'VISHING'

LA LLAMADA DE LA RUINA

Policía y oficinas de consumidores alertan del 'boom' de esta técnica delictiva usada para robar datos personales y bancarios. Esta estafa se aprovecha hoy de los altos precios de la luz y el gas y de la inquietud por la guerra en Ucrania

JORGE BENÍTEZ

«No tenía que haber cogido esa llamada», dice María B, de 51 años. Esa es la frase más repetida entre las víctimas de una técnica de engaño conocida como *vishing* que hace estragos en España y que inquieta tanto a la Policía como a las organizaciones de consumidores.

Se trata de un fraude que consiste en una llamada telefónica realizada para obtener datos personales o bancarios de una persona. Con el *vishing* –término que combina las palabras inglesas *voice* (voz) y *phishing* (estafa mediante un enlace web o un SMS)–, los delincuentes suplantan una identidad de una compañía reconocida o incluso de un organismo público para generar confianza en la víctima y hacerle picar el anzuelo.

La última estrategia de estos estafadores conocidos como *vishers* es aprovechar la incertidumbre generada por los desaforados precios de la luz y el gas de este invierno, a los que se ha añadido la perspectiva desoladora de la guerra de Ucrania y su influencia en el mercado. La energía es hoy un disfraz ideal para este delito. Pero no hay que olvidar que por las garras de estos suplantadores pasan también bancos, telefónicas, la Seguridad Social e incluso la OCU.

«Cualquier acontecimiento extraordinario que genera una carencia o una inusual demanda, como sucedió hace dos años con las mascarillas y como genera hoy la guerra, favorece la proliferación de estafas», reconoce Carlos J. Juárez, inspector jefe de la Policía especializado en fraude en el uso de telecomunicaciones. «En este engaño siempre se ofrece una solución ventajosa a un problema, a sabiendas de que muchas personas serán receptivas».

María B. fue víctima del *vishing* en su modalidad de la *doble llamada*. Su único *pecado* fue querer pagar menos por la factura de la luz.

Primero contactó con ella alguien que se identificó como miembro del servicio de atención al cliente de su compañía de energía para darle una mala noticia: la coyuntura hacía que su tarifa fija fuera a costarle 25 euros más. Diez minutos después, otro timador, conchabado con el primero, interpretaba en una segunda llamada el papel de un comercial de otra compañía para ofrecerle un descuento del 25% sobre lo que venía pagando en su factura.

En la conversación éste demostró tener mucha información sobre María: además de su nombre sabía su número de DNI. A lo largo de la de conversación recordó insistentemente que era el último día de vigencia de esta oferta.

Finalmente María, que no tiene un gran sueldo, aceptó y facilitó el número de su cuenta corriente. A continuación, como le indicó el comercial, recibió un SMS sin ninguna identificación de la supuesta compañía al que, siguiendo sus instrucciones, debía contestar con un «SI».

En este caso y en otras denuncias, al otro lado de la línea se emplea siempre un mismo estilo: mucha verborrea y muchas prisas. Una mala interpretación actoral del delincuente puede delatar sus intenciones. «Se habla con la víctima en tiempo real y por tanto éste debe ser capaz de responder de forma convincente a las preguntas que pueden surgir durante la conversación», explica Juárez. «Es por tanto una situación en la que la víctima podría percatarse del engaño si el defraudador no tiene a mano los argumentos necesarios»

Algo mosqueada tras colgar, María contactó con su compañía de gas de toda la vida. Esta le confirmó que seguía siendo cliente y que no iban a subir su tarifa. Además, le aclaró que un cambio de precio nunca sería comunicado por una llamada de ese tipo.

A María le habían hecho un *tocomocho* telefónico.

«El *vishing* es como un cajón de sastre donde confluyen muchas modalidades», explica Manuel Merino, abogado de la Asociación Nacional de Afectados de Internet y otras tecnologías. En su rama más turbia es utilizado por delincuentes para robar dinero de las cuentas o por Bizum, pero también se han denunciado casos del uso de sus técnicas en agresivas campañas de telemarketing de comisionistas que buscan cazar clientes de compañías dando información falsa, como puede ser un corte de suministro.

