



Cómo Ponerse en línea y Conseguir información

Este módulo cubrirá el proceso de conectar su computador al Internet. Incluye la configuración y los navegadores, las búsquedas en Internet, cómo evaluar si un sitio web es seguro, si la información en un sitio es precisa y cómo estar seguro al descargar elementos.

Vocabulario de Internet

Aquí hay algunos términos con los que debe estar familiarizado cuando utilizas el Internet.

Internet - Una conexión global de redes de computadoras conectadas entre sí.

WiFi - La tecnología que permite que los dispositivos se conecten a internet de forma inalámbrica.

Ethernet - Una conexión por cable a Internet; también el cable usado para esa conexión.

Enrutador o Punto de Acceso- Este es el dispositivo al que se conecta su computadora para dirigir su tráfico web.


3G, 4G, 5G - La tecnología inalámbrica que le permite a su teléfono acceder a Internet a través de su proveedor de telefonía celular.

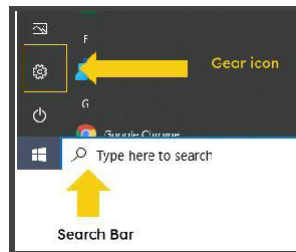
Red - Un grupo de computadoras en una sola ubicación, como una casa o una empresa, o en varias ubicaciones.

Hay muchas formas diferentes que la Nube puede tomar. Cuando hablamos de almacenamiento en la nube, nos referimos a una plataforma que guardará los archivos de la computadora que queramos almacenar en un lugar diferente, usar desde cualquier lugar o eliminarlos de nuestra computadora local pero aún así conservarlos. La Nube almacena esos archivos para nosotros en un servidor remoto en una red informática.



Conectarse al Internet

Para acceder a Internet, tendrás que ir a tu menú de Configuración. Para acceder a la configuración del sistema operativo Windows en una computadora con Windows, debe hacer clic en el ícono de Windows  en la esquina inferior izquierda de la pantalla y luego en el ícono

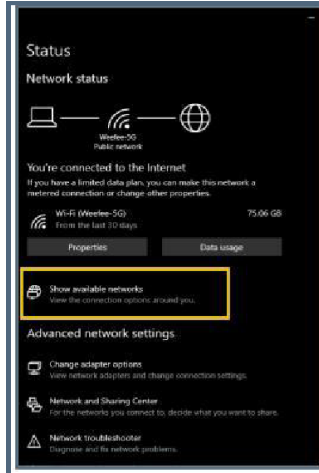


de la rueda dentada (ícono de engranaje).  (gear icon)

En Windows, puede encontrar la opción Red e Internet en Configuración.



En Redes e Internet, puede ver si está o no conectado a Internet. También puede ver propiedades avanzadas para su Internet. Si hace clic en "mostrar redes disponibles", puede cambiar a qué red WiFi está conectado.



Menú de Ajustes de Redes e Internet

Puede cambiar los ajustes específicos de su conexión de WiFi, como activar o desactivarlo (encendiéndolo o apagándolo).

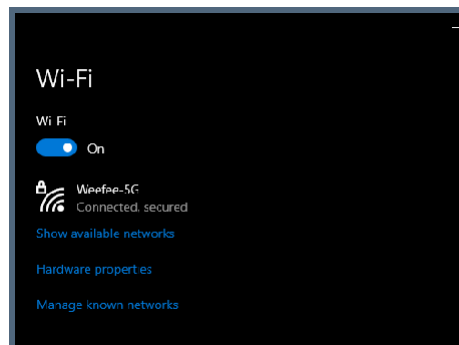


Imagen del menú de conexión de Red de WiFi

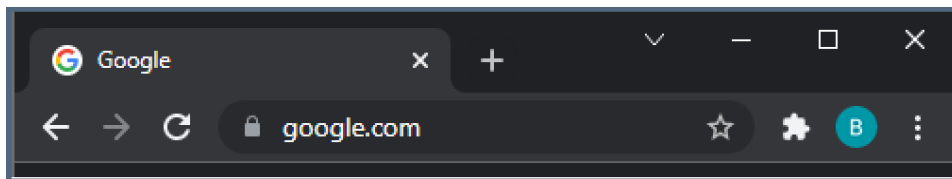
Navegadores de Internet

Usando un Navegador de Internet

Un **navegador de internet**, también conocido como un navegador de red, es una aplicación que puede usar para acceder el internet. Las aplicaciones mas comunes son Chrome, Microsoft Edge, Safari y Firefox.

