Cómo comprobar si un enlace es malicioso

En la actualidad muchos fraudes intentan obtener información confidencial de los usuarios o infectar sus dispositivos difundiendo enlaces fraudulentos de tal forma que si el usuario no sabe analizarlos, puede acabar resultando ser víctima de algún engaño.

¿Te gustaría saber cómo analizar un enlace? A través de esta simulación aprenderás a detectar páginas fraudulentas. ¡Adelante!

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

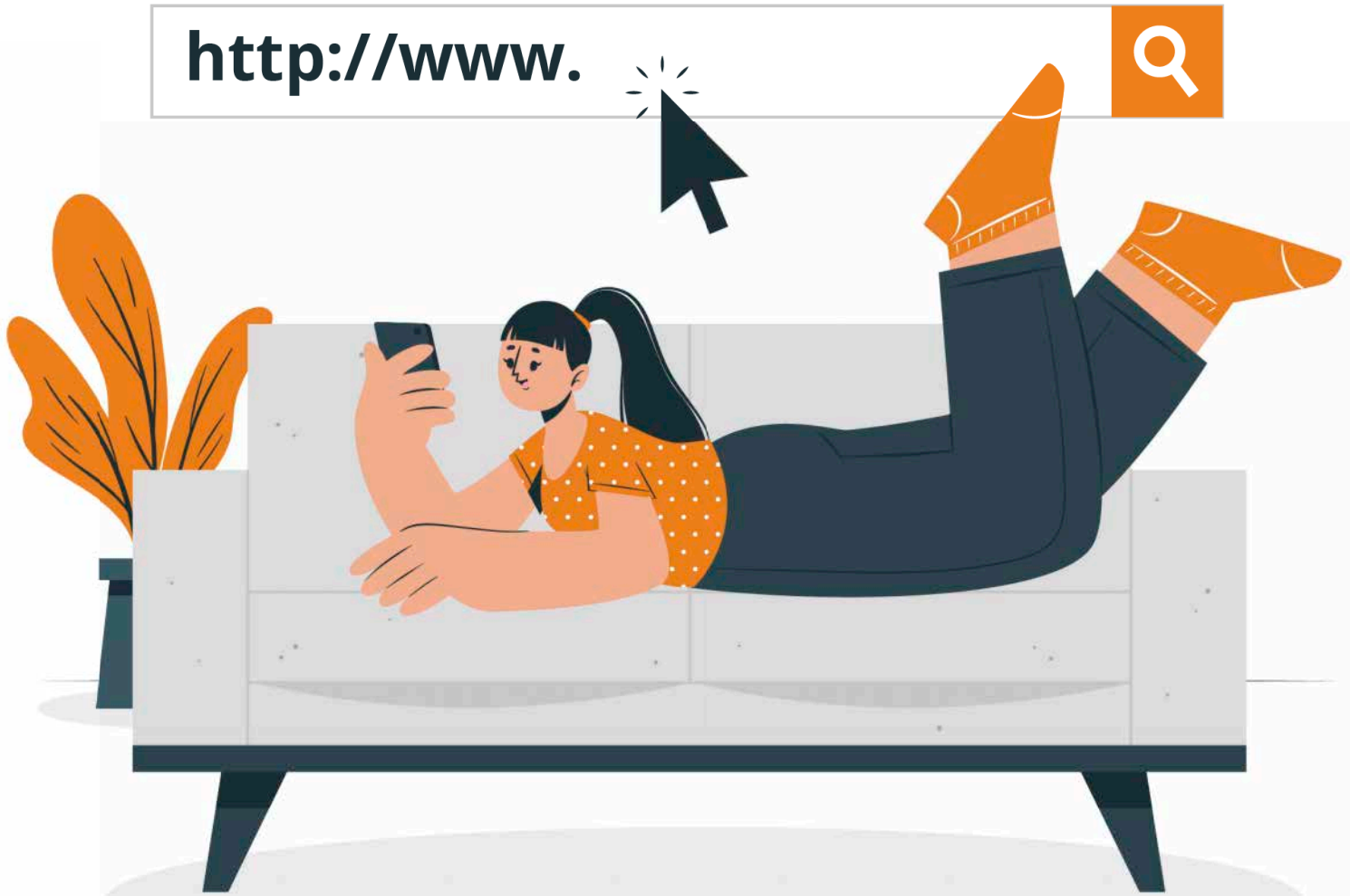
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

¿Cómo ha llegado hasta ti el enlace?

Un enlace puede llegar hasta ti de diferentes formas: correo electrónico, SMS, mensajería instantánea, red social, foros, anuncios, webs mientras navegas, etc.

Nunca pinches en un enlace sin antes realizar las **comprobaciones** que te proponemos a continuación.



Paso 1

¿Qué comprobaciones debes realizar antes de pulsar sobre él?

Paso 1: Comprueba si el enlace empieza por HTTP o HTTPS

Cuando navegas por Internet, es importante **prestar atención** si el enlace comienza por '**HTTP' o 'HTTPS**'. Esto te permite comprender el nivel de seguridad y privacidad que ofrece el sitio web al que te conectas.

Para verificar esto, solo necesitas **observar el inicio de la dirección web** en la barra de direcciones de tu navegador. Si la URL comienza con **'http://',** significa que el sitio web **no utiliza cifrado** y **no es seguro** para compartir información personal. Por el contrario, si comienza por **'https://',** significa que el sitio web utiliza un **certificado SSL o TLS** y **es seguro** para realizar transacciones y compartir información confidencial.

HTTPS indica que la **comunicación es segura** con esa web, pero no garantiza que sea la web a la que creemos que nos estamos conectando, hay que **revisar la URL** (pasos 2 y 3) y **que el certificado corresponda a la web oficial** (paso 6).

Paso 2

Paso 2: Contrasta si los caracteres del enlace, aparentemente, corresponden con la web legítima de la entidad o servicio que dice ser

Es crucial tomar medidas para **verificar los enlaces** para evitar estafas en línea. Debes estar atento a **errores de ortografía** o **cambios sutiles en el enlace**. Los atacantes frecuentemente intentan engañarte usando enlaces que **se parecen mucho** a los de páginas web legítimas, pero introduciendo pequeños cambios.

Por ejemplo, podrían utilizar '**www.tubanc0.com**' en lugar de '**www.tubanco.com**' en el que han cambiado una 'o' por un cero.

Paso 3: Revisa antes de pulsar a qué web te redirige el enlace

Cuando pongas **el cursor sobre un enlace**, si estás con un ordenador, o **pulsar** sobre el enlace **varios segundos**, si se trata de un smartphone o tablet, **fíjate en la dirección web** a la que te llevará el enlace. Esto te ayudará a **comprobar si coincide** con el sitio web que esperas visitar. Si te parece extraña o diferente, podría ser una **señal** de que se trata de un **intento de estafa** o **redireccionamiento** a un sitio **malicioso** o de dudosa reputación.

Los enlaces pueden llevarte a páginas diferentes de las que aparecen escritas en un mensaje, documento o web. Estas redirecciones pueden ser utilizadas para dirigirte a **sitios web peligrosos** que contienen **virus** o intentan **robarte información**.

Paso 4: Observa el final del enlace

Cuando navegas por Internet es importante fijarte en la **terminación del enlace**. Esto puede ayudarte a saber si es **confiable** o **sospechoso**. Por ejemplo, los sitios **web gubernamentales** suelen tener terminaciones **.gob** y los de **instituciones educativas**, **.edu**. Lo más habitual es que una web termine en **.es** si estás consultando servicios de **ámbito nacional** o **.com** para empresas o servicios a **nivel mundial**.

Además, algunas terminaciones como **.exe o .zip** suelen estar asociadas con **archivos descargables** y pueden contener ***malware***. Te aconsejamos tener cuidado al interactuar con ellos y evitar descargarlos si no estás seguro de su origen. Así podrás proteger tu dispositivo y mantener tus datos seguros.

Paso 5: Analiza los enlaces acortados

Los enlaces acortados en Internet son **versiones más cortas de las URL originales**, utilizados para compartir contenido de manera fácil. Sin embargo, **pueden ocultar la dirección web real** y representar riesgos de seguridad. Es importante tener precaución al hacer clic en ellos.

Para protegerte, **utiliza servicios en línea** que te permitan **expandir los enlaces acortados** y **mostrar la URL completa** antes de hacer clic para saber a qué sitio web te redirigen. Además, **presta atención a la fuente de los enlaces** y evita hacer clic en aquellos procedentes de fuentes no confiables.