«En ambos casos se produce un engaño», recalca Ileana Izverniceanu, directora de Comunicación de la OCU, que aclara que en el segundo caso no es un caso típico de *vishing*, pero que el objetivo es el mismo: empleo de llamada telefónica con un mismo fin: fraude al consumidor.

Sin duda los más vulnerables para caer en la trampa son nuestros mayores, que en muchos casos son los más sensibles a las subidas de precios y además no controlan muy bien su teléfono móvil. Pero cualquiera puede ser víctima.

Entre los casos rastreados por la Agencia de Protección de Datos está el modelo conocido como *a puerta fría*, que consiste en que el infractor pide a los titulares una factura de un servicio con el argumento de rebajar su importe. «Los comercializadores recogían los datos personales de la factura y procedían a realizar cambio de contrato a otra compañía», explican fuentes de la APD.

Según las tres últimas memorias publicadas por este organismo, la última de 2020, las sanciones impuestas a empresas con esa forma de captación fraudulenta superan los seis millones de euros.

Para evitar disgustos con el *vishing* del robo o del comercial sin escrúpulos los expertos consultados dan una lista con las siguientes recomendaciones:

-No dar nunca información confidencial por SMS o teléfono.

-Desconfíe de llamadas o SMS en que se menciona algo urgente o algo demasiado atractivo.

-No acceda a ninguna dirección web de un mensaje que de un número de teléfono desconectado.

-Introduzca sus datos confidenciales sólo en páginas seguras que comienzan por *https* y provengan de un dominio conocido.

Como primera herramienta de desconfianza, es importante saber cómo funcionan los servicios de atención al cliente y los del servicio técnico de una empresa. Su misión es resolver dudas o problemas, no al contrario. Se les llama a ellos, no al revés. Que se lo digan a las pobres víctimas del supuesto empleado de Microsoft, que te llama sin haberlo requerido para informarte de un problema en tu ordenador y te instala en remoto un virus que lo bloquea. Su solución es un chantaje: paga y volverás a poder usarlo.

Ante estas amenazas, la Guardia Civil informa en su web de una *defensa-personal* muy útil para desarmar al sospechoso que llama: «Si la víctima realiza preguntas que el operador no sabe responder o pone en duda su credibilidad, este último procede a colgar la comunicación».

Si te cuelgan, está claro: es un *visher*.

Pero, ¿por qué te ha llamado a ti? Manuel Merino describe cómo se eligen sus víctimas los piratas del *vishing*. Hay una forma de selección tosca que consiste en llamadas a diestro y siniestro para ver si alguien pica. Se utiliza cuando el timador no sabe de qué compañía eres cliente y busca sacarte esa información con un interrogatorio. Otra es mucho más sofisticada porque es personalizada. «Implica que tienen en su poder tus datos y estás identificado», dice Merino. Tu nombre no ha salido de forma fortuita, van por ti.

El sector bancario es uno de los más perjudicados

EL ANZUELO. "EN ESTE ENGAÑO TELEFÓNICO SIEMPRE EL DELINCUENTE SE OFRECE UNA SOLUCIÓN VENTAJOSA A UN PROBLEMA, A SABIENDAS DE QUE MUCHAS PERSONAS SERÁN RECEPTIVAS", DICE CARLOS J. JUÁREZ, INSPECTOR JEFE DE LA POLICIA

por el *vishing*. Bien directamente, cuando se llama en nombre de una entidad concreta, o como estación final del timo: cuando el ciberdelincuente ha obtenido los datos de la cuenta o la tarjeta.

La proliferación de casos ha hecho que en las webs de 10 bancos consultados todos alerten del *vishing*.

«En los fraudes de este sector siempre se envía un SMS alertando de una operación sospechosa que se acompaña de un enlace de una falsa página web donde el cliente introduce sus credenciales de acceso», explica Juárez. De esta manera, los ladrones ya pueden entrar en la banca *online* y realizar transferencias, contratar créditos y hasta adquirir criptodivisas. El problema (para ellos) es que ahora necesitan una segunda verificación.

Entonces es cuando recurren al *vishing*.

«Ya en el paso previo se avisa a la víctima de que en breve recibirá una llamada del banco para completar el bloqueo de la cuenta y evitar la salida de los fondos», prosigue Suárez. «Esta llamada se produce y una persona que dice ser empleada del banco solicita los códigos que le están llegando en ese momento a la víctima y que una vez en poder del defraudador permiten completar las operaciones bancarias no autorizadas».

Entonces ya está. Los malos ganan por K.O.

En el caso de María, los timadores contaban con información sobre ella. ¿Cómo la consiguieron? Cuando se le pregunta a Merino, el abogado se ríe. «Hay muchas rutas», dice. «Pueden sacarlos de la *deep web*, donde se trafica con datos de consumidores, de un empleado de una compañía que tengan comprado para que les pase información de clientes o incluso facilitados por la propia víctima si esta ha pinchado en un email infectado». Y hace una aclaración: «Pero esta recolección no tiene que ser siempre ilegal, puede que el cliente se los haya facilitado de forma torpe».

Al margen de una imprudencia individual, la APD es tajante respecto a la posibilidad de que los datos salieran de compañías a las que hemos contratado algún servicio: éstas tienen la obligación de protegerlos.

Muchas han demostrado lagunas al respecto. Como ha quedado patente con el caso del SIM Swapping que ha desembocado en multas muy importantes por no dar las garantías suficientes de seguridad. En ese caso el ciberdelincuente duplica un número de teléfono y la tarjeta SIM para usurpar nuestra identidad. Se identifica en nuestro banco y roba el dinero.

Pero regresemos a la víctima concreta. ¿Qué es lo que debería hacer María?

«Hay que verificar con el banco si ha sido víctima de un fraude y si lo ha sido, solicitar la anulación de cualquier movimiento realizado en su cuenta sin su autorización», explica el inspector jefe Juárez. «Deberá solicitar la cancelación de tarjetas si la hubiera dado y el cambio de contraseña de la banca *online* y si fuera el caso, de la firma digital que algunos bancos solicitan».

Además hay expertos que recomiendan buscarse a uno mismo por internet para comprobar si aparecen sus datos personales en páginas web que le resulten ajenas. Si el timo se hubiera efectuado a control remoto, como en el caso del técnico de Microsoft, hay que desinstalar la aplicación sospechosa y pasar un antivirus por todo el sistema operativo.

Esto no es todo. Queda un trámite tedioso pero que puede evitar dramas futuros: denunciar ante la Policía o la Guardia Civil. «Es importante presentar capturas de pantalla de los mensajes recibidos, extractos bancarios y cualquier información que permita acreditar los hechos y ofrecer algún indicio sobre los posibles autores», recomienda Juárez.

La próxima vez que suene el teléfono recuerde ese dicho que parece trasnochado desde que España entró en el euro: nadie da duros a pesetas.

SUPLANTACIÓN DE IDENTIDAD. LOS DELINCUENTES SE HACEN PASAR POR REPRESENTANTES DE GRANDES COMPAÑÍAS ELÉCTRICAS, TELEFÓNICAS, BANCOS Y HASTA DE ORGANISMOS PÚBLICOS COMO LA SEGURIDAD SOCIAL PARA GENERAR CONFIANZA

UN 'TRUCO' PARA DEFENDERTE DEL ESTAFADOR TELEFÓNICO. "SI LA VÍCTIMA LE HACE MUCHAS PREGUNTAS AL SOSPECHOSO PARA CONFIRMAR SU IDENTIDAD Y NO SABE CONTESTAR O SE CONTRADICE, COLGARÁ EL TELÉFONO SI ES UN 'VISHER'"