GUÍA ELECTRÓNICA PARA LA VIDA DIGITAL DE TrendLabs

5 motivos por los que las trampas de la ingeniería social funcionan

¿Qué es la ingeniería social?

La ingeniería social es el arte de engañar a las personas. Los ciberdelincuentes utilizan esta popular herramienta para apropiarse de su dinero. En el mundo actual, regido por la obtención de beneficios, los ciberdelincuentes ya no solo cometen actos reprochables, sino que también desean lucrarse económicamente.

Las amenazas de ingeniería social son peores que el malware más intrusivo, ya que es más difícil protegerse frente a ellas. ¿El motivo? El objetivo es usted, no simplemente su sistema.

La ingeniería social, un término popularizado por Kevin Mitnick, un hacker reconvertido en consultor, es el acto de engañar a la gente para que haga algo que no desea o para que proporcione información confidencial.

Fuente: http://es.wikipedia.org/wiki/Ingeniería_social_(seguridad_informática)

La forma más eficaz de protegerse frente a estas amenazas es mantenerse informado: saber cuáles son los peligros, qué se debe evitar y con qué hay que tener cuidado.

Las noticias importantes pueden convertirse en malas noticias

Los hechos de gran difusión, como los desastres naturales o los lanzamientos de productos o servicios muy esperados, siempre captan la atención de la gente. Los que disponen de un equipo de trabajo y acceso a Internet, navegan por la red de forma natural para mantenerse informados. Ni conocen ni les importan demasiado las trampas de los ciberdelincuentes que los acechan.

LO QUE VE: entradas de redes sociales con enlaces a vídeos o fotos a los que resulta difícil resistirse.

LO QUE NO VE: los ciberdelincuentes se apresuran a poner trampas, es decir, crear sitios Web maliciosos, cada vez que se produce un gran evento. Dichos sitios, normalmente cargados de malware, pueden causar estragos en su sistema de forma automática. Algunos le redireccionan a encuestas o anuncios, pero ninguno le conduce nunca donde prometía.

LOS PELIGROS CON LOS QUE DEBERÍA TENER CUIDADO: enlaces maliciosos que muestran sitios o páginas de noticias falsos.

HECHOS DE GRAN DIFUSIÓN QUE HAN APROVECHADO LOS CIBERDELINCUENTES

DESASTRES NATURALES

Unos minutos después de producirse el tsunami de Japón de marzo de 2011, determinados sitios Web de noticias falsos que alojaban malware FAKEAV infectaron los sistemas de los usuarios que pretendían mantenerse informados a través de ellos.

Fuente: http://blog.trendmicro.com/most-recent-earthquake-in-japan-searches-lead-to-fakea/

LANZAMIENTOS DE PRODUCTOS O SERVICIOS

Una falsa promoción para regalar un iPad engañó a las víctimas para que proporcionaran sus datos personales a través del correo electrónico.

Fuente: http://blog.trendmicro.com/ipad-giveaway-gives-users'-identities-away/


Los personajes
famosos acaparan
la mayor atención

Las noticias sobre personajes famosos generan más interés que cualquier otro tipo de noticias. Cautivan a una variedad de público mucho más amplia, la mayoría admiradores o seguidores, con lo que también captan más atención de los medios. En la batalla por obtener lectores, los medios de comunicación suelen utilizar el sensacionalismo y la exageración para despertar más interés entre el público. Cuanto más increíble es el titular, más lectores lo leen.

LO QUE VE: enlaces a historias con titulares llamativos que prometen revelaciones aún más increíbles y escandalosos al hacer clic en ellos.

LO QUE NO VE: como ocurre con otras noticias importantes, dichos enlaces suelen llevar a sitios Web maliciosos especialmente diseñados que se aprovechan del despliegue publicitario que rodea al famoso en cuestión. Al igual que en la mayoría de los fraudes, es probable que estos enlaces contengan malware o redirijan a las víctimas a sitios de encuestas o anuncios.

LOS PELIGROS CON LOS QUE DEBERÍA TENER CUIDADO: titulares increíbles con enlaces a vídeos o fotos relacionados.

NOTICIAS SOBRE PERSONAJES FAMOSOS MANIPULADAS POR CIBERDELINCUENTES

ESCÁNDALOS

La entrada de una red social que promocionaba un vídeo que "acababa con la carrera de Justin Bieber para siempre" redirigía a las víctimas a un sitio Web de encuestas y concluía en sus propias páginas.

Fuente: http://blog.trendmicro.com/facebook-attack-leverages-linkedin/

CONTROVERSIAS

Varios eventos relacionados con la muerte de Michael Jackson atraían a víctimas con el objetivo de que descargaran malware bajo la apariencia de una imagen difundida por *MSN Messenger*.

Fuente: http://blog.trendmicro.com/msn-bot-plays-on-controversy-over-michael-jacksons-death/

MUERTES FALSAS

Un sitio Web de noticias falso propagó rumores sobre la muerte de Jackie Chan para redirigir a las víctimas a un sitio malicioso.

Fuente: http://blog.trendmicro.com/how-much-can-today's-communication-media-be-trusted/


Manténgase cerca
de sus amigos,
pero aléjese
de sus enemigos

Millones de personas acceden a sus sitios preferidos de las redes sociales cada día. Por ello, no es de extrañar que los fraudes de las redes sociales, es decir, formas de redireccionamiento que utilizan determinados aspectos de las plataformas de dichas redes, se hayan convertido en una amenaza tan común.

LO QUE VE: entradas que promueven nuevas funciones de redes sociales solo disponibles durante un periodo de tiempo limitado que incluyen códigos sospechosos que se deben copiar y pegar en barras de direcciones de navegadores o aplicaciones que se deben descargar e instalar en sistemas.

LO QUE NO VE: estos códigos sospechosos o aplicaciones suelen dirigir a páginas maliciosas diseñadas para piratear cuentas, robar datos personales o propagar infecciones a través de cuentas.

LOS PELIGROS CON LOS QUE DEBERÍA TENER CUIDADO: enlaces sospechosos a sitios Web de descarga de funciones o aplicaciones.

ESTAFAS EN REDES SOCIALES UTILIZADAS POR LOS CIBERDELINCUENTES

TEMAS PARA DÍAS SEÑALADOS

La entrada de una red social que publicitaba un tema para el Día de San Valentín, en realidad forzaba a las víctimas a descargarse e instalar una extensión maliciosa para sus navegadores *Chrome* y *Firefox*.

Fuente: http://blog.trendmicro.com/facebook-valentines-theme-leads-to-malware/

NUEVAS FUNCIONES

Una aplicación falsa de *Twitter* que supuestamente vigilaba las actividades de los seguidores de las víctimas, en realidad facilitaba a los ciberdelincuentes el pirateo de las cuentas.

Fuente: http://blog.trendmicro.com/new-unfollowed-you-scam-hits-twitter-trending-topics/

Los ciberdelincuentes siempre intentarán asustarle para que claudique

El miedo es un gran motivador; incluso los ciberdelincuentes lo saben. Por ello, utilizan amenazas y un lenguaje alarmista para apremiarle a que ceda a sus deseos, es decir, les revele datos personales o les entregue su dinero.

LO QUE VE: un correo electrónico sospechoso con apariencia de notificación urgente (normalmente relacionado con la seguridad financiera o del sistema) que requiere una acción inmediata, como consultar un archivo adjunto, comprar una aplicación o realizar un pago en línea.

LO QUE NO VE: estas amenazas pueden compararse con un ladrón apuntándole con una pistola por la espalda para robarle su dinero y otros objetos valiosos. Independientemente de lo aterradoras que sean sus tácticas, no suelen infligir tanto daño como proclaman, a menos que ceda a sus deseos.

LOS PELIGROS CON LOS QUE DEBERÍA TENER CUIDADO: asuntos de correo electrónico turbadores y contenido que le solicita que realice una acción o sufra las consecuencias.

PROPOSICIONES ATERRADORAS UTILIZADAS POR LOS CIBERDELINCUENTES

RANSOMWARE

Los ciberdelincuentes amenazaron a determinados usuarios rusos para que pagasen aproximadamente 15 dólares estadounidenses por visualizar contenido inapropiado.

Fuente: http://blog.trendmicro.com/another-russian-ransomware-spotted/

FAKEAV

Los proveedores de FAKEAV son conocidos por engañar a sus víctimas para comprar aplicaciones inútiles utilizando avisos de infección del sistema aterradores.

Fuente: http://blog.trendmicro.com/targeting-the-source-fakeav-affiliate-networks/


Las amenazas, al igual
que las celebraciones,
vienen y van

La Navidad, o cualquier otra festividad que se celebre masivamente, y la Super Bowl, o cualquier evento deportivo popular, siempre serán los cebos preferidos de los ciberdelincuentes. Por lo tanto, cabe esperar que anuncien su llegada, los celebren y lamenten el final de estos eventos año tras año.

LO QUE VE: spam sospechoso y las entradas en redes sociales que promueven ofertas increíbles durante festividades o grandes eventos deportivos.

LO QUE NO VE: los enlaces incrustados en estos sitios Web personalizados a los que conducen, que bien alojan malware o le redirigen a sitios de encuestas o anuncios, pero nunca a regalos o grandes ofertas.

