



Estafas y fraudes de Internet: EL PHISING

Debido al auge de internet y al mayor uso de las nuevas tecnologías, así como las facilidades que nos plantean, cada vez son más frecuentes los casos de estafas en línea. Todo ello ha facilitado a los estafadores, sus fines que no son otros que engañarnos y quedarse con nuestro dinero, con métodos tan realistas que es difícil darse cuenta del engaño hasta que no nos percatamos en nuestras cuentas bancarias.

A continuación, vamos a comentar el fraude más habitual en estos días y que como casi todo lo que proviene de internet tiene nombre en inglés, nos referimos al *PHISING*. Igualmente comentaremos pequeñas recomendaciones para poder detectarlo y evitarlo.

¿Qué es el Phising?

El *phising* tiene por objetivo obtener los datos personales de su víctima, como son las claves del banco, DNI, teléfonos, claves de email, etc. Suele llevarse a cabo mediante el envío de correos electrónicos (spam), mensajes de redes sociales, SMS.

Todo ello para engañar la víctima haciendo creer que está siendo contactado por una entidad real como su banco o hacienda, por ejemplo y con ello entregar al estafador todos los datos y contraseñas personales, para luego haciéndose pasar por la víctima realizar cualquier tipo de transacción o gestión, desde compras hasta contratar préstamos bancarios, incluyendo transferencias de dinero.

Este comportamiento supone lo que es una SUPLANTACIÓN DE IDENTIDAD, que lleva aparejada una ESTAFA, siendo ambos delitos contemplados en el Código Penal español.

¿Cómo evitar el Phising?

Para evitar ser víctimas de estos engaños se pueden seguir las siguientes recomendaciones:

- Desconfiar de los enlaces que recibamos ya sea mediante SMS, redes sociales, etc. Debemos informarnos antes en internet los datos de la empresa o la dirección web.
- Ignorar cualquier petición de información o datos personales, que nos soliciten desde enlaces externos o mensajes.
 - Los dos primeros puntos están muy relacionados, un ejemplo son mensajes o emails de supuestas entidades bancarias indicando que ha habido un problema con una tarjeta bancaria y que debemos actualizar nuestros datos en una web. Debemos recordar que ninguna entidad bancaria u organismo público solicitara nuestros datos vía de SMS o email.



- En redes sociales evitar los perfiles falsos y/o solicitudes de amistad o seguimiento, limitándonos a personas conocidas.
- Usar contraseñas que no sean fácilmente de averiguar usando letras, caracteres, números y alternando mayúsculas y minúsculas.
- Usar el doble factor de verificación.
- Tener la última actualización del antivirus y el sistema antivirus.
- Desconfiar de archivos ejecutables que tengan extensiones como: .exe, .zip o .rar.
- Usar las redes públicas solo cuando sea necesario y no compartir en ellas nuestros datos personales ni realizar gestiones que necesiten nuestros datos personales.
- Tener diferentes cuentas de correo electrónico, diferenciando las personales de las laborales o una dedicada únicamente al ocio en internet.
- No descargar contenido pirateado.

¿Qué debemos hacer en caso de ser víctima de Phising o de una estafa en Internet?

1.- En primer lugar, contactar con la entidad bancaria a la mayor brevedad para informar de la estafa y comprobar si se puede cancelar la operación o retrotraer la transacción.

2.- Acudir a la Policía Nacional o a la Guardia Civil a fin de poner la denuncia correspondiente.

3.- Recabar toda la información posible a fin de que la denuncia sea lo más completa posible.

4.- Igualmente se puede reportar el fraude a través de la web del Instituto Nacional de Ciberseguridad (ICIBE), a fin de dar publicidad a lo sucedido y evitar con ello que siga pasando.

5.- Si la estafa ha sucedido en lo que se llama un Marketplace, lo que sería una web de compras tipo Ebay o Amazon, si bien no se harán cargo de la situación, si podrán tomar medidas contra ese vendedor fraudulento. Igualmente, estas páginas suelen tener algún sistema de resolución de conflictos o de protección al consumidor a los que acudir.

6.- Por último, también podrás acudir a las Oficinas o Servicios de Información al Consumidor del ayuntamiento de tu localidad, si bien una vez puesta la denuncia el asunto habrá quedado a cargo de la investigación de la policía y posteriormente del juzgado, en los servicios de información podrán informarte respecto a los primeros pasos a seguir en caso de haber sido engañado.

Angel Peinado Sánchez

Asesor Jurídico de Federación de Usuarios y Consumidores Independientes (FUCI)