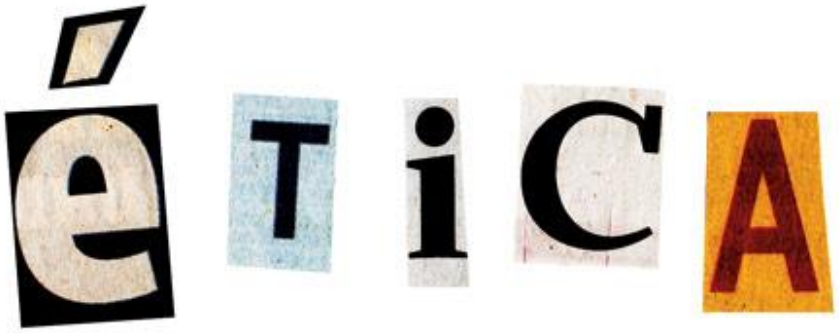
ÉTICA,
LEGISLACIÓN Y
PROFESIÓN

Trabajo de Utilidad Social



UCM - Fdi

ÉTICA, LEGISLACIÓN Y PROFESIÓN

INTRODUCCIÓN

El equipo de Amazon ha querido hacer una recopilación de pequeñas guías y consejos para realizar una navegación segura con nuestro ordenador de principio a fin. Sabemos que internet es un mundo complicado y a la vez poco seguro si no se tienen claras unas pautas a seguir. Nosotros te proporcionamos lo necesario para que puedas hacer todo lo que te propongas en la red, desde una simple navegación en un blog, hasta realizar una compra online.

Nuestra idea es tener un control completo a la hora de navegar por internet, sea cual sea la acción que queramos realizar en la red, tener constancia de que lo que estamos haciendo es seguro y evitar cualquier contratiempo. Agruparemos todos estos problemas que pueden surgir en un mismo documento.

Comenzaremos desde los aspectos más general de navegación y nos iremos adentrando poco a poco en el resto de aspectos.

CONSEJOS PARA NAVEGAR SEGUROS POR INTERNET

I. PREPARÁNDONOS PARA UNA NAVEGACIÓN SEGURA

Antes de todo y de abrir cualquier navegador debemos tener en cuenta

- ✓ **Mantener actualizado nuestro antivirus**
  Cuando navegues por internet es fundamental tener tu dispositivo seguro y actualizado, independientemente del sistema operativo usado, ya sea Android, IOS, Windows...

- ✓ **Utilizar una red Wi-fi conocida**
  Los paquetes de información transmitidos a través de conexiones públicas pueden ser capturados fácilmente por hackers o ciber delincuentes.

- ✓ **Actualizar el sistema operativo y aplicaciones**
  Se debe mantener actualizados con los últimos parches de seguridad no sólo el sistema operativo, sino también el software instalado en el sistema a fin de evitar la propagación de amenazas a través de las vulnerabilidades que posea el sistema.

- ✓ **Utilizar tecnologías de seguridad**: las soluciones antivirus, firewall y antispam representan las aplicaciones más importantes para la protección del equipo ante la principales amenazas que se propagan por Internet. Utilizar estas tecnologías disminuye el riesgo y exposición ante amenazas.

II. PRIMEROS PASOS

Una vez hemos tenido presente estos consejos, ahora sí, abrimos nuestro navegador para consultar información, realizar una encuesta, buscar información o queriendo realizar una compra entre otras opciones.

Deberemos tener en cuenta nada más tener nuestro navegador abierto los siguientes puntos:

- ✓ **Evitar los enlaces sospechosos**: uno de los medios más utilizados para direccionar a las víctimas a sitios maliciosos son los hipervínculos o enlaces. Evitar hacer clic en éstos previene el acceso a páginas web que posean amenazas capaces de infectar al usuario. Los enlaces pueden estar presentes en un correo electrónico, una ventana de chat o un mensaje en una red social: la clave está en analizar si son ofrecidos en alguna situación sospechosa (una invitación a ver una foto en un idioma distinto al propio, por ejemplo), provienen de un remitente desconocido o remiten a un sitio web poco confiable.

- ✓ **No acceder a sitios web de dudosa reputación**: a través de técnicas de Ingeniería Social, muchos sitios web suelen promocionarse con datos que pueden llamar la atención del usuario -como descuentos en la compra de productos (o incluso ofrecimientos gratuitos), primicias o materiales exclusivos de noticias de actualidad, material multimedia, etc. Es recomendable para una navegación segura que el usuario esté atento a estos mensajes y evite acceder a páginas web con estas características.

- ✓ **Evitar el ingreso de información personal en formularios dudosos**: cuando el usuario se enfrente a un formulario web que contenga campos con información sensible (por ejemplo, usuario y contraseña), es recomendable verificar la legitimidad del sitio. Una buena estrategia es corroborar el dominio y la utilización del protocolo HTTPS para garantizar la confidencialidad de la información. De esta forma, se pueden prevenir ataques de phishing que intentan obtener información sensible a través de la simulación de una entidad de confianza.

- ✓ **Tener precaución con los resultados arrojados por buscadores web**: a través de técnicas de Black Hat SEO , los atacantes suelen posicionar sus sitios web entre los primeros lugares en los resultados de los buscadores, especialmente en los casos de búsquedas de palabras clave muy utilizadas por el público, como temas de actualidad, noticias extravagantes o temáticas populares (como por ejemplo, el deporte y el sexo). Ante cualquiera de estas búsquedas, el usuario debe estar atento a los resultados y verificar a qué sitios web está siendo enlazado.

- ✓ **Aceptar sólo contactos conocidos**: tanto en los clientes de mensajería instantánea como en redes sociales, es recomendable aceptar e interactuar sólo con contactos conocidos. De esta manera se evita acceder a los perfiles creados por los atacantes para comunicarse con las víctimas y exponerlas a diversas amenazas como malware, phishing, cyberbullying u otras.

- ✓ **Evitar la ejecución de archivos sospechosos**: la propagación de malware suele realizarse a través de archivos ejecutables. Es recomendable evitar la ejecución de archivos a menos que se conozca la seguridad del mismo y su procedencia sea confiable (tanto si proviene de un contacto en la mensajería instantánea, un correo electrónico o un sitio web). Cuando se descargan archivos de redes

P2P, se sugiere analizarlos de modo previo a su ejecución con un una solución de seguridad.

- ✓ **Utilizar** contraseñas fuertes : muchos servicios en Internet están protegidos con una clave de acceso, de forma de resguardar la privacidad de la información. Si esta contraseña fuera sencilla o común (muy utilizada entre los usuarios) un atacante podría adivinarla y por lo tanto acceder indebidamente como si fuera el usuario verdadero. Por este motivo se recomienda la utilización de contraseñas fuertes, con distintos tipos de caracteres y una longitud de al menos 8 caracteres.

III. DESCARGAS, COMPRA ONLINE Y DOMINIOS

Una vez hemos tenido en cuenta las principales claves para acceder desde nuestro navegador a sitios web de confianza, no queremos quedarnos aquí y seguidamente vamos a pasar a detallar cómo realizar de forma segura compras en sitios web, descargas seguras y dominios web fraudulentos

Descargas Seguras

- ✓ **Descargar aplicaciones desde sitios web oficiales**: muchos sitios simulan ofrecer programas populares que son alterados, modificados o suplantados por versiones que contienen algún tipo de malware y descargan el código malicioso al momento que el usuario lo instala en el sistema. Por eso, es recomendable que al momento de descargar aplicaciones lo haga siempre desde las páginas web oficiales.

- ✓ **Usa el sentido común**: si estás buscando un programa que descargar y ves uno que tenga unas características que lo hacen demasiado cierto para que sea verdad, la probabilidad es que si lo sea. Un programa que te dice que puede hacer lo imposible debe de parecerte sospechoso.

- ✓ **Lee los comentarios:** si el sitio que estás buscando incluye comentarios de los usuarios de los archivos que ofrece “léelos” . Así podrás encontrar reportes de los archivos que pueden contener virus o malware.

- ✓ **Cuando encuentres un archivo que quieras descargar, lo primero que tienes que hacer es darte cuenta si viene de un sitio con buena reputación.** Muchos sitios de malware se aprovechan de los usuarios al escribir incorrectamente los vínculos de paginas conocidas (ejemplo: "yotube.com," "goggle.com" y "gmai.com"). Asegúrate de revisar la barra de direcciones en la parte superior de tu navegador y asegúrate de que la dirección se muestre exactamente como el sitio que estás buscando. Pon mucha atención al principio de la dirección – la parte entre http:// y .com, .org o .edu. Si el vincula se asemeja al sitio que estás buscando, entonces estás a salvo.

- ✓ **Después de descargar el archivo, asegúrate de que no sea un archivo que termine en una extensión ".exe”.** Este tipo de archivo es un archivo “ejecutable” , lo que quiere decir es que el programa va a correr en tu computadora. Los archivos de música, de imagen, o de video no deben de ser

ejecutables aunque algunas aplicaciones pueden ser de este tipo. Para ver los detalles de un archivo, has clic derecho y selecciona “Propiedades”.

- ✓ **Analiza los archivos que acabas de descargar para ver si no tienen virus o malware**. Cada vez que descargues un archivo completo corre el programa de descarga de virus que instalaste en el paso 1. Ahora puedes analizar el archivo dándole clic derecho en el archivo y escoger el comando de mando en el menú. Esto solo se toma unos minutos a lo mucho, y si encuentra algún virus inmediatamente se irá a cuarentena o lo puedes borrar. Si tu programa de antivirus te advierte que tu computadora puede estar infectada, corre múltiples análisis para borrar cualquier virus que haya encontrado.

Por último señalar que muchas webs informan de sitios webs seguros para descargar programas gratuitos, pero en nuestro caso no recomendamos este tipo de práctica ya que si es verdad que son sitios seguros pero a menudo al realizar la descarga también descargas publicidad o incluso otros programas adicionales.

COMPRA ONLINE

Vamos a realizar una pequeña guía para el comercio chino. Es una nueva forma de compra online que está muy de moda actualmente y creemos necesario tener claros unos pasos para poder comprar de forma segura.

1. Antes de comprar en cualquier tienda es muy recomendable leerse el apartado donde se especifican las condiciones de compra (Term And Conditions), donde tendréis detallados los tiempos de envío, pagos, gestión de garantías y demás temas de vital importancia.

2. Asegúrate de que tienen Stock real, muchas tiendas Chinas no tienen muchos productos en stock, esto puede hacer que se demore el envío mucho. Utiliza el email o el chat para que te confirmen el stock.

3. No te fíes de las fechas que dan en los productos que están en pre-venta, por lo general se suelen incumplir las fechas de salida y luego puedes tener problemas si necesitas hacer una reclamación.

4. La Verificación del Pago con visa o paypal suele tardar 2-3 días, no te van a enviar el paquete de inmediato.

5. Infórmate antes de las festividades Chinas, los Chinos también hacen vacaciones, como por ejemplo en año nuevo.

6. Garantías: Por lo general para ejecutar una garantía tendrás que enviar el producto de vuelta a China, asumiendo tú los costes de envío. Cada tienda tiene sus usos, por eso asegúrate de leer las condiciones de compra antes de comprar algo. Si tienes que contactar directamente con el comprador normalmente puedes consensuar una solución si el producto recibido está defectuoso.

7. Siempre que puedas compra con Paypal o Visa de Crédito. Esto último te puede facilitar la devolución de un pago por ejemplo, además de certificar que

la página es de confianza en el caso del uso con Paypal. Recomendamos que no se compre en páginas donde el único método de pago sea con Visa de Crédito.

