# BOLESTIC

Nº 2 Mayo 2024

Boletín de concienciación en ciberseguridad

Esta comunicación está destinada a los profesionales públicos de la Administración


## TITULARES

### Cuidado donde apuntas tu cámara, evita el QRshing

Un nueva técnica de phishing dirigida a los códigos QR ha aumentado su popularidad tras el auge que han tenido estos y que ya vemos en muchos lugares.

Pág. 2

### Navegación Segura en internet

El navegador web se ha convertido en una herramienta de uso cotidiano. Los delincuentes lo saben por lo que lo han convertido en su objetivo. Y nosotros como navegantes ¿somos conscientes de los peligros a los que nos exponemos?, ¿sabemos cómo navegar seguros?

Pág. 3

### Uso de Chatbots con inteligencia artificial

Muchas empresas utilizan Chatbots basados en IA para brindar asistencia al cliente a través de mensajes de texto. Estos pueden responder preguntas frecuentes, proporcionar información y ayudar en la resolución de problemas básicos.

Pág. 4

## Día Mundial de Internet


Con motivo de la celebración del Día de Internet el pasado 17 de mayo, ponemos a vuestra disposición esta píldora formativa Buenas prácticas en seguridad de la información desarrollada por el SOC de la Junta de Andalucía y esta página web de Andalucía Vuela sobre cómo la IA puede mejorar la vida personal y profesional.

## DE INTERÉS

### Los ciberataques y estafas más comunes en España.

| Ciberataques y estafas más frecuentes | | |
|---|---|---|
| 1 | Comprar en una web fraudulenta y no recibir nunca el producto | 22% |
| 2 | Descargar un virus sin querer que estropeó el ordenador o hizo que funcionara más lento | 20,5% |
| 3 | Recibir un mensaje pidiendo hacer clic en un enlace fraudulento e introducir los datos personales | 12% |
| 4 | Robo de datos bancarios | 10% |
| 5 | Comprar entradas para algún espectáculo (musical, deportivo...) y que estuvieran duplicadas o fueran falsas | 8,5% |
| 6 | Recibir un mensaje pidiendo hacer clic en un enlace y descargar un archivo malicioso | 8,5% |

Más información aquí.

## El POST-IT

**Uso de las aplicaciones y sistemas**

## LA PELÍCULA


## CONTRAPORTADA

- WhatsApp para iOS se actualiza y añade soporte para passkeys: qué es y qué significa
- ¿Te ha llegado un correo preguntándote por Pegasus?
- Las aplicaciones gratis son gratis por algo. Y sacan más de ti de lo que crees
- Los incidentes de ciberseguridad gestionados por INCIBE aumentaron en un 24%

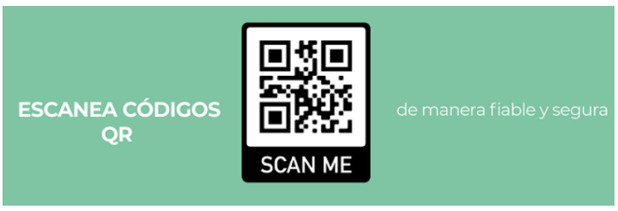
Comprueba si tu cuenta de correo está comprometida, https://haveibeenpwned.com/. Si es así, **cambia la contraseña**.

BOLESTIC
Nº 2 Mayo 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración

# TITULARES

## Cuidado donde apuntas tu cámara, evita el QRshing

El **QRshing** es la técnica de ingeniería social que emplea los códigos QR para lograr que la víctima, mediante el escaneo de este código, pueda ser engañada. Al accionar el código la víctima es conducida a una página web falsa donde el ciberdelincuente puede ejecutar un sin número de ataques como extraer información confidencial o instalar códigos maliciosos en el dispositivo, entre otros; se trata de una modalidad relativamente nueva de phishing.




