

## **Cuidado con la vuelta a casa, podemos encontrarnos, scam, malware, phishing..**

**Aunque parezca un lema de la DGT. No lo es, como es norma por parte de la Comisión de Seguridad de la Asociación de Internautas, alertamos una vez mas de los posibles peligros que podemos encontrar en nuestro correo electrónico, tampoco podemos olvidar que la campaña para realizar la declaración de hacienda acaba de empezar y no es la primera vez que los ciber-delincuentes se aprovechan de este tipo fechas tan importante para los declarantes.**

Seguridad y sentido común en fundamental en estos tiempos de uso de las nuevas tecnologías de la comunicación: Los ciberdelincuentes aprovechan los días festivos, fechas de eventos, recordatorios, etc, para atosigarnos con técnicas en el uso de ingeniería social para hacernos picar en alguna trampa.

Este tipo de trampas suelen venir por falsas web, anuncios de cualquier tipo y en su mayoría por correo electrónico, enumeramos los mas conocidos:

### **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, la más usada y conocida por los internautas, la recepción de un correo electrónico.

Recordamos que la estamos en fechas para realizar la declaración de hacienda, pues tengamos cuidado con los correos electrónicos trampa.

### **OFERTA FALSA DE TRABAJO**

#### **SCAM o PHISHING LABORAL / MULERO - OFERTAS FALSAS DE TRABAJO**

El Scam es la captación de personas por medio de correos electrónicos, anuncios en web de trabajo, chats, irc, etc... donde empresas ficticias le ofrecen trabajar cómodamente desde casa y cobrando

unos beneficios muy altos. Sin saberlo, la víctima esta blanqueando dinero obtenido por medio del phishing (procedente de estafas bancarias).

\* Siempre le piden que tenga o abra una cuenta bancaria.

\* Su trabajo consiste en recibir transferencias bancarias a su cuenta bancaria, sacar este dinero posteriormente para enviarlo a países extranjeros por medio de empresas tipo Western Union, Money Gram.

\*Frasas para captar a victimas:

¿Esta usted en paro y tiene ganas de trabajar?

¿Quiere obtener un dinero extra?

¿Quiere trabajar cómodamente desde casa?

¿Quiere tener beneficios de forma rápida?.

\*Nos mandan un contrato (falso) para hacer mas creíble la oferta.

Una vez obtenidos los datos de la victima y no colabora la victima será amenazada.

[En este momento tenemos detectados scam que simulan empresas petroleras \(Repsol-YPF\) y hospitales.](#)

## **PHISHING-CAR**

- OFERTAS FALSAS DE VEHÍCULOS. Phishing-Car

Captación de compradores de coches a un coste muy bajo, la venta nunca se efectúa, esta persona realiza un pago como señal, se queda sin dinero y sin coche.

- ¿Como se produce y en que consiste?

Se producen por medio de llamadas ofertas en vehículos lujosos, incluso tienen web trampas con nombre de dominios muy similares a empresas con mucho prestigio que se dedican a la venta de vehículos de ocasión, pero todas los fraudes tienen algo en común:

\* El pago se realiza por medio de empresas de envío de dinero a otros países (Tipo Western Union, Money Gram).

\* El vendedor le oferta la entrega a domicilio.

\* En un 90% el vehículo que venden esta fuera de su país, de esta manera usted solo puede verlo en fotos.

\* Le piden primero el 30% o el 40% del precio ofertado como primera señal.

\* Captan a las victimas por medio de anuncios en web de venta de coches o de segundamano y por supuesto la recepción de correos electrónicos.

\* Muchas veces el vendedor dice que es un español que vive en Gran Bretaña y por motivos laborales de estancia en el país ingles, tiene que cambiar de forma urgente de coche por que se conduce por la izquierda y su coche al estar matriculado en España el volante esta al lado contrario y no se adapta, por este motivo vende el coche de forma muy económica, te enseñan un coche matriculado en España.

\* La mayoría de los estafados enviaron el dinero a Reino Unido, esto no quiere decir que cambien.

## **PHARMING**

## PHARMING EL GRAN DESCONOCIDO POR EL USUARIO PERO EL MAS PELIGROSO.

Es una técnica para llevar a cabo estafas online, aunque en muchos medios comentan que no es necesario usar ingeniería social esta definición no es totalmente cierta ya que es necesario que nuestra maquina o la remota sea manipulada . El pharming consiste en manipular las direcciones DNS que utiliza el usuario, con el objetivo de engañarle y conseguir que las paginas que visite el usuario no sean realmente originales aunque su aspecto sea idéntico.

Resumiendo desvía el tráfico de Internet de un sitio Web hacia otro sitio de apariencia similar, con la finalidad de engañar a los usuarios para obtener sus nombres y contraseñas de acceso, que se registrarán en la base de datos del un sitio falso que fue creando antes y donde simula a la web que suplantan.

\* Hay gusanos y troyanos que realizan esta función.

\* La victima se entera cuando existe un movimiento extraño de dinero en sus cuentas.

## LOTERIAS FALSAS

Falso premio de loterías, el usuario recibe un correo electrónico donde le notifican que tiene un premio de loteria, si un usuario contesta a este correo le solicitaran a continuación todos datos bancarios para un falso ingreso del premio.

En otros casos se le solicita un parte del premio que tendrá que enviarlo a un país para poder cobrar el premio completo.

En todos los casos el premio es falso.

## WEB FALSA DE RECARGAS

- WEB FALSAS DE RECARGAS Es una variante del Phishing que solo busca un propósito, robar datos bancarios a los usuarios.

Detrás de llamativas ofertas prometiendo recargas más económicas se puede esconder una estafa, que lo único que busca es hacerse con información del usuario.

-Este tipo de fraude puede ser algunas veces mas peligroso que el tradicional phishing, el ataque no es directo, se encuentra en los anuncios de los enlaces patrocinadores de buscadores de Internet.

Todo estos son ejemplos conocidos que se sufre casi diariamente, pero pueden salir nuevos formatos, desde tarjetas falsas que descargan malwares que contienen troyanos bancarios o certificados falsos que es la ultima modalidad detectada, recuerden en todos lo casos usen el sentido común y actualicen sus sistemas operativos, tenga su antivirus y cortafuegos al día, para evitar en cierta medida el poder estar un poco mas seguro.

Fecha artículo: 2008-05-04 23:44:40 - url artículo: <http://www.internautas.org/html/4354.html>

**Logos y marcas propiedad de sus respectivos autores.  
Los comentarios son propiedad y responsabilidad de cada autor.  
© 1998-2009 Asociación de Internautas - <http://www.internautas.org>**

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: [asociacion@internautas.org](mailto:asociacion@internautas.org)