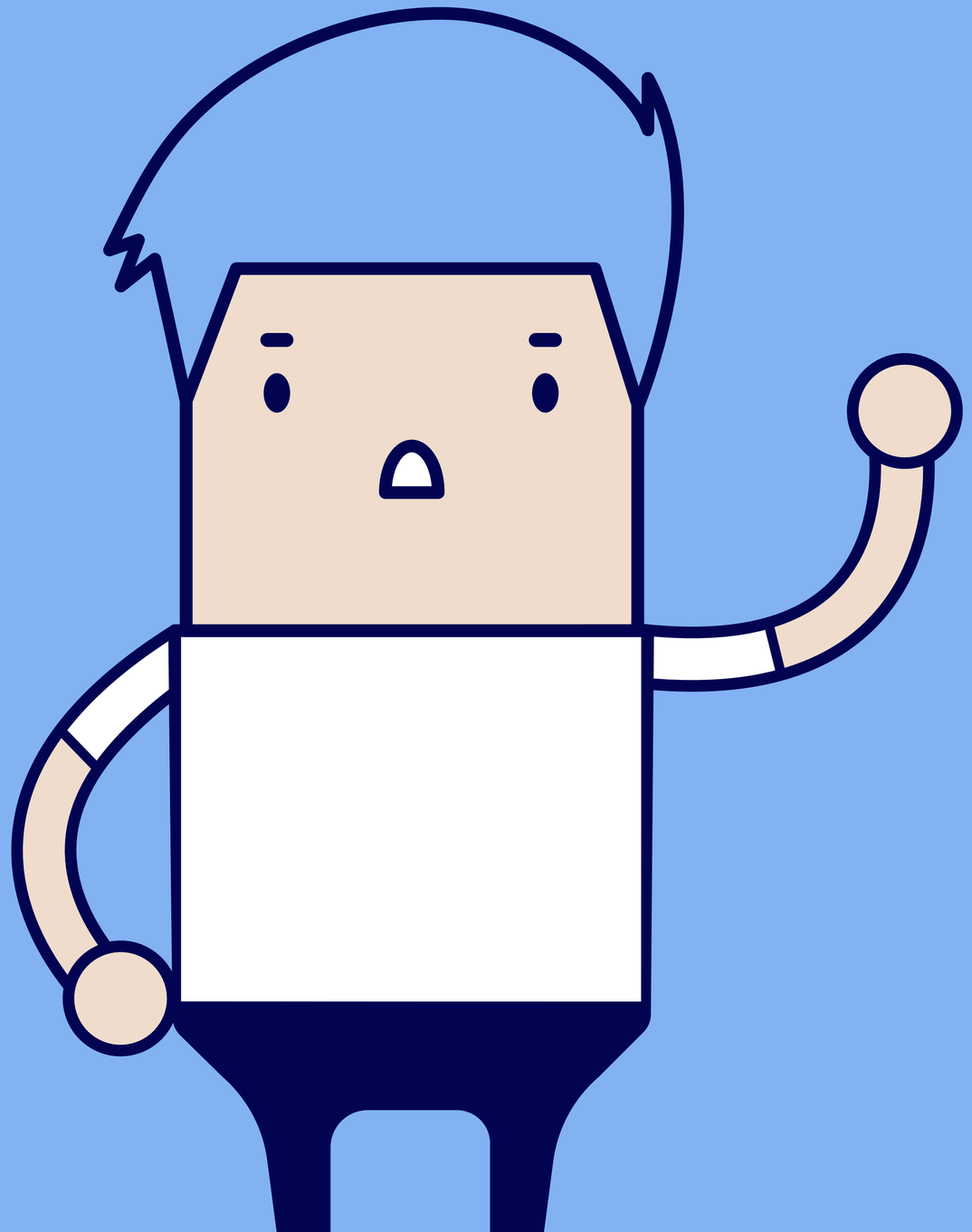
POR TU S€GURIDAD,

No piques

Protégete de fraudes y estafas digitales.

Ayuntamiento
ALBACETE



¿Dónde denunciar fraudes y estafas?

¿Dónde denunciar fraudes y estafas?

Fuezas y Cuerpos de Seguridad, Ministerio Fiscal y Tribunales

En caso de fraudes o estafas (conductas tipificadas como delitos), corresponde a las Fuerzas y Cuerpos de Seguridad (Cuerpo Nacional de Policía y Cuerpo de la Guardia Civil), el Ministerio Fiscal y los correspondientes Órganos Judiciales su investigación y persecución. Para los casos de ciberdelitos, se podrá dirigir la denuncia a la Brigada Central de Investigación Tecnológica de la Policía.

