Programa ineco RURALTIC

Fecha 20/11/2024

Población:
Carrizo – León

Presentación del programa INECO Social

Conferencia de Jordi Romeu y Jesús Hernado.

¿Qué es?

Ingeniería y consultoría de referencia en el ámbito de la movilidad sostenible y la transformación digital dependiente del MITMA

Más de 50 años diseñando **soluciones integrales, innovadoras y tecnológicas** que han permitido avanzar hacia un nuevo modelo de movilidad más sostenible y más segura. Soluciones que contribuyen de manera directa en la mejora de la calidad de vida de millones de personas.

- ✓ Comprometidos con la **sociedad** y la transformación digital
- ✓ Valor de Ineco: 5.000 profesionales.
- ✓ Conocimiento al servicio de Rural TIC

https://www.ineco.com/webineco/ o simplemente teclea en Google nuestro nombre

¿Quiénes somos?

Jordi Romeu Crespo

Ingeniero en Electrónica
Ingeniero en Telecomunicaciones
MBA, MPRL
Director de Obra Señalización Ferroviaria y Telecomunicaciones Fijas
ADIF-AV LAV León-Asturias

¿por qué estamos aquí?
Compartir experiencia y conocimiento práctico en el uso de las nuevas tecnologías y redes sociales, habiéndome trasladado de la gran ciudad a un entorno rural

Estos somos nosotros y vosotros ¿quién sois?

¿Quiénes somos?

Jesús Hernando

Formación académica

ANALISTA INFORMÁTICO DEL MINISTERIO DE JUSTICIA

¿por qué estamos aquí?

Quiero ayudar a dar el paso que nos da “respeto”

Estos somos nosotros y vosotros ¿quién sois?

1

Estafas

Estafas Online

Podemos empezar planteándonos las siguientes preguntas:

- ✓ ¿Qué?
- ✓ ¿Quién?
- ✓ ¿Dónde?
- ✓ ¿Cómo?
- ✓ ¿Cuándo?
- ✓ ¿Por qué?

Estafas Online

✓ **¿Qué?**

El objetivo de las estafas online es básicamente conseguir información personal haciéndose pasar por alguien de confianza. Llegando incluso a veces a suplantar la identidad

✓ **¿Quién?**

Ciberdelincuente

+

Intermediario (opcional)

+

Víctima

Estafas Online

✓ **¿Dónde?**

- ❖ Con una llamada telefónica
- ❖ SMS/WhastsApp
- ❖ Correo electrónico
- ❖ Web falsa
- ❖ Perfil falso

Estafas Online

✓ **¿Cómo?**

❖ Suplantando una identidad de confianza

❖ A través de la manipulación

Emocional

¡Oportunidad! ¡Premio!

¡Alerta! ¡Urgencia!

Estafas online

✓ Casos habituales en la Web

- ❖ Suplantación web (páginas web que simulan ser otra de confianza: banco, organismo público, comercio online…)
- ❖ Tiendas online fraudulentas (webs que simulan un comercio electrónico, pero realmente están "vacías")
- ❖ Perfiles falsos en alquileres o ventas de 2ª mano

✓ Casos habituales en los SMS

- ❖ Envíos no entregados (pendiente de realizar un pago o acción adicional)
- ❖ Dinero pendiente de ingresar (solicitud de confirmación de datos bancarios u otra información personal)
- ❖ Alertas sobre cuentas o tarjetas bloqueadas
- ❖ Ofertas, promociones especiales, premios…
- ❖ Siempre presentan un hipervínculo (enlace a web)

Estafas online

✓ Casos habituales en el correo electrónico

- ❖ Mismos casos que con sms pero con formatos más elaborados (imágenes, videos, descripciones..)
- ❖ Correos "tentadores" (relaciones, soluciones a carencias físicas o emocionales)
- ❖ Contactos desconocidos (interés por entablar una relación personal o sentimental)
- ❖ Siempre presentan un hipervínculo (enlace a web)
- ❖ Borrar siempre correos que su dirección esté compuesta exclusivamente de cadenas de números y letras

