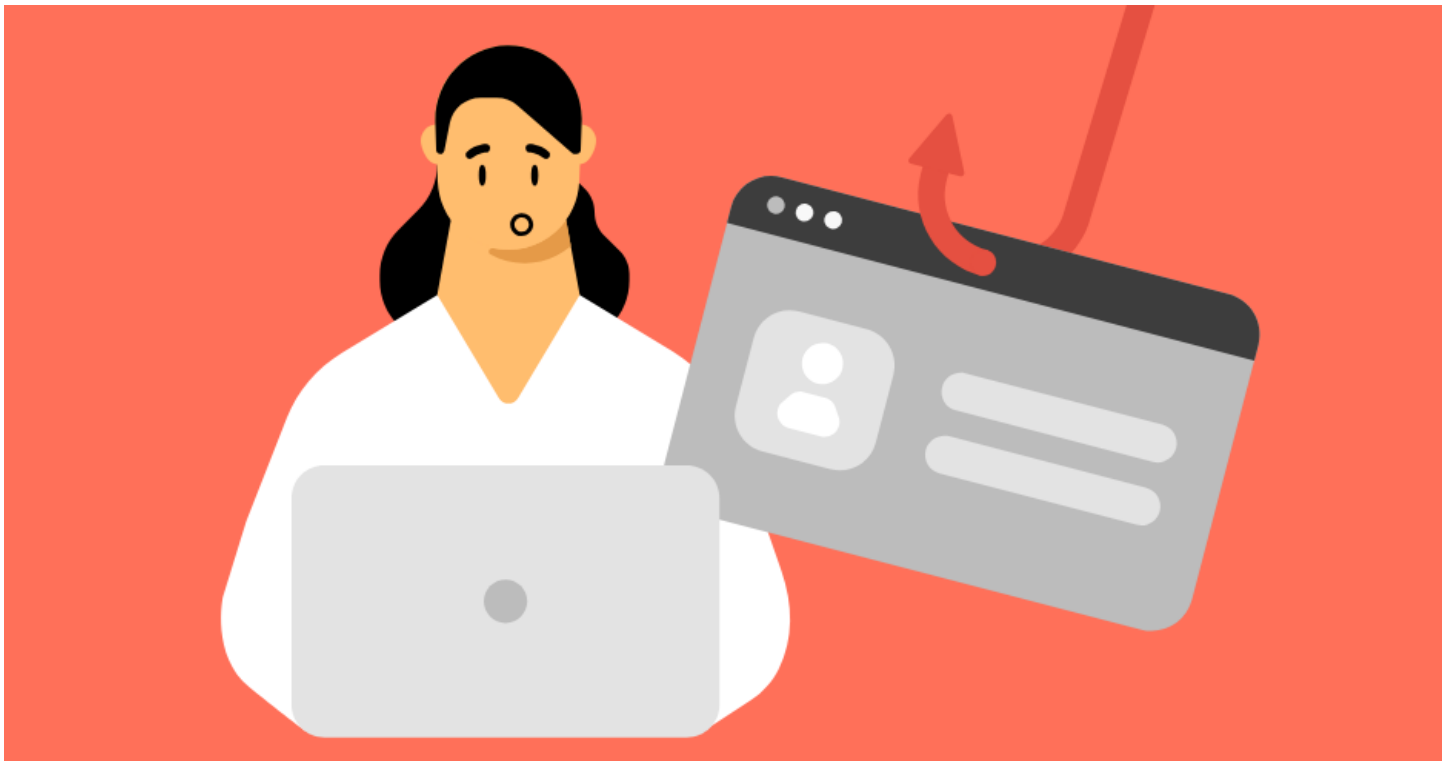
Hoy en día, y cada vez más en Internet, es común encontrar sitios que prometen ofertas increíbles, como productos a precios rebajadísimos, vales de regalo o incluso premios como iPhones (por lo menos por aquí).



Si bien muchos de estos sitios son obviamente fraudulentos, otros son lo suficientemente sofisticados como para engañar incluso a usuarios con experiencia en tecnología. Para protegerte, es crucial entender cómo funcionan estos sitios falsos y aprender a identificar las señales de alerta.

¿A que se le dicen sitios web falsos o fraudulentos?

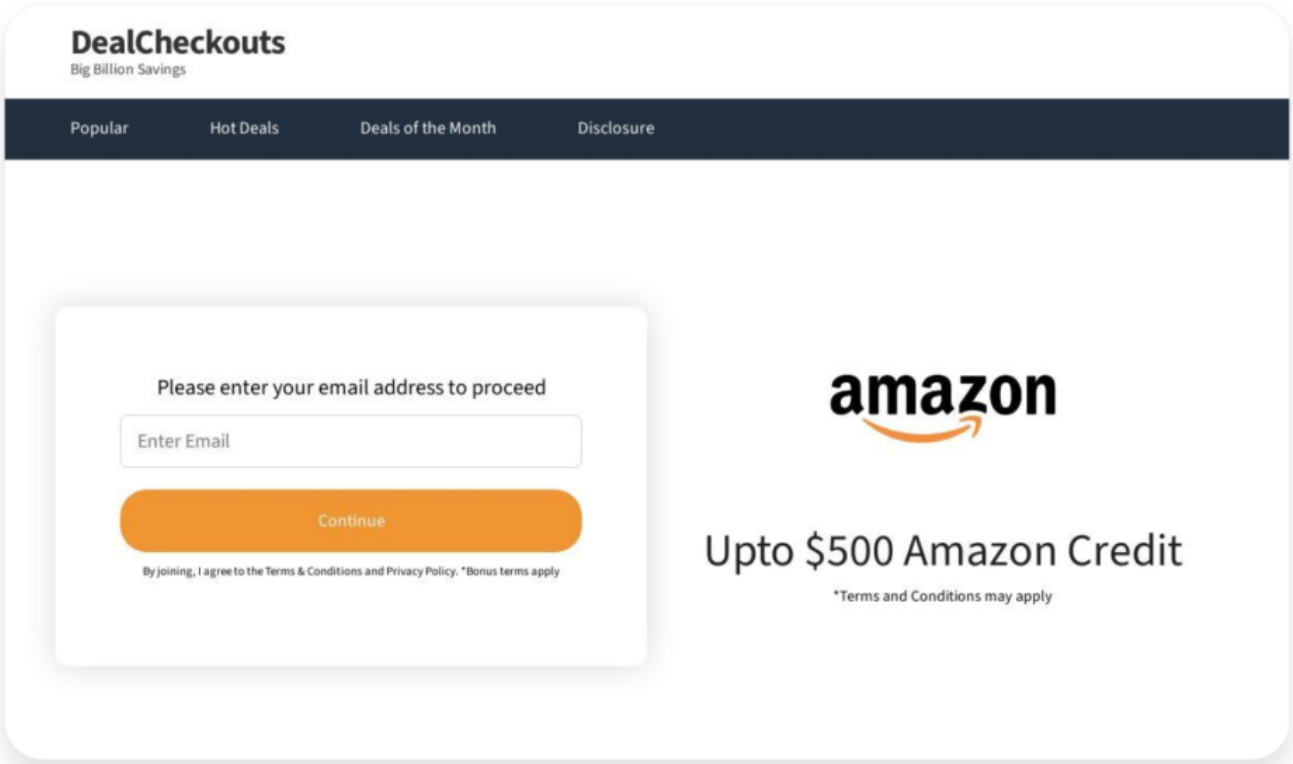
Los sitios web falsos están diseñados específicamente para engañar a los usuarios. Su objetivo principal es obtener información confidencial, realizar pagos fraudulentos o distribuir software malicioso (malware). Para lograrlo, los estafadores suelen copiar el diseño de sitios web legítimos de marcas o servicios populares, haciéndolos parecer auténticos.

Ejemplos de sitios fraudulentos incluyen:

- **Sitios de phishing**: se hacen pasar por páginas legítimas de empresas conocidas, como banca online o tiendas online, para robar datos como nombres de usuario, contraseñas y detalles de tarjetas de crédito.
- **Sitios clonados**: estos imitan el diseño y la funcionalidad de sitios oficiales, como páginas de gobierno o empresas reconocidas, para engañarte y que compartas información personal o realices pagos.
- **Páginas de malware**: se presentan como sitios seguros, pero en realidad descargan virus, spyware u otros tipos de software muy peligroso y dañino en tus dispositivos.

