

Cuando hablamos de los riesgos que afectan a los conductores, siempre nos centramos en la velocidad, las distracciones, el estado y tipo de vía, condiciones del vehículo... pero hay otro tipo de riesgos que consideramos que los conductores deben conocer para estar en guardia ante estas situaciones.

Nos referimos a las **tentativas de timos y fraudes cuyos destinatarios son los conductores.**

Veamos algunos de los recientemente detectados:

## EL TIMO DEL RETROVISOR

---

- Las víctimas de este timo suelen ser personas mayores. Se lleva a cabo chocando un coche con el de la víctima del timo. A partir de ese momento, el timador argumenta que el vehículo ha sido alquilado en otro país y tiene prisa por devolverlo por lo que pide al afectado que rellene el parte amistoso de accidente.
- Los estafadores indican que van a realizar una llamada telefónica a la aseguradora para averiguar cómo deben rellenar el documento.
- Solicitan a la víctima que hable con la supuesta aseguradora pero al teléfono se encuentra, en realidad, un cómplice. Se le pide al estafado que facilitarle sus datos personales, mientras le informan de que los trámites entre vehículos de distintos países son lentos y caros. Por eso, le recomiendan que pague en efectivo la reparación del retrovisor que valoran en un importe de entre 1200 y 1500 euros.
- Una vez han convencido a la víctima de tener que abonar el importe, los estafadores le acompañarán al cajero. **Aprovechan, así, para hacerse con el código PIN y robarle la tarjeta.**



### LAS RUEDAS PINCHADAS



- En esta modalidad de timo, los estafadores aprovechan la **parada de los vehículos** en un área de descanso, peaje o estación de servicio para pinchar una de las ruedas del vehículo del estafado. Cuando este retoma la marcha, irá perdiendo el aire de la rueda poco a poco.
- Una vez que el vehículo se vuelva a detener al notar el conductor el pinchazo, los timadores **ofrecerán su ayuda**, pero el motivo real del ofrecimiento es robar todo lo que esté a su alcance. Finalmente, le dejarán sin sus cosas y con una rueda pinchada.

### EL FALSO ABOGADO

- La víctima de este timo recibe **una llamada telefónica en la que un supuesto abogado** le informa de que su hijo/a está detenido/a por provocar un accidente grave. A continuación, el timador le ofrece la posibilidad a la víctima de la estafa de pagar una cantidad de dinero para pagar la fianza y de esta manera conseguir que se libere de ir a la cárcel.



### EL TIMO DEL ORO

- La táctica de los delincuentes que llevan a cabo esta estafa, consiste en **estacionar el coche a un lado de la vía simulando haberse quedado sin gasolina**. Después los estafadores aprovechan la buena voluntad de los conductores, que generalmente están acompañados por sus familias, para **solicitar ayuda a cambio de joyas de oro** supuestamente valiosas.
- En caso de que la víctima indique que no lleva dinero en efectivo, el estafador insiste en acompañarle a un cajero automático buscando excusas para no ir a la estación de servicio más cercana.
- No hace falta decir que las joyas ofrecidas son falsas.



### LA ESTAFA DE LA GRÚA PIRATA

- En este caso, los afectados son los conductores en situaciones de avería, accidente o incidente de tráfico. Los delincuentes, anticipándose a las grúas de asistencia contratadas por el seguro, se presentan con **vehículos similares a los de las empresas reales** confundiendo a las víctimas y engañándolas para que paguen en efectivo por un servicio que supuestamente será reembolsado por su aseguradora, lo cual nunca sucede.



Mención a parte merecen los intentos de fraude a través de canales digitales como es el correo electrónico. El INCIBE (Instituto Nacional de Ciberseguridad) alerta de dos modalidades de estafas o intentos de fraude a los que los conductores se ven expuestos más frecuentemente:

- Envío de falsas multas a través del correo electrónico suplantando al Ministerio del Interior con un asunto del tipo **“Bloqueo del Vehículo – Multa no pagada”**, donde aseguran que hay una sanción pendiente y que puede accederse a su notificación desde un enlace que dirige a una web externa desde donde, en realidad, se descarga un archivo comprimido (*zip*) que simula ser la multa y contiene el malware (software malicioso que va a infectar el ordenador con el fin de **robar datos, como los datos de la tarjeta de crédito utilizada en compras on line etc**).
- Debemos tener en cuenta que **la DGT indica que nunca notifica las multas de tráfico a través de correo electrónico**, si no que lo hace a través de correo certificado. En caso de fallar esta notificación (por ejemplo, el conductor ha cambiado su residencia y no lo ha notificado a la Jefatura de Tráfico) se comunica a través del TAU o del TESTRA o de los boletines oficiales o, si lo han solicitado, a través de la Dirección Electrónica Vial.
- Otra modalidad consiste en el envío de correos electrónicos en los que se avisa de la **presunta caducidad del permiso de conducir** y se solicitan datos tales como fotografía de las dos caras del DNI, del permiso de conducir e incluso una foto.

Ante esta situación, la DGT advierte a través de redes sociales que *“no se proporcione ningún dato ni pinches en ningún enlace en caso de recibir esta serie de correos. Elimínelos directamente”*.

Para evitar este tipo de fraude, el INCIBE nos informa de una serie de **consejos** que todos los usuarios deberíamos aplicar ante la llegada de cualquier correo que consideremos que puede ser sospechoso, del tipo que sea.

Son los siguientes:

- No abrir correos de usuarios desconocidos o que se no haya solicitado, y elimínelos directamente.
- No contestar en ningún caso a estos correos.
- Revisar los enlaces antes hacer clic, aunque sean de contactos conocidos.
- Desconfiar de los enlaces acortados.
- Desconfiar de los ficheros adjuntos, aunque sean de contactos conocidos.
- Tener siempre actualizados sistema operativo y antivirus (y que esté activo).
- Asegurarse de que las cuentas de usuario utilizan contraseñas robustas y no tienen permisos de administrador.

### » MISCELÁNEA DE CURIOSIDADES

Existen brigadas especiales encargadas de prevenir e investigar los delitos relacionados con la ciberseguridad como son:



- La Brigada de Investigación Tecnológica de la Policía Nacional.



- El Grupo de Delitos Telemáticos de la Guardia Civil.



- El Grupo de Apoyo Tecnológico de la Policía Foral de Navarra.



El spoofing viene del término inglés spoof, que significa suplantación. Los timos así llamado se basan en hacerse pasar por una persona o empresa con fines maliciosos, y para convencerte de hacer algo que ponga en peligro tu ciberseguridad.



Según el Ministerio del Interior, uno de cada cinco delitos se cometen en la red.



El número de estafas informáticas y cibercriminosos pasó de 277.599 en el periodo enero-septiembre del año 2022 a 337.251 en mismo periodo del año 2023 (un 21,5% más) según el Ministerio del Interior.