

# EL TIMO DE LAS RESIDENCIAS QUE DEBEN PAGOS



Proyecto P-  
45 "Audaz"



Buenas a todos ciber-navegantes. Hoy os quiero contar un timo muy reciente haciendo especial incidencia sobre nuestros mayores, y más concretamente **sobre la residencias** donde muchos de ellos reciben cuidados.

## ¿En qué consiste este timo?



El Gobierno del Principado de Asturias (entre otros) ha emitido recientemente una alerta previniendo de que existen una serie de personas que llaman sistemáticamente a diferentes residencias haciéndose pasar por empleados del públicos de dicha gobierno. El objetivo de la llamada es **reclamar unos supuestos pagos pendientes** por materiales que se han recibido pero aún no están abonados en su totalidad, o bien por pagos pendientes de algún servicio prestado durante la pandemia o por otro motivo.

 **Sí, como veis a pesar de que ya han pasado tres años todavía sigan intentando exprimir eso como excusa para defraudar. En cualquier caso, van a intentar usar cualquier cosa que esté de actualidad, por lo que mucho cuidado y atento a las noticias.**

Si bien la última oleada de timos de esta clase data del 2023, como estos fraudes se organizan por campañas de manera que cuando una se hace muy popular se frena temporalmente hasta que baja un poco la alerta pública, es necesario hacer llegar esta información a responsables o trabajadores de la residencias que conozcáis para cuando vuelvan otra vez a resurgir.

## ¿Cómo prevenirlo?

Aunque parezca un timo clásico y trivial, estos timos pueden ser muy elaborados. El delincuente suele tener entrenamiento para sonsacar información en una conversación y por tanto ser muy convincente. Algunas de las técnicas más comunes (aplicables en este timo y en otros) son:

- **Suplantación de identidad:** Se hacen pasar por una persona, empleado público o de un proveedor de confianza. La información para suplantar a la persona se puede sacar muchas veces de las webs, el BOPA/BOE (contratos públicos), redes sociales, etc. No olvides que **los nºs de teléfono se pueden suplantar fácilmente** con el equipo adecuado para reforzar el engaño.

- **Creación de historias convincentes:** Inventan historias convincentes para ganarse la confianza de la víctima y que esta revele información personal o haga el pago pedido. Para reforzar esta historia de nuevo pueden usar información que hayan encontrado en las mismas fuentes que en el caso anterior.
- **Uso de presión sicológica:** Amenazan a la víctima con consecuencias negativas si no revela la información que solicitan. **No tiene por qué ser algo agresivo** necesariamente, se pueden ofrecer descuentos por pronto pago, ventajas de alguna clase si se usa un medio de pago determinado (normalmente no trazable) y cosas similares.
- **Phishing:** Esta técnica consiste en enviar **correos electrónicos o mensajes de texto fraudulentos** que parecen provenir de una fuente legítima. El objetivo tradicional de estos ataques es engañar a la víctima para que haga clic en un enlace o abra un archivo adjunto que contiene malware. Una vez que el malware está instalado en el dispositivo de la víctima, el estafador puede acceder a su información personal y financiera. No obstante, en este caso se puede ser más creativo:
  - Se puede **mandar un email o SMS previamente a una llamada** para mejorar su credibilidad (enviando por ejemplo una factura, que no necesariamente tenga un malware para evitar que la detecten servicios de protección que tenga la víctima).
  - De la misma forma, **se puede enviar el correo o SMS posteriormente** a la llamada, para reforzar la historia contada durante la misma y que contengan documentos (no necesariamente maliciosos) que la respalden. Tanto en este caso como en el anterior, recuerda que es relativamente posible que se suplante una dirección de email real o se use una similar para engañar a la víctima. El origen de un SMS puede suplantarse más fácilmente aún
- **Vishing:** Esta técnica es similar al *phishing*, pero se realiza **por teléfono**. Obviamente este timo es uno de esta clase. No obstante, recuerda con la **proliferación de IAs modernas que clonian voces**, un atacante podría buscar una grabación de una persona conocida (no olvidemos que se hacen pasar por empleados del gobierno autonómico) y clonar su voz para que entonces la estafa sea mucho más difícil de detectar.

 **Todas estas técnicas pertenecen a la categoría de técnicas de ingeniería social: la manipulación psicológica de una víctima para que revele información personal o financiera.**

La forma de prevenirlo es muy clara: **el Principado de Asturias (ni ningún gobierno) jamás te va a pedir dinero por teléfono**. Por tanto cualquier llamada de este estilo debe ser **cortada de inmediato y denunciada ante las autoridades** para ver si pueden hallar a los culpables. Para ello, recuerda que puedes usar esta web:  
[https://www.policia.es/\\_es/colabora\\_informar.php?strTipo=CGPJDT](https://www.policia.es/_es/colabora_informar.php?strTipo=CGPJDT)

## SELECCIONA LA ESPECIALIDAD

Concreta la especialidad a la que quieras informar

< Selección del área policial

Selección de la especialidad

### Pornografía infantil

Comunicación de información sobre páginas web, publicaciones o cualquier situación que ponga en peligro al menor en el uso de las nuevas tecnologías (Ciber-bullying, Grooming, Sexting).

Seleccionar

### Redes sociales

Comunicación de cualquier actividad ilegal a través del uso de las Redes Sociales (Facebook, Twitter, Youtube, foros, newgroups, etc).

Seleccionar

### Amenazas y extorsiones

Comunicación de delitos de amenazas, extorsiones, calumnias o injurias cometidos a través de las Tecnologías de la Información y la Comunicación.

Seleccionar

### Fraudes en Internet

Comunicación sobre uso fraudulento de tarjetas de crédito en Internet, fraudes en subastas y comercio electrónico, estafas en la red.

Seleccionar

### Seguridad lógica

Seguridad lógica, virus, sustracción de datos, hacking, descubrimiento y revelación de secretos, suplantación de personalidad o sustracción de cuentas de correo electrónico.

Seleccionar

### Antipiratería

Comunicación de delitos contra la propiedad intelectual de programas de ordenador, música y productos cinematográficos o contra la propiedad industrial, uso indebido de señales de video.

Seleccionar

### Fraudes uso telecomunicaciones

Comunicación de delitos cometidos utilizando cualquier sistema de telecomunicación, fraudes telefónicos en sistemas de telefonía fija o móvil.

Seleccionar

### Otra información

Para comunicaciones no recogidas en los epígrafes anteriores.

Seleccionar

🔍 **Y no lo digo yo, ¡lo dicen ellos mismos! 😊**

## ¡Pero yo no soy una residencia! Este no me afecta...

No quería terminar sin recordar que este tipo de timos **son una variante de uno muy popular**, donde se escoge un negocio concreto y se le llama intentando convencerle de que debe un pago por algún concepto para que se lo ingrese al atacante. He visto variantes con negocios de hostelería y a pie de calle, que deben supuestamente impuestos, recibos de luz y gas (dedicamos un documento a esta variante en el pasado), o cualquier otro concepto que sirva para amenazarles con un corte inminente y por tanto la necesidad de cerrar el negocio.

🔍 **Los delincuentes saben bien lo que hacen: si el negocio cierra no tiene ingresos y a un autónomo eso puede suponerle un "roto" potencialmente inasumible, por lo que jugar con ese miedo les da buenos resultados.**

Y sin importar la variante, lo que podéis hacer **es siempre lo mismo**: si tienes dudas llama a la empresa que supuestamente te está contactando tú mismo, a su teléfono oficial y no a alguno que os ve la persona que os llama, y compruébalo.

🔍 **Esta estafa es tan común que mucha gente se sigue sorprendiendo de la de veces que un empleado de la empresa real le dice que no tiene ni idea de lo que le está hablando cuando les contacta...**

Y eso es todo, por favor estás muy alerta porque las campañas de timos están yendo a peor y cada vez son más sofisticadas. Tenemos que elevar nuestro nivel de alarma si queremos ponérselo difícil a los malos.

Y finalmente un poco lo de siempre. Por favor, **cuéntaselo a la gente** porque esto es una campaña activa que vuelve periódicamente, y nunca sabes cuando alguien conozcas va a ser una víctima mañana mismo o dentro de poco. **Especialmente si conocéis a alguien que trabaje en una residencia o tenga algún puesto de responsabilidad en ella. ¡Que corra la voz!**

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

**Y recuerda amigo/a, si tienes un negocio y alguien del gobierno te llama para reclamarte una factura...¡es mentira!**



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



- [Escúchalo en IVOOX](#)
- [Escúchalo en Amazon Podcast](#)
- [Escúchalo en mi canal de YouTube](#)
- [¿Tienes otro cliente de Podcast? Este es el feed RSS](#)

**¿Quieres leer alguna noticia/artículo relacionado?**



- [Alerta en las residencias asturianas por varios intentos de estafa \(07/02/2023\)](#)
- [Alerta en las residencias asturianas por un nuevo intento de estafa telefónica \(08/02/2023\)](#)

*Este documento usa material generado con IA<sup>2</sup>*

<sup>1</sup> Audio emitido en "Más de Uno". 95.2 Onda Cero Oviedo (<https://www.ondacero.es/emisoras/asturias/oviedo/directo/>) el 27/03/2023

<sup>2</sup> Algunas imágenes del texto del documento han sido generadas con la IA Bing Chat