CCOO Federación Servicios

Que es el Phishing y como protegerse

Que es el Phishing y como protegerse

Debido a la confusión que existe en algunos internautas noveles y a algún medio de comunicación, que puede llevar a confusión al internauta por el tratamiento de las noticias de forma alarmista, donde incluso se puede deducir que la banca online no es segura, dejando en entredicho la seguridad de las entidades bancarias. Por todo esto, la Asociación de Internautas quiere explicar que es el Phishing y cómo protegerse del mismo.

Seguro que estos últimos meses lleva escuchando en los medios de comunicación varias veces la palabra Phishing y además relacionándolo la mayoría de la veces con la banca por Internet. Debido a la confusión que existe en algunos internautas noveles y a algún medio de comunicación, que puede llevar a confusión al internauta por el tratamiento de las noticias de forma alarmista, donde incluso se puede deducir que la banca online no es segura, dejando en entredicho la seguridad de las entidades bancarias. Por todo esto, la Asociación de Internautas quiere explicar que es el Phishing y cómo protegerse del mismo.

¿Qué es el Phishing?

El "phishing" es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Resumiendo "todos los datos posibles" para luego ser usados de forma fraudulenta.

¿En que consiste?

Se puede resumir de forma fácil, engañando al posible estafado, "suplantando la imagen de una empresa o entidad publica", de esta manera hacen "creer" a la posible víctima que realmente los datos solicitados proceden del sitio "Oficial" cuando en realidad no lo es.

¿Cómo lo realizan?

El phishing puede producirse de varias formas, desde un simple mensaje a su teléfono móvil, una llamada telefónica, una web que simula una entidad, una ventana emergente, y la más usada y conocida por los internautas, la recepción de un correo electrónico. Pueden existir mas formatos pero en estos momentos solo mencionamos los más comunes;

- SMS (mensaje corto); La recepción de un mensaje donde le solicitan sus datos personales.
- Llamada telefónica; Pueden recibir una llamada telefónica en la que el emisor suplanta a una entidad privada o pública para que usted le facilite datos privados. Un ejemplo claro es el producido estos días con la Agencia Tributaria, ésta advirtió de que algunas personas están llamando en su nombre a los contribuyentes para pedirles datos, como su cuenta corriente, que luego utilizan para hacerles cargos monetarios.
- Página web o ventana emergente; es muy clásica y bastante usada. En ella se simula suplantando visualmente la imagen de una entidad oficial , empresas, etc pareciendo ser las oficiales. El objeto principal es que el usuario facilite sus datos privados. La más empleada es la "imitación" de páginas web de bancos, siendo el parecido casi idéntico pero no oficial. Tampoco olvidamos sitios web falsos con señuelos llamativos, en los cuales se ofrecen ofertas irreales y donde el usuario novel facilita todos sus datos, un ejemplo fue el descubierto por la Asociación de Internautas y denunciado a las fuerzas del Estado: Web-Trampa de recargas de móviles creada para robar datos bancarios.

http://seguridad.internautas.org/html/1/425.html
