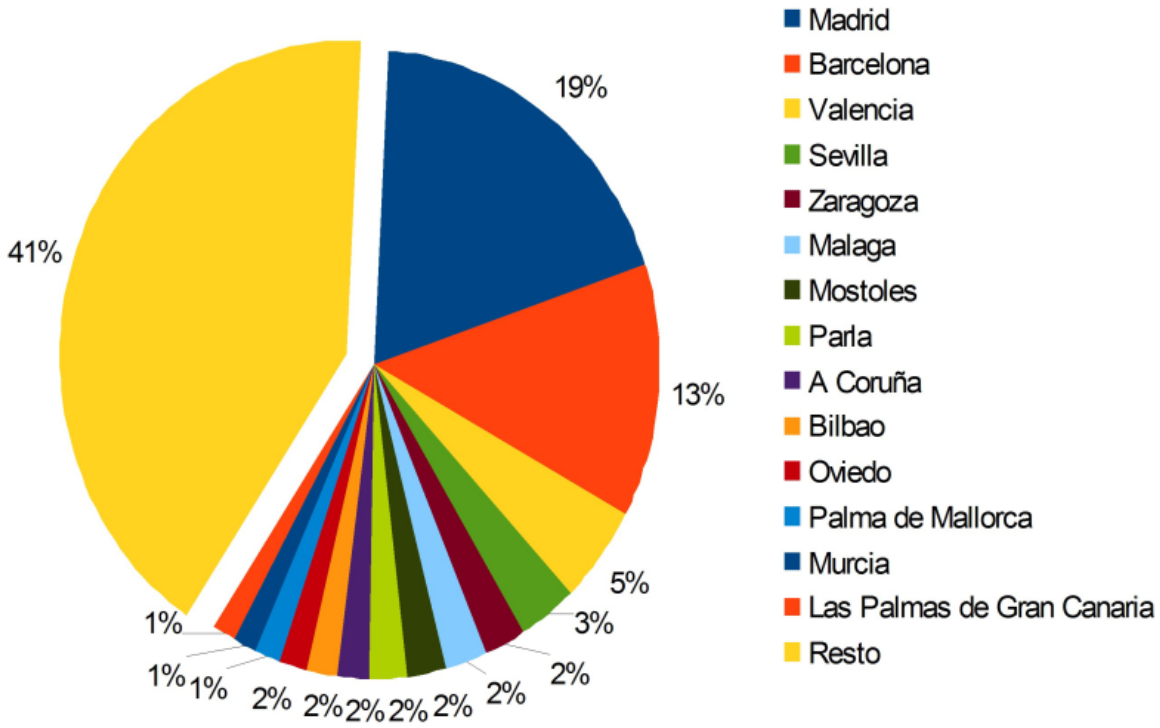
La página también incluye los comentarios más recientes (últimos 5 días), aquellos números que se han clasificado como fiables y peligrosos, así como los nuevos números añadidos en la base de datos de tellows.

# ¿De dónde vienen exactamente?

Nuestra comunidad (y los usuarios, en general) normalmente no tiene idea alguna del origen de las llamadas molestas, ni tampoco muy claro quién es exactamente la compañía o personas detrás del teléfono. A través de la base de datos de tellows, te proporcionamos una serie de gráficos que muestran, por un lado, de qué ciudad provienen las búsquedas en nuestra base de datos. De esta manera, podemos analizar qué regiones son las más afectadas y objetivo de llamadas fraudulentas o no deseadas con mayor frecuencia. Más adelante te ofrecemos una clasificación temporal comparando las cinco ciudades con mayor número de búsquedas, viendo una gráfica evolutiva anual.

Número total de búsquedas clasificadas por región, expresadas en porcentaje:

Gráfico 6: Ciudades con mayor número de búsquedas

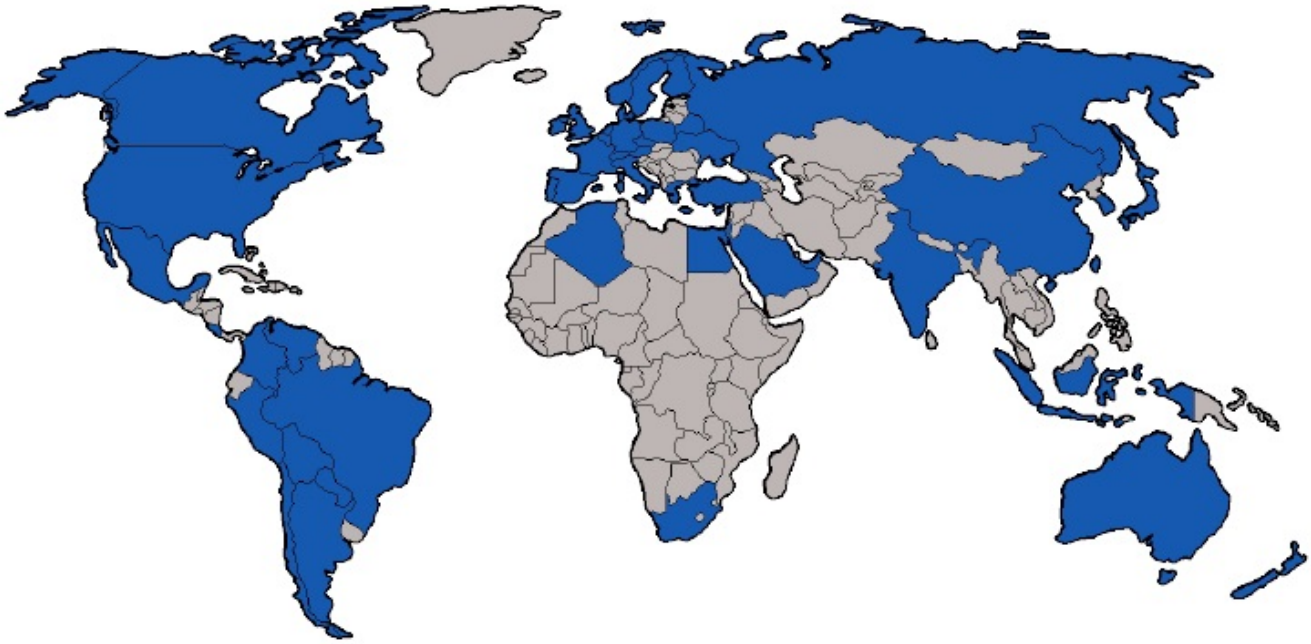



Tamaño de la muestra, n=103.425
Fuente: elaboración propia

Los datos presentes en el gráfico muestran que tanto Madrid como Barcelona encabezan el listado por número de búsquedas en los servidores de tellows. Le siguen de lejos Valencia y Sevilla. En un tercer grupo podríamos colocar al conjunto de ciudades que representan tan solo un uno o dos por ciento residual, mientras que el resto de búsquedas se reparten entre el resto de puntos de nuestra geografía.

Además de España, tellows también cuenta con una base de números de varios países. El siguiente mapa muestra dónde está presente tellows según los países marcados en azul.

Países con servicio de búsqueda inversa de tellows



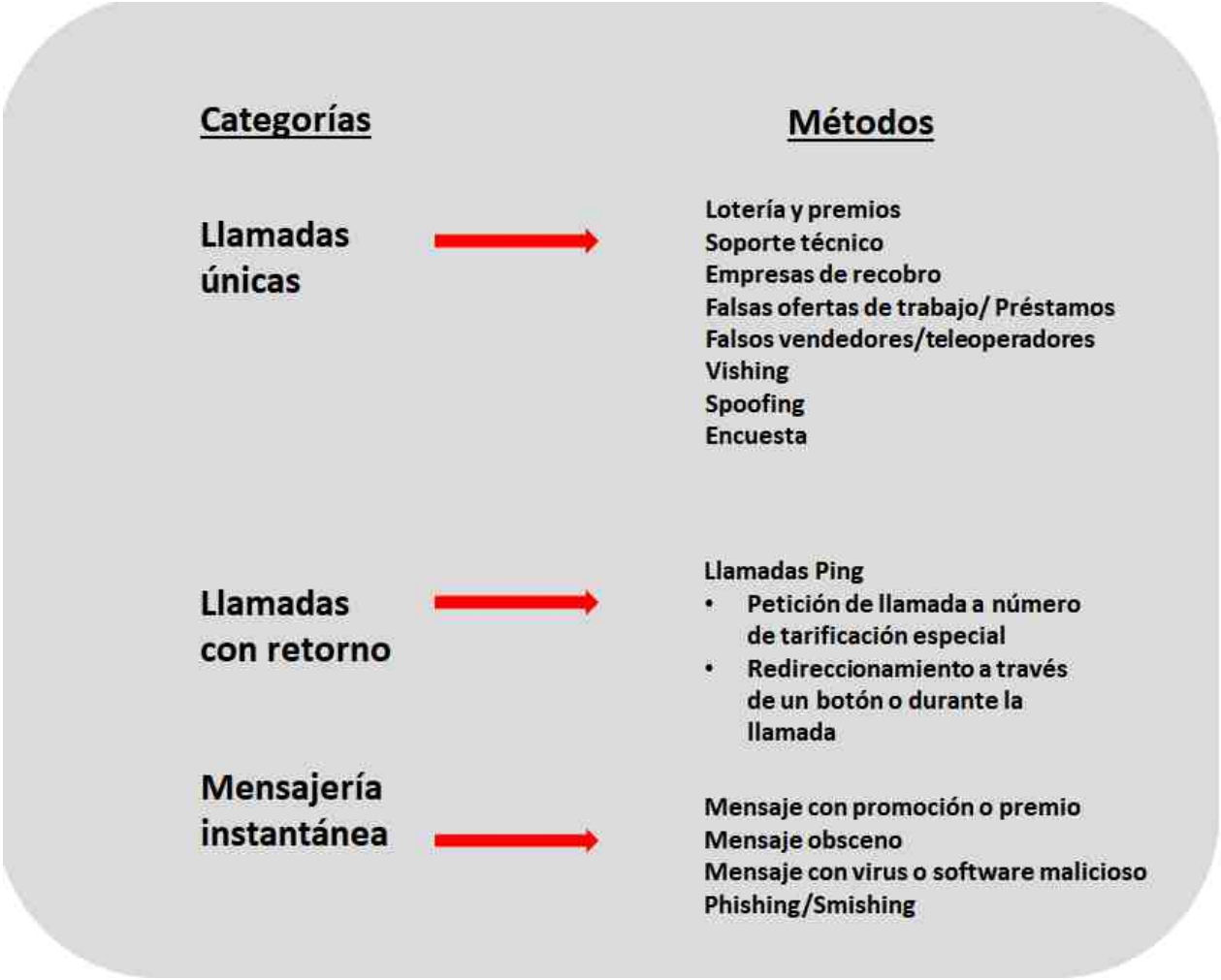
Fuente: elaboración propia

# En conjunto

La mejor protección contra las llamadas de tipo spam/scam es tener conocimiento del método. Los métodos de fraude a través del teléfono tienen un origen muy diverso. Los estafadores utilizan ingeniosas y creativas técnicas para sorprender a sus victimas con diversas tácticas. Algunos trucos de la vieja escuela son actualizados con las nuevas tecnologías. Algunos están incluso sobre explotados, pero nunca se cansan de encontrar nuevas víctimas.