8. Si eliges envío gratuito ármate de paciencia, tu paquete puede tardar hasta 45 días en llegar.

9. Tienda habituales: Focalprice, Ahappydeal, BangGood, BuySKU, Merimobiles, Aliexpress.

Después de estos sencillos consejos vamos a dividir en dos niveles para detectar las tiendas fraudulentas.

Nivel BÁSICO para detectar tiendas online fraudulentas

Simplemente teclea en el buscador de Google el nombre de la empresa o del dominio, seguido de la palabra “estafa” o “engaño”. En la red muchos particulares denuncian las estafas que han sufrido.

Te dejo aquí el enlace a un par de ellos colgados en fraudwatchers.org y en firetrust.com. La primera vez que vi las listas no me lo podía creer. Es increíble la cantidad de dominios de tienda online citadas como fraudulentas.

Si aparece la tienda online asocidada a la palabra 'estafa', yo no seguiría leyendo. Si no aparece, no cantes victoria porqué debes seguir investigando.

Nivel AVANZADO para detectar tiendas online fraudulentas

Como te decía, si no aparece como estafa en el buscador de Google o en los listados, no confíes aún.

Ahora te toca analizar A TI la tienda online y éstos son algunos de los aspectos en que debes centrar tu atención:

Primero encuentra quien es el propietario del dominio de la tienda. Lo puedes saber tecleándolo en whois.net. Si el propietario no es una empresa y aparece un nombre chino o similar, ya empezamos mal.

Fíjate en la misma página, si el dominio es muy reciente. Si es muy reciente, más posibilidad de engaño o estafa. Ya que estás "tiendas" abren y cierran de un día a otro. Menos de un año, malo.

Desconfía si la tienda no te permite pagar por Paypal y sólo admite pagos por Western Union, cuentas bancarias o similares.

No hay teléfonos de contacto, ni dirección de la empresa y el email de contacto es de un correo Yahoo, Hotmail, Google…

Textos de la página web están llenos de faltas de ortografía o frases con errores en la construcción o sin sentido. Una empresa 'seria' cuidaría estos detalles.

¿Te ofrecen gastos de envío gratis? Piensa en lo que pueden costar desde China hasta aquí y que además hay que pagar aranceles aduaneros. Hay algunas tiendas chinas que tienen sucursales en Europa pero si la tienda es sospechosa por otros aspectos, esto confirma aún más que estamos delante de un fraude.

DOMINIOS

Hemos obtenido una página donde se pueden compartir dominios fraudulentos relacionados con el comercio en China. Este sitio tiene licencia Copyleft otorgándonos permiso para copiar, distribuir y/o modificar este documento sin condiciones de ninguna clase, no hace falta citar la procedencia, puedes copiar total o parcialmente el contenido y modificarlo como quieras.

A continuación os dejamos el enlace a la página: http://webvivo.com/scam-china.php

Se puede observar como en el índice del principio de la página se aporta un foro con diferentes temas de interés donde se puede consultar o solucionar problemas. De este modo se podría incentivar el foro o utilizar esta aportación y ampliarlo con nuevas actualizaciones. Nuestras o de la comunidad.

BIBLIOGRAFÍA

http://webvivo.com/scam-china.php

http://www.outletbarcelona.info/blog/consejos-para-evitar-estafas-en-los-outlet-online/

http://www.taringa.net/posts/economia-negocios/15933927/Guia-para-una-compra-segura-en-las-paginas-chinas.html

http://www.periodistadigital.com/tecnologia/internet/2010/07/02/las-cinco-webs-mas-seguras-para-descargar-programas-gratuitos.shtml

http://www.pandasecurity.com/spain/mediacenter/consejos/navegar-seguro/

http://www.gadae.com/blog/10-consejos-de-seguridad-online-para-navegar-por-internet/

http://androidpc.es/blog/2013/04/13/guia-basica-para-comprar-online-en-china/

http://quesonlosvaloreseticos.com/wp-content/uploads/2012/08/etica.jpg