BOLESTIC

Nº 9 enero 2025

Boletín de concienciación en ciberseguridad

Junta de Andalucía | Agencia Digital de Andalucía

incidentes.soc@juntadeandalucia.es

TITULARES

Egosurfing: ¿Qué información hay sobre mí en Internet?

Internet es el mayor banco de información de la historia y como tal, también puede haber información sobre nosotros.

Pág. 2

Los Reyes me han regalado un móvil: estos son mis ajustes imprescindibles para configurarlo

Si te has portado bien, puede que los Reyes Magos te hayan regalado un estupendo teléfono móvil. Te indicamos algunas configuraciones básicas para poder disfrutarlo al máximo.

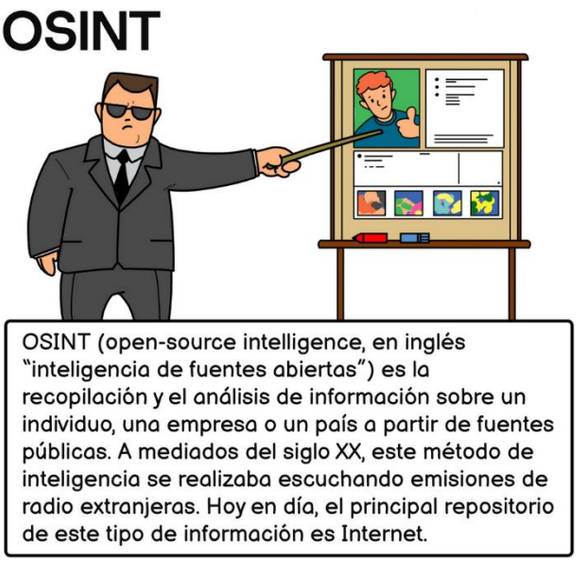
Pág. 3

¿Sabes que es el Doxing?

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

Pág. 4

¿Has hecho alguna vez una prueba de la cantidad de información que se puede averiguar sobre ti en Internet?



OSINT (open-source intelligence, en inglés "inteligencia de fuentes abiertas") es la recopilación y el análisis de información sobre un individuo, una empresa o un país a partir de fuentes públicas. A mediados del siglo XX, este método de inteligencia se realizaba escuchando emisiones de radio extranjeras. Hoy en día, el principal repositorio de este tipo de información es Internet.

Charla virtual

Lo que tus dispositivos inteligentes no te cuentan: Privacidad y Seguridad en IoT del hogar.

Con motivo del Día de Internet Segura que se celebra cada año el 11 de febrero, la Oficina de Formación y Concienciación del SOC de la Junta de Andalucía organiza esta charla virtual y gratuita para todos los públicos.

¡No te la pierdas! Ya puedes realizar tu inscripción!

Día: lunes, 10 de febrero.
Hora: 17.00 h.
Inscripción: Aquí.

El POST-IT

LA PELÍCULA

CONTRAPORTADA

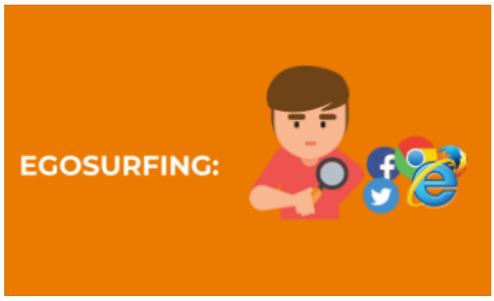
Comprueba si tu cuenta de correo está comprometida, https://haveibeenpwned.com/. Si es así, **cambia la contraseña**.

BOLESTIC
Nº 9 enero 2025
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.
incidentes.soc@juntadeandalucia.es

TITULARES

Egosurfing: ¿Qué información hay sobre mí en Internet?

Practicar el Egosurfing es una acción recomendada para proteger nuestra privacidad, pero ¿sabes lo que es y cómo hacerlo?



Sea cual sea el tema, en Internet encontraremos información al respecto, incluso podemos llegar a encontrar información sobre nosotros mismos. El conjunto de todos estos datos es lo que se conoce como identidad o huella digital y, del mismo modo que nuestra reputación puede ser dañada, la identidad digital también puede verse afectada debido a la información que puede ser encontrada sobre nosotros en Internet o, en el peor de los casos, cuando nuestra privacidad es vulnerada y nuestros datos personales acaban filtrándose.

¿Cómo puedo practicar egosurfing?