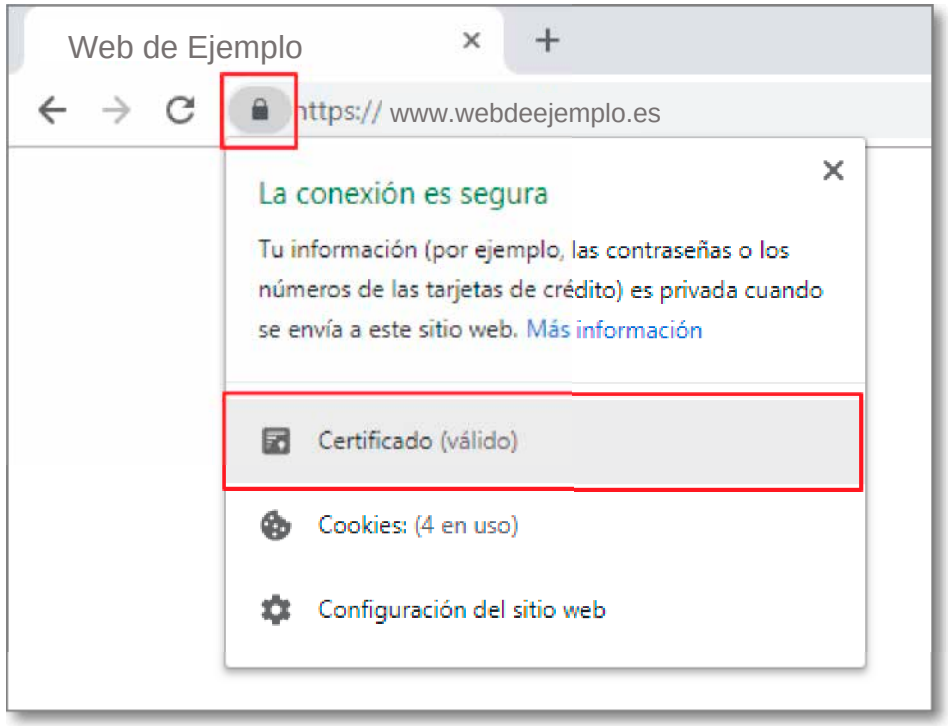
Comprobaciones adicionales si has accedido a la web

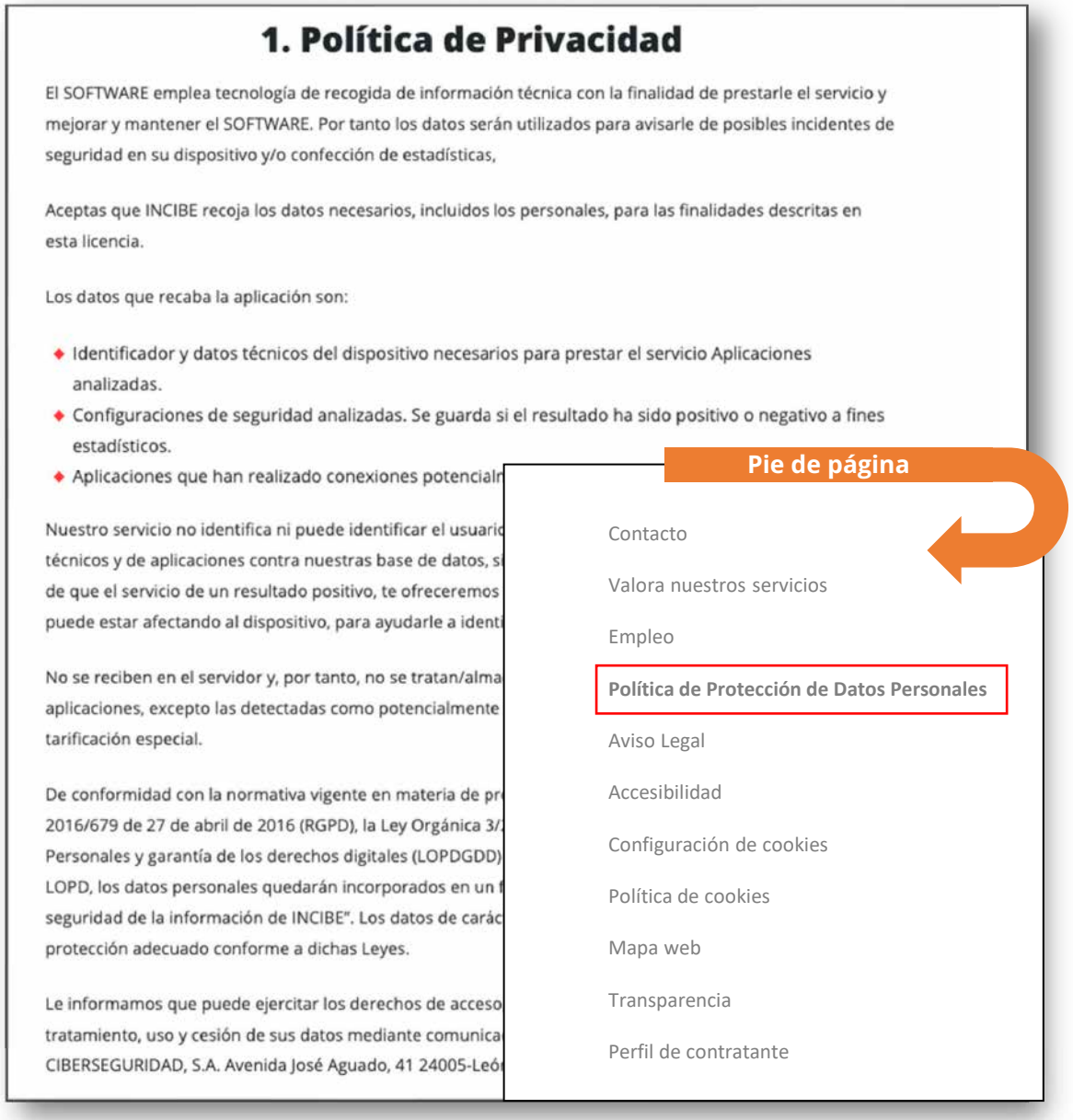
Paso 6: Chequea el certificado digital de la web

