# *Phising, nous models de delictes informàtics*

Habitualment relacionem el mon d'internet als avenços. Compra on-line, recerca, publicitat, mon laboral, i també gestions financeres. Però internet també és un espai per delinquir. Un nou àmbit on poder, per exemple, robar. I un dels sistemes per fer-ho és mitjançant l'anomenada tècnica del phising.

**El terme *phishing* prové del mot anglès " *fishing*" (pesca), fent al·lusió a l'intent de fer que els usuaris d'internet "mosseguin l'ham".** A qui el practica se li diu *phisher.* La majoria dels mètodes de *phishing* utilitzen la manipulació en el disseny del correu electrònic per aconseguir que un enllaç sembli una ruta legítima de l'organització per la qual es fa passar l'impostor. En un altre mètode popular de *phishing*, l'atacant utilitza contra la víctima el propi codi de programa del banc o servei pel qual es fa passar.

**Aquest tipus d'atac resulta particularment problemàtic, ja que dirigeix l'usuari a iniciar sessió en la pròpia pàgina del banc o servei, on la adreça de la web i els certificats de seguretat semblen correctes.** En aquest mètode d'atac els usuaris reben un missatge dient que han de "verificar" els seus comptes, seguit per un enllaç que sembla la pàgina web autèntica; en realitat, l'enllaç està modificat per realitzar aquest atac, a més és molt difícil de detectar si no es tenen els coneixements necessaris.

**Els danys causats pel *phishing* oscil·len entre la pèrdua de l'accés al correu electrònic a pèrdues econòmiques substancials.** Aquest tipus de robatori d'identitat s'està fent cada vegada més popular per la facilitat amb què persones confiades normalment revelen informació personal als *phishers*, incloent números de targetes de crèdit i números de DNI. Un cop aquesta informació és adquirida, els *phishers* poden usar dades personals per a crear comptes falsos utilitzant el nom de la víctima, gastar el crèdit de la víctima, o fins i tot impedir a les víctimes accedir als seus propis comptes.

**Davant d'aquests fets el primer que s'ha de fer és posar-se en contacte amb la entitat bancària. Si no trobem la solució el següent pas és adreçar-se a un Servei de Consum més proper (OMIC). I en darrer cas accedir a la via judicial.** Cada cop més sentencies judicials donen la raó al consumidor doncs només les entitats bancàries tenen els recursos per impedir aquests delictes, assegurant la identitat del ordenant (per evitar que sigui impostor) o implementant mesures de seguretat més eficaces.

Però **som els consumidors els primers que hem de tenir molta cura en obrir aquests correus electrònics.** I si desconeixem l'origen o els correus tenen una aparença "sospitosa" cal informar-se abans d'obrir-los.