A través del portal de tellows.es, te proporcionamos los métodos de estafa telefónica más comunes en España. Este gráfico no pretende ser una guía definitiva a tomar en consideración, pero sí un punto de partida para estar mejor informado.

De entre las tres categorías fundamentales podemos distinguir entre llamadas únicas, llamadas con retorno y SMS/mensajería instantánea. Para profundizar sobre cada tipo de fraude en concreto, hemos puesto a tu disposición una sección donde añadimos información básica y comentarios directos de nuestros usu.




Fuente: elaboración propia

# Loterías y premios

La persona que llama te comunicará que has sido seleccionado para un sorteo después de un número determinado de rondas. También puede invitarte a responder una pregunta del tipo “gana o pierde todo”. Después de esta pequeña operación, te pedirán que “guardes” tus ganancias para prevenir que otra gente pueda interferir en el cobro de tu supuesto premio, pero con el propósito de prevenir que busques más información o consejo.

Para finalizar, te pedirán que, a fin de cobrar el supuesto premio, pagues unas tasas. Según el interlocutor, estas tasas son para cubrir costes de seguro, tasas gubernamentales, bancarias y cargos de mensajería. Te pedirán que proporciones datos personales con el fin de “comprobar” que eres el ganador correspondiente y proporcionar tus datos bancarios para que el premio pueda serte transferido. No hace falta añadir que el defraudador utilizará estos detalles para robar deliberadamente dinero de tu cuenta bancaria.

*Opiniones en tellows:*

*(Antonio): Pues si yo también igual que el resto de estafados, en este mes me han quitado de la cuenta los 49€, como todos los meses anteriores, encima no he ganado nada, desde que me timaron y además dijeron que eran solo 3 meses y que si no salia favorecido con el premio devolvían la inversión y nada, todo esto es una mentira a ver si alguien se encarga de esta gente estafadora ladrones.*

*(Cali): No tiene nada que ver lo que promocionan por teléfono con la realidad. Ya está claro quiénes son y a qué se dedican. No dan a conocer los premios con claridad, así no hay forma de saber el premio. Hay que perseguirlos hasta pillarlos.*

*(Seint): Es una empresa de peñas de lotería. Te venden unas ganancias de más del 100% de lo invertido. Nada más lejos de la realidad. Yo jugué 2 meses y por una inversión de 100€ obtuve 8€... No digo más.*

Consejos:

- Si es demasiado bueno para ser verdad, probablemente lo sea.
- Ni se te ocurra proporcionar detalles de cualquier tipo a alguien a quién no confías plenamente.

# Estafa de soporte técnico

El emisor se presenta como un empleado de Microsoft quien llama debido a un virus que se detectó en la PC de la persona. Este supuesto técnico le pedirá a la víctima que abra el Visor de eventos de Windows, una parte del sistema operativo que regularmente emite advertencias de error, pero esto no tiene una influencia negativa en el funcionamiento de una computadora.

En consecuencia, la persona que llama le indicaría a la víctima que descargue el antivirus por una tarifa o incluso que se suscriba a una actualización regular de la aplicación que debería solucionar el problema de la computadora. Peor aún: en algunos casos, los estafadores solicitarían información personal y detalles de la cuenta bancaria para obtener el dinero de sus víctimas.

*Opiniones en tellows:*

*(Olivier): Se hacen pasar por técnicos de Microsoft para decirte que tienes que entrar en tu ordenador y seguir unos pasos que ellos te van a ir guiando a fin de supuestamente resolver el problema. Asi acceden a tus datos instalando un malvare (virus) para acceder a tus cuentas datos etc.*

*(Pedro): Me acaban de llamar. Pero hablo inglés y además soy informático. Dicen que son de MICROSOFT intentan que instales en tu ordenador un programa con el que se vana a apoderar de tus claves... ES UN TIMO... ES PELIGROSO...*

*(Paco): Llaman desde EEUU diciendo que son Microsoft y que enciendas tu ordenador para instalar un sofware que te protegerá de hackers y piratas. Hablan en inglés y son muy insistentes. Es una estafa. He llamado a Microsoft España y me lo han confirmado que es una estafa para instalarte un software para acceder a archivos y claves de tu ordenador.es*

Consejos:

- No compre ningún software o servicio de una fuente desconocida por teléfono.
- Nunca le dé el control de su computadora a un tercero a menos que pueda confirmar que es un representante legítimo de un equipo de soporte técnico del cual tú ya eres cliente.

# Empresas de recobro

Este tipo de llamadas se han hecho muy populares por el contexto de crisis en el que nos encontramos. Algunas de las llamadas son fraudulentas per se, como por ejemplo una supuesta empresa de cobranza que en realidad no lo es, reclamando una deuda inexistente. No obstante, las molestias causadas por empresas de gestión de cobros son muy significantes.

Dado que no es objeto del presente articulo, sólo mencionaremos que las empresas de gestión del cobro de deudas pertenecen algunas veces a las entidades bancarias y otras suscriben un contrato con ellas. Algunas prácticas abusivas se basan en molestar al usuario usando técnicas reprobables. Aún si la deuda es cierta, no todo vale para cobrar. El consumidor, por norma, no sabe cómo actuar y como todo, el acoso tiene un límite. Si estas empresas llegan a llamar a vecinos, e incluso al trabajo, esto es un hecho denunciable ante la Agencia de Protección de Datos. Para mas información referente a qué pasos realizar en caso de acoso, échale un vistazo a nuestra sección de asesoramiento jurídico en nuestra Comunidad de tellows.