LOS PELIGROS CON LOS QUE DEBERÍA TENER CUIDADO: las ofertas en línea son demasiado buenas para ser verdad.

CELEBRACIONES CON LAS QUE LOS CIBERDELINCUENTES HACEN NEGOCIO

VACACIONES

Una página de scam de *Facebook* ofrecía a las víctimas el complemento de un tema de Navidad, que en realidad permitía a los ciberdelincuentes piratear sus cuentas para enviarles spam.

Fuente: http://blog.trendmicro.com/christmas-theme-for-facebook-profile-leads-to-malspam/

EVENTOS DEPORTIVOS

A los seguidores de la Super Bowl que buscaban actualizaciones se les redirigía a sitios Web que alojaban FAKEAV.

Fuente: http://blog.trendmicro.com/search-for-news-on-the-super-bowl-and-bill-cosby's-supposed-death-lead-to-fakeav/

Consejos de seguridad de ingeniería social

AGREGUE A FAVORITOS LOS SITIOS WEB DE CONFIANZA

Dicen que la confianza hay que ganársela. Le recomendamos que trate los sitios Web nuevos igual que a personas que acaba de conocer. Del mismo modo que no confía en todas las personas que conoce en cuanto las ve, no confíe inmediatamente en sitios que solo ha visitado una vez.

SOSPECHAS FUNDADAS

Nunca haga clic en enlaces sospechosos, independientemente de lo prometedores que parezcan los mensajes que los acompañan. Las promesas demasiado buenas para ser verdad son solo eso.

EL MIEDO NO ES UNA OPCIÓN

No se deje intimidar por las amenazas. Muchos delincuentes utilizan el elemento sorpresa para asustarle y llevarle a hacer algo que, en otras circunstancias, no haría. Siempre es mejor ignorar con rotundidad las tácticas que pretenden atemorizar.

COMPARTA SUS CONOCIMIENTOS

Comparta toda la información de la que dispone con las personas de su entorno para que estén más protegidas. No permita que también caigan en las trampas de la ciberdelincuencia.

PREVENIR ES MEJOR QUE CURAR

Invierta en una solución de seguridad eficaz que proteja su sistema y sus datos de todo tipo de amenazas. Explore y utilice las funciones de seguridad incorporadas de los sitios y páginas Web que visite con frecuencia. Algunos sitios como *Facebook* incluso proporcionan información sobre las amenazas más recientes y consejos que le permitirán navegar de forma segura por sus páginas.

Infórmese acerca de las amenazas y los problemas de seguridad más recientes en los blogs de Trend Micro que se indican a continuación:

- *Fearless Web*
- *TrendLabs Malware Blog*
- *Internet Safety for Kids & Families*

TREND MICRO™

Trend Micro, Incorporated (TYO: 4704; TSE: 4704), líder global de seguridad en la nube, crea un mundo seguro para intercambiar información digital con sus soluciones de seguridad de contenidos de Internet y de gestión de amenazas para empresas y particulares. Trend Micro es una empresa pionera en seguridad de servidores con más de 20 años de experiencia que ofrece una seguridad basada en clientes, servidores y la nube del más alto nivel adaptada a las necesidades de nuestros clientes. Asimismo, detiene las amenazas más rápidamente y protege la información en entornos físicos, virtualizados y basados en la nube. Con el respaldo de la infraestructura líder del sector en seguridad para la computación en nube de Trend Micro™ Smart Protection Network™, nuestros productos y servicios bloquean las amenazas en su origen desde Internet. Además, cuentan con la asistencia de un equipo internacional compuesto por más de 1.000 expertos en amenazas.

TRENDLABS℠

TrendLabs es una red de centros de investigación, desarrollo y asistencia multinacional con una gran presencia regional cuyo objetivo es ofrecer vigilancia constante frente a amenazas, prevención de ataques y entrega oportuna de soluciones sin problemas. Con más de 1.000 expertos en amenazas e ingenieros de asistencia que ofrecen sus servicios las 24 horas del día en todo el planeta, TrendLabs permite a Trend Micro supervisar de forma permanente el panorama mundial de las amenazas; entregar datos en tiempo real para detectar, prever y eliminar las amenazas; investigar y analizar tecnologías que combatan las nuevas amenazas; responder en tiempo real a las amenazas dirigidas y ayudar a los clientes de todo el mundo a minimizar los daños, reducir los costes y garantizar la continuidad empresarial.

TREND MICRO™

Securing Your Journey to the Cloud

TrendLabs
Global Technical Support & R&D Center of TREND MICRO