

TITULARES

Cómo actuar en caso de un ataque de ransomware

El ransomware es un tipo de malware que se introduce en los equipos y dispositivos móviles conectados a Internet impidiendo el acceso a la información.

[Pág. 2](#)**¿Sabes qué es el Doxing?**

Se trata de una técnica utilizada para descubrir y difundir información personal sin su consentimiento. Se utiliza a menudo con fines maliciosos, como acoso, amenazas, extorsión y otros delitos cibernéticos.

[Pág. 3](#)**La privacidad de los demás también depende de ti**

Las redes sociales ponen a tu alcance distintos recursos para que puedas divulgar y compartir con otras personas la información que tú quieras sobre tu vida personal, la cual puede incluir a otras personas.

[Pág. 4](#)**[Así ha sido el 4º Congreso de Ciberseguridad de Andalucía](#)**

Bajo el lema "Cybersecurity: protecting data, saving lives", el evento ha puesto el foco en los desafíos de la seguridad digital en el ámbito sanitario, sin olvidar las claves de futuro para blindar también la seguridad digital de los ciudadanos, empresas y administraciones públicas.

La ADA, organizadora del congreso, ha tenido una presencia destacada a lo largo de todo el Congreso, liderando algunos de los debates más relevantes. Aquí puedes ver la [galería de fotos](#) del Congreso.

EI POST-IT**LA PELÍCULA****CONTRAPORTADA**

Notificaciones de muchas falsas por correo y mensaje suplantando a la DGT 

Aseguran haber robado los datos de la Lista Robinson: hay 500.000 personas afectadas 

La IA clona tu voz y puede meterte en un buen lío: así puedes evitarlo 

Cómo evitar que Meta utilice tu contenido publicado en Facebook, Instagram y Threads para entrenar su IA 

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

TITULARES

Cómo actuar en caso de un ataque de ransomware



Principales signos que pueden ponerte en alerta:

El ***ransomware*** es un tipo de ***malware*** que se introduce en los equipos y dispositivos móviles conectados a Internet impidiendo el acceso a la información.

Generalmente la cifran y, a continuación, piden un rescate para que vuelva a ser accesible o no sea divulgada. No siempre es posible revertir sus efectos, en particular si no podemos descifrar los archivos secuestrados y no tenemos copias de seguridad.

A continuación, te explicamos cómo puedes actuar si has sufrido un ataque de este tipo y estás intentando salvar tu información. Y recuerda, ¡no accedas nunca a las peticiones de pago para recuperar tu información! Son ciberdelincuentes y no hay ninguna garantía de que puedas recuperar tu información, solo les interesa tu dinero.

Antes de comenzar con los siguientes pasos, te recomendamos que hagas una copia de la información almacenada en el disco, aunque esté cifrada, ya que el proceso que se describe a continuación podría suponer la eliminación de archivos, provocando que no se puedan recuperar de ninguna forma.

[1. Iniciar el equipo Windows en modo seguro con funciones de red](#)

[2. Eliminar el *ransomware* con una herramienta de tipo *cleaner*](#)

[3. Realizar un segundo análisis para confirmar que el equipo está limpio](#)

[4. Restaurar los archivos cifrados por el *ransomware*](#)

¿Sabes qué es el Doxing?

DOXING

PRÁCTICA DE REVELAR INFORMACIÓN PERSONAL DE UNA PERSONA POR INTERNET SIN SU CONSENTIMIENTO

¿Qué te podría pasar si alguien practica *doxing* contra ti?



Además, te recomendamos:



Te animamos a que te pongas en contacto con la **Línea de Ayuda en Ciberseguridad de INCIBE** si necesitas más ayuda sobre este o cualquier otro tema relacionado con ciberseguridad.



La privacidad de los demás también depende de ti

Las redes sociales ponen a tu alcance distintos recursos para que puedas divulgar y compartir con otras personas la información que tú quieras sobre tu vida personal o profesional. Cuando se trata de compartir datos personales, la máxima fundamental siempre es la precaución. Ante la más mínima duda sobre la publicación de una imagen, es mejor no publicarla o limitar su difusión lo máximo posible, mediante los controles de privacidad.



EL POST-IT

Notificación de incidencias

[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.

Se notificarán a la mayor brevedad posible al responsable del tratamiento o encargado del tratamiento, en su caso, todas aquellas violaciones o vulnerabilidades de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales así como su comunicación o acceso no autorizados.



Si has sufrido un incidente de seguridad es muy importante que lo notifiques



Correo: incidentes.soc@juntadeandalucia.es

Teléfono: 955 060 974

Se notificará cualquier incidencia o anomalía que detecten en el uso de las TIC: pérdida o sustracción de información o de dispositivos, accesos no autorizados, uso inadecuado de sus credenciales, introducción de código dañino o malicioso, necesidad de recuperación de datos y, en general, toda situación que pueda comprometer la seguridad, el buen uso y funcionamiento de los recursos.



[Anécdotas que te han podido ocurrir en tus inicios, en el mundo de la informática.](#)



Utiliza los medios señalados en cada caso, por tu Consejería o Agencia.



LA PELÍCULA



LA VIDA DE LOS OTROS

Hay personas a las que les interesa la vida de los otros más que la suya propia.

No solo por cuestión de cotilleo, sino también por la posibilidad de realizar chantajes, extorsiones, saber cuándo te vas de vacaciones para robar en tu domicilio, usurpar tu identidad ...

Por todo ello, debes tener cuidado con la información personal que publicas.



Perfil



Juicio



Geolocalización



Consentimiento

01. Perfil

Tu perfil es tu tarjeta de presentación. Tu foto de perfil, tu profesión, tus estudios, tu opinión en las redes... proporcionan a personas desconocidas mucha más información de ti que tu DNI.

02. Juicio

Te van a prejuzgar. Cada vez más personas y empresas observan y analizan las redes sociales para adoptar un juicio sobre otras personas.

03. Geolocalización

Cuida tu geolocalización. Plantéate si te interesa estar siempre geolocalizado.

04. Consentimiento

No difundas información privada sobre otras personas sin su consentimiento. No etiquetes a otras personas que no tienen perfil en redes sociales sin solicitar previamente su permiso.

CONTRAPORTADA

Notificaciones de multas falsas por correo y mensaje suplantando a la DGT

Se han detectado varias campañas fraudulentas que suplantan a la Dirección General de Tráfico (DGT) mediante correos electrónicos y mensajes de texto. Los atacantes informan a las víctimas sobre una presunta multa de tráfico, incitándolas a realizar un pago de manera urgente. Para más información, pulsa [aquí](#).



Aseguran haber robado los datos de la Lista Robinson: hay 500.000 personas afectadas

Desde Adigital confirman que no se ha vulnerado la Lista Robinson, y los datos robados pertenecen a una antigua base de datos de otra empresa. Para más información, pulsa [aquí](#).



La IA clona tu voz y puede meterte en un buen lío: así puedes evitarlo

Esta técnica, conocida como 'voice cloning', ha sido utilizada en estafas telefónicas y fraudes bancarios. Una técnica que permite replicar con precisión la forma de hablar de una persona con tan solo unos segundos de grabación. Para más información, pulsa [aquí](#).



Cómo evitar que Meta utilice tu contenido publicado en Facebook, Instagram y Threads para entrenar su IA

Las cuentas de los 'productos de Meta' han comenzado a recibir notificaciones en las que se les informa y se les da la opción de excluir sus datos y contenido público del entrenamiento de Meta AI. Para más información, pulsa [aquí](#).