Hoy en día, a través de cualquier cámara de un smartphone o tablet se pueden escanear estos códigos para acceder directamente, por ejemplo, a una página web o descargar una aplicación. Ahora bien, no todo es de color de rosa cuando hablamos de códigos QR, y nos preguntaremos, ¿por qué? ¿Qué riesgos puede suponer escanear un simple código con la cámara del móvil?

A simple vista, resulta muy atractivo, ¿no? Solo por escanear el código podemos conseguir una hamburguesa gratis e incluso algún premio o descuento. ¡Qué fácil parece! Tras escanear el código, nos aparece un mensaje en la pantalla para solicitar confirmación sobre si realmente queremos acceder la URL que esconde el código QR. Es en este momento cuando seriamente debemos plantearnos si realmente queremos instalar una app o visitar una determinada página.


Obviamente, si alguien pretende que instales una app maliciosa, no le va a poner el nombre de "APKMaliciosa.apk" o "EstoEsUnaAplicacionFraudulenta"; al contrario, intentará por todos los medios poner un nombre al enlace o ruta que pase desapercibido y no te haga sospechar, por ejemplo, "AppHamburguesaGratis.apk".

Entonces, ¿cómo puedes saber si lo que vas a visitar o instalar no te expone a ningún riesgo? A continuación, te proporcionamos algunas recomendaciones que puedes aplicar:

- **Revisa que el código QR** no esté pegado encima de otro código.
- **Si a primera vista**, la URL nos parece sospechosa, directamente no debemos acceder a ella.
- **Asegurarnos de que la web** a la que vamos a acceder siempre cumple con estándares de protección y navegación segura, como, por ejemplo, que tenga HTTPS.
- **Hacer uso de analizadores de enlaces**, como VirusTotal y URLVoid. De esta manera, antes de abrir la web podremos comprobar que no se trata de ningún ataque de ingeniería social como *Qrishing*, conocido como el *phishing* o *smishing* de los códigos QR.
- **No proporcionar** ningún dato privado ni ninguna contraseña a páginas web que hayamos accedido a través de un código QR. Es conveniente que si accedemos a páginas de bancos o tiendas online donde introducimos datos de nuestra tarjeta bancaria, lo hagamos desde la URL completa o a través de su aplicación propia.

Os mostramos este ejemplo de una estafa llevada a cabo en Madrid, aprovechando el popular servicio público de bicicletas. La táctica empleada por los ciberdelincuentes es ingeniosa y efectiva: **adhieren pegatinas con códigos QR falsos en bicicletas y patinetes eléctricos,** que conducen a una plataforma de pago externa. Para más información, pulsa aquí.

BOLESTIC
Nº 2 Mayo 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración

## Navegación Segura en internet

El navegador web se ha convertido en una herramienta de uso cotidiano. Desde él accedemos a páginas de las Administraciones Públicas y a servicios corporativos internos. Consultas, noticias, compras on-line, trámites con entidades financieras y otros organismos, acceso al correo electrónico, a redes sociales, a servicios en la nube, acceso a aplicaciones ofimáticas online, etc. todo esto, y mucho más, lo hacemos a través del navegador. Con toda esta actividad no es de extrañar que los delincuentes los hayan convertido en su objetivo. Y nosotros como navegantes ¿somos conscientes de los peligros a los que nos exponemos?, ¿sabemos cómo navegar seguros?


Si necesitas ayuda o consultar cualquier duda de navegación, puedes ponerte en contacto con tu **CAU** de referencia.

