Alerta de la FTC para Consumidores

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer & Business Education

Después de un Desastre: Los Mensajes Electrónicos *Spam* Pueden Ser una Estafa

After a Disaster: Spam May Scam

¿Ha recibido mensajes electrónicos no solicitados o *spam* pidiéndole una donación para ayudar a las víctimas del Huracán Katrina o con información sobre el desastre? Si así fuera, es posible que lo hayan puesto en la mira de una estafa.

Según informa la Comisión Federal de Comercio (*Federal Trade Commission*, FTC), la agencia nacional de protección del consumidor, algunos defraudadores oportunistas están aprovechándose del desastre para estafar a las personas que desean ayudar a las víctimas o que están buscando noticias sobre el huracán.

Mensajes *Spam* Relacionados a Donaciones

Una de las estafas referidas al huracán involucra solicitudes de donaciones para entidades benéficas falsas. Los *spammers* envían mensajes de correo electrónico aduciendo que están brindando ayuda a las víctimas y redirigen a los consumidores a sitios Web que lucen como los de las organizaciones benéficas legítimas y reconocidas o que tienen nombres que suenan similares a los de las entidades de caridad legítimas, reconocidas y respetables. En realidad, los remitentes de estos mensajes *spam* se quedan con la mayoría de — o todos — los fondos recaudados.

Si recibe un mensaje de correo electrónico que le despierta interés en ayudar a las personas afectadas por el Huracán Katrina, la FTC le ofrece las siguientes recomendaciones para donar prudente y atinadamente:

- Haga sus donaciones a entidades de caridad o beneficencia con las cuales haya contribuido anteriormente. Tenga cuidado con las entidades de beneficencia aparecidas de la noche a la mañana. Puede que tengan buenas intenciones, pero tal vez no cuenten con la infraestructura necesaria para proporcionar asistencia.
- Haga su donación directamente a la entidad de beneficencia y no mediante recaudadores ya que éstos se quedarán con una parte de su dinero para cubrir sus costos, con lo cual las víctimas recibirán un monto de ayuda menor.
- No le suministre su información personal o financiera — incluyendo su número de Seguro Social o números de su cuenta bancaria o tarjeta de crédito — a nadie que le solicite una contribución. Los estafadores oportunistas usan estos datos para cometer fraude en su contra. Nunca envíe dinero en efectivo: no hay manera de asegurarse de que la organización haya recibido su donación.
- Antes de hacer una donación, verifique la legitimidad de la entidad de beneficencia. Consulte en Internet el sitio **www.give.org** de *Better Business Bureau's Wise Giving Alliance*.

Mensajes *Spam* con Noticias sobre el Huracán Katrina

Algunos *hackers* están pegando algunas noticias sueltas sobre el huracán al cuerpo de sus mensajes electrónicos junto con un enlace para "leer más". Si usted hace clic sobre el enlace, puede iniciar involuntariamente un proceso que instala secretamente un programa que permite que los *hackers* ejerzan control sobre su computadora. Esto se llama *spyware* y permite que el *hacker* acceda a los datos y programas de su computadora o hasta puede llegar a tomar el control de la computadora y utilizarla para enviar mensajes electrónicos masivos no solicitados, comúnmente llamados *spam*.

Los expertos en computación y los funcionarios federales indican que los consumidores no deben responder a los mensajes electrónicos no solicitados ni tampoco hacer clic sobre los enlaces o vínculos incluidos en los mensajes que ofrecen información sobre el Huracán Katrina o que solicitan donaciones para ayudar a las víctimas. Asimismo, advierten a los consumidores que no utilicen la función de cortar y pegar para copiar los enlaces incluidos en los mensajes electrónicos no solicitados en la barra de domicilio del navegador de Internet. Los estafadores pueden lograr que los enlaces aparenten ir a un lugar pero en realidad, dirigen a los usuarios de computadora a un sitio diferente.

¿Cómo puede detectar si le han instalado *spyware* en su computadora? Puede ser que repentinamente su computadora tarde mucho en abrir y operar los programas que usa habitualmente, posiblemente le aparezcan mensajes de error al azar, o tal vez encuentre barras de herramientas o íconos nuevos en su pantalla.

¿Qué puede hacer para eliminar de su computadora el *spyware*? Los expertos en seguridad informática recomiendan tomar estas tres medidas:

1. Compre un programa *anti-spyware* en un comercio confiable y conocido.
2. Instálelo programando un "escáner" rutinario del sistema — como mínimo, una vez por semana — y si fuera posible, cada vez que encienda su computadora.
3. Elimine todos los programas software que detecte y que no desee conservar guardados en su computadora.

Para obtener más información sobre el Huracán Katrina, visite sitios Web gubernamentales o de noticias conocidos. Los sitios Web gubernamentales tienen un domicilio de Internet terminado en ".gov". Un buen lugar para comenzar su búsqueda es **www.espanol.gov**.

La FTC trabaja en favor del consumidor para la prevención de prácticas comerciales fraudulentas, engañosas y desleales y para proveer información de utilidad al consumidor con el objetivo de identificar, detener y evitar dichas prácticas. Para presentar una queja o para obtener información gratuita sobre temas de interés del consumidor visite ftc.gov/espanol o llame sin cargo al 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866- 653-4261. La FTC ingresa todas las quejas relacionadas a fraudes de Internet y sistema de telemercadeo, robo de identidad y otras quejas sobre prácticas fraudulentas a una base de datos segura llamada Centinela del Consumidor (*Consumer Sentinel*) que se encuentra a disposición de cientos de agencias de cumplimiento de las leyes civiles y penales en los Estados Unidos y en el extranjero.

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER