BOLESTIC

Nº 4 Especial Vacaciones 2024

Boletín de concienciación en ciberseguridad

Esta comunicación está destinada a los profesionales públicos de la Administración

incidentes.soc@juntadeandalucia.es

TITULARES

Respaldo de tus recuerdos del verano en Google Fotos e iCloud

En vacaciones es común inmortalizar momentos y lugares con nuestra cámara para poder volver a revivirlos en un futuro. Imágenes y vídeos son recuerdos preciados que no nos gustaría perder, pero ¿aplicas alguna medida de seguridad para evitar esto?

Pág. 2

¿Qué es y cómo prevenir el carding?

Los ciberdelitos son cada vez más comunes, una de las estafas de fraude más recurrentes, es conocida como carding. Se trata de un tipo de fraude que utiliza información de tarjetas robadas, para utilizarlas de manera fraudulenta.

Pág. 3

Protección de datos personales en vacaciones

Durante las vacaciones de verano no podemos bajar la guardia y debemos seguir siendo activos en la protección de datos, afrontando las situaciones de riesgo que se presentan en la época estival.

Pág. 4

Talent Land España

Durante tres días, Talent Land España convirtió Andalucía en el epicentro del talento digital. Un encuentro lleno de actividad en el que la Agencia Digital de Andalucía tuvo su propio stand y se impartieron charlas sobre ciberseguridad. Ver más.

DE INTERÉS

Uso adecuado de tus credenciales

Más información 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 4 Especial Vacaciones 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración
incidentes.soc@juntadeandalucia.es

TITULARES

Respaldo de tus recuerdos del verano en Google Fotos e iCloud

Hay diversas situaciones por las cuales nuestros vídeos y fotos almacenados se pueden perder, como, por ejemplo: si nos roban o perdemos el teléfono, se avería el dispositivo de almacenamiento extraíble o la unidad de almacenamiento principal de nuestro equipo. Para evitar problemas y estar seguros de que nuestra información no se perderá pase lo que pase, debemos realizar copias de seguridad.

Copias de seguridad en la Nube

Para guardar nuestras copias de seguridad, una posibilidad es usar servicios de almacenamiento en la Nube. Éstos nos permiten almacenar nuestra información en sus servidores para que accedamos a ella desde cualquier dispositivo con acceso a Internet. De esta forma, aunque perdamos las imágenes y vídeos almacenados en la memoria de nuestro teléfono, cámara, etc. tendremos una copia guardada en sus servidores, la Nube. Esto es indudablemente una gran ventaja.

Google fotos

Este es el servicio de almacenamiento en la Nube para fotos y vídeos creado por Google disponible tanto para Android, iOS y ordenadores. Permite realizar distintas tareas de gestión como, por ejemplo:

1. Añadir, editar, eliminar fotos y vídeos.
2. Buscar personas, cosas y lugares en las fotos y vídeos.
3. Compartir tanto fotos y vídeos como los álbumes a los que pertenecen.
4. Crear copias de seguridad de fotos y vídeos.

Si quieres saber más acerca de todo el potencial de Google Fotos puedes visitar su página web desde el siguiente enlace:

https://support.google.com/photos

Servicio iCloud

Las copias de seguridad en iCloud se hacen sin necesidad de un ordenador, pero necesitaremos una conexión WiFi, y también saber el tamaño aproximado que ocupará la copia, así como el espacio que tenemos disponible en el dispositivo.

Hay una serie de pasos que tenemos que comprobar previamente. El

primero es que nuestro dispositivo haya iniciado sesión en iCloud, en caso contrario, procederemos a acceder al servicio. Para ello, accedemos a «**Ajustes**», buscamos la opción «**iCloud**» y si aparece con una Apple ID debajo es que la sesión está iniciada.

Si no hay sesión iniciada, hacemos click sobre «**iCloud**» e introducimos los datos de nuestro Apple ID. Nos mostrará el correo electrónico que estamos usando, el espacio libre, si permitimos que algunas aplicaciones que tenemos instaladas almacenen datos en la Nube (iCloud Drive) y qué tipos de datos se sincronizarán.

https://support.apple.com/es-es/icloud

BOLESTIC
Nº 4 Especial Vacaciones 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración
incidentes.soc@juntadeandalucia.es

¿Qué es y cómo prevenir el carding?

El *carding* es un tipo de fraude que utiliza información de tarjetas robadas, para utilizarlas de manera fraudulenta. Los datos que se sustraen son los relativos a dichas tarjetas, de ahí el término de "*carding*" (*card* es tarjeta en inglés).