INCIBE y OSI

En los casos de ciberdelitos, además de denunciar ante la Brigada Central de Investigación Tecnológica de la Policía, se recomienda notificar el caso ante INCIBE-CERT (Centro de respuesta a incidentes de seguridad del Instituto Nacional de Ciberseguridad). Este Centro dispone de información en su página web www.incibe.es. Cuenta también con distintos canales para contactar, como la línea telefónica gratuita 017, el canal de WhatsApp 900 116 117 o de Telegram @INCIBE017. La Oficina de Seguridad del Internauta (OSI) también proporciona información y el soporte necesario para evitar y resolver los problemas de seguridad online.

Agencia Española de Protección de Datos

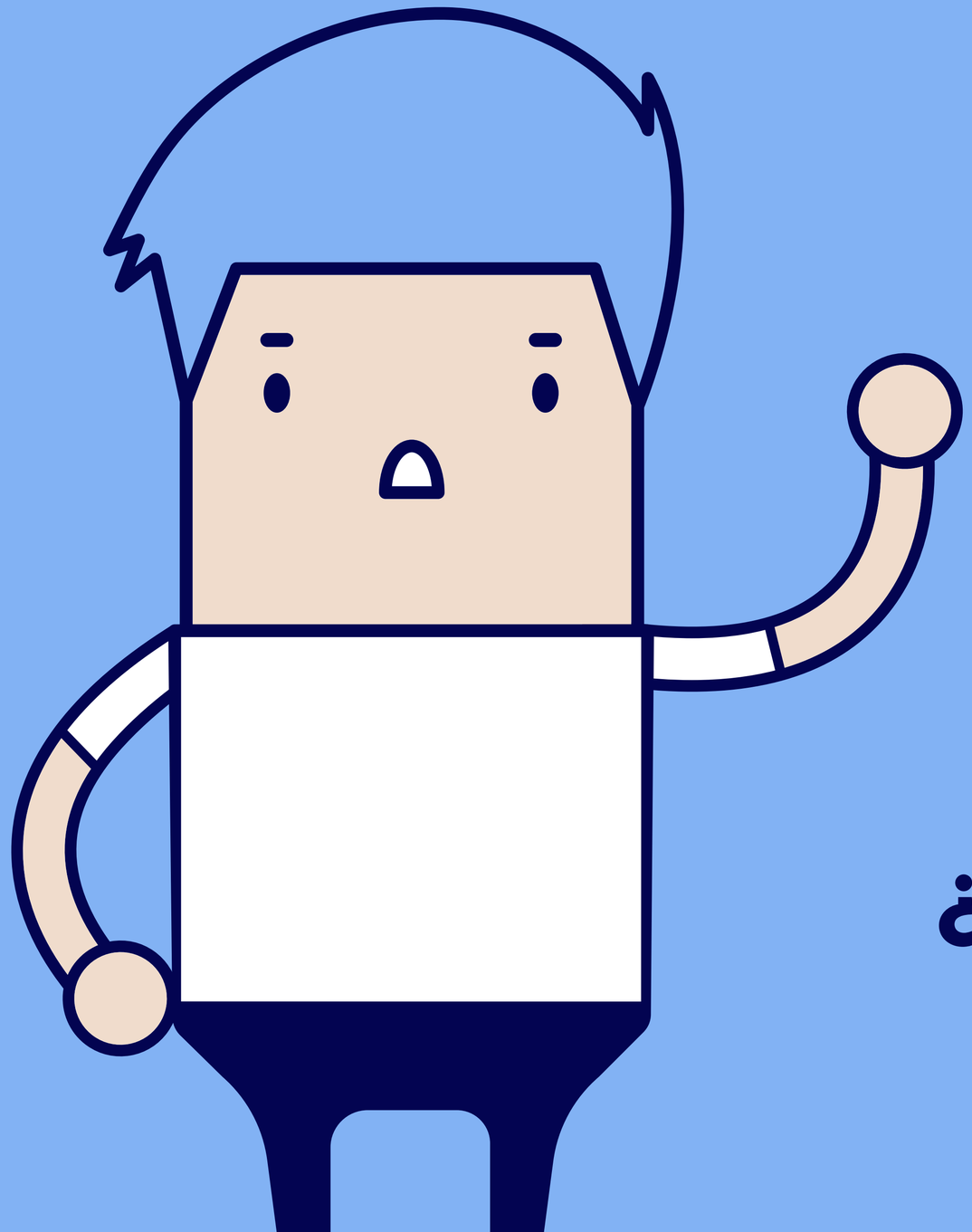
Si se hubieran facilitado datos personales como nombre, apellidos o el domicilio, también se recomienda notificar el fradue en la Agencia Española de Protección de Datos.