Búsqueda en el navegador
Sea cual sea el navegador que usemos (Google Chrome, Safari, Edge, Firefox…), o accediendo a los buscadores más comunes (Google, Bing…), podemos escribir directamente nuestro nombre entre comillas (o el dato que nos interese buscar) y pulsar en buscar para ver qué aparece en la Red. El hecho de incluir las comillas hace que la búsqueda sea más concreta y se centre solamente en los parámetros entrecomillados.

Google Alerts
Esta herramienta nos permite configurar previamente la llegada de notificaciones cada vez que se haga una publicación con los parámetros de búsqueda que hemos marcado.

Redes sociales
En este caso, la estrategia es muy similar a la de la búsqueda en el navegador. Escribiendo nuestro nombre en el buscador de las redes sociales podremos encontrar qué hay publicado sobre nosotros. Es importante hacerlo en todas las redes sociales, tengamos o no cuenta en ellas, ya que podrían aparecer perfiles falsos que publiquen contenido en nuestro nombre.

Y ahora, ¿qué hago si lo que encuentro NO quiero que esté publicado?

En primer lugar, si la información fue publicada por nosotros mismos, lo más sencillo es eliminarla de la plataforma en la que se encuentre.

Si la información no la hemos publicado nosotros y vulnera nuestra privacidad y/o reputación, podemos seguir los siguientes pasos:

- Solicitar directamente al responsable/administrador de la web donde está publicado, que rectifique o elimine dicho contenido. Para ello, deberemos demostrar la inexactitud de los datos, o bien que estos afectan a nuestro honor y reputación, siempre y cuando no prevalezcan los principios de publicidad registral y de interés público.
- En todo caso, si entendemos que dicha difusión de nuestros datos pudiera ser constitutivo de delito, podríamos interponer una denuncia por delito contra el honor de nuestra persona.

Para terminar, si encontramos un perfil falso que se hace pasar por nosotros, la solución es denunciarlo inmediatamente a la red social a través de los canales de soporte oficiales en la que se encuentre para que lo eliminen lo antes posible.

BOLESTIC
Nº 9 enero 2025
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.
incidentes.soc@juntadeandalucia.es

Los Reyes me han regalado un móvil: estos son mis ajustes imprescindibles para configurarlo

Queremos compartir contigo algunas configuraciones básicas que te servirán para disfrutar al máximo de tu nuevo teléfono.

Lo primero de todo, protégelo. A día de hoy nos encontramos con personas usuarias que desactivan la ubicación porque piensan que así están más protegidas. Tenemos malas noticias: desde el minuto uno que conectas tu teléfono a internet, tu información está expuesta. Activar la localización es un imprescindible para que tanto el teléfono como las apps funcionen correctamente, y no vas a estar más protegido por desactivarla.

En el caso de Apple, de forma automática el teléfono se registra en la red Buscar. En Android, a veces es necesario activarlo desde los ajustes. Abre los ajustes de tu teléfono, busca "Encontrar", y activa la función de "Encontrar mi Dispositivo". En el caso de que pierdas el teléfono o te lo roben, no podrás localizarlo de ninguna forma si no activas esto.

Cambia los datos de la zona WiFi. Es probable que, en algún momento del ciclo de vida útil de tu teléfono, tengas que usarlo como router porque andas fuera de casa. A todos se nos olvida configurar esto cuando recibimos el teléfono, y es bastante molesto tener que andar configurándolo si, por cualquier circunstancia, tenemos prisa y necesitamos conectarnos de forma rápida. No tienes más que ir a "Punto de Acceso" y cambiar tanto el nombre como la contraseña.

Un gran truco para ahorrar espacio en fotos y vídeos. Es muy probable que tu nuevo móvil venga con 128 GB de memoria interna. Si le das caña a la cámara o tienes bastantes grupos de WhatsApp, esta cifra se suele quedar corta en poco tiempo. Hay un truco que pocos conocen para que las fotos y los vídeos ocupen prácticamente la mitad.

En Android, abre la cámara de fotos, vete a los ajustes, y busca estos dos apartados:

Formato de vídeo eficiente (H.265)

Captura de foto/formato de foto eficiente (HEIC)

El nombre dependerá de tu ROM pero, básicamente, lo que vas a hacer es configurar la cámara para que haga fotos en HEIC y vídeos en H.265. Estos son dos formatos mucho más eficientes respecto a JPEG y H.264. De hecho, en los iPhone esta función viene activa por defecto.

Configura la carga inteligente. Uno de los aspectos que conviene configurar en tu móvil nuevo es la carga inteligente, presente en casi todos los teléfonos de última generación. Vete a los ajustes de batería del teléfono, y cacharrea con las opciones que vas a encontrar.

Una buena opción es la de limitar la carga al 80%, para protegerla del paso del tiempo. También, según el teléfono, podrás regular la velocidad de carga, optimizar el uso de apps cuando el dispositivo está en reposo y demás.

Desactiva la RAM virtual. Casi todos los teléfonos actuales vienen con extensión de RAM virtual, y esta la carga el diablo. Por lo general, un módulo físico de memoria RAM siempre será más rápido que una extensión virtual. Además, esta RAM virtual se logra a base de restar almacenamiento de tu teléfono.

Cada teléfono tiene este ajuste en una ubicación, pero basta con escribir "RAM" en el menú de ajustes para encontrar el menú.

BOLESTIC
Nº 9 enero 2025
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.
incidentes.soc@juntadeandalucia.es

¿Sabes que es el Doxing?

BOLESTIC

Nº 9 enero 2025

Boletín de concienciación en ciberseguridad

Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.

incidentes.soc@juntadeandalucia.es

EL POST-IT

Redes Sociales

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.

Brecha de seguridad en Telefónica

Se velará por el cumplimiento de la normativa en materia de protección de datos personales en el contenido que publiquen en los perfiles corporativos.

Cómo reducir los conflictos en las redes sociales

Se respetarán las opiniones de la ciudadanía, evitando cualquier tipo de enfrentamiento.

Se podrán utilizar para el desempeño de sus funciones las redes sociales como herramientas de comunicación, atención a la ciudadanía, participación y transparencia, con las directrices, medios y habilitación que, en su caso, les haya establecido la Administración de la Junta de Andalucía.

Suplantación del perfil de la Alcaldesa de Las Palmas

No se realizará ni admitirá un uso del perfil que sea sustitutivo de otros canales oficialmente establecidos.

No se emitirán opiniones personales desde los perfiles corporativos.

BOLESTIC
Nº 9 enero 2025
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.
incidentes.soc@juntadeandalucia.es

LA PELÍCULA

El Golpe

Correos que parecen proceder de fuentes fiables pero en realidad nos conducen a páginas falsas para robarnos las claves.

El falso local de apuestas de carreras de caballos que aparece en la película, es un 'Phising'.

01. Comprueba

Comprueba que la URL o dirección de la web que visitas es la que dice ser (por ejemplo, buscando la original en un buscador).

02. Desconfía

Desconfía, los bancos y otras entidades similares nunca te van a solicitar datos personales por correo electrónico.

03. Rechaza

Rechaza cualquier correo que solicite facilitar datos y no utilices el enlace adjunto al correo. Si quieres acceder a esa web, utiliza el buscador o tus marcadores guardados.

04. Actúa

Ante cualquier duda sobre cómo actuar con un correo de dudosa reputación en contacto con el Centro de Atención de Personas Usuarias (CAU) de tu Consejería.

BOLESTIC
Nº 9 enero 2025
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración.
Algunos de los enlaces mostrados pueden requerir de la aceptación de cookies.
incidentes.soc@juntadeandalucia.es

CONTRAPORTADA

Así es la estafa que se hace pasar por familiares y amigos

Básicamente, el voice hacking es una nueva modalidad de estafa que emplea inteligencia artificial para imitar la voz de una persona con una precisión realmente alta. Este tipo de fraude se ha popularizado gracias a los avances en tecnología de síntesis de voz. Para más información, pulsa aquí.

El CCN-CERT advierte de las tácticas y procedimientos de las principales ciberamenazas

El Centro Criptológico Nacional (CCN) ha presentado el informe IA-04/24 Ciberamenazas y Tendencias. Edición 2024, que analiza las principales amenazas y tendencias del ciberespacio a nivel nacional e internacional. Para más información, pulsa aquí.

Ciberestafa con documentos de Word como caballo de Troya

Cuidado con los correos enviados por supuestos departamentos de recursos humanos con un archivo ".docx" que no se abre bien, puede ser un taque cibernético. Para más información, pulsa aquí.

5 mitos sobre ciberseguridad que debemos dejar atrás

Se trata de un llamamiento a las personas usuarias para que rompan con varios mitos falsos de ciberseguridad, que aumentan la vulnerabilidad y que están ampliamente extendidos. Para más información, pulsa aquí.