

## DICCIONARIO PARA EJECUTIVOS

### «Phising»

**YANIRE BRAÑA**

PROFESORA DEL IE

Cualquier cliente de banca «on line» ha podido recibir, especialmente en estos dos últimos años, un mensaje, una llamada e, incluso, un correo electrónico, aparentemente de su entidad financiera, encaminados a la obtención de sus datos personales.

El «phishing», un término acuñado en los años 90, es una modalidad de estafa encaminada a intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Mediante el envío masivo de mensajes o correos electrónicos, donde se suplanta la identidad de una empresa o entidad financiera, se pretende hacer creer a la víctima que la información solicitada procede del sitio oficial, con la intención clara de obtener sus datos, y poder así lucrarse. Este hecho delictivo, además del im-

pacto negativo que supone sobre la confianza de los usuarios en Internet, se ha incrementado en un 28% respecto al 2004, que costó 990 millones de euros a las compañías financieras americanas.

En España, el sector financiero es el destinatario del 86% de los ataques aunque también ha afectado a instituciones como el INE o empresas como Ebay o PayPal. Los clientes de banca «on line», son los más expuestos a los riesgos que conllevan este tipo de estafas, encaminadas a obtener todos los datos posibles para poder ser usados de forma fraudulenta. A pesar de las diferentes variantes o canales que pueden ser utilizados para este tipo de delitos, el caso más habitual se basa en el envío de un e-mail, que en la mayor parte de las ocasiones va acompañado de un enlace a la supuesta web de la entidad financiera defraudada. El «phishing» basado en el envío masivo de correos electrónicos o incluso SMS, se ha convertido en un ac-

to tan habitual, que se está pasando a llamar «emishing» o «móvil phishing».

Existen motivos para el optimismo en la lucha contra este tipo de fraude, a pesar del importante número de entidades financieras que se han visto recientemente afectadas, así como el creciente grado de sofisticación que está adquiriendo. Esto se debe fundamentalmente a varias razones. Además de las técnicas propias de la inteligencia artificial, que permiten identificar modificaciones en los correos electrónicos no solicitados (también denominado «spam») y establecer criterios de filtrado, existen reco-

mendaciones y nuevas prácticas preventivas de este tipo de actos fraudulentos. Los usuarios cada vez son más conscientes de que, al igual que procuran tener a buen recaudo sus tarjetas de crédito físicas y sus datos personales asociados a la misma, también evitan acceder a la banca online o realizar transacciones financieras desde lugares públicos como universidades o Ciber-Cafés.

Este fenómeno está generando nuevas fuentes de ingresos para muchas empresas. Conscientes de la importancia de preservar la seguridad de la información, especialmente para las instituciones financieras y usuarios de banca «on line», muchas están ofreciendo nuevas soluciones y recomendaciones tanto tecnológicas como no, encaminadas a mantener la confidencialidad, identidad e integridad de la información por medios electrónicos. A su vez, los delitos cometidos a través de medios electrónicos, están duramente penalizados.

**«Este  
fenómeno está  
generando nuevas  
fuentes de  
ingresos para  
muchas empresas»**