Deben guardarse siempre los justificantes de pagos, teléfonos de contacto, correos electrónicos o cualquier otro justificante que pueda contribuir a perseguir el delito.

ECC-Net

Los Centros Europeos del Consumidor no tienen competencias para actuar en caso de fraudes o estafas.

La Red de Centros Europeos del Consumidor (ECC-Net) es un organismo que trata de alcanzar acuerdos amistosos para resolver reclamaciones de consumo transfronterizo europeo entre consumidores y empresas.
Los casos de fraude llevados a cabo por presuntos delincuentes o redes organizadas no son un asunto propiamente de consumo, sino presuntas estafas, tipificadas dentro de lo penal, por lo que corresponde a las Fuerzas y Cuerpos de Seguridad del Estado, así como a Jueces y Tribunales de Justicia investigar y resolver los hechos.



Compras online seguras, compras de confianza

El comercio online ofrece grandes ventajas como poder comparar distintos proveedores y ordenar la compra cómodamente. Sin embargo, hay que comprobar la seguridad de la tienda y la calidad de los productos para no caer en un fraude o comprar un producto falso. Recuerda, si una persona compra productos falsificados, no solo perderá sus derechos, adquirirá productos de menor calidad, perjudicará la innovación empresarial y formentará la competencia desleal. También estará arriesgando su salud y seguridad.

¿Cómo evitar ciberestafas y fraudes online?

Ayuntamiento ALBACETE

Cómo evitar ciberestafas y fraudes online

Compra en canales oficiales

Utiliza páginas web y apps oficiales o de confianza. Verifica que el e-mail coincide con la empresa que supuestamente envía el correo. Generalmente, se utilizan dominios públicos o que se parecen al que sería el correo oficial. Sospecha de correos tipo @gmail, @outlook o similar. Los enlaces del correo deben ser comprobados antes de hacer clic en ellos. Comprueba la seguridad de la web colocando el cursor del ratón sobre el hipertexto de la URL (candado o llave). En caso de sospecha, contacta con el proveedor oficial.

Comprueba la identidad del comprador/a o vendedor/a

La identidad del comercio como la dirección, CIF/NIF, la razón social, los datos de contacto, o registro mercantil deben aparecer de forma clara y accesible. Normalmente, en “Aviso legal”, Términos y condiciones” o “Política de privacidad”. En caso de duda, consulta la web oficial de la marca para conocer cuáles son los vendedores autorizados e identificar las tiendas fraudulentas.

- **Productos de segunda mano**. Infórmate de quién es el comprador/a o vendedor/a.
- **Productos reacondicionados**. Pueden tener una garantía distinta y que las expectativas del consumidor/a no se correspondan con las que ofrece el producto nuevo.

Exige buenas prácticas profesionales

Corrobora que la tienda está adherida a un código de conducta y código de buenas prácticas de comercio electrónico. Algunos de los sellos de confianza más conocidos son Confianza Online, Trusted Shops, AENOR, e-comercio, entre otros.

Cómo evitar ciberestafas y fraudes online

Protege tus datos personales

La empresa debe informar sobre los datos personales que se recogen, su uso y la finalidad. Esta información normalmente se encuentra en el área de "Privacidad" o en "Términos y condiciones". Debe facilitar también información sobre el uso de cookies.

Consejo:

No facilitar datos personales (financieros, códigos, contraseñas, etc.) por internet o teléfono e informar a la entidad del que supuestamente procede el e-mail, el SMS o la llamada. Las entidades bancarias ni ningún otro proveedor legítimo pedirá al cliente datos personales o claves secretas de acceso.

Comprueba la información del producto

La información del precio total del producto debe ser clara y precisa, debe indicar si incluye o no los impuestos, los gastos de envío si los hubiera y la política de devoluciones. Esta información suele aparecer en los "Términos y condiciones" o el "Aviso legal". Deberá sospecharse de las páginas web sin estos apartados.

Comprueba tus derechos como consumidor/a

La web deberá incluir información sobre los derechos del consumidor y las garantías. Por ejemplo, el derecho a desistir en un plazo de 14 días, así como los mecanismos para reclamar, como la plataforma ODR para litigios online.