*Opiniones en tellows:*

*(Lucas):* *Me cambié de operadora de internet-teléfono y Ono continuó facturando servicios. Entiendo que al tramitar la potabilidad deberían de haberme dado de baja. Ahora me reclaman unos 90 euros que no pienso pagar, y se dedican a acosarme desde este número.*

*(Iro):* *Me llamaron a las 8 y cuarto de la mañana, estaba durmiendo (había trabajado hasta tarde la noche anterior) y llamé al momento a ver de qué era ese número, enseguida me di cuenta de que era de un call center y les dije que colgaba, que estaba durmiendo y quería seguir haciéndolo, se pusieron a gritar que no lo hiciera, obviamente no hice caso.*

*(Guillermo):* *Llaman cobrando algo que no debo a Ono (18,83 euros) pero lo triste es que la persona que lo hace profiere amenazas inaceptables.*

Consejos:

- La mayoría de empresas de recobro son entes privados, que han comprado deuda a empresas de mayor embergadura con el fin de obtener algún tipo de beneficio. Sus prácticas (algunas veces rozando a la ilegalidad) no deben intimidarte. Contrasta sus datos y haz valer tus derechos como ciudadano y consumidor.

# Falsas ofertas de trabajo

Este esquema aprovecha la situación de las personas con bajos ingresos, como los estudiantes o los desempleados. Por lo general, ofrecen programas de capacitación pagados con la promesa de un trabajo al final. Con titulares tan llamativos como "trabaja desde casa y sin esfuerzo" y requisitos tan obvios como "Ud. tiene que ser ciudadano nacional" o "ser mayor de edad", los fraudes de este tipo se concentran en Internet, pero los dispositivos móviles no se quedan cortos al poder recibir emails de este tipo.


Algunos defraudadores preguntarán por tus datos bancarios para realizar un depósito o transferir dinero a tu cuenta, o incluso abrir una nueva cuenta para que les proporciones información adicional. La razón por la que te pedirán hacerlo es para poder "procesar tu solicitud de empleo". Algunas supuestas agencias van un paso más allá, mintiendo sobre posibles oportunidades de empleo y citándote personalmente.

*Opiniones en tellows:*

*(Soraya):* *No llamen! es una estafa! dan ofertas de trabajo de infojobs! obligan a estar cierto tiempo y sorpresa en la factura, dan datos de empresas que no existen! es una empresa que cambia continuamente de nombre! tienen anuncios en periódicos de todo el país! están en Salamanca!*

*(Nina):* *He llamado al 638937320 por una oferta de trabajo "personal para supermercado" y me han dicho que llamara al 807517887, como me ha parecido sospechoso, he buscado en google y parece ser que es una estafa, son ofertas de webs de trabajo que nunca llegan ha gestionar pero cobran la llamada. Ya está bien de reírse de la gente que lo pasa mal!!*

*(Rafael):* *Es una estafa para sacarnos el poco dinero que nos queda, atentos a la facturación, últimamente lo ponen en los periódicos locales camuflados con un número móvil para luego darte el 807517887.*

Consejos:

- Si no has buscado este tipo de oferta de empleo o no recuerdas haber enviado tu solicitud, muy seguramente se trate de un fraude.
- Antes de confirmar y pagar por tu participación, primero investiga un poco sobre los detalles de la empresa a través de Internet. Nunca confíes sobre detalles que provengan exclusivamente de códigos postales o números del móvil.
- Nunca proporciones información confidencial como tu cuenta de banco, número de tarjeta de crédito o número de la seguridad Social.

# Falsos vendedores/ teleoperadores

Mientras hay compañías que legalmente ofrecen servicios de tele mercadeo, los consumidores y negocios pierden millones de euros al año por prácticas fraudulentas. A veces es muy difícil diferenciar a una compañía que se dedique a esta función o simplemente a robar mediante este método. El supuesto operador de tele mercadeo te preguntará si puedes aportar una cuantía de dinero por avanzado para comprar algo y así obsequiarte con un regalo o incrementar tus posibilidades de ganar algo.

Entre sus técnicas se incluyen la presión para que decidas en el mismo momento de la llamada de forma inmediata; negarse a proporcionarte información por escrito, petición de pago a través de mensajería, uso de técnicas para hacerte creer que estás bajo algún tipo de riesgo, pago de una cuantía de mensajería o impuestos y petición de datos bancarios aunque no hayas contratado ninguno de sus servicios, promesas para recuperar el dinero que hayas perdido a través de otras apuestas, promesas de que puedes obtener mucho dinero trabajando desde tu casa y lo más común, renunciar a no llamarte más en caso de que no estés interesado.

*Opiniones en tellows:*

*(Ildefonso): Son Call Center, contratados por canal + para vendernos la tv de canal+. Si quieren canal+, contratela directamente a través de su web, o de cientos de tiendas que hay en el país.*
*No confíen en esta gente, que usan nuestros datos para decirles a otras empresas que tienen una base de datos a las que venderles mil y un productos.*

*(Belen): Me han llegado ha llamar hasta 3 veces en el mismo día y se lo dices por la buenas y encima te cuelgan, aparte llaman a horas que no son muy normales como a las once de la noche y te faltan el respeto si les dices que te dejen y se ponen chulos, yo no se si se podría hacer algo porque me parece acoso en vez de publicidad.*

Consejos:
- Contacta directamente la compañía para confirmar antes de dar información.
- No dudes en colgar directamente si crees que la llamada es sospechosa.
- Regístrate en Listas Robinson para prevenir ser molestado.
- Puedes Contactar con la compañía directamente para que no te molesten de nuevo.

# Vishing y Spoofing

El Vishing es una práctica criminal fraudulenta en donde se hace uso del Protocolo Voz sobre IP (VoIP) y la ingeniería social para engañar personas y obtener información delicada como puede ser información financiera o información útil para el robo de identidad. El término es una combinación del inglés "voice" (voz) y "phishing" (ver página 26 saber sobre este término).

El criminal llama a números telefónicos en una determinada región. Cuando la llamada es contestada, una grabación salta y alerta al "consumidor" que su tarjeta de crédito está siendo utilizada de forma fraudulenta y que éste debe llamar al número que sigue inmediatamente. El número puede ser gratuito falseado para la compañía financiera que se pretende representar. Cuando la víctima llama a éste, es contestada por una voz computerizada que le indica al cliente que su cuenta necesita ser verificada y requiere que introduzca los dígitos de su tarjeta de crédito. Cuando la persona provee la información, el visher tiene todo lo necesario para realizar cargos fraudulentos a la tarjeta de la víctima. La llamada puede ser también utilizada para obtener detalles adicionales como el PIN de seguridad, la fecha de caducidad, el número de cuenta u otro dato importante. Estos datos serán utilizados para prácticas ilegales de todo tipo, incluyendo Spoofing o suplantación de identidad, generalmente con usos maliciosos o de investigación.

*Opiniones en tellows:*

*(Barcelona): CUIDADO con este teléfono 640012002, se dedican a la suplantación de identidad, mediante la recopilación de datos, esto ocurre al darte de alta en paginas de buscadores de empresas, páginas amarillas, qdq, vulka, 11811 etc... aprovecharan vuestro nombre, nif o dni, datos de la empresa, para intentar suplantar vuestra identidad en Internet, con la infinidad de posibilidades que esto tiene, pedidos a proveedores, cuentas bancarias, facturaciones a vuestro nombre etc... aconsejo avisar a la VERDADERA guardia civil, ellos dirán que ya están informados y que la unidad de delitos telemáticos, están trabajando en ello, igualmente dar el aviso.*

*(Cuca): A mi me acaba de ocurrir lo mismo. Que suerte! Me acaban de llamar para informarme que por sorteo notarial me han correspondido una pareja de relojes de 390 €. Se hacen pasar por la tienda en casa del Corte Inglés, incluso tienen el morro de decirme que están de aniversario y sortean 6000€ diarios en premios. Ante mi desconfianza me hablan de su experiencia y los productos anunciados en TV y luego copiados de forma fraudulenta.*

Consejos:

- El control de tus datos en la red es fundamental.
- Vigila muy bien y distingue entre datos genéricos (como tu nombre o email) y tus datos de vital importancia, como tu número de teléfono, dirección física o otras cuentas de correo de mayor importancia.

# Llamadas con retorno (Llamadas ping)

A modo de introducción, este tipo de fraudes son perpetrados a través de mensajes cortos, que levantan curiosidad, textos incógnito que te piden que respondas. Aunque sospechosos para algunos, se interpretan como una llamada de socorro por algunos usuarios. ¿Qué pasa si un conocido está de vacaciones o en otro país por alguna razón y te llama? ¿O si un compañero/a no es de tu país y se cambia de número de teléfono?

Este tipo de fraudes funcionan igual que los que requieren tan solo una única llamada. Los defraudadores emplean centralitas que llaman aleatoriamente con un toque, y desconectan. Si devuelves la llamada el coste de esa llamada es cargado a tu factura de teléfono. Para prolongar la duración de la llamada (y el coste), se utilizan técnicas tan básicas como reproducir hilos musicales.

Consejos:

- Si ves códigos de área (especialmente internacionales) con los que no estás familiarizado, no descuelgues el teléfono. Consulta tu contestador para verificar si este número ha dejado algún mensaje.

# Petición / redireccionamiento de llamada

Este tipo de fraude es bastante común. Con la excusa de la entrega de un paquete, o incluso abusando de la buena voluntad del usuario aludiendo necesidad o urgencia, se proporciona un número al que llamar. Este número corresponde en la mayoría de los casos a un número de tarifa especial con coste variable. No obstante, ni resulta haber ninguna urgencia ni ningún mensaje o paquete a recoger, pero la llamada ya se ha realizado.

Más temible es lo que en algunos casos puede suceder. A continuación te ponemos algunos ejemplos;

- Robo de llamadas: Conexiones fraudulentas a líneas telefónicas desde las cuales se efectúan llamadas locales, a larga distancia, a móviles y a líneas Premium sin autorización del suscriptor.
- Interceptar las llamadas: Conexiones fraudulentas a líneas telefónicas desde las cuales se escuchan conversaciones privadas, se realiza espionaje de información clasificada, se hacen extorsiones, todo sin conocimiento ni autorización del suscriptor.
- Robo de líneas o traslados desautorizados: Personas inescrupulosas roban o trasladan líneas sin autorización de la empresa o el usuario y las revenden o utilizan para cursar tráfico a cargo del usuario afectado.
- Clonación de teléfonos móviles: A través de equipos de radio se interceptan los números de serie de los terminales (ESN) móviles y con estos datos re programan otros terminales desde los cuales se realizan llamadas a cargo del suscriptor titular del ESN.

*Opiniones en tellows:*

*(Justo):* *Es una estafa te llaman haciéndose pasar por una empresa de mensajería diciéndote que tienen un paquete para entregarte y te cuelgan para que tu les llames, cuando lo haces te dicen que llames a un 905551806 y te cobran llamadas y mensajes premiun. Mucho ojo con este tipo de llamadas. Lo mejor de todo, recibí la llamada de madrugada.*

*(Milongas):* *Ojo! timo en toda regla con mensajería incluida. Acabo de recibir una llamada desde el número 667332548 pero al no poder contestar a tiempo he llamado yo, ya que justamente estoy esperando una llamada de un número que seguro que no tengo registrado. Se ha puesto en marcha un contestador que decía que llamaban de una mensajería porque tenían que entregarme un paquete y que llamara al 90 55 51 80 7 (lo pronuncian así, de dos cifras en dos cifras y, al final, el siete).*

*(Eduardo):* *A mi también me han llamado.. es lo mismo que han contado los demás.. "te llamo desde una mensajería..no le oigo...oiga...oiga.." devuelves la llamada y llames desde donde llames, tienes un paquete asociado al numero de teléfono desde el que llamas, y claro, tienes que llamar a un 905.*

Consejos:

- Al devolver una llamada de este tipo, la locución puede pedirte que llames a un número. Éste te será comunicado de forma que tu, al principio, no puedas darte cuenta que es un número de tarifa especial; por ejemplo “noventa, cincuenta y ocho”, en lugar de “nueve cero cinco ocho”.