Tipos comunes de sitios web fraudulentos

Estos son algunos de los tipos de sitios web falsos más comunes que puedes encontrar en la web:

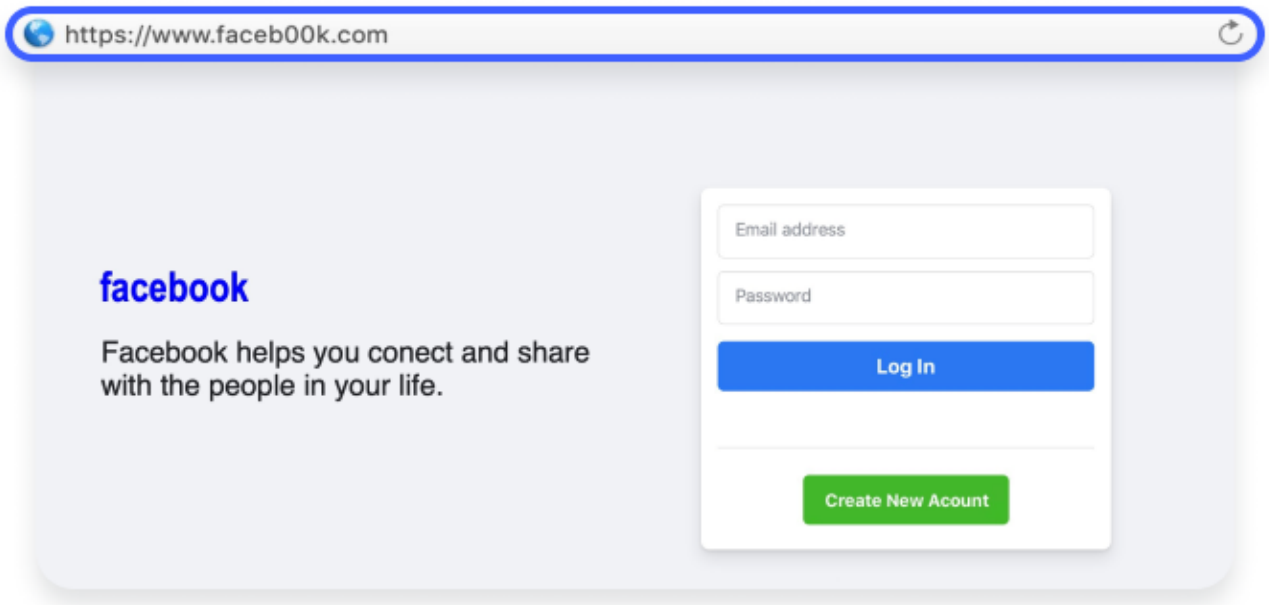


1. **Sitios de phishing**: Estos son páginas que intentan obtener tus datos personales al hacerse pasar por sitios web legítimos. Los estafadores suelen enviar correos electrónicos con enlaces a estas páginas falsas, que imitan a servicios populares como **PayPal**, **Amazon** o incluso tu banco. Una vez que ingresas tus datos, los estafadores los utilizan para robar tu identidad o vaciar tu cuenta.
2. **Sitios de distribución de malware**: Estos sitios parecen ofrecer descargas legítimas, como actualizaciones de software o programas gratuitos. Sin embargo, al descargar el archivo, en realidad estás instalando malware en tu dispositivo. Esto puede resultar en la pérdida de información, control del sistema o incluso un secuestro de tus archivos mediante Ransomware.
3. **Sitios clonados**: Imitan a la perfectamente el diseño y contenido de sitios web originales, como bancos, servicios del gobierno o empresas de seguros, etc. Su finalidad es convencerte a hacer pagos falsos, dar información confidencial o renovar servicios inexistentes.
4. **Tiendas en línea falsas**: Son comercios electrónicos que imitan a minoristas confiables, ofreciendo productos con grandes descuentos. Sin embargo, una vez que realizas el pago, puedes recibir productos falsos, de baja calidad o, en muchas veces, inclusive no recibir nada.
5. **Estafas de beneficencia**: Los estafadores crean sitios web que se hacen pasar por organizaciones benéficas legítimas, especialmente en momentos de crisis, como desastres naturales o pandemias. Te piden donaciones que, en lugar de ir a una buena causa, terminan en los bolsillos de los cibercriminales.
6. **Estafas de soporte técnico**: Utilizan tácticas como ventanas emergentes o popups o llamadas falsas para hacerte creer que tu computadora tiene problemas graves. Luego, los estafadores se ofrecen a «arreglar» el problema, cobrándote por servicios innecesarios o robando tu información personal.
7. **Estafas de inversión**: Prometen oportunidades de inversión con rendimientos altos y sin riesgo. Por ejemplo, en el mundo de las cripto divisas. Estas estafas son atractivas para personas que buscan hacer crecer su dinero rápidamente, pero en realidad, los estafadores desaparecen con tu dinero sin darte ninguna ganancia.
8. **Estafas de lotería o premios**: En estas estafas, te hacen creer que has ganado un premio o una lotería, pero para reclamarlo, debes pagar una tarifa o proporcionar información personal. Una vez que lo haces, los estafadores desaparecen con tu dinero o datos.

