

Tu día a día digital más seguro

Aprende a actuar ante los riesgos digitales más comunes



Nadie debería quedarse fuera de **Internet** por miedo a no saber usarlo o a sufrir un **ciberataque**.

En tu día a día digital puedes tener que afrontar diferentes retos, pero teniendo presente unas sencillas pautas, puedes navegar con más tranquilidad.

En esta guía recopilamos **situaciones cotidianas en el entorno digital** —trámites, llamadas, mensajes, compras...— y explicamos cómo actuar en cada una de ellas para evitar riesgos.

Situación 1: Te llega un mensaje urgente pidiendo “verificar tus datos”

Situación 2: Te llaman o escriben diciendo ser del “soporte técnico” de tu ordenador o router

Situación 3: Recibes una notificación para un pago urgente

Situación 4: Un familiar te escribe por WhatsApp pidiendo dinero con urgencia

Situación 5: Dudas si una tienda online o una oferta es de fiar

Situación 6: Alguien ha entrado en una de tus cuentas de redes sociales

Partiendo de cada una de estas situaciones, te ofrecemos pequeñas **dosis de aprendizaje** para ayudarte a conseguir que la ciberseguridad forme parte de tu rutina diaria de manera natural.

Además, también te ofrecemos **consejos para apoyarte en la Inteligencia Artificial (IA)** como si fuera tu asistente personal de ciberseguridad, y compartimos información sobre recursos gratuitos a tu alcance para mejorar tu seguridad en Internet.

Situación 1: Te llega un mensaje urgente pidiendo “verificar tus datos”

Te llega un mensaje que dice ser de tu banco, de la Junta de Andalucía o de un servicio de paquetería.

Te avisa de que tu cuenta se bloqueará, que hay un problema con un envío o que debes “confirmar” algo, y te invita a pinchar en un enlace.

Cómo actuar:



Para y piensa antes de actuar

El mensaje dará sensación de urgencia para que actúes lo antes posible indicando que tienes pocas horas para resolver la incidencia o similar, repasa el texto del mensaje y piensa si realmente podría estar dirigido hacia ti, ¿tienes cuenta en el banco que pretende ser? ¿Estás realizando algún trámite con la Junta de Andalucía? ¿Estás esperando un paquete?



Si acabas de recibir el mensaje

No pinches en el enlace, aunque el mensaje parezca oficial. Si el mensaje menciona una entidad real, contacta con ella a través de su web oficial (escribiendo la dirección en el navegador) o por su teléfono habitual, pero **nunca** a través de los datos que aparecen en el mensaje sospechoso.



Si llegas a acceder al enlace

Justo estabas esperando este tipo de mensaje y has accedido al enlace. De repente te piden que facilites datos con los que se supone que ya contaban o te solicitan que vuelvas a pagar. Te empieza a sonar extraño. Piensas que puede ser una estafa. En este caso, no introduces ningún dato y cierra inmediatamente esa página.



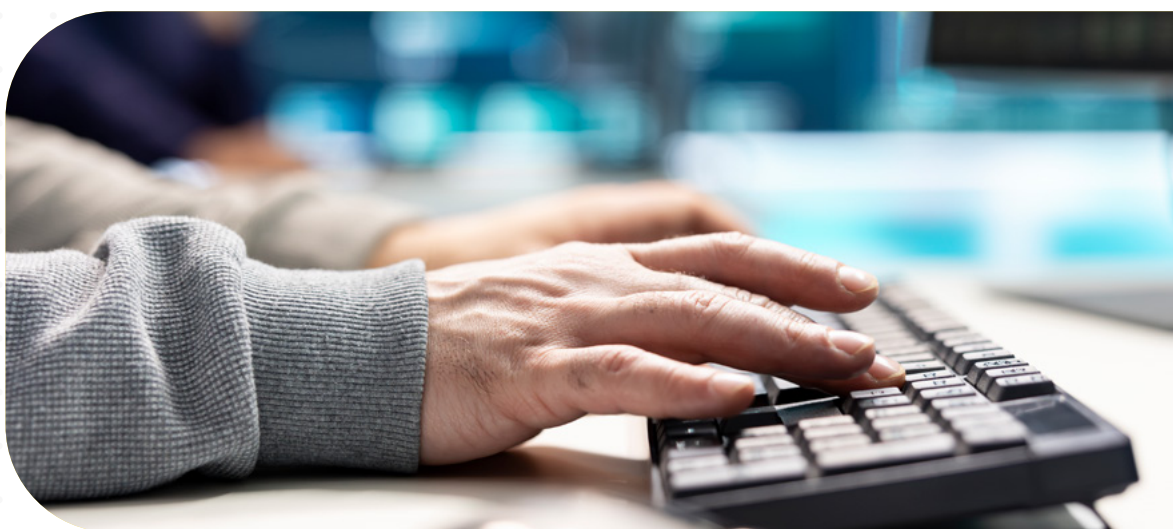
Si llegas a introducir datos

Todo cuadraba, no sospechaste nada y decidiste compartir tus datos. Un tiempo después empiezan a llegar cobros desconocidos a tu cuenta bancaria. ¿Qué debes hacer?

- ↪ Contacta con tu banco urgentemente para bloquear la cuenta afectada.
- ↪ Recopila capturas de pantalla y todas las evidencias posibles para denunciar ante las Fuerzas y Cuerpos de Seguridad del Estado.
- ↪ Una vez presentada la denuncia, compártela con tu banco y abre una reclamación para recuperar el dinero perdido.

Además, te recomendamos, para futuras ocasiones:

- ↪ No acceder a enlaces sin verificar previamente su veracidad con la entidad que te lo ha enviado por teléfono u otra vía de contacto. Siempre accede a la entidad escribiendo su dirección web en el navegador, por teléfono o correo electrónico, nunca desde el enlace que se indican en los mensajes
- ↪ Hacer uso de analizadores de URLs para comprobar la seguridad de un enlace antes de entrar.
- ↪ En caso de haber accedido a un enlace sospechoso, analizar el dispositivo utilizado con un antivirus antes de continuar utilizándolo.
- ↪ Activa el segundo factor de autenticación en las plataformas que lo permitan.



Situación 2: Te llaman o escriben diciendo ser del “soporte técnico” de tu ordenador o router

Una persona te contacta por mensajería o teléfono, se identifica como técnico y explica que ha detectado un problema en tu dispositivo o en tu red WiFi.

Te pide acceso remoto al dispositivo y que instales un programa.

Cómo actuar:



Si sospechas que hay algo raro desde el principio

No te termina de encajar lo que te están diciendo y piensas que puede ser una estafa. Cuelga la llamada o cierra el chat directamente.

Ninguna empresa detecta problemas en tu dispositivo o en tu cuenta por iniciativa propia y te llama para solucionarlo.

Llama de todas formas al teléfono oficial de la empresa para confirmar si el aviso era real, y para alertar de la situación para que puedan tomar las medidas oportunas.

Si has seguido sus instrucciones



↪ Si has dado acceso remoto a tu ordenador o a cualquier otro dispositivo, desconéctalo de Internet inmediatamente (apaga el WiFi o quita el cable) para cortarles el acceso.

↪ Busca ayuda técnica para revisar tu dispositivo en busca de software malicioso y utiliza otro aparato diferente para cambiar contraseñas importantes, especialmente las contraseñas de los servicios con datos más privados y personales (bancos, redes sociales, servicios en la nube con copias de seguridad de fotos o documentos, datos médicos, etc.).

↪ Recopila todas las evidencias posibles para denunciar ante la Policía Nacional o la Guardia Civil.

↪ Formatea tu dispositivo.

↪ Si crees que han podido acceder a datos sensibles como tu DNI, tu cuenta bancaria o tu certificado digital, intenta localizar usos no autorizados de esta información personal y denúncialo a las entidades competentes.

Situación 3: Recibes una notificación para un pago urgente

Llega una notificación electrónica de la Agencia Tributaria o de Hacienda Local para hacer un pago urgente.

Cómo actuar:



Recibes el aviso electrónico por SMS o email:

No pinches en ningún enlace que traiga el mensaje. Para comprobar si es real, entra en la sede electrónica oficial del organismo (escribiendo tú la dirección en el navegador, nunca entrando a través del enlace del propio mensaje recibido) y consulta tu buzón de notificaciones con tus propias claves de acceso (certificado digital, DNle o Cl@ve).

Si no aparece ninguna notificación, el mensaje recibido era un intento de suplantación de identidad, por lo que debes eliminarlo inmediatamente.

Si no sabes entrar en la sede electrónica o te quedan dudas, también puedes acudir a las oficinas de atención presencial o llamar al organismo directamente para que te confirmen si la notificación es real.



Si pinchaste en un enlace o has seguido los pasos del mensaje

En caso de que hayas seguido los pasos que te pedían en el mensaje sin comprobar si era una notificación real, ten en cuenta lo siguiente:

- ↪ Contacta con el organismo y comprueba si la notificación era real. En caso contrario, reporta el incidente y aporta todas las evidencias posibles.
- ↪ Si has introducido tus credenciales al pinchar en un enlace fraudulento, cambia inmediatamente tu contraseña en todos los servicios en los que la utilices.
- ↪ Activa un doble factor de autenticación cuando sea posible.

Situación 4: Un familiar te escribe por WhatsApp pidiendo dinero con urgencia

Recibes un mensaje supuestamente de parte de un familiar o de una persona conocida contando que necesita que le ingreses dinero o le compres algo de manera urgente.

Cómo actuar:



Cuando recibes el mensaje

No respondas por ese mismo chat ni envíes dinero todavía, aunque te haya llegado por el canal por el que habláis habitualmente. Desconfía siempre de la urgencia: es la herramienta principal de la que se vale este tipo de fraude.

Para confirmar la veracidad de la petición, llama a esa persona directamente por teléfono, o pregúntale algo que solo ella sabría.

Si no logras contactar con esa persona, consulta con alguien más que pueda confirmar la situación antes de mover cualquier dinero.



Si has hecho el pago y descubres que era una estafa

Ponte en contacto con tu banco. Explica que has sido víctima de una estafa para que intenten bloquear el pago o la transferencia, o retroceder la operación.

Acude a la Policía Nacional o a la Guardia Civil a interponer una denuncia aportando capturas de pantalla de la conversación y justificantes del banco.





Si desde tu propia cuenta de WhatsApp envían estos mensajes a tus contactos

También puede ocurrir que tu propia cuenta de WhatsApp sea hackeada y ciberdelinquentes estén contactando con tus contactos solicitándoles dinero. En este caso, debes:

- ↪ Avisar a los contactos por llamada, correo o SMS de que tu cuenta ha sido hackeada y que no realicen ningún pago dirigido a ti.
- ↪ Entrar en tu cuenta de WhatsApp, revisar los dispositivos vinculados y cierra todas las sesiones. Si no ves sesiones que no reconozcas, verifica la seguridad de los equipos donde tengas una sesión vinculada.
- ↪ Desinstalar y volver a instalar la aplicación de WhatsApp.
- ↪ Activar la verificación en dos pasos desde los ajustes de la aplicación.
- ↪ Actualizar con regularidad el sistema operativo de tu teléfono móvil y las aplicaciones instaladas en él.



Situación 5: Dudas si una tienda online o una oferta es de fiar

Ves un anuncio con un precio muy por debajo de lo normal, o una web que no conocías te ofrece algo que te interesa, y no sabes si es seguro realizar la compra.

Cómo actuar:



Antes de decidir la compra

En primer lugar, comprueba que la web tenga datos de contacto reales y una dirección física, no solo un formulario.

También es recomendable buscar el nombre de la web seguido de la palabra "opiniones" o "estafa" en un buscador de Internet, para ver qué información sobre la misma han podido publicar otras personas anteriormente.



En el momento del pago

Si parece que todo está bien y te decides a comprar, a la hora de realizar el pago, elige la opción de pagar por tarjeta o a través de plataformas de pago reconocidas en vez de otras opciones como transferencia bancaria o Bizum. En caso de que sea una estafa, podrás recuperar tu dinero más fácilmente.



Si has comprado y descubres que es una estafa

Intenta contactar con el vendedor (para dejar constancia). Comunica también la situación a tu banco y solicita la devolución del pago mediante tarjeta argumentando fraude.

Reúne evidencias como capturas de pantalla de la web, posibles comunicaciones o justificantes de pago y presenta una denuncia ante la Policía Nacional o la Guardia Civil.

Situación 6: Alguien ha entrado en una de tus cuentas de redes sociales

Te llega un aviso de inicio de sesión desde un lugar que no reconoces, o te avisan de movimientos que no has hecho en tu perfil de Instagram, Facebook o cualquier otra red social.

Cómo actuar:



Recibes un email alertando de un inicio de sesión extraño

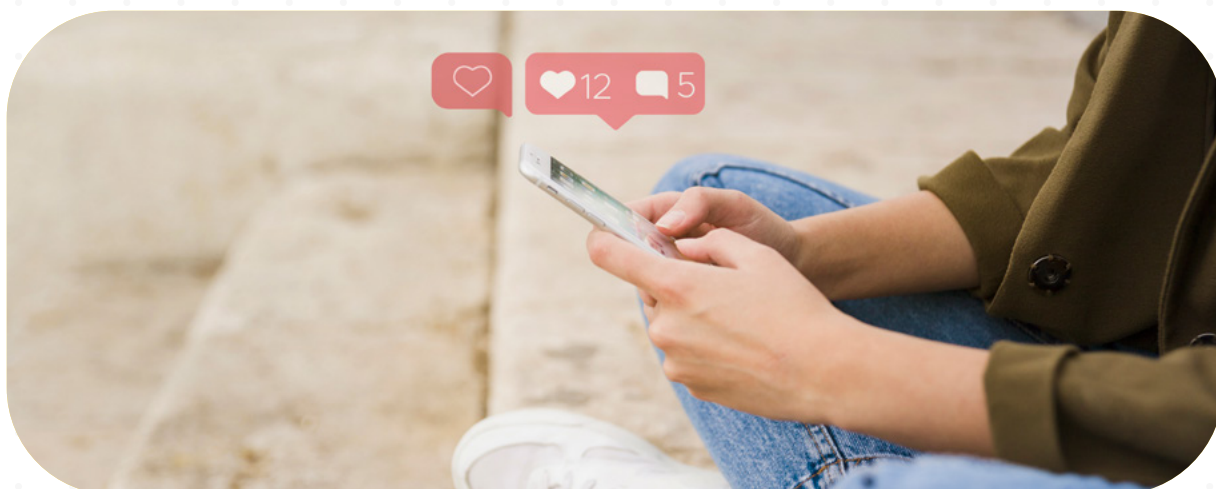
Es importante que tengas en cuenta que a veces estos correos son falsos y tienen como objetivo robarte la clave. Para evitarlo, no uses el enlace del correo, es mejor que accedas directamente a la aplicación o web oficial y revises el apartado de "Seguridad", en el que puedes consultar desde dónde se ha iniciado sesión en tu cuenta.

Además, como medidas preventivas es recomendable actualizar la contraseña con frecuencia, y activar la autenticación en dos pasos, para reforzar la seguridad en el acceso a tus redes sociales.



Si confirmas que hay accesos o movimientos sospechosos

Cambia la contraseña de esa cuenta de inmediato, y también la de cualquier otra cuenta donde uses la misma contraseña. Revisa si hay dispositivos conectados que no reconoces y en ese caso ciérrales la sesión desde la propia cuenta.



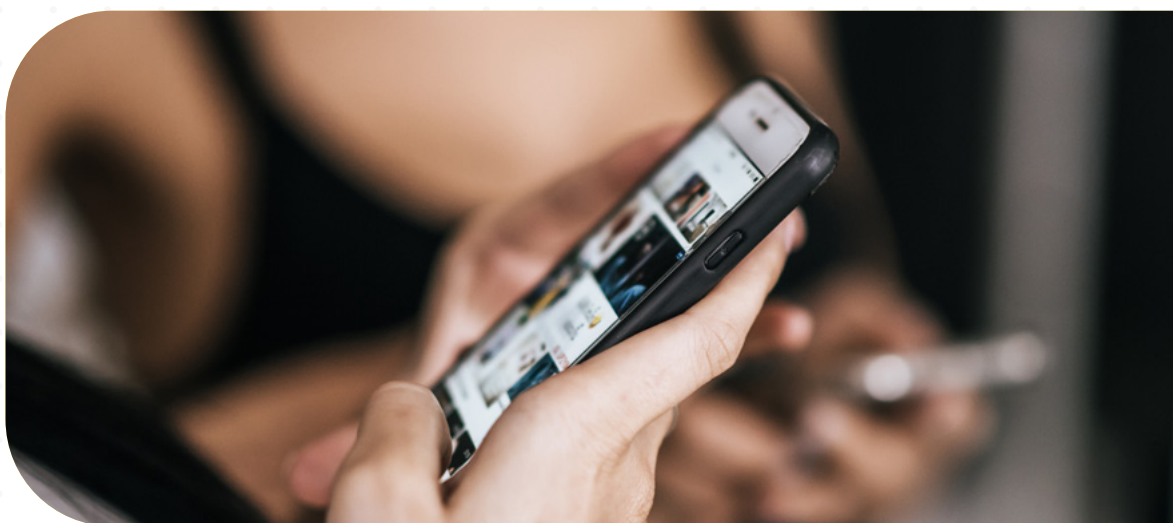


Si te han cambiado la contraseña y ya no puedes entrar

Utiliza las opciones de "He olvidado mi contraseña" o "Mi cuenta ha sido hackeada/comprometida" que ofrecen estas redes sociales para recuperar tu acceso y sigue los pasos indicados.

Una vez recuperada tu cuenta, cambia la contraseña de inmediato, y también la de cualquier otra cuenta donde uses la misma clave. Además, sigue estos consejos:

- ↪ Activa la verificación en dos pasos si esa cuenta lo permite: añade una capa extra de seguridad, aunque alguien consiga tu contraseña.
- ↪ Mantén actualizado el navegador y las aplicaciones móviles, así como los complementos o plugins instalados. Ten en cuenta siempre descargarlos desde sitios oficiales.
- ↪ Elimina cada cierto tiempo los datos de navegación, como las cookies, el historial y el caché.
- ↪ Revisa detenidamente las notificaciones o mensajes que aparezcan al acceder a una web antes de aceptarlos.
- ↪ No guardes las contraseñas dentro del navegador y utiliza gestores de contraseñas en su lugar.
- ↪ Ignora cualquier mensaje directo que te llegue solicitando alguna acción en tu perfil.



Utiliza la IA como tu asistente de ciberseguridad

La Inteligencia Artificial también puede ayudarte a protegerte, pero recuerda no compartir nunca con estas herramientas tus datos personales ni contraseñas.



Cuentas más seguras

Pídele a la IA que te ayude a proteger tu cuenta de correo o tus cuentas en redes sociales.

Si no sabes cómo hacerlo, tener activada la verificación en dos pasos es uno de los mecanismos más efectivos. Pídele a la IA lo siguiente:

"Dame las instrucciones exactas, paso a paso, para activar la verificación en dos pasos en mi cuenta de [nombre de la app, ej. Google o WhatsApp]."

También, es importante mantener privada tu información personal en tus perfiles de redes sociales. Si no sabes cómo, copia y pega esto en la IA:

"Quiero que mi perfil de [indica la red social, ej. Facebook o Instagram] sea completamente privado para que solo las personas que yo apruebe puedan ver mis fotos e información personal. Dime los pasos exactos que debo seguir dentro de la aplicación del móvil para configurar esta privacidad máxima."



Contraseñas

El mayor riesgo es usar la misma contraseña para todo o usar como clave alguna información fácil de adivinar, como la fecha de nacimiento.

La IA puede enseñarte trucos mnemotécnicos para crear contraseñas robustas sin que tengas que apuntarlas en un post-it. Haz la prueba, copiando y pegando este prompt:

"Actúa como un profesor de ciberseguridad. Explicame la técnica de combinar palabras aleatorias para crear una contraseña muy segura pero fácil de recordar."

"Dame 3 ejemplos prácticos que cumplan con los requisitos de seguridad actuales (mayúsculas, números y símbolos) y explicame por qué son seguras."

Una vez creada tu contraseña con este truco, lo más recomendable es que la uses como tu contraseña maestra para acceder a un gestor de contraseñas.

Antes de despedirnos

Saber manejarte en Internet no significa hacerlo todo sin ayuda, sino saber a quién y a qué recurrir cuando surge una duda, sin importar tu edad o nivel de conocimiento.

Verificar antes de hacer clic, apoyarte en la IA para entender un trámite o pedir ayuda a alguien de confianza son ideas recomendables para moverte con seguridad por Internet.

En Andalucía Vuela, contamos con recursos y servicios para ayudarte a manejarte con más seguridad en el mundo digital.

Aprende Volando

Cursos gratuitos de 10 horas para mejorar tu nivel digital sin importar tu punto de partida o tu edad.

Más información aquí

Click_A

Proyecto en colaboración con Cruz Roja en el que una red de voluntariado ayuda a personas con necesidades de apoyo a manejarse mejor con dispositivos y herramientas digitales.

Más información aquí

Puntos Vuela

760 centros abiertos a todas las edades y repartidos por toda Andalucía para explorar el mundo digital y aprender competencias digitales con apoyo personalizado.

Más información aquí

*Guía generada a partir de la "Guía de ciberataques" de INCIBE y el servicio de la Oficina de Seguridad del Internauta (OSI) publicada en <https://www.incibe.es> y en colaboración con el Centro de Ciberseguridad de Andalucía.

vuela

Más cerca, más digitales, más oportunidades

andaluciavuela.es