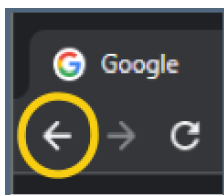


Cuando usted abre un navegador de Internet, es llevado a su pagina de inicio. Todos los navegadores de Internet tendrán una barra en la parte de arriba, llamada la **barra de dirección**.

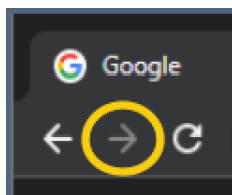


Barra de dirección en Chrome

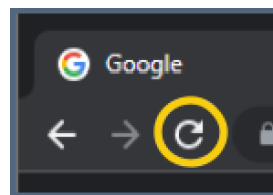
La barra de dirección tiene varios controles diferentes para navegar sitios web. Puede darle clic a la flecha de hacia atrás para regresar al ultimo sitio web que ha visitado. Si vas hacia atrás, puede darle clic a la flecha de hacia adelante para regresar al sitio web del que navego. También puede recargar/refrescar un sitio web para asegurar que esta viendo la información mas reciente dándole clic a la flecha circular.



Haga clic aquí para regresar



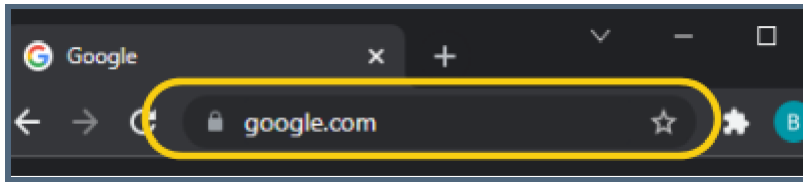
Haga clic aquí para avanzar



Haga clic aquí para refrescar

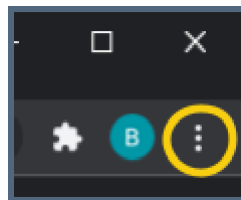


Puede escribir la dirección electrónica en la barra de direcciones para navegar a una pagina electrónica.



Escriba la dirección electrónica aquí

Los tres puntos abrirán un menú que muestra mas información y dejara que usted pueda acceder los ajustes de su navegador de internet.



Haga clic en los tres puntos para acceder a las opciones de menú.

Usted puede abrir nuevas pestañas para poder tener varios sitios web abiertos a la misma vez. Las pestañas serán visibles encima de la barra de dirección.

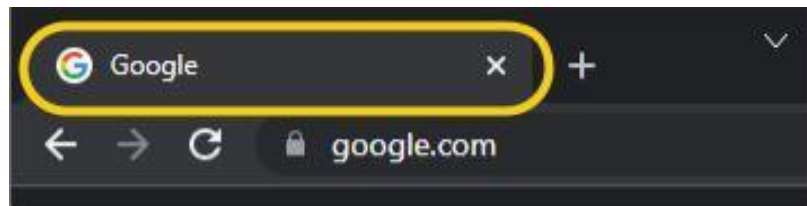
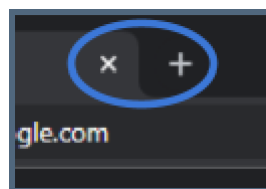


Imagen de una pestaña en Google Chrome

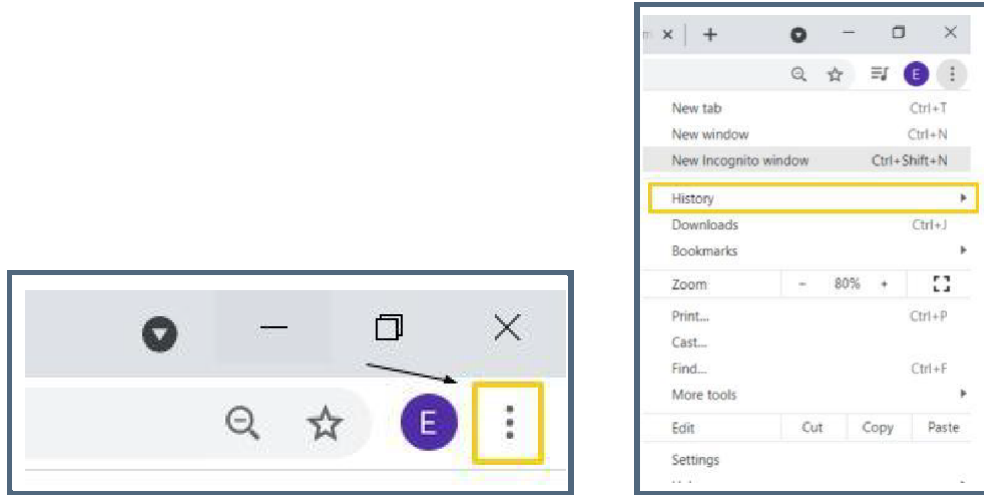
Para abrir una nueva pestaña, haga clic en el signo de mas +, y para cerrar una pestaña, haga clic en la x.



