



Mensaje del falso hijo. FOTO: DT

que el barítono le dio total credibilidad. Le 'alertaban' de que estaba sufriendo una ciberestafa y le hicieron entrar en la aplicación del móvil. Siguió las indicaciones y, sin ser consciente, transfirió 5.000 euros a una cuenta de Turquía.

El responsable policial recalca que de las ciberestafas, las que más se dan son las del falso banco y el falso hijo. Las primeras, que se realizan a través de llamadas o mensajes de textos, se han mantenido estables. Si que se producen picos cuando la entidad de crédito o la empresa donde guardan los datos han tenido una filtración, como pasó el año pasado con Deutsche Bank, que conllevó centenares de denuncias en toda España. Con este tipo de engaños, los cibercriminales pueden llegar a conseguir hasta 60.000 euros. «Son *call center* de personas reales que simulan ser un banco. Y tienen 'muleros' que no saben lo que hacen realmente. Solo lo conoce la cúpula y los que están en medio de la cadena». Son grupos organizados, cu-

Las ciberestafas que más se dan son las del falso banco y el falso hijo

yos autores intelectuales algunos son de España y otros viven en Sudamérica o países del Este.

El cabo recuerda el caso de una víctima de Tarragona a la que quitaron 38.000 euros. El autor se hizo pasar por un banco, accedió a la banca *on line* de la víctimas y realizó una transferencia por Bizum. Asoció otro teléfono a la cuenta bancaria y lo utilizaba para los pagos. «Resultó difícil llegar hasta él». Era un vecino de Vilanova i la Geltrú con muchos arrestos anteriores. «Era un 'mulero' avanzado pero ya se atrevía a estafar por su cuenta». Fue imputado por estafa infor-

Un caso Un coche que no llegó: ocho meses de prisión

Una de las últimas sentencias que ha dictado la Audiencia Provincial de Tarragona por un delito de estafa tiene fecha del pasado 4 de febrero. El acusado ha sido condenado a ocho meses de prisión y a devolver a la víctima los 4.000 euros que había adelantado por la compra de un turismo que nunca vio.

El fiscal pedía para el encausado dos años de prisión y cinco o medio para un segundo procesado. Pero en este caso ha sido absuelto.

mática y falsificación y usurpación de estado civil.

Los falsos hijos o familiares

La estafa del falso hijo o familiar supone entre un 5 y un 10 por ciento del volumen de casos. Los autores envían un mensaje: «Hola mamá, se me ha estropeado el móvil. Ahora estoy usando este número. Puedes escribirme por WhatsApp? <http://wa.me/+34667536459>». Normalmente piden envío de cantidades de entre 1.300 y 1.500 euros, y pueden conseguirlo en varias transferencias.

Los autores del falso hijo utilizan la misma dinámica que en el caso de los bancos, pero la estructura no es tan grande. Unos envían los mensajes y los otros reciben el dinero. A una vecina de Tarragona le estafaron 8.000 euros. «Logramos detener a los cuatro intermediarios en Sabadell».

Actualmente, la Unitat d'Investigació del Mossos d'Esquadra del Tarragonès tiene abiertos dos casos de este tipo: uno de 1.000 euros y otro de 1.200. «Son investigaciones muy largas por la respuesta de los bancos. No todos contestan rápidamente».

El falso alquiler o vehículo

Hay otras estafas que también se sirven de las falsedades, como el del falso alquiler –lo que más se da–, el falso vehículo o el buen empleado. En el primero de los casos son web falsas –duplicadas de originales o bien creadas de nuevo– que muchas veces no solo sirven para conseguir dinero sino también información personal. Uno de buena fe vende una moto y pide el dinero por Bizum. El supuesto comprador –estafador– le dice que le hará un Bizum con parte del importe y el resto después. Pero pide que le envíe el DNI para verificar a quién está enviando el dinero. Y el delincuente, con dicho documento, tiene las puertas abiertas para abrir cuentas corrientes, realizar compras, pedir créditos, etc.

La sentencia declara probado que en mayo de 2018 se publicó un anuncio en la plataforma web Milanuncios. En el mismo se ofertaba un Volkswagen Tiguan 2.0 TDI por valor de 18.000 euros. Se indicaba el número de teléfono del vendedor, y con posibilidad de comunicarse con él desde la propia página web.

El denunciante se interesó por dicho vehículo y contactó con el supuesto vendedor a través de la página web, facilitando su número de teléfono.

El día 28 del mismo mes, sobre las diez de la mañana, el ahora condenado contactó con el comprador en varias ocasiones, tanto por llamada como por

WhatsApp –a través de un número de teléfono diferente al del anuncio– para culminar la transacción. Apremiaba al denunciante a adelantar la cantidad de 4.000 euros en concepto de reserva, so pretexto de que había varias personas interesadas en el vehículo.

La víctima transfirió 4.000 euros una cuenta bancaria, cuyo titular era el ahora condenado. Dicha cantidad de dinero ingresada fue extraída en una sucursal bancaria. Finalmente, poco después de haber realizado la transferencia, el denunciante recibió una llamada del teléfono del supuesto vendedor. «Te han timado tonto» e «imbécil», le dijo.