# Mensaje con promoción/premio/obsceno

Este tipo de práctica varia del método anterior únicamente por que el soporte a través del que se intenta cometer el presunto fraude. Con un simple clic, éste se consuma a través del acceso a un servicio premium no deseado, o servicios inexistentes. Las consecuencias son muy variadas (ver siguientes secciones), pero nunca positivas.

# Phishing/Smishing

El pishing es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.


El smishing es una variante del phishing pero con el uso de los mensajes cortos o SMS. Son textos cuya actividad criminal es la de obtener, mediante engaños a los usuarios de telefonía móvil, información privada o suscripciones falsas online y ofertas de trabajo en sitios web. Luego se introducen spyware o programas con intenciones maliciosas sin el consentimiento del usuario.

Los ejemplos que podemos proporcionar se asemejan a los de falsos vendedores/tele-operadores. En definitiva, alguien que utiliza un nombre de una empresa o entidad conocida con fines fraudulentos.

# “Spim”, mensaje con virus o software malicioso

Este tipo de mensajes, también conocidos como Spim, son recibidos la mayoría a través de aplicaciones de mensajería instantánea tipo Whatsapp o Telegram. Tienen como objetivo la ejecución de software malicioso de diferente índole en el teléfono de la víctima. Dado que cada vez más ordenadores y móviles comparten espacio de uso como en su programación, los resultados nefastos para el móvil se asemejan bastante a los del primero. Estos incluyen des de el simple y conocido hackeo, o acceso fraudulento a tu dispositivo con el fin de ejecutar todo tipo de acciones para beneficio propio o de terceros, a peores consecuencias. Técnicas más sofisticadas incluyen páginas web que solicitan la descarga e instalación de aplicaciones que establecen conexiones fraudulentas con otro proveedor de Internet internacional o destinos con servicios Premium. Las consecuencias más extremas pueden llegar incluso a controlar el propio dispositivo.

# Directiva 97/66/CE y la Directiva 95/46/CE de la Comisión Europea

¿Es ilegal que la información de un particular esté disponible en Internet? La respuesta es SÍ.

De acuerdo con lo dispuesto marco jurídico concebido por la Directiva 97/66/CE y la Directiva 95/46/CE de la Comisión Europea, la búsqueda inversa o multi criterio constituye un uso totalmente diferente de la finalidad establecida de las guías telefónicas convencionales (como por ejemplo las páginas amarillas), por lo que queda fuera del marco legal convencional para el uso de datos del abonado. La Directiva establece que "el abonado deberá dar su consentimiento informado sobre si sus datos personales pueden incluirse en una guía pública, con qué fin específico y en qué medida". De lo contrario, estos no pueden estar registrados en la misma (Fuente; Agencia española de Protección de Datos y Dictamen 5/2000 sobre el uso de las guías telefónicas públicas para servicios de búsqueda inversa o multi criterio (Guías inversas).

# Directiva europea 2011/83, del 25 de octubre

La transposición de la normativa comunitaria de protección de los consumidores a la legislación española, afecta sobre todo al comercio electrónico y la contratación de servicios por vía telefónica.

Rasgos que destacan y que afectan al usuario final son los siguientes:

1) La ampliación de los requisitos de información que debe ofrecer el empresario al consumidor acerca de la transacción, así como de la manera de confirmar el acuerdo del consumidor al respecto.

2) El refuerzo de las opciones del consumidor para ejercer el derecho al desistimiento, con mayores garantías de que ello no le supondrá costes excepto los derivados de la devolución por correo de los bienes o la parte proporcional a precios de mercado de los servicios ya consumidos.

3) La definición de otros derechos del consumidor, referentes a la entrega, al coste de los medios de pago, a la tarifa de la comunicación telefónica o a los pagos adicionales que no figuren en el precio solicitado en principio al consumidor.

4) Derecho de desistimiento, que se amplía de 7 a 14 días. Este es el plazo que tendrán los consumidores para ejercer el derecho de desistimiento desde la adquisición del bien o la formalización del contrato de servicios, aunque si el empresario no ha informado al consumidor al respecto el plazo se amplía hasta los dos años.

Fuente; Directiva europea 2011/83, de 25 de octubre.

# Reglamento General de Protección de Datos

El 25 de mayo de 2018 entró en vigor el Nuevo Reglamento General de Protección de Datos.

Esta normativa regula los derechos de los ciudadanos en materia de privacidad y protección de datos y por tanto regula las relaciones que tenemos con otras entidades, empresas y organismos que tratan con nuestros datos personales.

El nuevo reglamento se basa siempre en los derechos ARCO (Acceso, rectificación, cancelación y oposición) pero ahora se le añaden otros derechos en materia de protección de datos, los cuales son:

El derecho de supresión (o derecho al olvido), es más completo que el anterior de cancelación, de forma que, en determinadas circunstancias, los usuarios podrán exigir a las empresas que supriman sus datos personales, incluso que se elimine cualquier enlace a esos datos personales.

El derecho a la portabilidad de los datos: si mis datos son míos, yo, consumidor, puedo decidir y pedir que me faciliten en formato electrónico los datos personales que una empresa u organismo tenga de mi, o pedir que se los manden a la entidad o empresa que yo decida.

El derecho a la transparencia en la información y el derecho a limitar el tratamiento de los datos personales también se amplían en la nueva norma.

Gracias a esta nueva reforma, para que tus datos puedan ser recopilados y tratados, tendrás que prestar un consentimiento “inequívoco”, es decir, las empresas o entidades deberán informarte claramente del tipo de datos que van a recoger y con qué finalidad, qué van a hacer con ellos, y solicitar tu consentimiento de forma clara afirmando que autorizas el uso de tus datos.

# 7 Alternativas para interponer una denuncia en caso de Spam

(Todas las opciones las tendrás disponibles en nuestra sección de asesoramiento jurídico).
En España múltiples leyes nos amparan en este tipo de situaciones, incluyendo la Ley 34/2002 de Servicios de la Sociedad de la Información, la Ley 32/2003 General de Telecomunicaciones y la Ley Orgánica de Protección de Datos (LOPD). Contacta con la Agencia Española de Protección de Datos o con la Comisión Nacional de los Mercados y la Competencia para mayor información. Estos entes también te
pueden asesorar en caso que necesites poner una denuncia.

1. Como primera opción, puedes presentar una denuncia formal ante la Oficina de Atención al usuario de telecomunicaciones (opción "presentar denuncias/reclamaciones"). En cada sección se muestran claramente los pasos a seguir ante, por ejemplo, denuncias relacionadas con números de tarificación especial como los 803 – 806 – 807 – 907 – 905 o SMS Premium.

2. Como segunda opción, puedes presentar una denuncia formal ante la Agencia Española de Protección de Datos en su sección de denuncias, a través de su formulario. En la misma página, encontrarás los pasos a seguir para completar satisfactoriamente tu denuncia.

3. Acceder al departamento de colaboración ciudadana facilitado por el Cuerpo Nacional de Policia. A través de su formulario podrás notificar de forma telemática tu caso y también informar de las acciones tomadas por tu parte para denunciarlo.

4. Darse de alta en la Listas Robinson, un servicio gratuito gestionado por la Asociación Española de la Economía Digital. Mediante un formulario online los usuarios pueden indicar que no desean recibir publicidad ni comunicaciones comerciales por parte de empresas con las que no mantengan ninguna relación como clientes. Y, además, indicar cuál es el medio por el que no quieren ser molestados: teléfono, mail, SMS, correo postal o ninguno de ellos.

5. Poner el hecho en conocimiento de organizaciones o asociaciones de consumidores, como OCU o FACUA (os aconsejarán sobre cómo actuar, qué denunciar, etc.).

6. Puedes acudir al Instituto Nacional de Ciberseguridad (INCIBE) a través del Centro de Seguridad e Industria (CERTSI) el cual ha habilitado el correo electrónico incidencias@certsi.es para reportar casos de fraude como correos de phishing, tiendas online fraudulentas, sitios web que alojan malware, entre otros.

7. Un paso más drástico, denunciarlo a las autoridades competentes, bien a la policía o al juzgado de la zona de residencia.

Si deseas hacer conocer tu experiencia en otros foros de Internet, por favor no dudes en hacerlo. Contra más usuarios estén informados, mucho mejor se podrán prevenir experiencias relacionadas con prácticas fraudulentas.

# ¡tellows te ayuda!

Con tellows.es, hemos creado una plataforma que ayuda a clasificar mejor los números desconocidos y las llamadas no deseadas. Es una comunidad de miembros que se ayudan mutuamente compartiendo sus experiencias en relación a números de teléfono molestos. A diferencia de los directorios de búsqueda directa, la web proporciona información de la persona que llama. Además de poder leer testimonios directos, también puedes encontrar información en relación a los últimos métodos de scam y maneras de protegerte de llamadas no deseadas a través de nuestro blog y las contribuciones en nuestra página de Facebook con más de 15.000 seguidores.

Con más de 7 millones de visitas al mes y más de 80.000 números de teléfono registrados en nuestra base de datos, tellows te ofrece la plataforma perfecta para acabar con las llamadas no deseadas y spam. Nuestra propia Comunidad nos avala. Sin vosotros, tellows no sería posible...

*(Eleivlc):* *Hola, yo acabo de recibir una llamada perdida cortísima de este numero...el prefijo me resulto raro. GRACIAS a vosotros no devolvía llamada..entré en google a comprobar el prefijo y caí aquí..gracias otra vez y creo que este asunto se merece una denuncia.*

*(Eulalia):* *Me ha ocurrido lo mismo que el caso este de 807... me llama un 667332537 de "mensajería expres" una tal Gloria diciendo que tengo un paquete y se corta la llamada, devuelvo la llamada y salta un contestador diciendo que esta lleno y que llame al 905404090.*
*Gracias a esta página no les hago ganar un solo céntimo. Un saludo!*

*(Felipe):* *Me han llamado, un tono y cuelgan. Gracias a los que escribisteis estos mensajes en esta página, ya sé que no tengo que devolver la llamada.*

# ¿Como funciona tellows Score?

tellows proporciona una plataforma gratuita para los que buscan información sobre números de teléfono desconocidos. tellows dispone de un sistema especial, la tellows score, una puntuación dada a los números telefónicos con la que podrás ver si supone un riesgo o no contestar el teléfono.

El objetivo principal de tellows es ofrecer una plataforma interactiva gratuita a través de la cual se puede intercambiar información sobre llamadas desconocidas. El enfoque principal de la puntuación de tellows es dar a los usuarios la posibilidad de evaluar cualquier número. ¡Este mecanismo de calificación se encuentra disponible para más de 50 países!. El mecanismo funciona de la siguiente forma:


Calificación positiva

Se trata de un número serio. Según los comentarios de la mayoría de usuarios de tellows las llamadas de este número son fiables.


Calificación neutral

O bien se trata de un número desconocido, o existe muy poca información como para juzgarlo adecuadamente. Sin embargo, podría ser también el caso que se trate del equilibrio de comentarios positivos y negativos.