Abrir y cerrar una pestaña

Su Historia de Navegador de Redes

Los navegadores de redes mantienen un registro de los sitios redes que ha visitado en algo que se llama su **historia**. Esto puede ser extremadamente útil si quiere visitar un sitio red que ha visitado previamente. Para ver su historia, haga clic a los tres puntos para abrir su menú y de clic a "Historia."



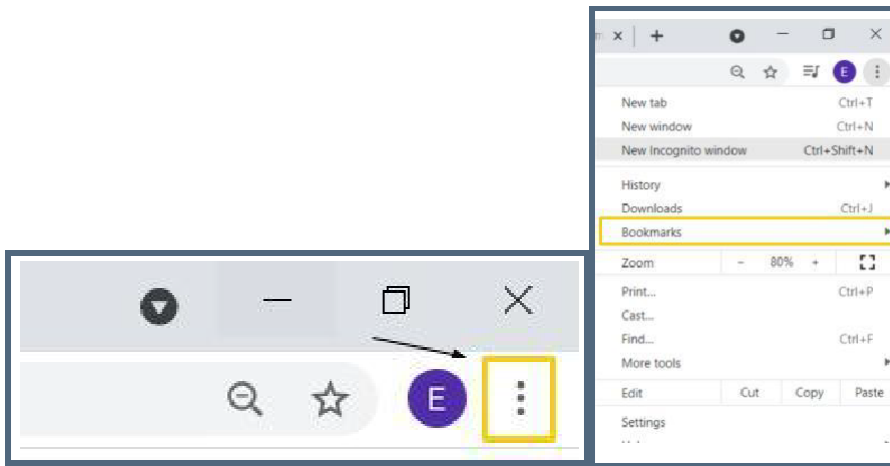
Primero haga clic en los tres puntos para abrir el menú, después seleccione historia dándole otro clic.

Marcadores

Los **marcadores** son como usted puede guardar paginas que visita comúnmente. Usted puede guardar marcadores en su barra de marcadores o en un su folder de marcadores. Marcadores pueden ser guardados/sincronizados en varias computadoras mientras tanto que su navegador de internet tenga esta función y usted este iniciado a su sesión. Esto significa que si añade un marcador a su teléfono, usted podrá verlo en su laptop.

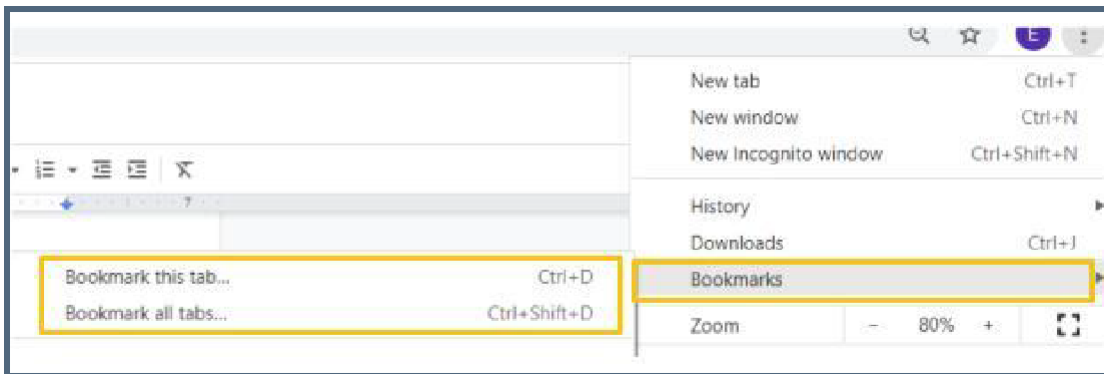
Para crear un marcador, haga clic a los tres puntos para abrir el menú. Seleccione "Marcadores" para abrir el menú de marcadores.





