

Capítulo 2 Seguridad

- [Seguridad](#)
- [Ciberataques](#)
- [Enlaces y Phising](#)
- [Privacidad](#)
- [Peligros](#)
- [Recursos](#)
- [Control parental](#)
- [Cuida tu identidad digital](#)
- [Para saber +](#)

Seguridad

En este capítulo nos centramos en la prevención de problemas y en la concienciación de los alumnos sobre el buen uso de Internet.



Ciberataques

Los delincuentes siempre están al acecho, y se aprovechan de nuestro desconocimiento. Los contenidos de este apartado están en esta sencilla guía que te ayudará a disminuir nuestras vulnerabilidades:

[GUIA DE CIBERATAQUES](#)

https://www.scribd.com/embeds/482238967/content?start_page=1view_mode=scroll&access_key=key-jjelulDY94wQ2IWj8hsX

[Guía de de la OSI by Maldita.es](#)

Enlaces y Phising



Imagen de Tumisu en Pixabay

No pinches en los enlaces alegremente.

Pincha en este enlace <https://www.catedu.es>

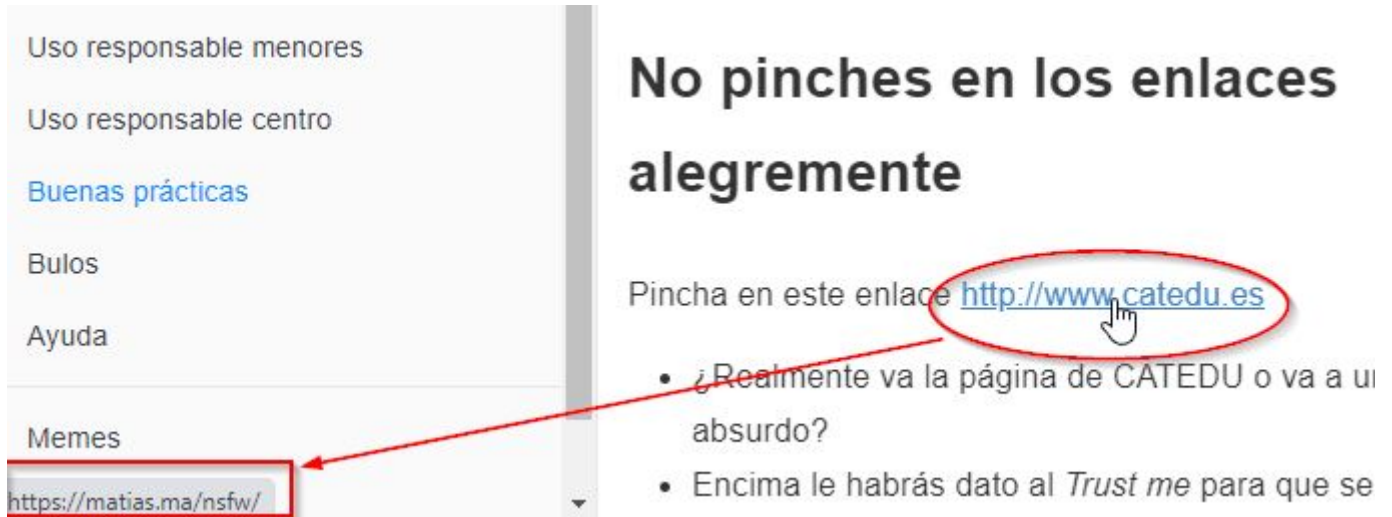
- ¿Realmente va a la página de CATEDU?
- ¡¡¡Encima le habrás dato al *Trust me* para que se ejecute el Script de la página!!!
- ¿Sabes que podrías haber ejecutado código malicioso??

¿Qué puedo hacer para que esto no me pase?

Fijarte dónde va exáctamente el enlace. **EL TEXTO DE UN ENLACE Y EL ENLACE SON COSAS INDEPENDIENTES" como has visto.

Para detectarlo

Pon el cursor encima sin hacer click ("hover") y fíjate abajo a la izquierda :



The image shows a screenshot of a website's navigation menu on the left and a main content area on the right. The menu items are: 'Uso responsable menores', 'Uso responsable centro', 'Buenas prácticas', 'Bulos', 'Ayuda', and 'Memes'. The 'Memes' item is highlighted with a red box, and a red arrow points from it to a red box containing the URL 'https://matias.ma/nsfw/'. In the main content area, there is a large heading 'No pinches en los enlaces alegremente'. Below it, the text says 'Pincha en este enlace' followed by a blue link 'http://www.catedu.es' which is circled in red. A mouse cursor is hovering over the link. Below the link, there are two bullet points: '• ¿Realmente va la página de CATEDU o va a un absurdo?' and '• Encima le habrás dado al Trust me para que se'.

Igualmente en correos electrónicos, links en imágenes, whatsapps, ... este es un correo real que me ha llegado, parece que es de Endesa, pero no lo es ☹ :

From Atención al Cliente Endesa <atencionalcliente@endesaonline.com> ☆

Subject **Solicitud de documentación 28528392**

To javierquintana [redacted] ☆

endesa Información adicional respuesta solicitud nº 28528392

Estimado/a JAVIER,

Mi nombre es María P, soy el responsable de gestionar tu solicitud. Para poder gestionar de forma correcta tu solicitud nº **28528392**, necesitaría que corroborases tu identidad mediante algún documento identificativo.

Puedes acceder al siguiente enlace para adjuntar una copia o fotografía de tu DNI, NIE o

Adjuntar NIF **¡¡ TRAMPA!!**

Quedamos a la espera de recibir el documento para poder continuar con la gestión de tu caso.


Que el remitente sea endesaonline.com no significa que sea real


De hecho si vamos al menú de Gmail - ver original vemos que el origen no es endesaonline.com :

Received: from [10.211.179.55] ([10.211.179.55:38982] helo=eu31-app1-8-cdg.ops.sfdc.net) by mx3-cdg-sp2.mta.salesforce.com

curiosamente estos enlaces son correctos

RECUERDA QUE DESDE [ÁREA CLIENTE](#) PUEDES:

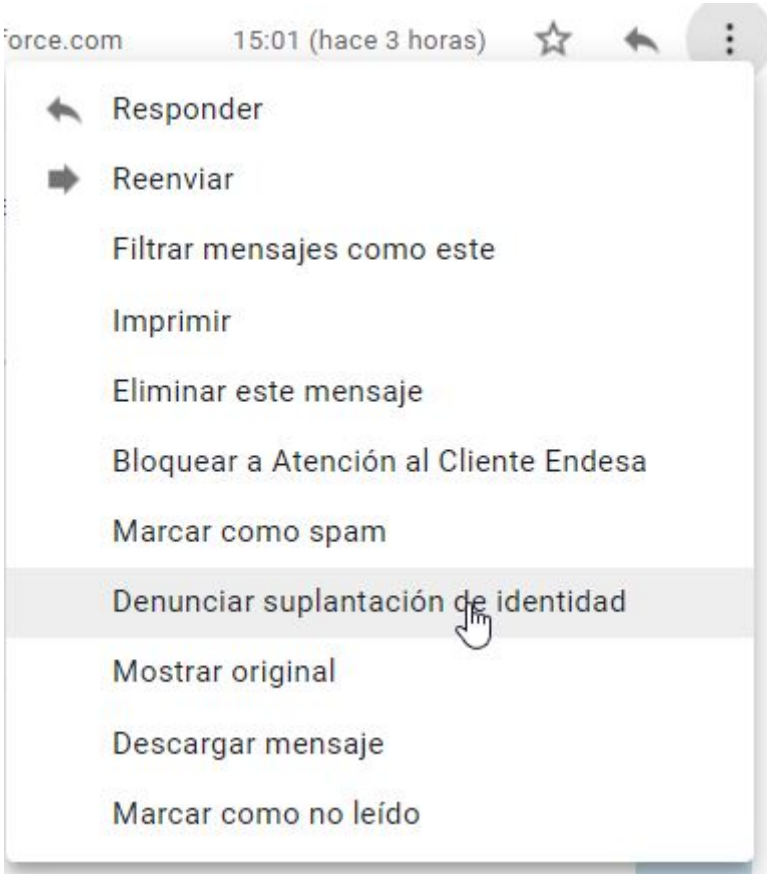
 Consultar los datos de tus [contratos y facturas](#).

 Realizar todas las [modificaciones contractuales](#) (modificación de cuenta bancaria, titular, datos de contacto, etc.).

<http://endesab2c.force.com/enviarnif?id=a5t51000000ftJMQAY> Today Pa

Me pregunto para qué quieren mi DNI escaneado .. ☐

Lo que tenemos que hacer por **ética** es **denunciar** es la única manera de mantener a raya estos delincuentes, una manera fácil es desde el mismo gestor de email:




En resumen: Una de las técnicas del Phishing: hacerse pasar por una entidad, banco, etc.. y sus enlaces van a otro sitio, con la intención de coger tus claves bancarias, tarjetas...




[Un ejemplo típico es ofrecer el robot de cocina Lidl por 2€.](#)

Te recomendamos leer este consejo de la Guardia Civil :

“ ¡Evita caer en el [#phishing!](#)

Aprender a identificar cualquier correo fraudulento  con esta infografía de [@osiseguridad](#)

 <https://t.co/ZojDB7HLW1> pic.twitter.com/kNeGm68NkX

— Guardia Civil  (@guardiacivil) [May 11, 2020](#)

Si no es HTTPS no te fies

El protocolo HTTPS (o candado en la barra de navegación) es para que los datos vayan cifrados.




Imagen de skylarvision en Pixabay

Por lo tanto **SI NO LO LLEVA, NO TE FIES** un banco, un comercio **nunca** navegaría sin cifrar los datos. [ver](#)

Pero que lo lleve NO es garantía, [la mitad de páginas Phising ya tienen https](#)

“ ¿Sabes qué es una "Banca electrónica fraudulenta o phishing bancario"?

¿Sabrías identificar una [#Web](#) "clonada" antes de hacer clic en ella?

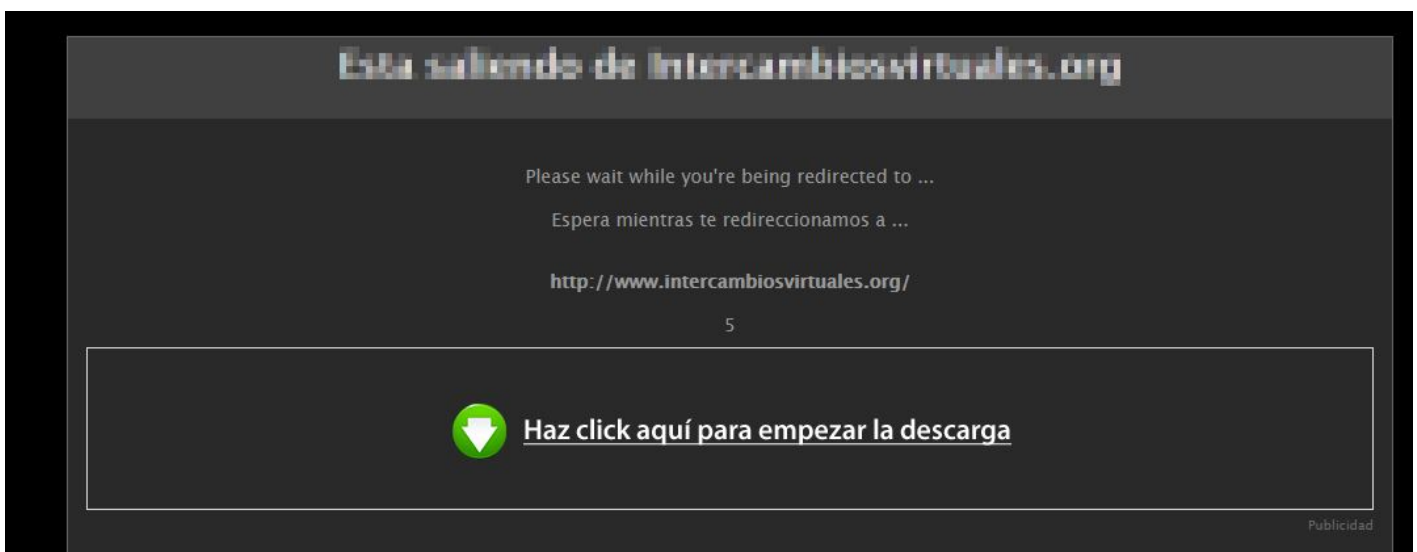
Si estás "pez"...  no está de más que le eches un vistazo a las

recomendaciones de esta infografía [\[\] \[\] \[\] \[\] #SeguridadInternet](#)
pic.twitter.com/pEvcoD19Gj

— Guardia Civil [\[\] \[\] \[\] \[\] \(@guardiacivil\)](#) [May 25, 2020](#)

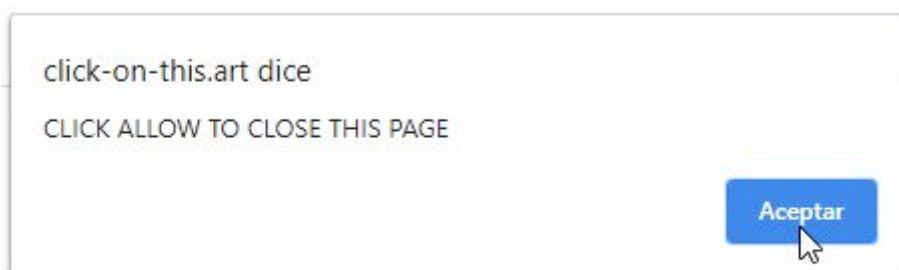
No te precipites pinchando anuncios

Imagina que pulsas en **descargar algo** y te sale esta página



¿Clicas en "Haz click aquí para empezar la descarga"? **NO** eso es un anuncio (mejor dicho, una página con código malicioso), fíjate bien!! abajo a la derecha pone *Publicidad* con un tamaño de letra no apto para mayores de 50.

Y **bajo ningún concepto** des "Permisos" para descargar o continuar. Se instala código malicioso.



Por favor toque el **Permitir** botón para continuar



Regla de oro

No descargues software ni archivos de sitios no oficiales o de confianza.

y por supuesto ..

Nada de piratería!! Si te llega un programa de pago pero de manera gratuita piensa... ¿por qué lo hacen? ¿altruismo? No, lo más probable será para que tú ejecutes un código malicioso.

todo esto ya lo sabes ?.....

Pues listillo/a pincha [en este simulador](#) a ver si aciertas:



[/simulador-phishing-1](#)

Origen: SDA Servicios Digitales de Aragón y Aragonesa de servicios Telemáticos

Privacidad

Recomendamos leerte estas fichas

Guía de privacidad y seguridad en Internet

VER LAS FICHAS EN <https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet>

https://docs.google.com/presentation/d/e/2PACX-1vQ5sb3v_OHUwBGBWP-POE9rYTedRx7H27SNry0kQPE8n6QzWEtsOXJAo4OM84nniUuFZEIw8nHLQjGi/embed?start=false&delayms=3000

Autoría: OSI Oficina de Seguridad el Internauta www.osi.es

Si quieres configurar tu privacidad en las principales RRSS mira estos [tutoriales](#)

Privacidad en Facebook



Ver videotutorial

Privacidad en Twitter



Ver videotutorial

Privacidad en Instagram



Ver videotutorial

Privacidad en Youtube



Ver videotutorial

Privacidad en Whatsapp



Ver videotutorial

Privacidad en Snapchat



Ver videotutorial

(<https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet>)

Peligros

<https://docs.google.com/presentation/d/e/2PACX->

[1vTH2IKdapM_1zHbUzFUedKtTPCg_LhQJvnj9TeWoQ0bEgL_yZ5grBUheoXDzwaUtzPjVYU_hHOaocIC/embed?start=false&loop=false&delayms=3000](https://docs.google.com/presentation/d/e/2PACX-1vTH2IKdapM_1zHbUzFUedKtTPCg_LhQJvnj9TeWoQ0bEgL_yZ5grBUheoXDzwaUtzPjVYU_hHOaocIC/embed?start=false&loop=false&delayms=3000)

Recursos

<https://docs.google.com/presentation/d/e/2PACX->

[1vQo9_h5R21G8n3tZNUzAoTjjwBnZ6ZX6SqtFj2I9IjIJeHeDPEBYrF26Tq3JThy_YnhjfDjzkjvIaQ/embed?start=false&loop=false&delayms=3000](https://docs.google.com/presentation/d/e/2PACX-1vQo9_h5R21G8n3tZNUzAoTjjwBnZ6ZX6SqtFj2I9IjIJeHeDPEBYrF26Tq3JThy_YnhjfDjzkjvIaQ/embed?start=false&loop=false&delayms=3000)

Control parental

Situémonos

Según <https://www.qustodio.com/es/product-why-qustodio/> el 34% de estudiantes en colegios e institutos ha experimentado cyberbuying, el 41% de niños ha contactado con desconocidos peligrosos o no deseados y el 31% de niños han mandado o recibido mensajes con contenido sexual. (enero 2020).

RECOMENDADO: DNS de control infantil

Una manera sencilla sin instalar un software es configurar unos DNS que nos filtren los contenidos. Puedes buscar en Internet que hay varios y con distintos filtros pero **es obligatorio en los centros educativos públicos de Aragón [configurar los DNS del Gobierno de Aragón](#)**.

No obstante existen aplicaciones

Normalmente el control parental se hace instalando un software de control. Hacemos un repaso de los que existen en el mercado.

https://docs.google.com/presentation/d/e/2PACX-1vS_Bxv3YZUFySWFK-o1bFj9YLxmGg9IMV8w9FJEy4ehB329qWRNv3nEC43uL8pa81tq-X0poDoh4I7/embed?start=false&loop=false&delayms=3000

Cuida tu identidad digital

Cuida tu identidad digital

Tu identidad digital está formada por toda la información que hay sobre ti en internet, **tanto la que tú compartes como lo que otros comparten sobre ti.**

Tus perfiles de redes sociales, el contenido que publicas, las fotos y vídeos que compartes, los comentarios que haces en páginas web, etc. todo es información personal tuya que queda expuesta en Internet.



Y también hay que **contar con los terceros.** Puede haber contenido en el que aparezcas en las redes sociales de tus familiares o amistades, enlaces con tu nombre publicados por servicios que has usado o incluso información desde lugares de ocio, clubs deportivos o asociaciones.

Consejos para proteger tu información personal:

El primer paso es cambiar la forma de pensar: antes de compartir cualquier información, **valora primero si esa información es personal** y, en caso de que consideres que lo es, no la compartas a no ser que sea estrictamente necesario.



Algunos ejemplos de información personal que debes cuidar son:

1

Tu domicilio y si estás o no en casa:
Pónselo más difícil a los ladrones, pero también a quien quiera saber dónde encontrarte.



2

Fotos o vídeos comprometedores:
Evitarás que en el futuro puedan ser utilizados para intentar dañar tu imagen o que alguien se lleve una impresión equivocada sobre ti.





Para saber +



[https://aplicaciones.aragon.es/fusi/elige-tu-propia-](https://aplicaciones.aragon.es/fusi/elige-tu-propia-aventura/)

[aventura/](#)

En **AULARAGON** tenemos [un curso exclusivo](#) para esta temática

[Aquí](#) tienes el libro de contenidos

- **MÓDULO I: IDENTIDAD DIGITAL**
 - Privacidad e identidad digital.
 - Suplantación de identidad.
- **MÓDULO II: Riesgos en la red I**
 - Prevención de virus y fraudes
 - Acceso a contenidos inapropiados.
- **MÓDULO III: Riesgos en la red II**
 - Tecnoadiciones.
 - Cyberbullying, sexting y grooming.
- **MÓDULO IV: CIBERAYUDANTES un programa de centro**
 - Justificación, objetivos y contenidos.
 - Iniciativas