MESA REDONDA

MARTES
6 DE JUNIO
16:30 H

DELITOS TECNOLÓGICOS Y PHISHING

ONLINE
PRESENCIAL

JESÚS GÁLVEZ
RESPONSABLE RESPUESTA
INCIDENTES CAJAMAR

DIEGO TOMÁS MARTÍNEZ
INSPECTOR DEL CUERPO
NACIONAL DE POLICÍA

ICAMUR
Ilustre Colegio de la Abogacía de Murcia

El Banco de España advierte en su página web -clientebancario.bde.es- que el aumento del comercio electrónico, una banca cada vez más digitalizada y el creciente *uso de* la tarjeta como medio de pago son aprovechados por los ciberdelincuentes para conseguir tus datos bancarios. El cebo o artimaña de mensajes como: "*su cuenta ha sido bloqueada o va a serlo de forma inminente*".

Recientemente, el 12 de enero de 2023, ha entrado en vigor la Ley Orgánica 14/2022, de 22 de diciembre, de transposición de directivas europeas y otras disposiciones para la adaptación de la legislación penal al ordenamiento de la Unión Europea, que entró en vigor el 12 de enero de 2023.

Como relata su Exposición de Motivos la relevancia de los delitos informáticos ha sufrido un crecimiento exponencial a lo largo de los años, como consecuencia del incremento del denominado ciberespacio y el consecuente aumento de la ciberpoblación en el ámbito de Internet.

El artículo primero modifica, entre otros los artículos 248 y 249 del Código Penal. En particular el artículo 249.1.a) y b) castiga a los que consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro o utilicen de forma fraudulenta tarjetas de crédito o débito.

En los delitos de manipulación o estafa informática no es precisa la concurrencia de engaño alguno, como sostiene el Tribunal Supremo [08/05/2020].

Insertas en el tipo encontraríamos aquellas estafas que nos afectan como titulares de cuentas bancarias. En particular, hemos sido objeto de sustracción de los datos de acceso, claves o credenciales e información personal que conllevan que un tercero suplante nuestra identidad y opere con los depósitos realizando transferencias, extractos o copiando tarjetas, entre otras prácticas ilegales.

Todo comienza al recibir en nuestros dispositivos un SMS, correo electrónico, llamada o similar. Si nos tragamos el anzuelo, el delincuente nos conduce de la mano a una web clonada que simula la de la entidad y nos invitan a entrar tecleando las claves de acceso.

Lo habitual en el delito de *phishing* es que actúen de manera coordinada varias personas; por un lado el denominado *phisher*, y por otro el/los «mulero/s bancarios» que han proliferado en los últimos años [APMU 35/2022, 01/02]. En cuanto a la figura del «mulero» estos son personas que, a cambio de una comisión, reciben en una cuenta bancaria el dinero que se ha obtenido por medio de la estafa informática y que debe transferir el dinero al estafador.

Pudiera pensarse que el único responsable es el usuario, pero no es así. Éste únicamente está obligado a adoptar todas las medidas razonables a fin de proteger sus credenciales y a notificar al proveedor el extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada [41].

En este punto conviene tomar en consideración el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera. En caso de que se ejecute una operación de pago no autorizada, el artículo 45.1 señala que el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación.

El Banco suele subrogarse en la posición del perjudicado, apareciendo como acusador particular y ejercitando la pertinente acción civil. Si no devuelve las cantidades objeto de las transferencias inconsentidas puede resultar condenado como responsable civil subsidiario [APV 335/2016, 26/05].