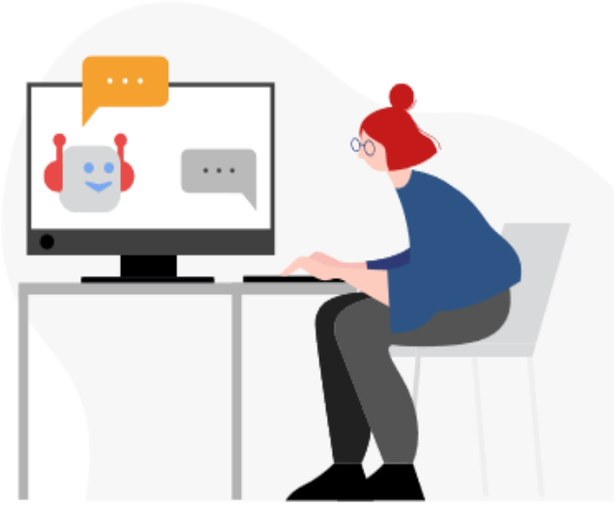
BOLESTIC
Nº 2 Mayo 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración

# Chatbots con inteligencia artificial

## RECOMENDACIONES PARA USUARIOS EN LA UTILIZACIÓN DE CHATBOTS CON INTELIGENCIA ARTIFICIAL

aepd agencia española protección datos

### Consejos generales en cuanto a los sistemas. Revisar que se ofrece:



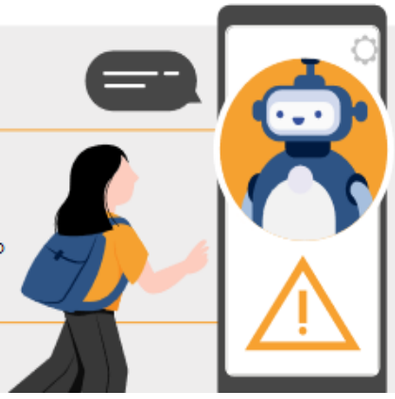
- una política de privacidad y aviso legal que incluya: identificación clara y precisa del responsable del tratamiento, y de sus datos de localización, fiscales y contacto;
- información clara de protección de datos con referencia al RGPD;
- información para poder ejercer los derechos de protección de datos;
- información sobre si el chatbot continúa aprendiendo de las conversaciones mantenidas con los usuarios y qué operaciones realiza con esos datos una vez mejorado.

### Consejos para los usuarios. No aceptar que:

- se soliciten datos de registro que no sean necesarios;
- se solicite consentimiento sin definir para qué se van a tratar los datos y sin que permitan retirarlo en cualquier momento, o se realicen transferencias a países que no ofrezcan garantías suficientes
- La Agencia también recomienda limitar los datos personales que se exponen, no dar datos personales de terceros si hay dudas de que el tratamiento va a trascender el ámbito doméstico y tener en cuenta que no hay garantías de que la información proporcionada por el chatbot sea correcta. Dependiendo del sistema, puede producir daño emocional, desinformación o inducir a engaño.

### Menores

Un chatbot no es un juguete.
No permitas que los menores a tu cargo lo utilicen sin tu supervisión.



aepd agencia española protección datos

BOLESTIC
Nº 2 Mayo 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración

# EL POST-IT

## Uso de las aplicaciones y sistemas

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.

**Los profesionales utilizarán exclusivamente las aplicaciones y sistemas que para el desempeño de sus funciones les haya habilitado la Administración de la Junta**

**Las aplicaciones y sistemas podrán pertenecer a otras Administraciones Públicas u otras entidades.**

**Se atenderán a las guías, instrucciones y manuales establecidos para el uso de las aplicaciones y sistemas.**

**Se seguirán los protocolos y mecanismos establecidos para gestionar incidencias y solicitudes de permisos.**

**Se deberán cerrar las sesiones al finalizar el uso de la aplicación. Se recomienda utilizar las funcionalidades dispuestas para ello en la misma («desconexión», «cerrar sesión», «salir» o similar) y no simplemente «cerrando» la ventana de trabajo.**

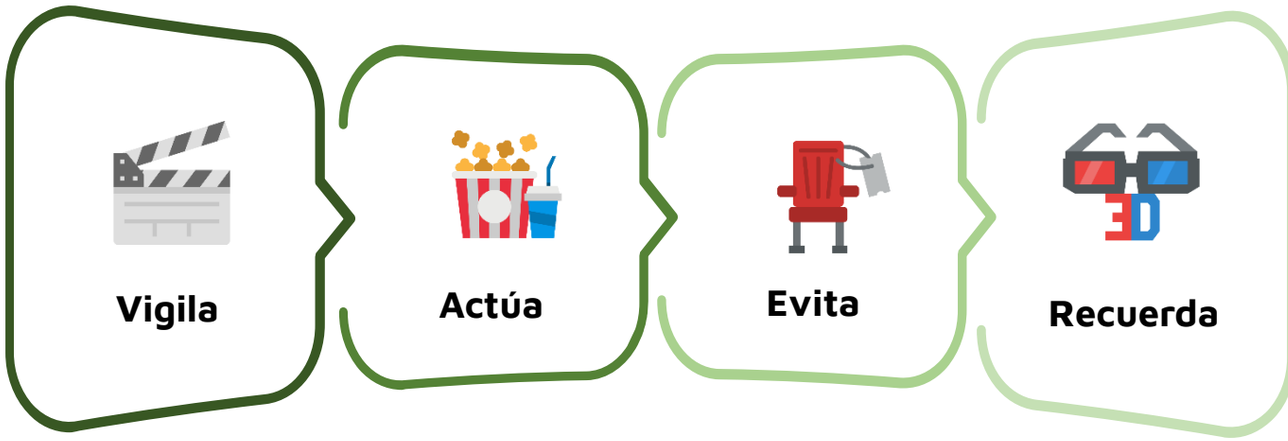
BOLESTIC
Nº 2 Mayo 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración

# LA PELÍCULA


## No es país para viejos

Las actualizaciones tratan de mejorar la funcionalidad y seguridad de nuestros dispositivos. Por lo que es de vital importancia no dejarlos envejecer.

Más vale actualizar y no tener que lamentar.




## 01. Vigila

Vigila el estado de actualización de todos tus dispositivos y aplicaciones.

## 02. Actúa

Instala las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores y programas antivirus.

## 03. Evita

Evita hacer uso de aplicaciones y sistemas operativos antiguos que ya no dispongan de actualizaciones de seguridad.

## 04. Recuerda

Las actualizaciones de software no son un fastidio. Al contrario, son esenciales para mantener la seguridad de nuestros dispositivos.

BOLESTIC
Nº 2 Mayo 2024
Boletín de concienciación en ciberseguridad
Esta comunicación está destinada a los profesionales públicos de la Administración

# CONTRAPORTADA

## WhatsApp para iOS se actualiza y añade soporte para passkeys: qué es y qué significa

Esta función, que lleva disponible en Android unos cuantos meses, permite proteger el acceso a la cuenta de una forma muy sencilla y usando algo que todos llevamos siempre en el bolsillo: el móvil. Para más información, pulsa aquí.


## ¿Te ha llegado un correo preguntándote por Pegasus?

Se ha identificado una campaña de correos electrónicos fraudulentos que buscan extorsionar a los destinatarios, solicitándoles un pago en un monedero virtual de bitcoin a cambio de no divulgar supuestas grabaciones íntimas. Para más información, pulsa aquí.

## Las aplicaciones gratis son gratis por algo. Y sacan más de ti de lo que crees

Es tan extraño pagar por la descarga de una aplicación que seguramente ni te lo plantees. Aun así, las apps gratis se llevan una buena parte de ti más allá del dinero, están pensadas para actuar como gancho con la intención de atraerte hasta que las instales. Para más información, pulsa aquí.


## Los incidentes de ciberseguridad gestionados por INCIBE aumentaron en un 24%

El Instituto Nacional de Ciberseguridad (INCIBE), ha publicado su Balance de Ciberseguridad relativo al año 2023, donde se refleja un incremento del 24% de los incidentes respecto al año anterior. Para más información, pulsa aquí.