Las denuncias 2024 por Área Básica Policial

Comisaría	Casos conocidos	Resueltos	Detenidos
Tarragonès	3.868 (4.016)	437 (411)	92 (48)
Baix Camp-Priorat	2.838 (2.961)	319 (267)	59 (43)
Baix Penedès	1.692 (1.795)	169 (151)	28 (22)
Baix Ebre	1.297 (1.314)	148 (160)	19 (12)
Montsià	975 (1.086)	111 (125)	16 (8)
Alt Camp-Conca	947 (956)	97 (127)	11 (2)
Ribera d'Ebre-Terra Alta	319 (367)	39 (34)	4 (1)
TOTAL	11.936 (12.495)	1.320 (1.275)	229 (136)

ENTRE PARENTESIS, LOS DATOS DE 2023

FUENTE: MOSSOS D'ESQUADRA

Y es que portales de compra-venta de objetos se han convertido en un sistema para captación de datos personales.

Si el objetivo es conseguir dinero, por una moto que se vende por entre 3.000 y 4.000 euros, el delincuente puede conseguir estafar entre 500 y 1.000.

Son denuncias que se van recibiendo periódicamente y que, por ejemplo, este año ya han llegado a la comisaría de Tarragona.

La estafa del buen empleado consiste en llamar al trabajador de una empresa –del que saben datos– diciendo que conocen a su jefe y que este ha dicho que envíe un dinero o, de lo contrario, le van a poner una multa.

El seductor virtual

El seductor virtual –o falso amante– consiste en establecer una relación social con una persona a través de las redes sociales. Cuando ya se ha establecido una conexión, el estafador (o estafadora) empieza una manipulación psicológica y emocional. Y comienza a pedir dinero con cualquier excusa: que tiene que operar a su hijo, para realizar una inversión, una enfermedad, etc.

La Unitat d'Investigació del Tarragonès resolvió el año pasado uno de estos casos. La víctima era un hombre de 70 años vecino de Salou. Le estafaron 70.000 euros, por lo que incluso tuvo que pedir un préstamo. Eran dos

mujeres, vecinas de Huelva –fueron detenidas por la Guardia Civil a requerimiento de los Mossos–. Una estableció el vínculo y la otra recibió el dinero a través de diversos envíos.

Los 'mailers'

En el caso de los *mailer*, el delincuente tiene información de las transacciones comerciales entre dos empresas. Y él se pone en medio. Dice que sabe que una de estas tiene que enviar dinero a la otra pero le dice que ha cambia-

Un vecino del Baix Gaià perdió 700.000 euros con el timo de los falsos inversores

do el número de cuenta. Y se lo comunica a través de un correo cuya dirección tiene cambiada una sola letra. La víctima lo envía y ya ha caído en la trampa.

Por otra parte, el falso inversor son plataformas o personas a título personal que realizan anuncios a través de las redes sociales para captar a las víctimas. Estas invierten dinero y van teniendo ganancias, por lo que van incrementando la inversión. Cuando la cifra es alta, los estafadores se quedan con el dinero. El año pasado, un hombre mayor de la zona del Baix Gaià perdió 700.000 euros. No los recuperó.

Consejos

- Verifique la autenticidad de los correos. En los correos electrónicos, por ejemplo, las direcciones sospechosas suelen tener errores tipográficos o dominios desconocidos. En el caso de los sms revise el contenido del mensaje en busca de enlaces con dominios parecidos al de la supuesta empresa emisora del mensaje, pero no exactamente iguales.
- Utilice contraseñas fuertes y únicas para cada una de sus cuentas. Una contraseña fuerte debe tener al menos ocho caracteres e incluir una combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
- Active la autenticación en dos pasos siempre que sea posible. Este método añade una capa extra de seguridad al requerir dos formas de verificación para acceder a tu cuenta.
- Mantenga su software y sus aplicaciones actualizados. Las actualizaciones suelen incluir parches de seguridad que protegen contra las últimas amenazas.
- Consulte fuentes oficiales en caso de duda. Si no estás seguro de la autenticidad de un mensaje, contacta con la empresa a través de sus canales de comunicación oficiales.

La amenaza No ha llegado la IA... por ahora

El cabo de la Unitat d'Investigació del Tarragonès de los Mossos d'Esquadra asegura que, por ahora, no han detectado en ninguna denuncia en la que los delincuentes hayan utilizado la inteligencia artificial para cometer la estafa. Es consciente de que el momento llegará, y seguramente pronto. Si ahora es difícil investigar estos casos, cuando se suplanten voces será todavía más complicado.

Con la llegada de la IA, los fraudes, estafas y suplantaciones de identidad van a agravar todavía más la problemática, al generar contenidos falsos que, en ocasiones, uno no podrá o no sabrá diferenciar entre lo real (hecho por el humano) o por un ordenador.

Ante una llamada o un mensaje de voz, antes de reaccionar, ponerse en contacto con la supuesta persona que está en apuros o a la que presumiblemente han suplantado.