Calificación negativa

¡Cuidado! La mayor parte de usuarios de tellows han denunciado actividades cuestionables realizadas a través de este número. Por favor tened cuidado o ignoradlo por completo.

# La aplicación de tellows para Android y iPhone

## un identificador de llamadas para tu Smartphone

¡Con la aplicación tellows, ahora puede identificar a personas desconocidas mientras suena!

La aplicación le informará en tiempo real si la persona que llama es confiable o no. En el primer timbre de su teléfono, la puntuación de tellows aparecerá automáticamente para ayudarlo a decidir si contesta el teléfono o lo cancela; la puntuación de 7 a 9 son los números más confiables.

La aplicación también le permite leer las calificaciones de los usuarios sobre este número. Publica tus propias experiencias a través de esta aplicación para que también puedas advertir a otros. El servicio es totalmente gratuito. También tenemos una versión Pro de nuestra aplicación.

Descubre los beneficios de la aplicación en la siguiente página.

### iPhone


*(Luis):*
*„Muy buena para saber quién te está llamando si no lo tienes en la agenda“*

*(Mike):*
*„Una gran ayuda.“*

*(Eukeni):*
*„Lo cierto es que esta muy bien,hace un buen trabajo y eso da garantias de tener la seguridad de quien te llama y no va a volver a llamarte.Merece la pena.“*

### Android

# Características de la app de tellows para Android y iPhone

Características básicas de la aplicación (versión gratuita):

- Identificación de llamadas entrantes (detección de llamadas no deseadas) con la visualización del tellows score (calificación), el nombre de la persona que llama y el tipo de llamada.
- Búsqueda inversa de números de teléfono y visualización de todos los comentarios/calificaciones de los números telefónicos.
- Reportar/comentar números telefónicos.
- Inicio de sesión en la cuenta de tellows y la asignación entre dispositivos de los comentarios a la cuenta de usuario.

Funciones Premium (de pago o desbloqueables por código):

- Bloquear las llamadas no deseadas importando una lista negra.
- Lista negra personal disponible con todos los números con calificación negativa del usuario (posible después de iniciar sesión).
- Identificación de llamada fuera de línea y bloqueo posible.
- Sin publicidad.


Si eres un usuario registrado, puedes tener las características premium de la aplicación de Android de forma gratuita durante un mes. Tienes la ventaja de crear una lista negra personal. Si realizas comentarios negativos sobre los números, se agregarán de inmediato a su lista negra personal, aunque el tellows score indique una mejor calificación. La lista negra personal funciona así independientemente de las calificaciones de otros usuarios. Se puede ver en el área de miembros. También puedes ver cuántos números de teléfono hay en tu lista negra.

Cabe destacar que las listas negras también funcionan en multidispositivo. Las listas negras se pueden usar con todos los productos de tellows, pero la lista negra personal solo se puede usar como usuario registrado. Si desea saber más sobre nuestros productos, puede visitar nuestra tienda.

# ¿Alguna pregunta más?

Todo el equipo de tellows espera que el magazine ayude a tantos consumidores como sea posible en la lucha contra el "terror" telefónico. Está claro que las llamadas molestas nunca se van a poder prevenir totalmente, pero el conocimiento sobre las técnicas de scam y la protección legal son un buen comienzo para defenderte adecuadamente. Si aún tienes preguntas o quieres darnos tu opinión, contáctenos a través de una de las siguientes opciones:

1. ¿Tienes algún comentario sobre el magazine? ¿Alguna opinión sobre los artículos presentados? ¡Entonces escríbenos!

**kontakt@tellows.de**

*Tu opinión es bienvenida y nos ayuda a combatir más eficazmente las estafas telefónicas.*

2. ¿Has experimentado la misma llamada molesta varias veces? ¿Fuiste lo suficientemente hábil para esquivar los métodos de engaño de los defraudadores? ¿Has descubierto algún método nuevo de fraude? ¡Entonces te invitamos a que lo registres en nuestra web!

**www.tellows.es**

*De esta forma, avisarás a otros usuarios a lidiar con esta situación.*

3. ¿Te gustaría estar informado de las últimas novedades legislativas así como de los nuevos métodos de fraude? ¡Entonces visita nuestro blog o nuestra página de Facebook!

**www.facebook.com/tellows**

**https//blog.tellows.es/**

*Recibe las noticias y participa en las discusiones. sobre números dudosos o temas actuales.*

# Direcciones de interés

Agencia Española de Protección de Datos
C/ Jorge Juan, 6, 28001 Madrid
Teléfono 901 100 099.
http://www.agpd.es/

Comisión Nacional de los Mercados y la Competencia
C/ Alcalá, 47. 28014 Madrid
C/ Bolívia, 56. 08018 Barcelona
http://www.cnmv.es/

Listas Robinson
C/Muntaner, 92 Pral 3ª - 08011 Barcelona
https://www.listarobinson.es

Oficinas centrales de de OCU
Dirección: Calle de Albarracín, 21, 28037 Madrid, España
Teléfono: 913 00 00 45
http://www.ocu.org/

Oficinas Centrales de FACUA
Calle Bécquer, 25 A - 41002 Sevilla (España)
Teléfono 954 90 90 90
http://www.facua.org/

Grupo de Delitos Telemáticos.
Unidad Central Operativa
https://www.gdt.guardiacivil.es/webgdt/pinformar.php

**El magazine de tellows es un proyecto de**
tellows UG
Eschenring 6
D-04828 Bennewitz
Alemania

1a Edición, 2014
2da Edición, 2018

**Nota del grupo Editorial**

A pesar del riguroso examen al que el contenido de este magazine ha sido sometido, los errores no pueden ser totalmente controlados. Así pues, la total veracidad y precisión sobre la información incluida en este magazine no puede ser garantizada.