Consejo:

Comprueba si existe un servicio de atención al cliente y llama para verificar si funciona correctamente.

Cómo evitar ciberestafas y fraudes online

Sospecha de ofertas sorprendentes

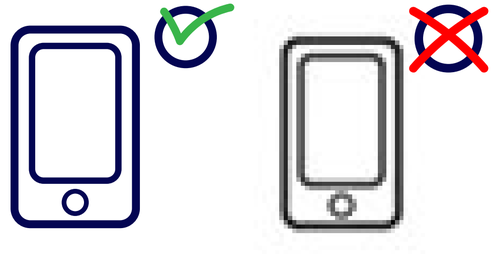
Desconfía de aquellas webs que ofrecen precios excesivamente bajos en relación con los del mercado o las tiendas oficiales, así como si todos los artículos se venden al mismo precio. Sospecha si un producto aparece con un precio inicial muy inflado al que se le aplica un descuento muy alto u ofertas demasiado llamativas como para dejarlas pasar.

Consejo:

Cuidado con los mensajes que obligan a tomar una decisión rápida. Comprobar si la urgencia es real. Para ello, consulta otras fuentes de información de confianza.

Duda de las webs con fallos en los contenidos

Desconfía de las páginas web que tienen fallos de diseño, imágenes y logotipos de baja calidad o poco profesionales, errores ortográficos o gramaticales. Las imágenes de los productos deben mostrar la totalidad del producto. En caso de duda, solicita más información al vendedor.



La mayoría de los sitios web que venden productos originales parecen profesionales.

Busca opiniones y reseñas

Busca en Internet referencias y opiniones de otros consumidores/as y comprueba el tiempo que lleva el vendedor/a con presencia en el comercio online. En caso de duda, desconfiar.

Consejo:

Buscar en Internet:

“Nombre de la empresa + estafa”

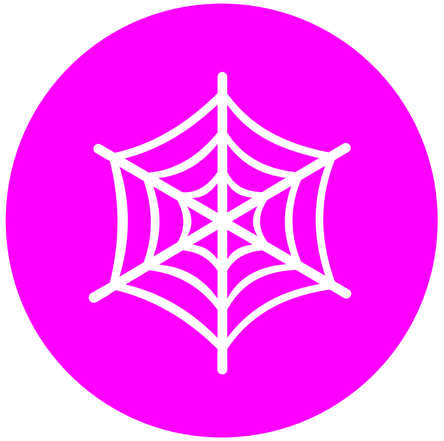
Cómo evitar ciberestafas y fraudes online

