¿QUÉ HAY DE MALO EN UNOS CUANTOS ANUNCIOS?

AUTOR: HELLEN CUBERO

NOVIEMBRE: 2020

San Marcos

INTRODUCCIÓN

El creciente acceso a la tecnología ha generado un incremento en la cantidad de personas usuarias, su frecuencia en la navegación de Internet a través de distintos dispositivos y la cantidad de datos que generan en el intercambio de información producido. Este aumento de tráfico de información en redes también significa una oportunidad para quienes persiguen datos de cada usuario con diferentes causas y motivos.

La fuerte y constante expansión del uso de Internet también implica un aumento en los riesgos y amenazas a la privacidad de datos que corre una persona usuaria, por lo que es de suma importancia adoptar hábitos para una navegación óptima y segura, protegiendo la información personal y la de los dispositivos desde donde se accesa, ya sea computadora o móvil.

Contenido

Google Chrome

Uno de los navegadores Web más reconocidos y utilizados desde el año 2010, es Google Chrome. Aunque existan otros navegadores predeterminados en las computadoras como Safari o Microsoft Edge (anteriormente Internet Explorer) muchos usuarios que navegan en Internet, prefieren descargar la aplicación de Google. Así lo confirma el informe de Market Share de W3Counter publicado en Noviembre de 2020, donde Google Chrome continúa siendo el navegador más popular en la última década.

Uno de los cimientos de su popularidad está en sus diversas características enfocadas a que las personas usuarias tengan una experiencia de navegación segura. Al manejar la opción de añadirse como usuario, las personas tienen configuraciones propias y sus historiales o cookies se manejan por separado (Lowe Richard, 2017).

La popularidad del navegador ha provocado que existan una gran cantidad de extensiones, temas y aplicaciones disponibles para personalizar y mejorar la experiencia de navegación. Se destacan algunas que poseen un énfasis en la seguridad del navegador, como AdBlock que bloquea anuncios repentinos o indeseables de algunos sitios Web, o Privacy Manager que facilita el manejo de los controles de privacidad por parte del usuario.

Se debe tomar en cuenta que, la incorporación de extensiones, temas o aplicaciones puede ralentizar el navegador e incluso vulnerar la seguridad del mismo, por lo que se debe analizar con detenimiento la instalación de estos elementos.

Open DNS

OpenDNS es una empresa que ofrece el servicio de resolución de nombres de dominio gratuito y abierto en su versión más básica y original. La función básica del DNS (Sistema de nombre de dominio) es habilitar enlaces entre los nombres de dominio y las direcciones IP con la que están asociados.

La empresa enfoca su servicio en torno a la seguridad para redes y dispositivos, gestando acciones como el bloqueo de sitios maliciosos o con posibilidades de ataques de phising, o bien, se puede elegir qué tipos de sitios o contenidos bloquear, como apuestas o pornografía.

Richard G Lowe (2017) cita dos ventajas de la configuración de Open DNS ya sea con un enrutador o una actualización de ordenador: *La ventaja de actualizar su enrutador es que todos los ordenadores, teléfonos inteligentes, tabletas y el resto de los elementos de su red utilizarán OpenDNS sin necesidad de ninguna configuración más. La ventaja de actualizar su ordenador directamente es que los servidores OpenDNS se utilizarán independientemente de la red a la que se conecte su dispositivo. (*Richard G Lowe 2017*).*

Las Cookies

Las Cookies son recursos (archivos de texto) utilizados por los servidores para registrar información con diversos objetivos. Un servidor crea un archivo y este, solo puede ser revisado posteriormente por el servidor que lo creó, así lo explica Richard G Lowe: el servidor crea un pequeño archivo de texto en su sistema llamado cookie. Este solo puede ser consultado por ese servidor y contiene un número único que le identifica. Cada vez que vaya a una página web, el servidor web primero buscará cookies que hayan podido ser registradas en su equipo con anterioridad.

Más allá del propósito de generar registros para los DNS, las cookies han sido utilizadas con otras intenciones. Las Agencias de Publicidad aprovechan estos recursos en las computadoras de las diferentes

personas usuarias para conocer sus hábitos de navegación, es así como descubren cuáles son los sitios Web más recurrentes y generan información para otras empresas o bien, para enfocar campañas de publicidad. Esta actividad es legal y el envío de estos datos es anónimo, sin embargo, los navegadores como Google Chrome, permiten la configuración de estas cookies para evitar consecuencias indirectas de su utilización.

Es importante mencionar que una gran cantidad de cookies puede generar un funcionamiento lento de la computadora o dispositivo móvil, provocando afectaciones incluso en la batería.

Navegando por la red

Con el acceso a la tecnología a través de móviles o computadoras, la navegación por la Web, a través de diferentes aplicaciones, es un acto diario y constante por parte de millones de usuarios alrededor del mundo. Esa gran cantidad de personas que se conectan con frecuencia, generan una sociedad interconectada que inevitablemente se expone a amenazas a la seguridad de diferente índole y por tanto se convierte en una primicia para cada persona usuaria, el conocimiento de hábitos para una navegación segura.

Existen varios consejos que colaboran con una navegación óptima por la Web y que reducen el riesgo y la vulnerabilidad del usuario a ser víctima de fraudes, robo o suplantación de información o ataques directamente al software como virus.

Si al ingresar a un sitio Web, el inicio de la URL (dirección) no inicia con HTTPS, significa que el acceso no es seguro y eso se traduce en que, hay un riesgo en que diferentes actores en la Web pueden monitorean la actividad que realiza en ese sitio que se está visitando. El HTTPS asegura que hay una conexión ideal entre el servidor Web y la computadora, evitando que otros usuarios vean sus movimientos y además, verifica que realmente se está conectando con el servidor Web visitado. El HTTPS resulta de suma importancia en sitios donde se

efectúen compras o se intercambie información sensible como contraseñas o datos personales.

Hay sitios reconocidos por contener anuncios no deseados o ventanas que descargan software maliciosos. Juegos de apuestas, Pornografía o Juegos en línea, contienen muchas ventanas emergentes que al activarse por el usuario descargan en la computadora virus que luego generarán problemas en el computador.

Hoy en día, la práctica de clickbytes ha provocado que muchos usuarios caigan en sitios no deseados. Esta práctica consiste en llamar la atención del usuario a través de titulares o imágenes llamativas para llevarles a sitios que no visitarían con normalidad (Lowe, 2017.) Una variante de Clickbyte es el Likebyte, que consiste en dar “Me Gusta” o “Favorite” en alguna publicación en redes sociales con el fin de promocionarla y generar alcance entre los usuarios, con el fin también de que alguno caiga en el click.

Otra práctica reconocida y relacionada con la visitación de sitios Web indeseados, es el LikeJack, la cual consiste en intentar que los usuarios visiten enlaces que posteriormente solicitarán al usuario completar formularios o solicitudes con diferentes propósitos, ya sea colectar información y generar dinero por ella o incluso utilizarla para otros usos ilegales. El problema del LikeJack, es que utilizan motivos o causas falsas para que el usuario acceda a completar o brindar información creyendo que es para un uso específico, cuando no es así. Por ejemplo, se solicita información o donaciones de dinero para causas benéficas, participación en rifas o becas de estudio que no existen.

Existen sitios con aplicaciones cuyas licencias son de pago (como Microsoft Office) disponibles y gratuitas al alcance de los usuarios. Estas aplicaciones son conocidas como Warez y funcionan de forma ilegal, bajo la modalidad de piratería de Software. Muchos usuarios con el fin de ahorrar dinero o tiempo, descargan estas aplicaciones para acceder a programas sin tomar en cuenta que, al descargarlas podrían estar dando acceso a otro tipo de Software o programas maliciosos que pueden robar información de las computadoras o dañarlas, además de estar cayendo en un acto ilegal.

El modo incógnito es una manera de resguardar los datos de navegación y mantener su privacidad ya que al concluir la navegación, no dejará las

cookies en su dispositivo. Esto significa que su historial de búsquedas y navegación será más discreto, sin embargo es válido indicar que, aquellos sitios que requieran accesos con información como Bancos o Redes Sociales, no recordarán las claves ni datos para relleno automático.

Cómo descargar archivos

Una práctica frecuente pero que produce recelo entre los usuarios de Internet es la descarga de archivos, ya que existen múltiples experiencias negativas relacionadas con descargas que contienen software maliciosos. Los antivirus son ideales para este tipo de prácticas porque escanean los archivos antes que se descarguen y advierten al usuario si existen anomalías en la descarga.

A pesar que este análisis es un buen paso para evitar descargas no deseadas, se recomienda siempre leer las condiciones y uso de los software que se están descargando para comprender a plenitud su utilización.

Cómo llevar a cabo una búsqueda segura

Los navegadores como Google Chrome disponen de configuraciones para mejorar las búsquedas y no caer en sitios sospechosos. Algunos pueden crear filtros para no permitir el acceso a sitios con contenido específico como pornografía o juegos de apuestas.

CONCLUSIONES Y RECOMENDACIONES

Existe una innumerable cantidad de sitios Web que un usuario puede visitar cuando realiza una navegación por Internet, sin embargo, este proceso no se limita solamente a generar una búsqueda de información. Integralmente, la navegación en la Web se completa con una serie de componentes y acciones que están en constante cambio y evolución, y las personas usuarias deben adaptarse a las normas que se establecen día con día pensando primordialmente en la seguridad de su información personal y la de su computador.

Se recomienda instalar aplicaciones y extensiones seguras y debidamente certificadas, contar con antivirus y adblocks para evitar la descarga y presencia de elementos no deseados, así como la configuración de los navegadores para filtrar las búsquedas para evitar contenidos sospechosos o que aumenten el riesgo y vulnerabilidad para nuestras redes.

Conforme la experiencia del usuario en la Web sea más constante y prolongada, así deberían de ser sus acciones para resguardar su seguridad.

REFERENCIAS BIBLIOGRÁFICAS

W3Counter. (2020). Browser & Platform Market Share. Recuperado de https://www.w3counter.com/globalstats.php

Rockcontent. (2019). ¿Qué son las cookies y para qué sirven en Internet?. Recuperado de https://rockcontent.com/es/blog/que-son-las-cookies/

OpenDNS. (2020). Improve your Internet. Recuperado de https://www.opendns.com/

Google Chrome. (s.f). Borrar, habilitar y administrar cookies en Chrome. Recuperado de https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DDesktop&hl=es

Lower, R. (2016). La seguridad informática es como el sexo seguro. Babelcube, INC.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica