

COMPRAR POR INTERNET

Seguridad en compras online;
prevención de estafas y fraudes.



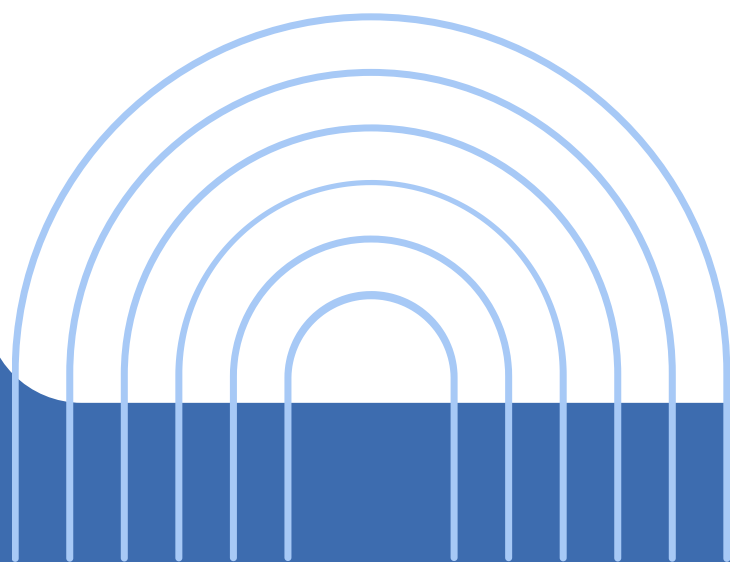
**Ayuntamiento
de Salamanca**



**Oficina Municipal de
de Información a
Personas Consumidoras**
Ayuntamiento de Salamanca



**Escuela
de Consumo**
Ayuntamiento de Salamanca



¿QUIENES SOMOS LA OMIC?

La Oficina Municipal de Información al Consumidor es un servicio gratuito dependiente del ayuntamiento de Salamanca para atender a las personas consumidoras y usuarias.

- Informar
- Reclamar
- Educar



01. ¿QUIÉN COMPRA ONLINE AQUÍ?





- ¿Quién compra online?
- ¿Qué es lo último que habéis comprado?
- ¿Habéis tenido alguna mala experiencia?
- ¿Alguna vez os han intentado estafar?

VENTAJAS

Comodidad

Precio

Variedad

DESVENTAJAS

Estafas

Datos

Problemas de devolución

02.

MOMENTOS DE UNA COMPRA ONLINE



ANTES



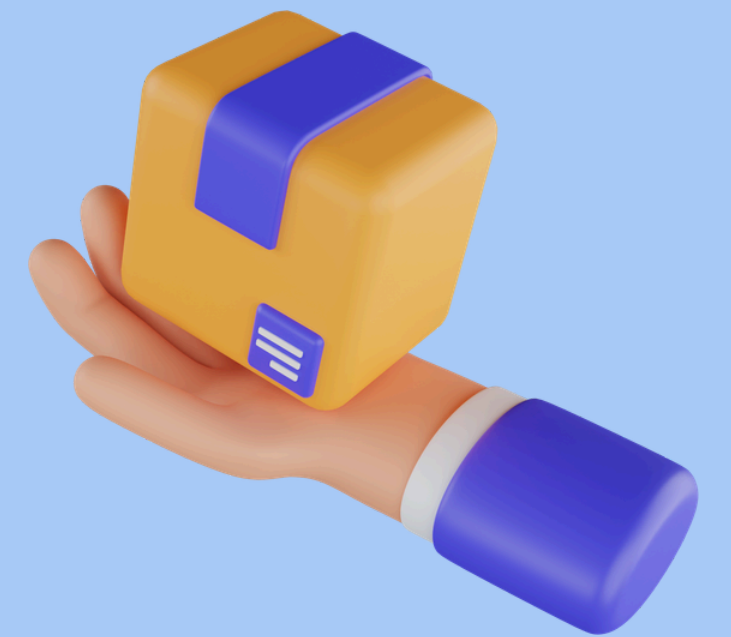
DURANTE



PAGO



DESPUÉS



Comprar online no es solo clicar. Hay cuatro momentos críticos.

03.

SEÑALES EN UNA COMPRA ONLINE



SEÑALES PARA CONFIAR

- https
- Candado
- Datos de contacto de la empresa (reales)
- Reseñas/opiniones
- Política clara de devoluciones
- Medios de pago seguros



SEÑALES DE ALARMA

- Precio demasiado bajo
- Urgencia artificial
- Faltas ortográficas
- URL sospechosa
- No hay datos de la empresa /vendedor
- Pago solo por transferencia ó Contrareembolso.



04.

TIPOS DE ESTAFA





NOMRE

EJEMPLO

Phishing, smishing, vishing

Email / SMS / llamada del banco

Marketplace fraud

Wallapop / Vinted

Web fantasma

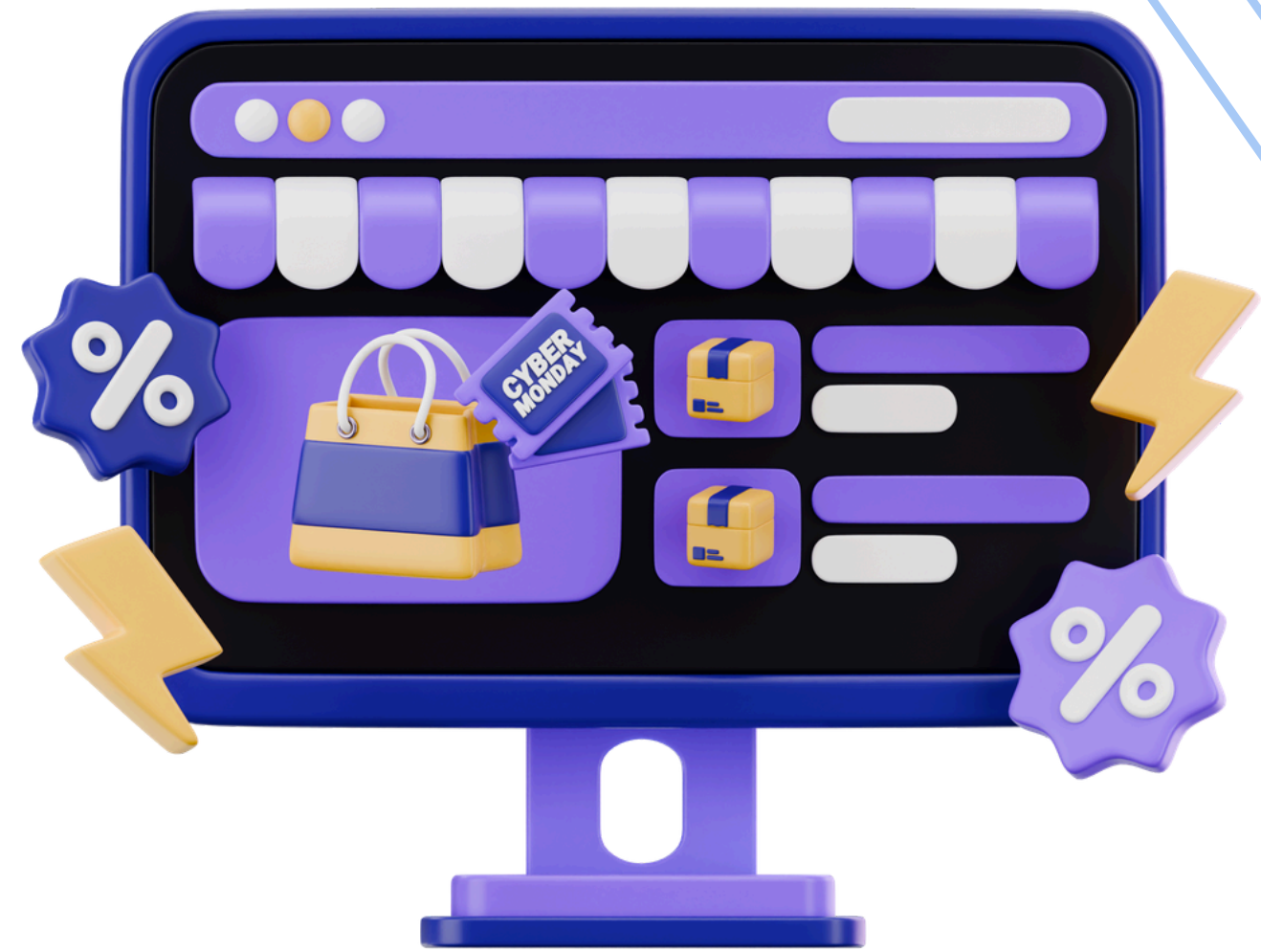
Stock infinito / ofertas imposibles

Job scam

Trabajo fácil / adelanto

05.

CASOS REALES



1. Crear grupos de 3-4 personas

2. Coger un caso por grupo

3. Analizar:

a. ¿Qué señales rojas hay?

b. ¿Qué haríais vosotros?

c. ¿Cómo podríamos evitarlo?



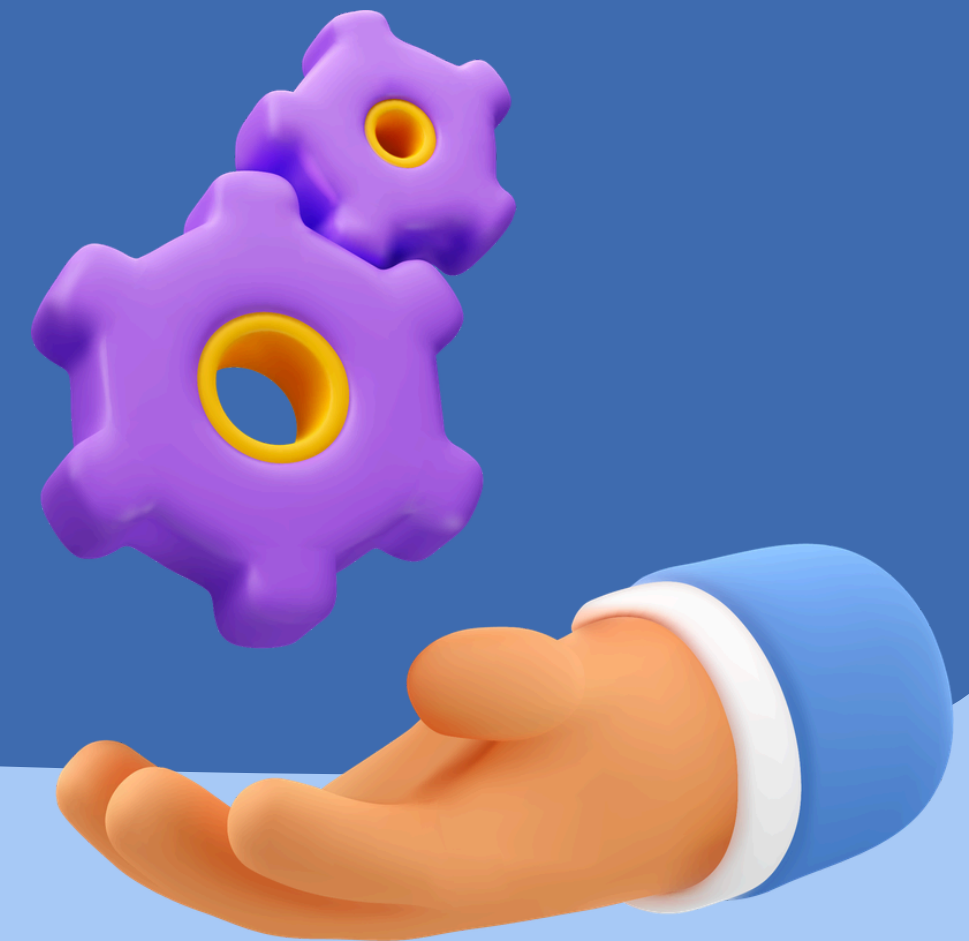
06.

CONSUMO RESPONSABLE APLICADO



MICRO-HERRAMIENTAS PRÁCTICAS

- Regla 24 horas antes de pagar.
- Comprar precios en tres webs diferentes.
- Mirar opiniones y/o reseñas.
- Desconfiar de lo urgente.
- Apagar notificaciones de ofertas.
- Nunca pagar sin seguridad.
- Revisar compras compulsivas.



07.

**¿Y SI YA NOS HA
PASADO?**



DERECHOS

- Devolución
- Desistimiento
- Garantía
- Reclamación



RECLAMACIONES

¿Dónde hacerlas?

- Banco (bloqueo de tarjetas)
- 017 (INCIBE)
- Policía / Guardia Civil (cuando hay delito)
- OMIC (cuando hay relación con consumo)



Glosario

Phishing: Se trata de correos o mensajes que parecen venir de bancos o instituciones oficiales, pero son falsos. Buscan engañarte para que des tus datos personales o bancarios y así acceder a tu información o a tu dinero.

Suplantación de identidad (Smishing y Vishing): Formas de estafa en las que se utilizan mensajes SMS (smishing) o llamadas telefónicas (vishing) falsas, haciéndose pasar por entidades de confianza, con el objetivo de obtener información personal o realizar cobros engañosos.

Ransomware: Este tipo de malware bloquea el acceso a los archivos o sistemas del usuario y solicita un rescate para liberarlos. Suele llegar a través de enlaces o archivos maliciosos en correos o páginas web.

Fraude en comercio electrónico: Creación de tiendas falsas, estafas en las que se solicita un pago sin la intención de entregar el producto y el robo de información financiera en plataformas poco seguras.



Contactos

Avd. Villamayor 55 - 37007
Salamanca
Teléfono: 923282306
E-mail: omic@aytosalamanca.es

¿Quieres saber más cosas sobre consumo?
¡Síguenos en nuestras redes sociales!

@omic_salamanca 660 68 35 94 OMIC ayto Salamanca

ESTAFAS Y FRAUDES TELÉFONICO Y ONLINE: ¿CÓMO PREVENIRLO?



**Escuela
de Consumo**
Ayuntamiento de Salamanca

OMIC
Oficina Municipal de
Información al Consumidor

**Ayuntamiento
de Salamanca**

ciberdelinquentes para engañar a los usuarios a través de llamadas de teléfono fraudulentas y obtener así información personal sobre ellos, guiarles para que descarguen e instalen programas maliciosos, así como intentar que realicen algún pago bajo algún pretexto.

OMIC
Oficina Municipal de
Información al Consumidor

**Ayuntamiento
de Salamanca**

¿Qué nos puede hacer desconfiar?

Urgencia o presión

- Que nos pidan una acción inmediata y con premura (una transferencia de dinero, compartir información sensible,...).

Errores evidentes

- Que en las comunicaciones haya, faltas de ortografía evidentes, direcciones web que no coinciden con el remitente oficial o que desconozcamos el contenido de la comunicación.

Ofertas demasiado buenas

- Como, por ejemplo, que nos ofrezcan productos o servicios excesivamente baratos o premios inesperados, entre otros.

Petición de datos sensibles por vías no ordinarias

- Cuando se recaban tus datos de carácter personal, el responsable del tratamiento debe facilitar una información básica, de forma resumida, en el mismo momento de cómo y para qué se utilizarán tus datos y quien tendrá acceso a ellos. En cualquier caso, nadie te pedirá datos sensibles. Si lo hacen, desconfía.

Falta de datos identificativos

- Desconfía de comercios electrónicos que:
- No tengan información de contacto ni política de devoluciones.
 - Que no se identifiquen (normalmente en un apartado de "Aviso Legal")
 - Aquellas cuyas imágenes son deficientes
 - Aquellas cuya pasarela de pagos no es de confianza

¿Qué hacer si caemos en una estafa?

Denunciar rápidamente

Contacta con el banco para bloquear tarjetas:

- Si has facilitado tus datos bancarios por error o sospechas que han sido utilizados de forma fraudulenta, solicita el bloqueo de las tarjetas afectadas y revisa los movimientos recientes para detectar cargos no autorizados. El banco podrá ayudarte a anular operaciones indebidas y a reforzar la seguridad de tus cuentas.

Informar a las autoridades (Policía, Guardia Civil):

- Ante cualquier indicio de estafa o fraude, es imprescindible presentar una denuncia formal. Acude a la Policía Nacional o a la Guardia Civil con toda la documentación que puedas aportar (capturas de pantalla, correos, números de teléfono, justificantes, etc.).

¿Dónde acudir?

- En caso de indicios claros de delito, la OMIC no tiene potestad, pero las Fuerzas y Cuerpos de Seguridad del Estado, sí. Acude a ellos a poner la denuncia y dejar constancia de el hecho delictivo.
- Es posible también, reportar el fraude en la página web del Instituto Nacional de Ciberseguridad (INCIBE): www.incibe.es
- El teléfono 017 está a disposición de la ciudadanía para este tipo de consultas

OMIC
Oficina Municipal de
Información al Consumidor

**Ayuntamiento
de Salamanca**

**SI TUVIERAS QUE DARLE
UN CONSEJO A UN
AMIGO, ¿CUÁL SERÍA?**





¡MUCHAS GRACIAS!

“Estafar es un delito, reclamar es un derecho.”



omic@aytosalamanca.es



@omic_salamanca



Oficina Municipal de
de Información a
Personas Consumidoras

Ayuntamiento de Salamanca



Escuela
de Consumo

Ayuntamiento de Salamanca