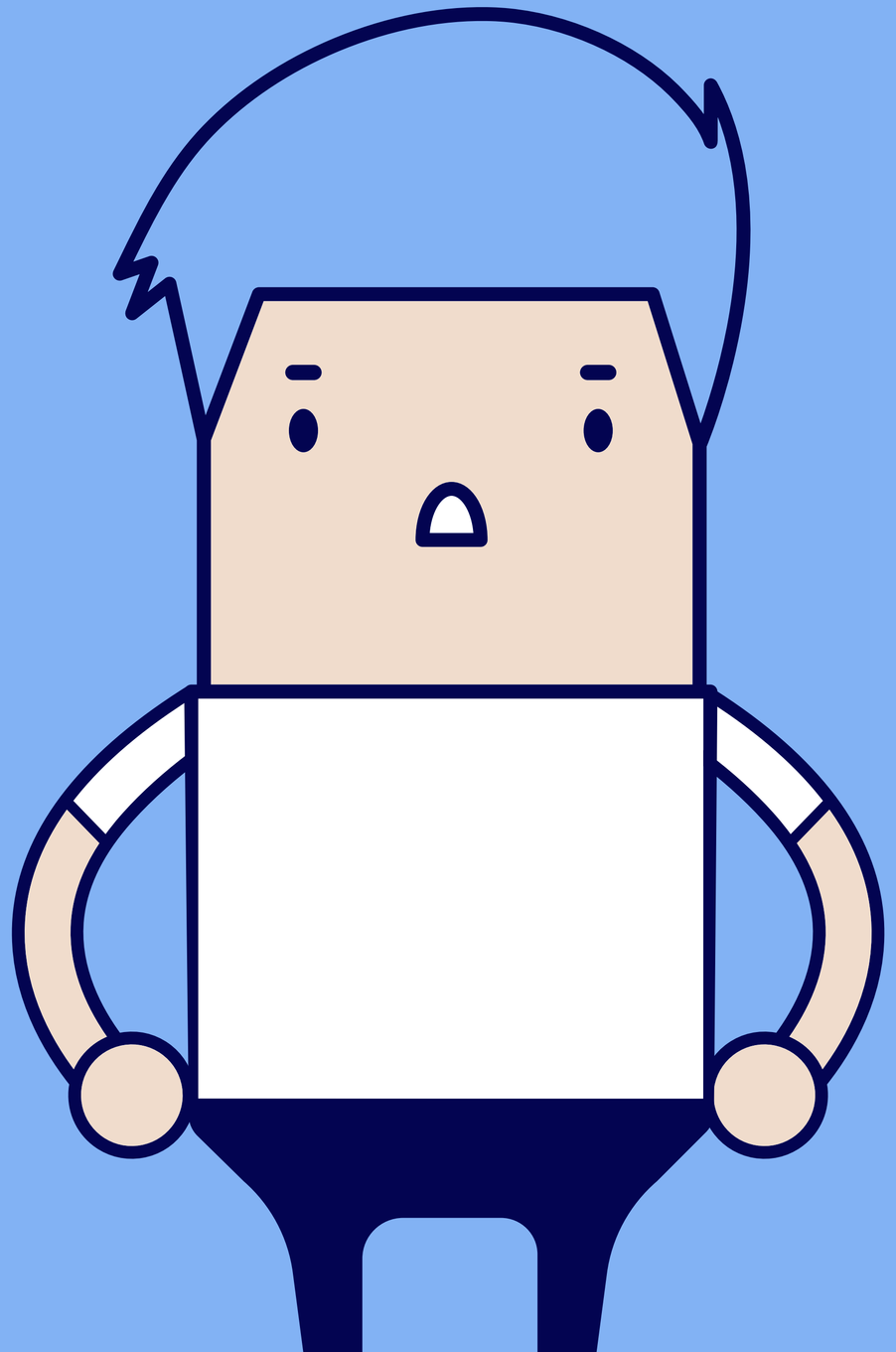
No descargues mensajes, archivos y enlaces sospechosos

No descargues archivos adjuntos o entres en enlaces en caso de que no se pueda confirmar que se trata de un e-mail o SMS legítimo. Es mejor acceder a la información que se ofrece a través de las apps o webs oficiales.

Consejo:

Sospechar de correos con mensajes no esperados, alarmistas o extraños. Desconfiar si la comunicación es anónima del tipo “Estimado/a cliente/a”, “Notificación a usuario/a” o “Querido/a amigo/a”.





Recomendaciones de seguridad

Utiliza conexiones seguras

Comprueba que la web muestre un candado o llave y que su URL comience por https. Evita conexiones wifi públicas gratuitas o abiertas y cierra siempre la sesión al finalizar la compra. Por lo general, para verificar que el certificado digital de la web es válido, basta con hacer clic sobre el icono con forma de llave o candado. Así se verifica quién ha emitido el certificado, para quién y el plazo de validez.

Usa claves y contraseñas seguras

Utiliza contraseñas alfanuméricas y caracteres especiales que no sean deducibles como cumpleaños, aniversarios... No compartas contraseñas y usa una diferente para cada servicio. Crea contraseñas para acceder al dispositivo y establece un bloque de tiempo. Si es posible, utiliza sistemas de autenticación biométrica.

Actualiza el antivirus y software

Comprueba que el sistema operativo y aplicaciones de seguridad del ordenador o dispositivo están actualizados. Las actualizaciones ayudan a proteger los dispositivos de múltiples amenazas y permiten un funcionamiento eficaz de los equipos, reduciendo las probabilidades de fallos.

Paga con sistemas seguros

¿La página web ofrece varias formas de pago, pero a la hora de pagar solo acepta tarjeta de crédito? Este es un motivo para desconfiar.

Consejos:

- **Evitar pagar con transferencias directas** de dinero (como Western Union, Worldremit, Worldplay o Moneycorp).
- **Pagar preferentemente con tarjeta de crédito**, sistemas de pago a contrareembolso u otros sistemas de pago seguros como PayPal que aseguren que recibimos el dinero o el producto.
- **Sospechar si se solicita continuar la gestión fuera de la plataforma de venta**.
- **Desconfiar si se pide dinero por adelantado**, o pagar más por el producto sin motivo.
- **Dudar si el vendedor está en el extranjero y exige pagar a un intermediario** para ver el producto.

Ayuntamiento
ALBACETE