

TITULARES

¡Falso espíritu navideño! Fraudes más habituales que se propagan

Cuando llega la Navidad nos relajamos y bajamos la guardia al tratarse de épocas festivas para compartir con nuestros amigos y familiares. Este periodo es aprovechado por los ciberdelincuentes para propagar noticias falsas y fraudes.

[Pág. 2](#)

Consejos para unas Navidades ciberseguras

Durante la temporada navideña, debemos extremar las precauciones en nuestra actividad online. Son fechas elegidas por los ciberdelincuentes para llevar a cabo sus ataques, especialmente aquellos en los que interviene la ingeniería social.

[Pág. 3](#)

Tienda Online, ¿es de fiar?

¿Has visto una oferta online que no puedes dejar pasar? Te mostramos unas recomendaciones para identificar si la página es segura o no.

[Pág. 4](#)

Nueva vía para distribuir software ilegal: listas de reproducción de Spotify

Utilizan la reputación de Spotify para distribuir software sin licencia.

Esta característica está llevando a algunos ciberdelincuentes a crear listas de reproducción públicas que enlazan a sitios externos que contienen software ilegal y otros contenidos.

[Ver más.](#)



EL POST-IT



Correo electrónico

DE INTERÉS

Recuerda que tus publicaciones también pueden afectarte en Navidad

Las celebraciones navideñas están repletas de momentos especiales y que muchas personas comparten en las redes sociales con todos sus seguidores. Sin embargo, deberás estar atento al contenido que se publica teniendo en cuenta los siguientes factores:

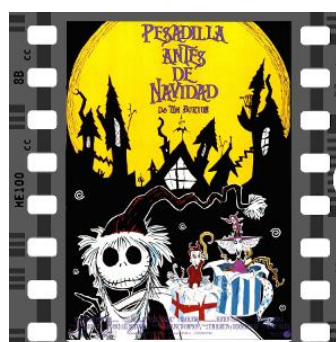
*Localización que estás compartiendo.

*Piensa si el contenido puede afectar a tu reputación online, a corto o largo plazo.

*Deshabilita la ubicación a la hora de subir tus fotos y vídeos.



LA PELÍCULA



Comprueba si tu cuenta de correo está comprometida, <https://haveibeenpwned.com/>. Si es así, **cambia la contraseña.**

TITULARES

¡Falso espíritu navideño! Fraudes más habituales que se propagan

¿Cuáles son los fraudes más habituales que se propagan por la Red en periodos navideños?



Ofertas y descuentos: los ciberdelincuentes tratan de publicar anuncios en distintas páginas web o plataformas de redes sociales. También envían mensajes por redes sociales, SMS, correos electrónicos o incluso los viralizan a través de plataformas de chats. En ellos suelen introducir enlaces a páginas webs fraudulentas bajo el reclamo de obtener descuentos irresistibles. Si facilitas tus datos, acabarán en su poder y podrán utilizarlos para fines maliciosos.

Bromas o felicitaciones: detrás del inocente aspecto de una tarjeta de felicitación o una broma inofensiva puede ocultarse un archivo infectado. Analiza el documento o el enlace para ver si está libre de amenazas.



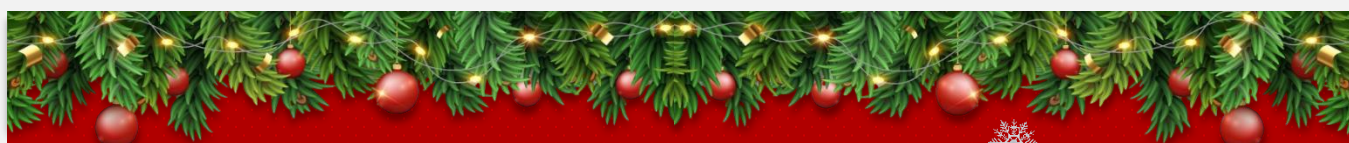
Emails con facturas: atento si recibes alguna factura a través del correo electrónico, incluso si has hecho un pedido online. Es habitual que los ciberdelincuentes pongan en circulación correos con facturas falsas, con el fin de que el usuario descargue o abra el archivo adjunto para infectar su dispositivo.

Solicitudes de ONG's: es frecuente en Navidad que se compartan peticiones de ayuda que suplantan entidades sin ánimo de lucro para contribuir económicamente con alguna causa benéfica. Comprueba bien el mensaje para cerciorarte si realmente es legítimo o no.



Aplicaciones con malware con temática navideña: en estas fechas, es común la instalación de programas para el diseño y envío de felicitaciones u otras cuestiones similares. Es importante que revises la reputación de la app antes de instalarla y por supuesto, que la descargues de los repositorios de aplicaciones oficiales (verificando con cautela los privilegios a conceder a las distintas aplicaciones)

Consejos para unas Navidades ciberseguras



Consejos para tener unas

NAVIDADES CIBERSEGURAS

Sorteos. Ten cuidado con los cupones, sorteos y premios navideños que recibas por email, SMS, aplicaciones de mensajería, como Telegram o WhatsApp, o redes sociales, como Instagram o Twitter.

Contraseñas robustas.

Aprovecha las vacaciones para actualizar tus contraseñas.

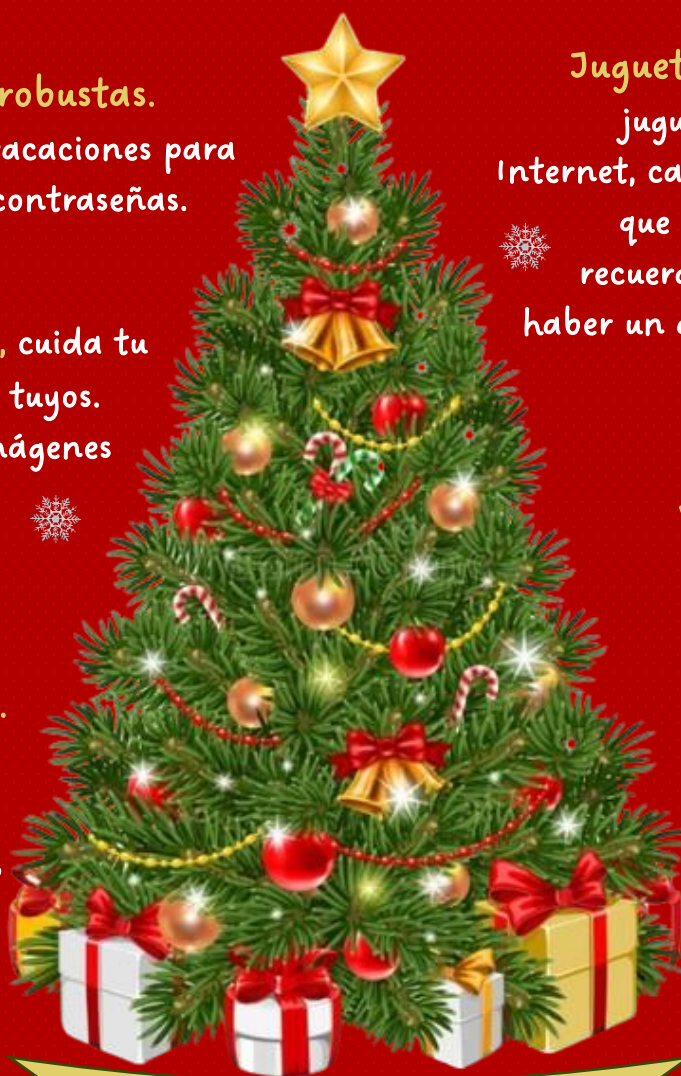
Juguetes. Cuidado con los juguetes con conexión a Internet, cambia la contraseña que traen por defecto y recuerda que siempre debe haber un adulto supervisando su uso.

Estas Navidades, cuida tu imagen y la de los tuyos. Evita compartir imágenes en Internet comprometidas.

Viajes. Si te vas a ir de vacaciones en estas fechas, no lo compartas en las redes sociales hasta tu vuelta, sin saberlo estarás dando valiosa información a las personas amantes de lo ajeno.

Actualizaciones.

Mantén actualizado tu sistema operativo, antivirus y aplicaciones en todos tus dispositivos.



Felices Fiestas

Compras. Realízalas en webs de confianza, siempre en sitios oficiales y desconfía de las ofertas demasiado atractivas.

Navega por Internet de forma segura, protegiendo tu privacidad y evitando dejar un rastro.

Recuerda, no todo lo que circula por Internet tiene por qué ser cierto, acude a fuentes fiables y contrasta la información.

Tienda Online, ¿es de fiar?

Hoja de ruta para comprobar si una tienda online es segura o fraudulenta

Experiencia **SENIOR**

¿Has visto una oferta online que no puedes dejar pasar? Sigue estos pasos e identifica posibles fraudes:



Web de compra online

Haz estas comprobaciones sobre la web y contesta a las preguntas:

¿La URL tiene HTTPS y un candado cerrado junto a ella? **Sí** **No**

¿La URL coincide con el nombre de la empresa? **Sí** **No**

Algunas webs fraudulentas utilizan certificados digitales válidos, por lo que hay que analizar más factores.

Algunas webs fraudulentas copian el nombre de una marca o la web original, modificando solo alguna letra o carácter.

Dentro de la web haz estas comprobaciones:

¿Hay información de contacto de la empresa? **Sí** **No**

¿Hay un apartado de aviso legal? **Sí** **No**

¿Dispone de un sello de confianza? **Sí** **No**

¿Hay información sobre la devolución de productos? **Sí** **No**

Si no incluye estos datos, es probable que se trate de una web fraudulenta.

Reflexiona. Sin esta información, ¿qué ocurrirá si tu producto no llega o tienes que devolverlo?

Ahora comprueba los productos y sus precios:

¿Los productos tienen una gran rebaja respecto al precio medio del mercado? **Sí** **No**

¿Todos los productos tienen el mismo precio? **Sí** **No**

¿Las imágenes son copiadas o de mala calidad? **Sí** **No**

¿La información está incompleta, mal traducida o presenta errores? **Sí** **No**

No te fíes, son aspectos clave de cualquier web fraudulenta.

Podemos comprobarlo si las buscamos en Google imágenes.

Busca comentarios y valoraciones dentro de la web y en un buscador:

¿Las valoraciones que has encontrado en Internet son positivas? **Sí** **No**

¿Los comentarios de otros compradores en la propia web son positivos? **Sí** **No**

Es importante fijarnos en las valoraciones de otros usuarios, pero algunas webs fraudulentas falsean comentarios positivos. Se cauteloso, y ante la duda, comprueba el usuario, otras valoraciones, fecha de registro, etc.

Analiza los métodos de pago disponibles:

¿Permite PayPal, tarjetas de crédito, Bizum, Google Pay o Apple Pay? **Sí** **No**

¿Solo permite MoneyGram, Western Union o transferencia bancaria? **Sí** **No**

En el momento de efectuar el pago asegúrate de que te redirigen a la pasarela de pago segura de cada servicio. Se abrirá una nueva ventana con "https" que te llevará al servicio de pago seguro seleccionado.

Si solo permite métodos de pago poco seguros, como MoneyGram, Western Union o transferencias, es mejor no comprar.

Si alguna respuesta es esta opción, mejor no realices la compra, es un indicio de tienda fraudulenta.

Si tu respuesta es esta opción, puedes seguir avanzando para comprobar otros aspectos.

Finalmente, recuerda que desde INCIBE ponemos a tu disposición nuestra guía sobre compras seguras online y la Línea de Ayuda en Ciberseguridad, 017, para resolverte cualquier duda o problema.

EL POST-IT

Correo electrónico

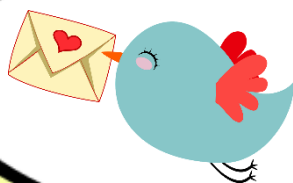
[Código de conducta](#) en el uso de las tecnologías de la información y la comunicación para profesionales públicos de la administración de la Junta de Andalucía.

[Comprueba que tu cuenta no está vulnerada en portales no corporativos.](#)



No se usarán cuentas de correo electrónico personales para el desempeño de funciones profesionales.

[Campaña de correos fraudulentos dirigida a proveedores suplantando a la Junta de Andalucía.](#)



El correo electrónico corporativo se usará exclusivamente con fines profesionales y no se facilitará como medio de contacto o registro para otros propósitos.

[A los hackers les encanta que te registres en Tinder con el email del trabajo.](#)

[Las cuentas no se utilizarán para almacenar, de forma permanente, información relevante.](#)



[Se tendrá cuidado con los mensajes de correos sospechosos, sin acceder a ellos y notificándolo.](#)



LA PELÍCULA



Pesadilla antes de Navidad

Estamos inmersos en las compras navideñas, y es un hecho que cada vez compramos más por Internet. Para que tus compras no sean una "Pesadilla Antes de Navidad", te damos unos consejos básicos para comprar de forma segura en internet.

Y te facilitamos esta "[Guía](#)" para no caer en una estafa.



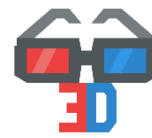
Compra



Evita



Desconfía



Cuida

01. Compra

Compra en webs de confianza (reconocidas, seguras, con reputación, etc).

02. Evita

Evita las transferencias y envíos de efectivo, solo tarjeta. Te recomendamos usar tarjetas de pago, solo para Internet.

03. Desconfía

Desconfía de las ofertas demasiado atractivas (smartphones a 10 euros, etc).

04. Cuida

Cuida tu dispositivo y tu conexión. Evita comprar usando zonas wifi-públicas donde puede haber otras personas monitorizando el tráfico de tus datos.

Prevención

Formación

Feliz Navidad

Cibersegura

Detección

Respuesta

Concienciación

Divulgación

GRC (Gobierno, Riesgo y Cumplimiento)

*Nuestros mejores deseos para estas fiestas
y próximo año 2025*