Como dice el dicho: «*cuando la limosna es grande, hasta el santo desconfía*«

Cómo identificar un sitio web legítimo

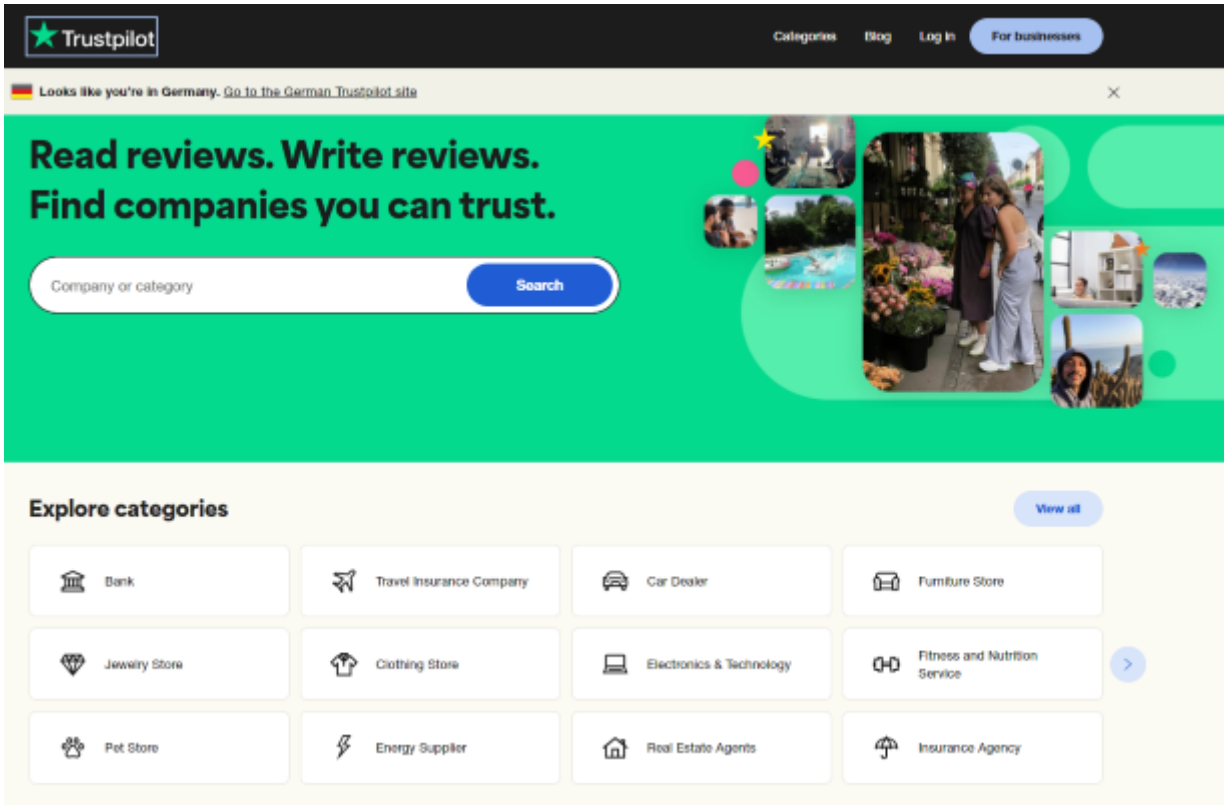
Aunque algunos sitios falsos son muy convincentes, hay varias señales o indicios que podés buscar para determinar si un sitio web es legítimo o una estafa.
Aquí hay algunas recomendaciones para detectar un sitio fraudulento:



1. **Revisar la fuente del enlace**: los sitios fraudulentos suelen ser promocionados a través de correos electrónicos sospechosos o mensajes en redes sociales de perfiles desconocidos. Si recibes un link inesperado, especialmente de una fuente no confiable, es mejor no hacer clic. Los estafadores a menudo compran anuncios y optimizan sus sitios para que aparezcan en los resultados de búsqueda, por lo que es importante verificar siempre la fuente.
2. **Verificar el nombre de dominio y la URL**: antes de hacer clic en un enlace, revisa detenidamente la dirección web. Los sitios falsos a menudo utilizan nombres de dominio que se parecen mucho a los de sitios originales, con pequeñas variaciones. Por ejemplo, en lugar de "www.facebook.com", podrían usar "www.faceb00k.com" (con ceros en lugar de las letras «o»). También puedes utilizar verificadores de enlaces, como la herramienta de **Google Safe Browsing**, para comprobar si la URL es segura.
3. **Comprobar si el sitio es seguro**: un sitio web legítimo debe tener un certificado de seguridad **SSL/TLS**, lo cual se indica con un candado en la barra de direcciones y el prefijo "**https://**" antes de la URL. Si ves solo "**http://**", es una señal de que el sitio no es seguro. Para esto, normalmente el navegador Google Chrome te lo advierte automáticamente.
4. **Examinar el diseño y el contenido**: los sitios web fraudulentos suelen ser mal diseñados, con errores de gramática, imágenes borrosas y anuncios invasivos. Si notas muchos errores en la página o contenido de baja calidad, es probable que sea una estafa.
5. **Verificar la antigüedad del dominio**: los sitios legítimos suelen tener dominios registrados durante años, mientras que los sitios fraudulentos pueden estar activos solo por unas semanas o meses. Podes verificar la antigüedad de un dominio usando herramientas de búsqueda **Whois**.
6. **Busca opiniones y reseñas**: las páginas webs confiables suelen tener una mezcla de reseñas positivas y negativas de usuarios. Si encuentras un sitio con solo opiniones extremadamente positivas o muy pocas reseñas, es una señal de advertencia. Una buena plataforma que desde años yo mismo utilizo es **Trustpilot**.
7. **Verificar la información de contacto**: los sitios legítimos ofrecen detalles de contacto claros y formas de atención al cliente. Si un sitio no proporciona esta información o parece sospechosa, es

posible que estés ante una estafa. En Alemania o países de habla germana, al pie de las páginas, el término utilizado para identificar a los responsables es «**Impressum**«

8. **Tener cuidado con la urgencia o las ofertas demasiado buenas**: si un sitio te empuja a que tomes una decisión rápida o te ofrece productos de alta calidad a precios ridículamente bajos, es probable que sea una estafa. Los estafadores suelen usar tácticas que crean una sensación de urgencia para que actúes sin pensar.
9. **Usar software de seguridad confiable**: utilizar herramientas anti-phishing y software de seguridad actualizado puede ayudar a detectar y bloquear sitios web peligrosos antes de que puedas caer en una estafa. Estas herramientas suelen identificar sitios fraudulentos y advertirte antes de que los visites.



Conclusión

En el mundo digital, los sitios web fraudulentos son cada vez más comunes y sofisticados. Sin embargo, teniendo en cuenta estos consejos y teniendo un enfoque cuidadoso, podes reducir el riesgo de caer en una estafa. Verifica los detalles de un sitio antes de dar información personal o hacer pagos. Y como siempre digo: «*el mejor anti-virus es el sentido común*«

Y recuerda como decía el **Martín Fierro**:
«A caballo regalado no se le mira el diente, pero tampoco se monta sin cuidado»
(lo dijo realmente...?)

Por favor, síguenos y danos «me gusta»: