Asociación de Internautas

Phising: Seis millones de correos a la pesca de claves bancarias

Conseguir las claves de miles de cuentas bancarias es el objetivo de un nuevo tipo de estafa, el llamado 'phising', un método que consiste en enviar hasta seis millones de correos electrónicos de una tacada, en los que se simula ser un banco respetable para 'pescar' a los clientes más confiados.

Esos correos aparentan proceder de una entidad real que pide a sus clientes que confirmen sus datos y sus contraseñas pero, en realidad, los envían grupos de estafadores que intentan capturar esos datos para hacerse con los ahorros que sus víctimas tienen depositados en el banco.

Prácticamente, ninguna entidad española se ha librado de uno de estos ataques indiscriminados, que se han multiplicado en España en los últimos meses. Entre los últimos objetivos han estado Caja Madrid, Cajamar, Banesto o BBVA, aunque en meses anteriores también lo fueron otros como Santander o el Popular.

Las entidades -como cabría esperar- aseguran que casi ningún cliente 'ha picado' y que, por tanto, el fraude ha sido mínimo.

Los cálculos de los expertos consultados por EFE dicen, sin embargo, que de los seis millones de correos enviados en cada ataque, entre 2.400 y 6.000 consiguen su objetivo, aunque para ello tengan que insistir en dos o tres ocasiones, incluso con amenazas de bloqueo de cuentas.

Una vez que se han hecho con las claves, los estafadores tratan de hacerse con el dinero depositado en las cuentas, con la 'mínima' dificultad añadida de tener que hacerlo en varias veces porque las transferencias por Internet están siempre limitadas a cuantías no muy grandes.

Pese a que es un timo cada vez más intentado en España, la sociedad pública Red.es o la Asociación de Internautas (AI) creen que la situación no es 'alarmante', pues todavía está muy lejos de los niveles alcanzados en Estados Unidos, Gran Bretaña o Australia.

Y es que el grupo internacional creado para luchar contra este fraude tecnológico, el 'Anti-Phising Working Group', calcula que en estos países entregan sus claves en torno al 5 por ciento de los clientes que reciben uno de estos correos.

A favor del mercado español juega que la banca electrónica no es un producto de masas aún y las personas que lo utilizan, por el momento, tienen cierta cultura informática o financiera y se muestran bastante reticentes a dar sus datos.

El presidente de la AI, Víctor Domingo, aseguró a EFE que 'lo más preocupante es la sensación de inseguridad que se transmite', aunque también reconoció que los ciudadanos están cada vez más concienciados -lo que dificulta el éxito del timo- y, sobre todo, las entidades.

Y es que si Internet es bueno para intentar este tipo de fraudes, lo es mucho más para transmitir a

velocidades impresionantes mensajes de advertencia, tanto de las entidades a sus clientes como entre los propios usuarios. En el mundo físico, eso sería imposible.

Lo peor del 'phising' no es sólo el perjuicio económico que causa a los afectados -en algunos casos lo asumen las entidades-, sino también el daño a la imagen de la entidad y las reticencias que provocan en los usuarios que aún dudaban de lanzarse a este mundo.

Y este último efecto no es cosa de poco en un país donde el desarrollo de Internet está en pleno apogeo. Los números de Red.es así lo demuestran: a final de noviembre usaban la Red 12 millones de personas (el 32,9 por ciento de la población mayor de 14 años), frente a los 9,8 millones de un año antes.

Ante la avalancha de ataques, las entidades se sienten en cierta manera indefensas, pues todas sus inversiones para hacer fuertes sus sistemas frente a los 'hackers' son inútiles para este timo, ya que el 'phising' no ataca directamente la página de la entidad sino que 'engaña' a los clientes.

Sus únicas armas son prevenir, mediante el contacto constante con sus clientes, y reaccionar lo antes posible tras conocer los ataques, intentando bloquear los servidores de los que proceden y, por supuesto, denunciándolo ante la Policía o la Guardia Civil, que tienen sus propios departamentos especializados en este tipo de delitos.

Estas denuncias tuvieron su resultado la semana pasada en Barcelona, donde la Policía Nacional detuvo a siete personas acusadas de 'phising'.

Claro que en la mayoría de los casos no se puede hacer prácticamente nada, porque los fraudes se lanzan desde diferentes países y los estafadores cambian de servidor constantemente.

Ya sean las entidades, los organismos oficiales o los representantes de los internautas, todos ofrecen los mismos consejos para evitar ser estafado: no entregar las claves a nadie porque su entidad nunca se las pediría y estar pendiente de que la dirección en la que estemos empiece por https y, además, aparezca el candado en la parte de abajo de la pantalla.

Además, existen en diferentes páginas de Internet -la del Centro de Alerta Antivirus (CATA), entre ellas- herramientas anti-phising y anti-spam (correos indiscriminados) que se pueden descargar de manera gratuita.

Visto así podría parecer fácil, pero empiezan a aparecer modalidades nuevas de 'phising' con las que el estafador introduce un virus en el ordenador que le permite capturar las claves sin que el propietario lo sepa.

Aunque cada vez son más sofisticados, los fraudes por Internet son todavía ínfimos comparados con los que se dan en la vida real.

Terra Actualidad - EFE

- CONSEJOS DE SEGURIDAD -

Normas de Seguridad para acceder a la banca por internet

Normas de Seguridad para una clave perfecta en Internet

Programa que te ayuda a Generar Claves Seguras.

COMPARATIVA DE SEGURIDAD:

Los internautas exigen más seguridad a la banca por Internet.El ataque de "phishing" que recibe estos últimos meses la banca on-line hace
replantear la política de seguridad que dan los bancos a sus clientes.

Mas Información sobre Phising;
Comision Seguridad Asociación de Internautas

Seguridadenlared.org
