Así es un fraude online paso a paso: "Quería romperle las piernas, pero ni siquiera era quien decía ser"

En 2020 hubo en España más de un cuarto de millón de estos delitos, cuatro veces más que en 2016

Autor: **Jordi Pérez Colomé**

“Poca cosa voy a decir, no lo adornaré, que llevo una mala virgen con esto que si sé quién es lo fulmino de un palizón”, dice por teléfono una víctima de fraude por internet. No quiere revelar su identidad, más allá de que es propietario de una pequeña empresa de Huesca. Un día recibió por correo electrónico una factura real de 14.500 euros de un proveedor suyo. Transfirió el dinero al número de cuenta indicado. Al día siguiente el proveedor no había recibido nada. ¿Qué había pasado? La cuenta que ponía en el e-mail no era la del proveedor. Había ingresado 14.500 euros en la cuenta de un desconocido.

El empresario fue corriendo a la policía y a su banco. La denuncia sirvió para bloquear la cuenta de destino, pero ya quedaban solo algo más de 3.000 euros. El dinero se había esfumado. Esto ocurrió en junio de 2020. Poco después se encargó del caso Carlos Solano, economista que colabora en el despacho local Sáez-Benito & Calvo. “Al principio [mi cliente] quería romperle las piernas al que había recibido el dinero. Suerte que le dije que lo más probable era que le hubieran suplantado la identidad”, dice Solano en conversación con EL PAÍS en Huesca.

El dinero de Huesca voló a una cuenta abierta con el nombre de un joven de Tarragona, que aparentemente vivía en Coslada (Madrid), donde el banco mandó una tarjeta de crédito. Con esa tarjeta se extrajo dinero en Viena (Austria) y el resto se transfirió a otra cuenta, presuntamente de una joven de Castellón. Ahí se pierde casi toda la pista del dinero y de los delincuentes.

Solano ha tirado de todos los hilos para ir sacando información a cuentagotas de policía y bancos. Este periódico ha reconstruido con su ayuda el caso paso a paso para entender la tremenda complejidad del fraude online y por qué es una terrible lacra para miles de ciudadanos españoles. La pérdida del DNI, compartirlo por engaño con un desconocido por internet o caer en una trampa y entregar la contraseña del correo electrónico de la empresa a un tercero pueden ser el inicio de un calvario mucho peor que el de un robo tradicional.

En 2016 hubo en España 70.178 casos conocidos de fraude informático, según un informe del Ministerio del Interior. En 2020 esa cifra se multiplicó casi por cuatro y alcanzó los 257.907 casos. Los fraudes son el 90% de los ciberdelitos en España, que suman casi 288.000. De estos, solo en 11.280 hay alguna persona investigada o detenida.

“Me la suda que sea una banda organizada. Si me entero de algún nombre, lo encontraré y lo pagará con creces. No confío en la justicia”, dice la víctima del fraude. Como prueban las cifras de casos resueltos, es extremadamente improbable que ocurra.

Todo empezó un viernes del verano de 2020. Recibió un e-mail real con una factura de 14.500 euros pero con las cifras de la cuenta corriente cambiadas. ¿Cómo puede ser que alguien tenga un acceso tan directo a una bandeja de entrada? No es nada raro, dicen en el Incibe, el instituto de cibercrimen español que se ocupa de las pymes. “Es un caso de fraude de BEC [compromiso del correo de la empresa, en sus siglas en inglés]”, dice Jesús García, técnico en ciberseguridad del Incibe. El delincuente obtiene las contraseñas con ingeniería social: el típico correo falso de “alguien ha entrado a tu correo, cambia las claves”. Con ese acceso, observan los correos que entran. Cuando uno es una factura, borran el original, copian y pegan todo idéntico menos el número de cuenta corriente y lo mandan de nuevo copiando incluso el nombre del emisor.

No es banal, pero no hay que ser un hacker para hacer esto. “Tienes que saber algo de español y debes hacer un análisis de los correos, lleva trabajo”, dice García. A la víctima de este caso intentaron estafarle en otro correo, pero los delincuentes se dejaron el nombre del titular de la cuenta corriente, que no coincidía con el proveedor. Es una prueba de su falta de sofisticación.

De Huesca a Tarragona

Mientras esto ocurría en Huesca, otra víctima caía en las redes de esta banda. Un joven repartidor de pizza de 25 años en Tarragona respondía a un anuncio en la página Jobandtalent. La oferta era un caramelo: 2.000-2.500 euros al mes, coche cedido, horas trabajadas en fin de semana pagadas el doble. Aparte de una oferta tan extraordinaria, había otros elementos que podían despertar sospechas: el e-mail era del tipo nombre.apellido2015(@)gmail.com, el nombre de la empresa no aparecía y la ciudad donde repartir, tampoco. Pero era la época posterior al confinamiento y las ofertas de empleo escaseaban.

