

Phishing

Desde hace tiempo, se vienen produciendo intentos de estafa a usuarios de servicios de banca en web de entidades financieras, algunas españolas. Para ello, los delincuentes están utilizando un caso concreto de suplantación, bautizado por los fisgones como *phishing*, vocablo que no tiene traducción al español.

El *phishing* es un caso específico de suplantación de la página web de un banco o caja para mediante el engaño, solicitar al cliente por correo electrónico, so pretexto de una confirmación del propio banco o caja, su nombre de usuario y contraseñas para acceder a sus cuentas y desplumarle. Para poder hacer esto, el delincuente debe conocer la dirección de correo electrónico del usuario en cuestión. (Este es uno de los asuntos más interesantes en el fenómeno).

Ya en septiembre de 2003 la entidad norteamericana Office of the Comptroller of the Currency (OCC) alertó del asunto a las entidades financieras, instándoles a tomar medidas para proteger a los clientes ante este tipo de delito.

La pregunta que conviene hacerse hoy es ¿qué tipo de medidas hay que tomar? ¿Sólo informativas, o merece la pena hacer un esfuerzo tecnológico generalizado para renovar los mecanismos de autenticación débil actualmente en uso de forma generalizada (números de contratos, contraseñas... etc.). Quizás la manera de salir menos en los papeles por hechos que no fomentan la confianza en el ámbito telemático, sea invertir en información para los clientes, y también dotar a los servicios de banca en web de mecanismos de seguridad robustos, porque una cosa puede aventurarse sin temor a error: que los estafadores tienen mucha imaginación. La historia lo confirma. ●