El ciberdelincuente obtiene un listado de tarjetas de crédito robadas. Para probar que los datos robados son verdaderos, el ciberdelincuente se ayuda de *bots* que realizan pequeñas compras en comercios electrónicos de forma repetida hasta dar con tarjetas válidas.

Los ciberdelincuentes utilizan distintas técnicas para obtener los datos de las tarjetas de las víctimas. A continuación, enumeramos algunas de las más conocidas.

- Usuarios víctimas de fraudes como: *phishing*, *smishing*, *vishing* o *shoulder surfing*.
- Distribución de *malware*, como *Keyloggers*, capaces de capturas las pulsaciones del teclado.
- Base de datos de clientes/usuarios de sitios webs cuya seguridad haya sido vulnerada, y que están publicadas en Internet.
- Webs fraudulentas en las que los usuarios hayan introducido sus datos bancarios.
- Empleo de lectores con comunicación inalámbrica RFID o NFC capaces de obtener los datos de la tarjeta. Se acercan a la tarjeta de la víctima a una distancia inferior a los 15 centímetros y en cuestión de segundos, se guardan los datos.

BOLESTIC
Nº 4 Especial Vacaciones 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración
incidentes.soc@juntadeandalucia.es

Protección de datos personales en vacaciones

Durante las vacaciones de verano no podemos bajar la guardia y debemos seguir siendo activos en la protección de nuestros datos, afrontando las situaciones de riesgo que se presentan en la época estival.

La actividad estival hace que la cámara de nuestro teléfono móvil tenga más trabajo del habitual: detalles de los lugares que hemos visitado, gente con la que hemos estado, fiestas a las que hemos asistido, etc. Compartir parte de esas fotografías en las redes sociales es algo habitual para muchas personas, pero entraña algunos riesgos.

Según datos del Centro de Investigaciones Sociológicas (CIS), una de cada cuatro personas se ha arrepentido en alguna ocasión de haber subido algo en una red social. Es importante pensar en quién podrá ver tus fotos antes de pulsar el botón "compartir". La AEPD dispone de una serie de vídeo tutoriales explicativos elaborados junto a INCIBE en los que explica cómo acceder a la configuración de privacidad y seguridad de algunos de los servicios más populares en Internet para que tu perfil no se muestre cuando, por ejemplo, introduzcan tu nombre en un buscador.

Incluso aunque tu perfil no sea accesible para los buscadores, o bien lo tengas en modo "privado", piensa también en que las personas a las que das acceso a tu información eligen a su vez quién puede tener acceso a su perfil: amigos, amigos de amigos o todo el mundo. Si compartes una foto con tus seguidores o amigos en una red social, y uno de ellos indica que algo le gusta, un amigo de amigo, al que no tienes por qué conocer, puede terminar viendo esa imagen. Y es posible que haya situaciones que quizás no quieras compartir con desconocidos.

Por último, debemos recordar que necesitamos consentimiento de las personas que aparecen en las fotos que tomamos antes de compartirlas en Internet, o bien de sus padres o tutores en el caso de que aparezcan menores.

BOLESTIC
Nº 4 Especial Vacaciones 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración
incidentes.soc@juntadeandalucia.es

EL POST-IT

Uso de la información

[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 debe proteger la información a la que tienes acceso y prevenir y evitar cualquier operación que pueda producir una alteración indebida, inutilización, destrucción, robo, revelación o uso no autorizado de la misma.

El acceso a la información, incluyendo documentos e información elaborados por el propio profesional en el desempeño de sus funciones, no confiere derecho alguno en cuanto a posesión, titularidad, derecho de copia, de cesión o divulgación de la misma, o cualquier otro derecho.

Se usará la información únicamente para el desempeño de tus funciones, sin destinarla a otros fines o incurrir en actividades no autorizadas o ilícitas.

Se atenderán a las prácticas de seguridad y protección de la propiedad intelectual que se hubieran establecido en lo que respecta a documentos o ficheros que pretendan introducir en el equipamiento del puesto de trabajo, en los servidores informáticos, en las redes de comunicación y en las aplicaciones y sistemas.

Se protegerá la información en formato papel que vaya a incorporarse a los sistemas de información o sea resultado de su tratamiento, tomando las precauciones necesarias para evitar que esta información pueda ser conocida por personal no autorizado. En particular, no abandonarán documentos en impresoras, escáneres o faxes (ya sean de uso exclusivo o compartido), almacenarán la documentación en lugar seguro evitando que quede sobre las mesas de trabajo al final de la jornada y seguirán las reglas para su custodia y destrucción.

Cuando participes en proyectos de investigación o que impliquen el tratamiento de datos masivos, el desarrollo de modelos predictivos o de inteligencia artificial, deberán atender las prácticas, directrices y códigos éticos que en su caso resulten de aplicación.

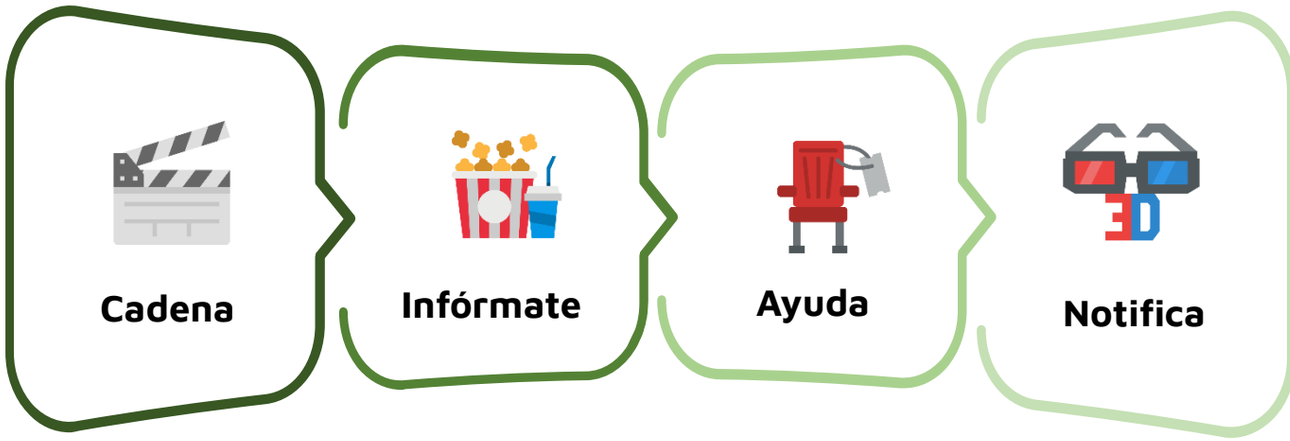
BOLESTIC
Nº 4 Especial Vacaciones 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración
incidentes.soc@juntadeandalucia.es

LA PELÍCULA

Sígueme El Rollo

Correos con bulos, leyendas urbanas y noticias falsas con contenido impactante que suelen ser distribuidas en cadena por sus receptores.

¿De qué sirve seguirles el rollo ?



01. Cadena

Promesas de felicidad y riqueza al reenviar el correo. No lo reenvíes, rompe la cadena.

02. Infórmate

Historias irreales pero creíbles convertidas en "leyendas urbanas". Ante la duda, busca información en otras fuentes.

03. Ayuda

Llamamientos falsos a la solidaridad pidiendo de manera urgente trasplantes o donaciones de sangre. Si alguien te lo envía, hazle ver el error.

04. Notifica

Siempre que recibas algún mensaje de este tipo, notifícalo al Centro de Atención de Personas Usuarias (CAU) de tu Consejería.

BOLESTIC
Nº 4 Especial Vacaciones 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración
incidentes.soc@juntadeandalucia.es

CONTRAPORTADA

Iníciate en ciberseguridad

Con este curso gratuito aprenderás a identificar las medidas necesarias para garantizar el correcto funcionamiento de los sistemas de tus dispositivos y a gestionar la seguridad con las metodologías y herramientas adecuadas. Para más información, pulsa aquí.

Ciberataques en vacaciones: los peligros de las redes WiFi públicas

Los peligros de las redes WiFi públicas que puedes encontrarte en tu próximo hotel o incluso en el aeropuerto, y que tanto investigadores como la Policía Nacional no recomiendan. Para más información, pulsa aquí.

El error habitual al elegir una contraseña que puede poner en riesgo tu ciberseguridad

Compartir contraseñas en el correo electrónico y las redes sociales puede ser una idea NO demasiado buena, teniendo en cuenta que cada vez hay más ciberataques, y a las posibilidades que genera la propia IA. Para más información, pulsa aquí.

Fraudes en transacciones digitales: cómo detectarlos para poder prevenirlos

Las transacciones digitales han revolucionado la manera en que realizamos compras y manejamos nuestras finanzas. Sin embargo, con el aumento de estas transacciones también ha crecido la amenaza del fraude digital. Para más información, pulsa aquí.