

Top Scam en Internet

IC³ (*Internet Crime Compliant Center*) ha emitido su **informe anual sobre el cibercrimen del 2009**. Los datos muestran que el número de denuncias recibidas se ha incrementado un 23% y la cantidad de dinero estafado ha aumentado un 48% respecto al año anterior.

Las denuncias cubren distintas categorías, entre ellas destacan: el fraude en subastas, compra de productos que nunca llegarán a su destino, fraude de tarjetas de crédito, intrusiones en ordenadores, spam, y pornografía infantil.

En el *ranking* de países perpetradores, España se sitúa en la octava posición.

El **scam ocupa una de las primeras posiciones en las denuncias recibidas**. El scam no sólo se refiere a estafas por correo electrónico, sino también a sitios web que tienen como finalidad ofrecer un producto o servicio falso.

En el Top Scam del 2009 se destacan:

- **La extorsión.** La víctima recibe un correo de un supuesto asesino a sueldo contratado por una organización terrorista en el que es amenazado de asesinato, a no ser que envíe una cantidad de dinero determinada y se le perdonará la vida.
- **Lecturas astrológicas.** La víctima recibe spam o pop-ups que ofrecen lecturas astrológicas gratuitas. Después de recibir la primera lectura, se tienta a la víctima con otra lectura de pago completa, prometiéndole que algo bueno le va a suceder. Una vez realizado el pago nunca recibe la lectura, y al intentar contactar con el supuesto astrólogo recibe un mensaje que indica que no existe tal destinatario de correo.
- **Estímulos económicos.** Muchas víctimas informaron que habían recibido llamadas telefónicas con un mensaje grabado con la voz del presidente Obama, en donde se ofrecían fondos del gobierno durante un periodo de tiempo limitado. Para obtenerlo debían visitar unos sitios web y recibirían el supuesto dinero. Una vez insertados sus datos personales y después de pagar una pequeña cantidad de dinero en concepto de honorarios, nunca llegaron a recibir la supuesta ayuda económica.

- **Ofertas de trabajo.** Se informa a la víctima de supuestas ofertas de tele-trabajo, en donde se requiere el uso de un hardware o software necesario que deberán abonar, pero su inversión se verá recuperada con creces. Otras víctimas reciben una encuesta indicándoles que en época de crisis es necesario conocer las relaciones empresa/empleador, y para poder verificar su identidad deben enviar una copia del cheque de su nómina. Pasado un tiempo ven como los fondos de su cuenta bancaria han sido alterados.
- **Antivirus falsos.** Como ya hemos hablado en varias ocasiones, son pop-ups que informan a la víctima que ha sido infectada por un virus, y se le ofrece un antivirus de pago para solucionarlo. Una vez pulsado el falso pop-up, un malware es instalado en su máquina y se le redirige a una página para comprarlo. Además de pagar por un falso antivirus, la víctima tiene un troyano o un *key logger* instalado.

Es recomendable seguir unas **buenas prácticas** para evitar caer en este tipo de timos:

- No acceder a información de fuentes no confiables.
- Eliminar correos electrónicos y mensajes de móvil en cuyas fuentes no confiemos, y no hayamos solicitado.
- No realizar pagos con tarjeta de crédito en servicios o productos de los que no tenemos la total certeza que provengan de fuentes confiables.

La **ingeniería social** es el método más usado en este tipo de estafas, aprovechándose siempre de lo ingenuos que podemos llegar a ser los humanos. Por mucha seguridad que le pongamos a nuestras máquinas, nunca debemos olvidar que *el ser humano es el eslabón más débil*.

Fecha: 09/05/2010

Fuente: securitybydefault.com