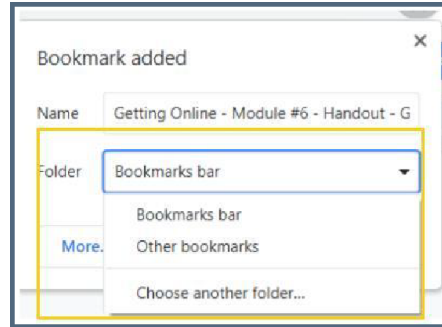
Abriendo los Marcadores

Cuando usted le da clic a “Marcadores,” podrá ver las opciones para escoger si quiere marcar la pestaña en la que esta viendo en ese momento, o si quiere marcar todas las pestañas que tiene abierta.



Desplácese por encima de Marcadores y escoja si quiere marcar la pestaña actual o todas las pestañas.

Puede después escoger donde quisiera guardar el marcador para accederlo después: la barra de Marcadores, Otros marcadores, o en otro folder.



Elija si quiere el marcador en tu barra de marcadores o en otro lugar.

Buscadores

Una habilidad importante que debe tener cuando trabaje con Internet es saber buscar recursos, información y ayuda a través de un **buscador**. Un buscador es un software que busca datos en Internet. Para usar un buscador, utilice **palabras clave**.

Las **palabras clave** son palabras que describen el tema que está buscando. Por ejemplo, si está buscando ejemplos de currículum, buscar por palabra clave de "Ejemplos de currículum" proporcionará mejores resultados que simplemente buscar por la palabra "Currículum".

Asegúrese de que sus palabras clave sean lo suficientemente específicas, pero no demasiado específicas. Por ejemplo, si desea buscar ejemplos de un currículum cronológico, busque "Ejemplos de currículum cronológico" en lugar de "Ejemplos de currículum" o simplemente "Currículum". Esto proporcionará resultados de búsqueda más específicos para lo que está buscando. A menudo, necesitará realizar múltiples búsquedas para encontrar exactamente lo que está buscando.



Google es el buscador más común aquí en los Estados Unidos, pero hay muchas otras opciones de buscadores como **DuckDuckGo** y **Microsoft Bing**. Bing es similar a Google pero es alojado y administrado por Microsoft. DuckDuckGo se basa en la privacidad y no guarda ni vende su información. Esto puede ser útil si desea minimizar el seguimiento de su información en línea.



Logo de Google



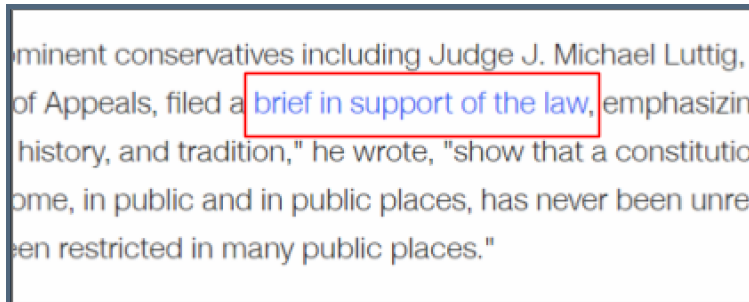
Logo de DuckDuckGo



Logo de Bing

¿La información es correcta?

Siempre vea si el sitio web proporciona un enlace o una cita que muestre de dónde proviene la información. Lo mejor que puede hacer para asegurarse de que la información sea correcta es usar sitios web que hagan referencia a fuentes validadas.



Ejemplo de un enlace dentro de un artículo en línea que lo llevará a una cita.

CanCode Communities. (2021, October 29). *CanCode communities, Microsoft team up to introduce students to Tech Careers*. CanCode Communities. Retrieved November 2, 2021, from <https://cancode.org/albanycancode/cancode-communities-microsoft-team-up-to-introduce-students-to-tech-careers/>.

Ejemplo de una cita en un artículo en línea



Revise un sitio web en busca de errores ortográficos y gramaticales para evaluar rápidamente si el sitio web es legítimo o potencialmente inseguro de usar. Trate de visitar solamente sitios web confiables de fuentes como los principales medios de comunicación o sitios web de empresas u organizaciones que conoce.

 INCLUSO LAS FUENTES DE CONFIANZA PUEDEN TENER INFORMACIÓN INEXACTA.

Preguntas para hacer al realizar búsquedas web

- ★ ¿Es este sitio web una fuente de información imparcial o tiene algo que ganar al compartir esta información?
- ★ ¿Puede encontrar otras fuentes que digan lo mismo y citen las mismas referencias?

- ★ ¿Quién dirige este sitio web? ¿Es un individuo o una organización?
- ★ ¿Tiene este sitio web un historial de publicación de información falsa o engañosa?
- ★ ¿Este sitio web está ofreciendo algo demasiado buena para ser verdad?
- ★ ¿Es esto algo en lo que necesito hacer clic?
- ★ ¿Es el sitio web fácil de usar?
- ★ ¿Hay algo frustrante o extraño en el sitio web?
- ★ ¿Hay muchas ventanas emergentes?
- ★ ¿Son la ortografía y la gramática del sitio web correctas?
- ★ ¿Quién es el autor de este sitio web?
- ★ ¿Dónde se publicó la fuente?
- ★ ¿Por qué el autor creó este sitio web?

Datos en línea

Cuando Ud. publica o da información o datos en línea, es importante ser consciente de lo que está compartiendo y la posibilidad de mal uso.

Ud. siempre debe tener en cuenta la información y los datos cuando Ud. publique en plataformas de redes sociales, compre en línea, registre cuentas y cada vez que ingrese su información personal de identificación en un dispositivo.

La **información personal de identificación** es cualquier información que se puede usar para descubrir quién es Ud. y potencialmente robar su identidad. Esto incluye su nombre, cumpleaños, dirección, número de Seguridad Social, información de tarjeta de crédito y más.

- ★ Asegúrese de que los archivos con información personal de identificación se almacenen en lugares donde su empleador u organización desee que se almacenen.
- ★ Asegúrese de que los archivos descargados a su computadora se borren para evitar que las personas que no deberían acceder a ellos los abran.
- ★ Asegúrese de que cualquier archivo o imagen que Ud. almacene en un dispositivo móvil se guarde en el lugar correcto y se elimine de cualquier lugar que no sea seguro, en caso de pérdida o robo del dispositivo.



Seguridad para Redes Sociales

Consejo para Redes Sociales: ¿Hay una tendencia de redes sociales que crea un nombre de personaje divertido basado en cosas como su mes de nacimiento, segundo nombre, y la calle donde vive? Tenga cuidado con este tipo de publicación: ¡Su publicación pudiera ser usada para coleccionar información sobre usted!

Seria mejor no participar en esta tendencia.

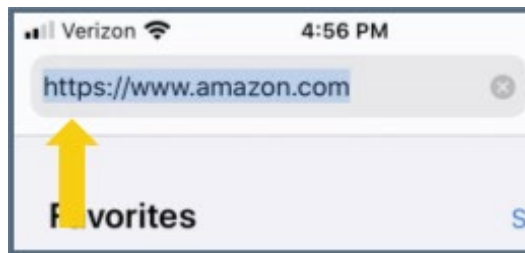
Consejos para las redes sociales...

- ★ Sea cuidadoso y no comparta demasiado
- ★ Ajuste su configuración de privacidad
- ★ Verifique con quien se esta conectando
- ★ No comparta detalles personales
- ★ Recuerde que lo que pasa en el internet, se mantiene en el internet
- ★ Mantenga contraseñas fuertes

HTTP versus HTTPS

¿Es seguro este sitio web?

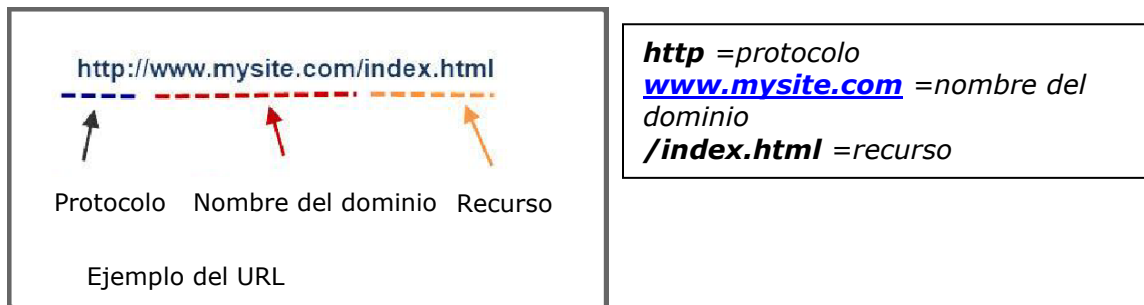
Hay dos protocolos sobre cómo llega la información de su navegador a un sitio web y cómo llega del sitio web la información a su navegador. **HTTP** significa Protocolo de Transferencia de Hipertexto y **HTTPS** significa Protocolo de Transferencia de Hipertexto Seguro.



Amazon.com está usando HTTPS

La principal diferencia es que HTTPS es seguro (encriptado) y HTTP no lo es.

- ★ Alguien que intercepte maliciosamente nuestros datos cuando usamos HTTP puede ver o leer lo que hemos enviado
- ★ Alguien que intercepta maliciosamente nuestros datos cuando usamos HTTPS no puede ver o leer lo que hemos enviado



La estructura de URL de un sitio web alojado por http:

Nunca debe enviar información de identificación personal por HTTP. Solo envíelo por HTTPS. Nunca publique información de identificación personal en una unidad compartida. La información debe compartirse solo con aquellos que necesitan conocerla.

Seguridad de contraseñas

Contraseñas seguras son efectivas para mantener su seguridad en línea.

Con una contraseña, se debe:

Crear una contraseña única para cada cuenta que usa.

Usar una mezcla aleatoria de números, letras, y símbolos.

Utilizar un procesador de contraseñas para gestionar sus contraseñas únicas.

Introducir las contraseñas solo en los sitios apropiados.

Con una contraseña, no se debe:

Usar frases comunes o información personal (por ejemplo, un nombre de una mascota)

Escribir sus contraseñas.

Compartir sus contraseñas.

Escoger contraseñas cortas.

Escoger una contraseña que se adivina fácilmente.

Usar la misma contraseña por mucho tiempo.

Guardar su contraseña en un lugar que se encuentra fácilmente.

Ejemplos de contraseñas buenas y malas

Ejemplos de contraseñas malas	Ejemplos de contraseñas buenas
Contraseña	@H76cxgV90\$\$jKTsk
Juan2021	IegtDL2021!
03-21-1990	S0pAd3VeRdURa5
Mago22	nwso^d-scr23ap(hk3dh

Estafas & Phishing

¿Qué es una estafa?

Una estafa es un término que se usa para describir cualquier esquema fraudulento que toma dinero u otros bienes de una persona desprevenida. Las estafas en línea se han vuelto muy frecuentes. Aunque solían ser bastante obvios, se han vuelto más sofisticados en los últimos años. Las estafas pueden ser simples o más complejas. Son de naturaleza similar a las estafas telefónicas. Se pueden encontrar en correos electrónicos, sitios web y redes sociales. Recuerde: si algo parece demasiado bueno para ser verdad, ¡probablemente lo sea!

Tipos de Estafas

Una **Estafa de Donación** es cuando un estafador finge ser una organización benéfica para que usted le <<done.>> Sin embargo, en realidad termina dándole su dinero al estafador.

Catfishing es cuando un estafador crea una personalidad o identidad falsa para engañar a alguien para que le dé algo que quiere.

Una **estafa 419** o “**Carta Nigeriana**” es una estafa en la que el estafador solicita que se le envíe una cantidad de dinero para cubrir algún costo para otorgar al destinatario de la carta/correo electrónico una gran suma de dinero.

Una **Estafa de Encuesta en Línea** es una estafa en la que un estafador generalmente ofrece dinero o un buen premio, como un iPad, pero usted debe completar una encuesta. Estas encuestas a menudo solicitarán información personal, especialmente la que se encuentra en las preguntas de seguridad, para tratar de identificarlo y obtener acceso a sus cuentas.

Los estafadores usarán correos electrónicos o mensajes de texto para engañarte y que les des tu información personal. Pueden intentar robar sus contraseñas, números de cuenta o números de Seguro Social. Si obtienen esa información, podrían obtener acceso a su correo electrónico, banco, tarjetas de crédito u otras cuentas. Los correos electrónicos y mensajes de texto de phishing a menudo cuentan una historia para engañarlo para que haga clic en un enlace o abra un archivo adjunto.

Tácticas usadas en Estafas de Phishing:

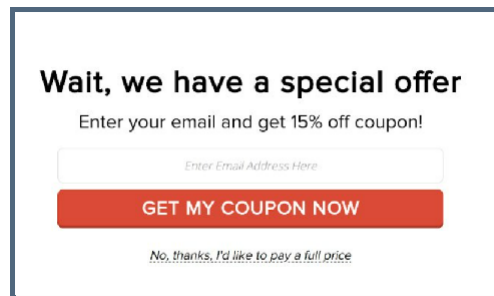
- ★ Los estafadores dicen que han notado alguna actividad sospechosa o intentos del login
- ★ Pedirle que confirme su información personal
- ★ Pedirle que haga clic en un enlace para hacer un pago
- ★ Ofrezca un cupón para cosas gratis

Ventana Emergente y Anuncios

Cuando usa un navegador de internet, tiene que tener en cuenta las ventanas emergentes y los anuncios.

Ventanas Emergentes son ventanas (o texto/cuadrados gráficos) que bloquean su acceso a una pagina o algo mas hasta que las cierra.

Anuncios son cosas que tratan de que hagas algo como dar clic e ir a paginas de compras. Ellos pueden ser maliciosos porque pueden obligarte a dar clic a algo, obtener información de usted, o intentar estafarlo.



Ejemplo de un anuncio de forma de ventana emergente

Es importante tener en cuenta que no todas las ventanas emergentes y anuncios son maliciosos. La manera de saber si una ventana emergente o anuncio es malicioso es analizar su contenido. Por ejemplo, si una pagina te pregunta por tu correo electrónico para un boletín informativo puede que no sea malicioso. Por otra mano, si una ventana emergente dice "¡Acaba de ganar un iPad gratuito!" o "Su computadora tiene 20 virus, ¡Límpiala ahora!" pueden ser maliciosos. Cosas importantes de tener en cuenta siempre son: ¿Es un contenido que tiene sentido con el de la pagina? ¿Es demasiado llamativo o demasiado bueno para ser verdad? **¿Esto es algo que debería darle clic?**

Hábitos de descarga segura

El hábito de descarga segura más importante es descargar archivos de solamente sitios web confiables. Use las preguntas anteriores para evaluar si debe o no confiar en un sitio web antes de descargar archivos en su computadora.

Una bandera roja para tener en cuenta es un sitio web que ofrece una descarga que tiene un anuncio que pretende ser un botón de descarga. En la imagen abajo, observe el triángulo azul resaltado en amarillo a la izquierda sobre el botón verde "Iniciar descarga". Ese icono de triángulo significa que el botón "Iniciar descarga" es en realidad un anuncio.

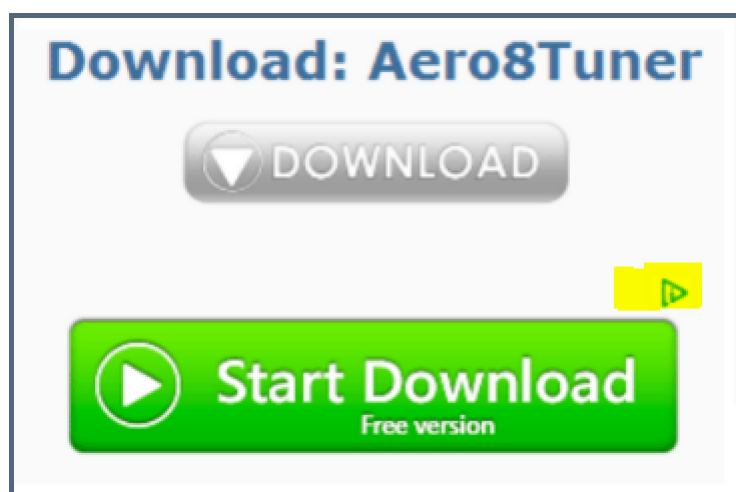


Imagen de un anuncio de sitio web con un botón de descarga

Sea siempre consciente y cauteloso de las opciones gratuitas para las cosas por las que normalmente esperaría pagar. Esta es una señal de que el archivo puede no ser seguro. Estos hábitos de seguridad en línea también se aplican al hacer clic en enlaces, archivos adjuntos e imágenes en su correo electrónico, así como en otras plataformas que permiten a los usuarios compartir archivos.

Un buen consejo general.

Confíe en su instinto. Si un sitio web le da un mal sensación, no envíe ninguna información confidencial ni descargue nada de él.