Cuando el joven dio su DNI por las dos caras y su número de cuenta corriente, la “empresa” dejó de responder a sus mensajes. Acababan de robarle la identidad. Con esos datos, los delincuentes le suplantaron la identidad y crearon cuentas online en tres bancos. El dinero de la empresa de Huesca pasó por una de ellas.

Al cabo de unos meses, lo siguiente que supo el joven de Tarragona de aquella oferta fue una llamada de la Guardia Civil. Debía ir a la comandancia y quedarse detenido. Solo sus abogados lograron sacarle de ahí. En el casi año y medio que ha pasado, según sus abogados Héctor Calero y Alejandro Caballero, este joven ha tenido dos procesos en Madrid y uno en Gandesa, Huesca, Pamplona y Guadalajara. Excepto el caso de Huesca, todos fueron por estafas de falsos alquileres vacacionales, donde las víctimas pagan por adelantado una cantidad a modo de reserva. La cantidad de Huesca fue la más alta, con diferencia.

“A quien le toca enfrentarse a procedimientos por toda España teniendo un sueldo de 800 euros como repartidor de pizza con la moto, no le hace ninguna gracia”, dice Calero. Eso sin contar que la víctima de Huesca buscaba a alguien a quien partir las piernas y el único candidato que había era su nombre, hasta que quedó claro que su identidad había sido suplantada.

Solano pidió el número de teléfono con el que el banco ratificó la cuenta donde acabó el dinero de su cliente. Le dieron un número. La policía le confirmó que en el móvil desde el que se había usado también había otros ocho. La policía encontró que eran ciudadanos que usaban documentos rumanos, pero la policía de Rumania dijo que eran numeraciones falsas. Solano introdujo los números de teléfono en su WhatsApp. Tres números seguían activos, alguno con el estado de WhatsApp en español. Cuando Solano escribió a uno de ellos, le bloquearon. La jueza dijo que la policía había dicho que era imposible encontrarles. Ahí moría otro hilo.

La sensación del economista Solano y el abogado Calvo de Huesca y Calero y Caballero de Tarragona es que estos casos no paran de crecer. Los tribunales los conocen bien pero por la dificultad de esclarecer los hechos y las cantidades, lograr algo es complicado.

Solano ha calculado las comisiones que recibió un banco y la entidad de crédito en una de las cuentas suplantadas: “Sacaron 18.500 euros en efectivo. Hubo cargos por 19.300. La diferencia es el 4,5% de comisiones: 832 euros generados en comisiones para el banco por extracciones a repartir entre ambas compañías. En una cuenta con nada domiciliado, solo de meter y sacar dinero. Solo con eso, 832 euros de negocio bancario”, explica.

En verano de 2021, el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (Sepblac) advirtió sobre el fraude en estas cuentas online. El BBVA, consultado por este periódico, eliminó la opción de abrir una cuenta por internet solo por tener otra en otro banco. Ahora exige un selfie o una videollamada. El OpenBank, también consultado, permite aún abrir una cuenta en su entidad a partir de una cuenta en otra, pero exige que se demuestre acceso a ella: el banco manda un código en el concepto de una transferencia para comprobar si el usuario puede entrar y verlo. Es similar al sistema de ING, que manda una transferencia de céntimos y el cliente debe decir de cuánto es.

Son medidas necesarias para disminuir una lacra que afecta sobre todo a ciudadanos que por algún motivo han clicado sin querer en un enlace o han dado unos documentos innecesarios tras ser engañados. Tanto la administración como los bancos exigen más concienciación y controles a la ciudadanía, pero los malos suelen ir algún paso por delante: su trabajo es buscar agujeros en el sistema. “Los bancos dicen que la culpa es de sus clientes, que es lo que me decía a mí la directora de la entidad de mi cliente, que ellos no tenían la culpa de que le hubieran estafado”, explica Solano. “Y yo le decía, cierto, pero que hayan usado su negligente infraestructura bancaria respecto a verificación de identidades no es culpa de mi cliente, sino vuestra”, añade.

Su cliente, sin embargo, tiene tiempo para pocas historias. “Hay tantos casos que no les prestan la atención que deberían, los bancos pasan, queda la justicia por tu mano”, dice. El caso de Huesca sigue en la vía penal. Luego llegará a la vía civil, donde esperan ganar y recuperar el dinero por la negligencia bancaria.

Fuente: El País

Hay, sin embargo, algo que chirría a todos: ¿cómo puede ser tan sencillo abrir una cuenta online en un banco grande? Solano hizo la prueba en febrero de 2021. Necesitó un DNI, un teléfono y una cuenta en otro banco a su nombre. Nada más. Era un coladero. En el caso del joven de Tarragona, con su número de cuenta y DNI, que le pidieron en la falsa oferta de trabajo, los criminales ya tenían todo lo que necesitaban. Con esa información podían suplantar la identidad en otros bancos. Los abogados del joven de Tarragona han pedido al Banco de España que les diga si hay más cuentas a nombre de su cliente que no hayan localizado. No han recibido respuesta por ahora.