Estafas Online

✓ **¿Cuándo?**

Habitualmente estás situaciones se producen cuando existe una vulnerabilidad

- ❖ Desconocimiento o manejo limitado
- ❖ Necesidad, desesperación
- ❖ Inmadurez personal o tecnológica
- ❖ Modas
- ❖ Momentos de gran actividad

Estafas Online

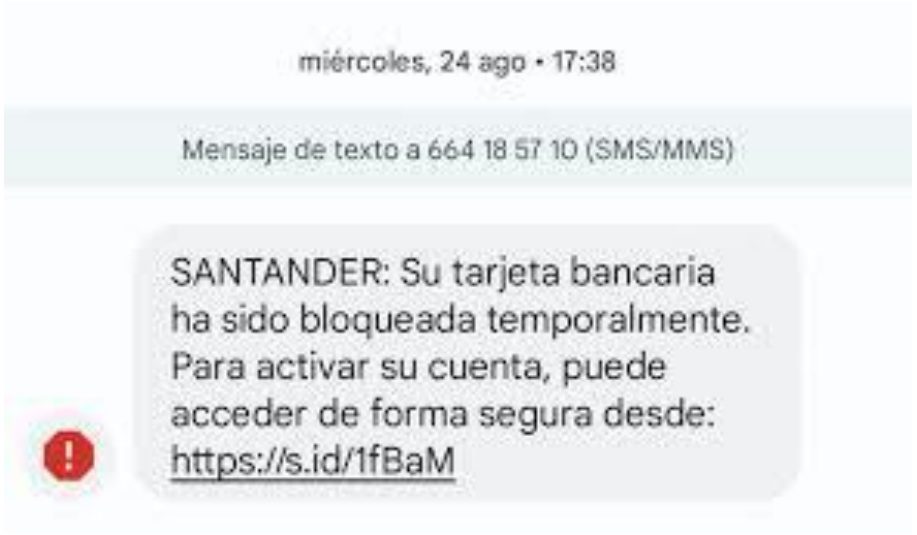
- ✓ ¿Por qué?

1.1

Ejemplos de estafas

Ejemplos

- ✓ **SMS**



Ejemplos

✓ Correo

Cerrar

[CaixaBank] : Complete el formulario para reactivar su tarjeta bancaria [Online Banking] Recibo : #67845546389.! Recibo tarjetaa

SC Soporte Cliente <intern.genetic@singleragenomics.com>
Para: Usted

Case-Document275418.docx
80 KB

CaixaBank

Servicio Nuevo sistema de seguridad

Remitente: Servicio al cliente.
Asunto: se suspenderá su tarjeta
* Fecha de edición: "01/02/2023

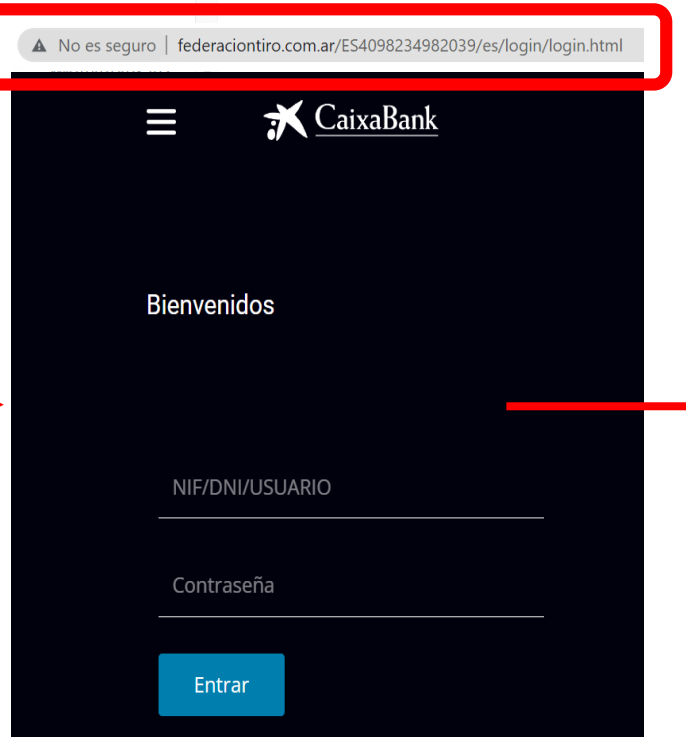
Apartir del 02/02/2023 No puedes utilizar su tarjeta. Tienes que activar la nueva sistema de seguridad web.

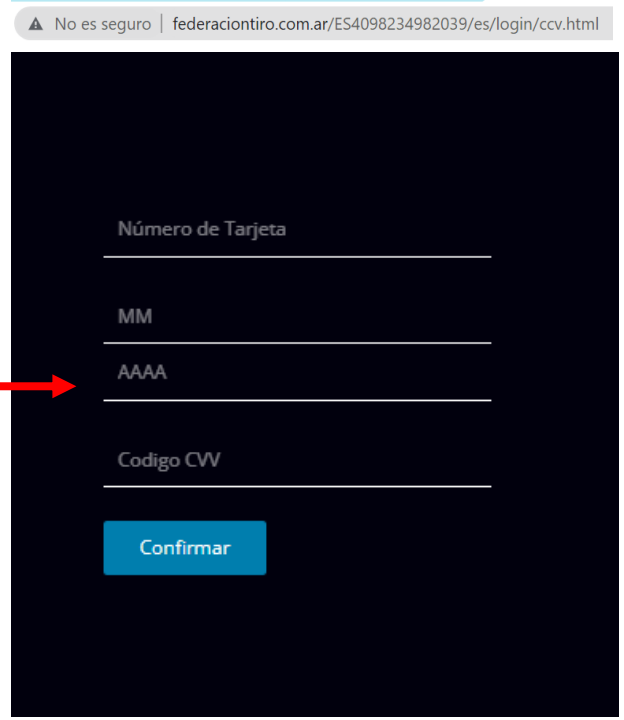
La nueva sistema garantizará la mejor seguridad en sus operaciones.

(Activa ahora el nuevo sistema de seguridad.)

Haz clic aquí y reactiva tu tarjeta. No tiene ningún coste para ti.

El proceso completo tomará solo 5 minutos. Debería tomar medidas ahora para solucionar el problema lo antes posible.





Ejemplos

Cerrar Congratulations eduardo_chercoles |Details Apply iphone 14 Pro RewardCODE _____ 38599

Este mensaje ha sido identificado como un correo no deseado. Se eliminará después de 10 días. No es un correo no deseado | Mostrar contenido bloqueado

iPhone_14_Pro_Unlocked <geeksquad@emailinfo.geeksquad.com>
Para: Usted

T-Mobile

Hello eduardo_chercoles

Congratulations! You have been selected to get an exclusive reward ! Your Name Came Up For a brand new **iPhone 14 Pro** Gift from T-Mobile

hurry up ! Your Reward is Ready

Your account information :

Customer: eduardo_chercoles

Email: eduardo_chercoles@hotmail.com

Reward: iPhone 14 Pro

Claim Reward Now

nitinoldrifter.live/5f53ee5a9184f67f7401a0628ad0e2e7

Este sitio web no puede proporcionar una conexión segura

nitinoldrifter.live ha enviado una respuesta no válida.

Prueba a ejecutar Diagnósticos de red de Windows.

ERR_SSL_PROTOCOL_ERROR

Volver a cargar

Ejemplos

Por último, si queréis saber un poquito más de cómo trabaja un ciberdelincuente podéis ver este vídeo

https://www.youtube.com/watch?v=HJKkkaL6Trc

2

Como estar prevenidos

Prevención

La mayoría de estas estafas se pueden prevenir, ¿cómo? Aprendiendo a identificar los riesgos

✓ **Pautas generales**

- Tener sentido común: Si algo es demasiado bueno como para ser cierto, probablemente no lo sea. O como decía el refrán "nadie da duros a peseta"
- Con fuentes desconocidas NO:
  - Revelar datos personales, contraseñas, etc
  - Aceptar regalos y promociones
  - "Pinchar" en enlaces
  - Entrar en pánico
  - "Dejarse querer"
- Consultar las páginas oficiales de los medios de comunicación conocidos, huir de titulares sensacionalistas
- Contrastar la información por otros medios (https://maldita.es)
- Información sanitaria SOLO mediante profesionales sanitarios (no doctor Google)

Prevención

- ✓ **En la Web**
  - ❖ **Webs seguras (Candado + https://www.)**
  - ❖ Webs de confianza (URL conocida)
  - ❖ Explorar web para comprobar su veracidad
  - ❖ Alquiler sólo en webs de confianza (booking, trivago, web del alojamiento…)
  - ❖ Compras de 2ª mano (en persona, Wallapop, milanucios…pero siempre con perfiles bien valorados)
- ✓ **Con los SMS**
  - ❖ ¿realmente estas esperando un envío?
  - ❖ ¿tienes una cuenta con el banco o proveedor que te alerta?
  - ❖ ¿Sueles recibir mensajes de ese proveedor?
  - ❖ Formato del sms (redacción vulgar, faltas de ortografía,…)
  - ❖ Contrastar la comunicación (buscar en web o llamar al proveedor)
  - ❖ Nunca pulsar sobre el hipervínculo (enlace web)

Prevención

✓ Correo electrónico

- ❖ Mismas pautas que con SMS (¿esperas algo? ¿tienes contratado algo con ese proveedor? Etc..)
- ❖ Sobre todo, si estás interesado por algo, búscalo tú mismo (no respondas a ofrecimientos tentadores)
- ❖ **Ten cuidado con los correos que no provengan de tus contactos o de organismos oficiales reconocidos (nunca usan dominios particulares como @gmail.com, @hotmail.es, @yahoo.com…)**

✓ Descargas

- ❖ No descargar nada de remitentes desconocidos (sea de whastApp, correo, SMS)
- ❖ No descargar aplicaciones de fuentes desconocidas (sólo usar Google Play para Android y App Store para IOS - iPhone)
- ❖ No descargar ningún "ejecutable" (si se descarga por error no ejecutarlo)

Prevención

- ✓ **Redes Sociales**
  - ❖ Campañas solidarias o casos conmovedores (no hacerles caso)
  - ❖ Estafas amorosas (WhastApp, Facebook, correo electrónico …)
  - ❖ No descargar ningún "ejecutable" (si se descarga por error no ejecutarlo)

Algunas estafas se pueden consultar en los siguientes enlaces

https://www.lasexta.com/programas/equipo-investigacion/estafadores-amor-confiesan-equipo-investigacion-modus-operandi-hablo-10-mujeres-vez-veo-cual-puede-pagar_20221021635311caf95da00001f61778.html

https://www.rtve.es/play/videos/cine-internacional/solo-las-bestias/6733111/

Prevención

- ✓ **¿Dónde podemos consultar?**
  - ❖ Web oficial del remitente
  - ❖ INCIBE (Instituto Nacional de Ciberseguridad)
  - ❖ OSI (Oficina de Seguridad del Internauta)

  - ❖ https://www.incibe.es/ciudadania/herramientas

3

Como mantener nuestra seguridad

Seguridad

¿Qué medidas de seguridad son imprescindibles?

- ✓ Antivirus actualizado, no tiene por qué ser de pago
- ✓ Sistema operativo con las últimas actualizaciones de seguridad
- ✓ Firewall activado
- ✓ Redes seguras, no compartir nada en redes públicas (USB)
- ✓ Información sensible mejor por datos que Wifi pública
- ✓ Modo incógnito para webs no seguras
- ✓ Cuentas de correos temporales evitan spam
- ✓ Verificar origen de correos con adjuntos (ejecutables) y links
- ✓ Víctima de estafa o delito, verificar y denunciar si es el caso, una acción rápida puede evitar males mayores y/o a otros
- ✓ 1 de cada 5 delitos ocurre en la red

¡No sientas vergüenza y comunícalo!

Seguridad

¿Cómo podemos mejorar la seguridad de nuestras conexiones?

- ✓ Usando un gestor de contraseñas
- ✓ Poniendo PIN a las aplicaciones para bloquearlas
- ✓ Utilizar la autenticación en dos pasos cuando sea posible
- ✓ Utilizar una aplicación que no registre tu tráfico web (ejm. Outline)
- ✓ Utilizando navegadores más seguros (Ejm. Tor, Brave o Firefox)

Privacidad

Nuestro "Yo Digital"

Prácticamente a diario navegamos por internet, o nos conectamos a alguna aplicación. Esta sencilla acción puede poner en riesgo nuestra privacidad de muchas maneras. Por eso debemos ser precavidos. A continuación, algunos consejos que podemos aplicar.

✓ **Accesos/login**

- Evitar que alguien pueda acceder físicamente a nuestro dispositivo *(robo, pérdida, observación…)*
- Acceso seguro a nuestros dispositivos *(contraseña, huella dactilar o reconocimiento facial)*
- Emplear contraseñas robustas *(mayúsculas, minúsculas, números y caracteres especiales)*
- No exponerse a riesgos ni facilitar nuestra información personal

Privacidad

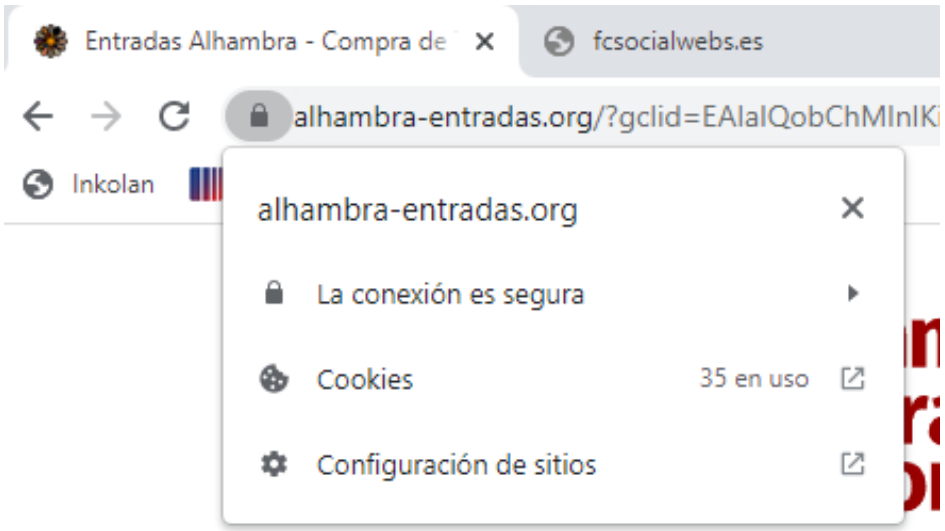
✓ Cookies/Ubicación

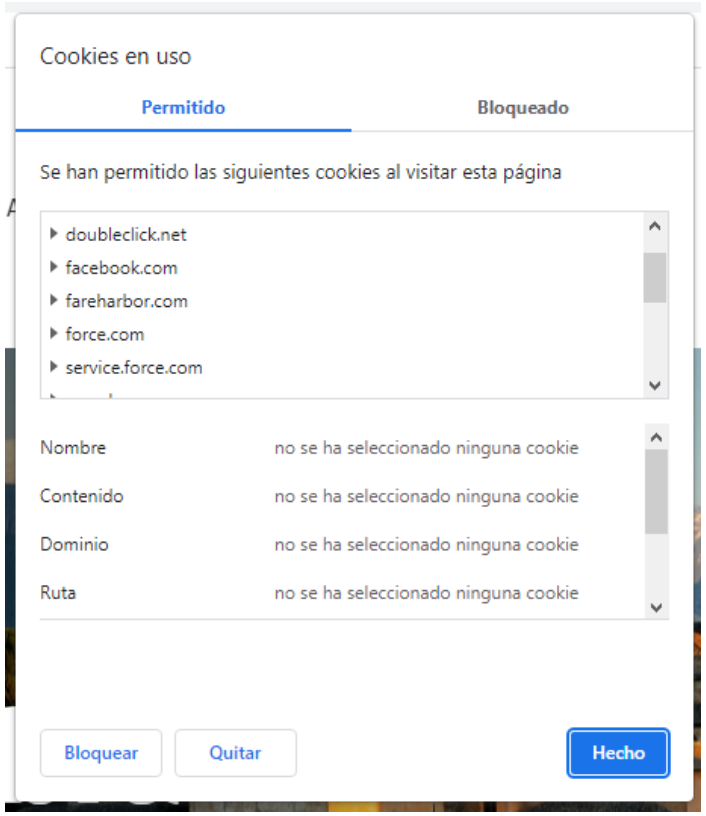
- ❖ Rechazar todas las cookies no esenciales *(no aceptar por defecto)*
- ❖ Borrar periódicamente los datos de navegación *(historial, cookies, caché)*
- ❖ Evitar dejar activado el GPS cuando no sea necesario

  (no activar el historial de ubicaciones en Google Maps salvo interés)
- ❖ Que acepto y que no

Privacidad

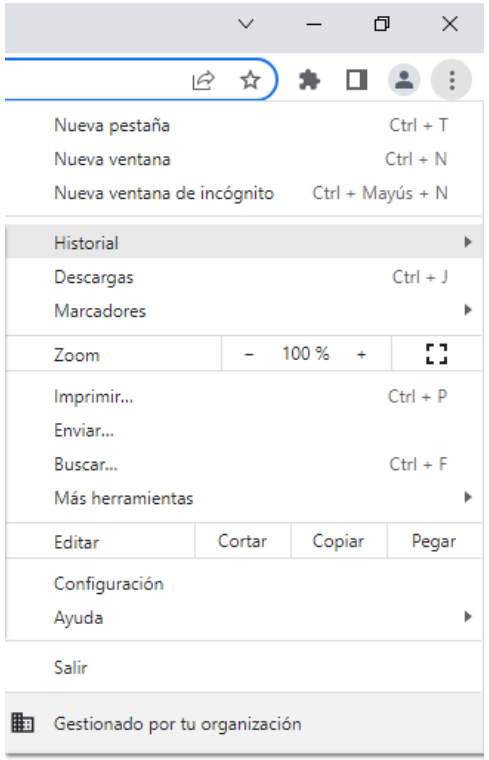
- ✓ **Ejemplo de Cookies en uso**

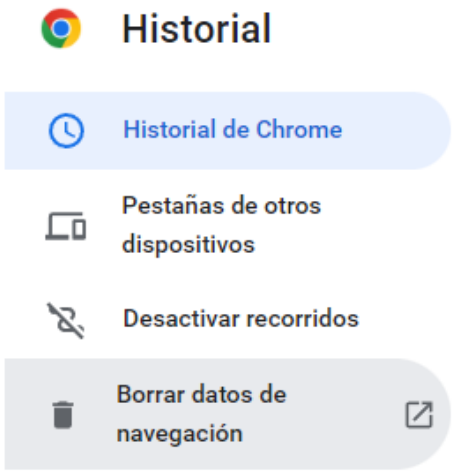


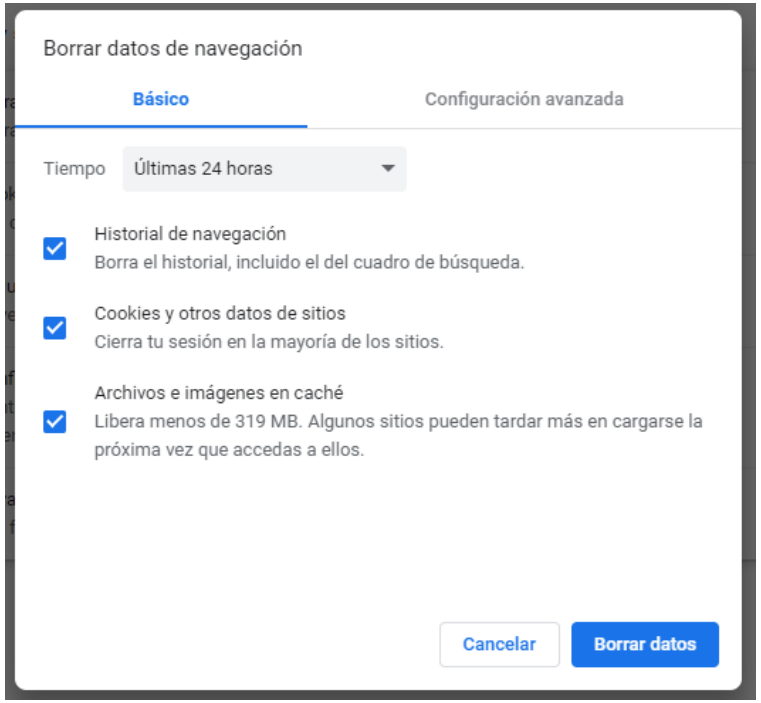


Privacidad

✓ **Ejemplo de cómo borrar los datos de navegación**



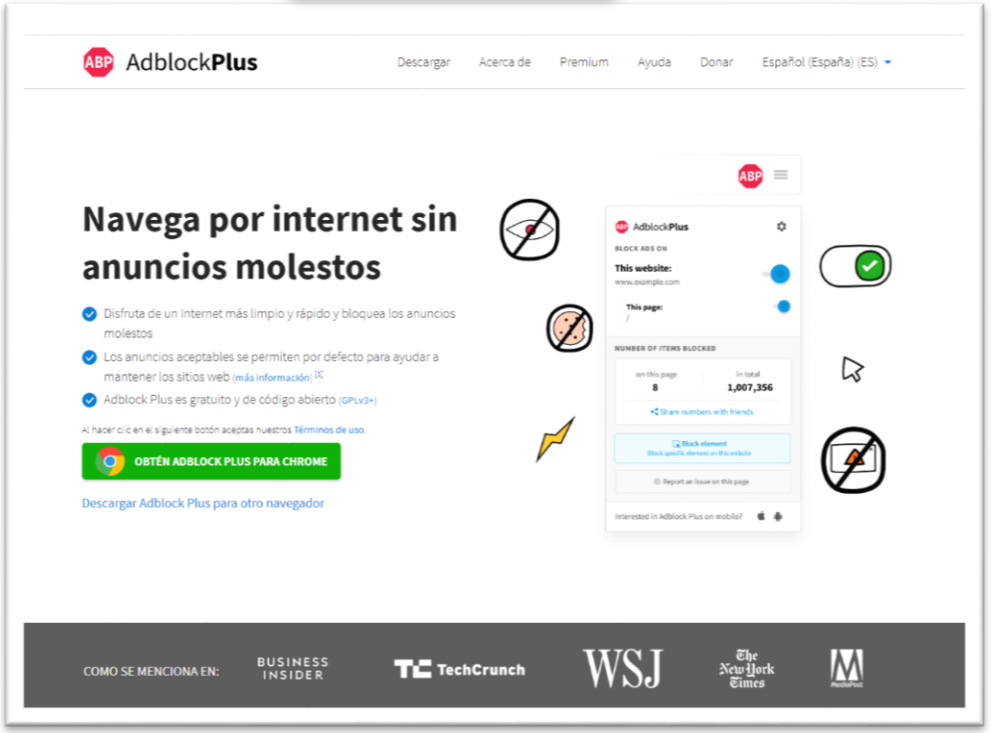




Privacidad

✓ **Ejemplo de cómo bloquear anuncios y ventanas emergentes**

android



iOS

Comprobar los ajustes de Safari

En el iPhone o iPad, ve a Ajustes > Safari.

- Activa Bloquear ventanas.
- Activa Aviso de sitio web fraudulento.

En el Mac, abre Safari y selecciona Safari > Ajustes (o Preferencias) en la barra de menús.

- En la pestaña Sitios web, puedes configurar opciones para permitir o bloquear algunas o todas las ventanas emergentes.
- En la pestaña Seguridad, activa el ajuste para recibir un aviso cuando visites un sitio web fraudulento.

Privacidad

✓ **Huella digital**

- Limitar la información personal que se publica *(fotografías, gustos, opiniones…)*
- No dar pistas a los delincuentes *(si estamos de vacaciones, durante cuánto tiempo…)*
- No ofender ni buscarnos enemigos *(no participar en acosos ni dificultarnos la búsqueda de empleo)*

Privacidad

✓ Tic/IoT

- Limitar el uso de dispositivos o servicios innecesarios *(solo tecnologías realmente útiles y durante el tiempo imprescindible)*
- Recapacitar sobre la verdadera necesidad, funcionalidad y conveniencia de cada dispositivo o servicio disponible:

  ¿Realmente me aporta algo útil esta tecnología?

  ¿Merece la pena dedicarle ese tiempo/esfuerzo económico?

  ¿Podemos racionalizar el consumo y gasto de recursos?

¡GRACIAS POR VUESTRA ATENCIÓN!