Es importante **comprobar** si un sitio web al que hemos accedido dispone de **certificado digital** para asegurarte de que estás visitando un **sitio legítimo** y **no** uno **falso** o **peligroso**. Los certificados digitales son emitidos por entidades de confianza y confirman la identidad del propietario del sitio web.

Además, si un sitio web dispone de certificado digital, la **comunicación** entre tu **navegador** y el **sitio web estará cifrada**, lo que significa que cualquier información personal que envíes, como contraseñas o números de tarjetas de crédito, estará protegida y no podrá ser vista por otras personas.

El **certificado digital** indica que la comunicación es segura con esa web, pero no garantiza que sea la web a la que creemos que nos estamos conectando, hay que **revisar la URL** (pasos 2 y 3).





Paso 7: Lee las políticas de privacidad de la web

Revisar las **políticas de privacidad** es importante para **proteger tus datos** personales en Internet.

Estos **documentos legales** te muestran cómo se **recopilan**, **usan** y **protegen** tus **datos** en un sitio **web**. Al leer estas políticas, puedes saber qué información se recopila, cómo se utiliza y si se comparte con otras personas.

Esto te ayuda a **tomar decisiones informadas** sobre la seguridad y confianza del sitio web en relación con tus datos personales.

¿Qué herramientas te pueden ayudar a desenmascarar un enlace malicioso?

En muchas ocasiones, aún tomando todas las precauciones comentadas, puede que sigas con dudas de si un enlace es malicioso o no. Por ello, si necesitas un recurso extra en el que apoyarte, haz uso de **Analizadores de URL y archivos**.

Escanea este código QR para descubrir algunos analizadores interesantes.

Hacer uso de este tipo de herramientas es muy sencillo:

1. **Accede a la herramienta.** Algunas ofrecen servicio online y no requieren de instalación.
2. **Copia o introduce la URL** que deseas analizar en el campo de texto específico para ello.

Si quieres **analizar otro enlace**, repite de nuevo este proceso.

3. Pulsa sobre el botón "**Analizar URL**" o sobre la tecla "**Enter**".
4. **Revisa los resultados**: Si los resultados muestran que se trata de un sitio web que está **limpio, puedes acceder** a él. Si algún resultado indica que podría ser **malicioso**, entonces mejor **no accedas** para evitar problemas. Si quieres **analizar otro enlace**, repite de nuevo este proceso.

¿Sigues con dudas?

Recuerda que tienes a tu disposición **la Línea de Ayuda en Ciberseguridad de INCIBE**, llamando al **017** de manera gratuita y confidencial o chateando por **WhatsApp (900 116 117)** o **Telegram (@INCIBE017)**.

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta