#SiNoEsComercioNoEsSeguro
es una iniciativa de

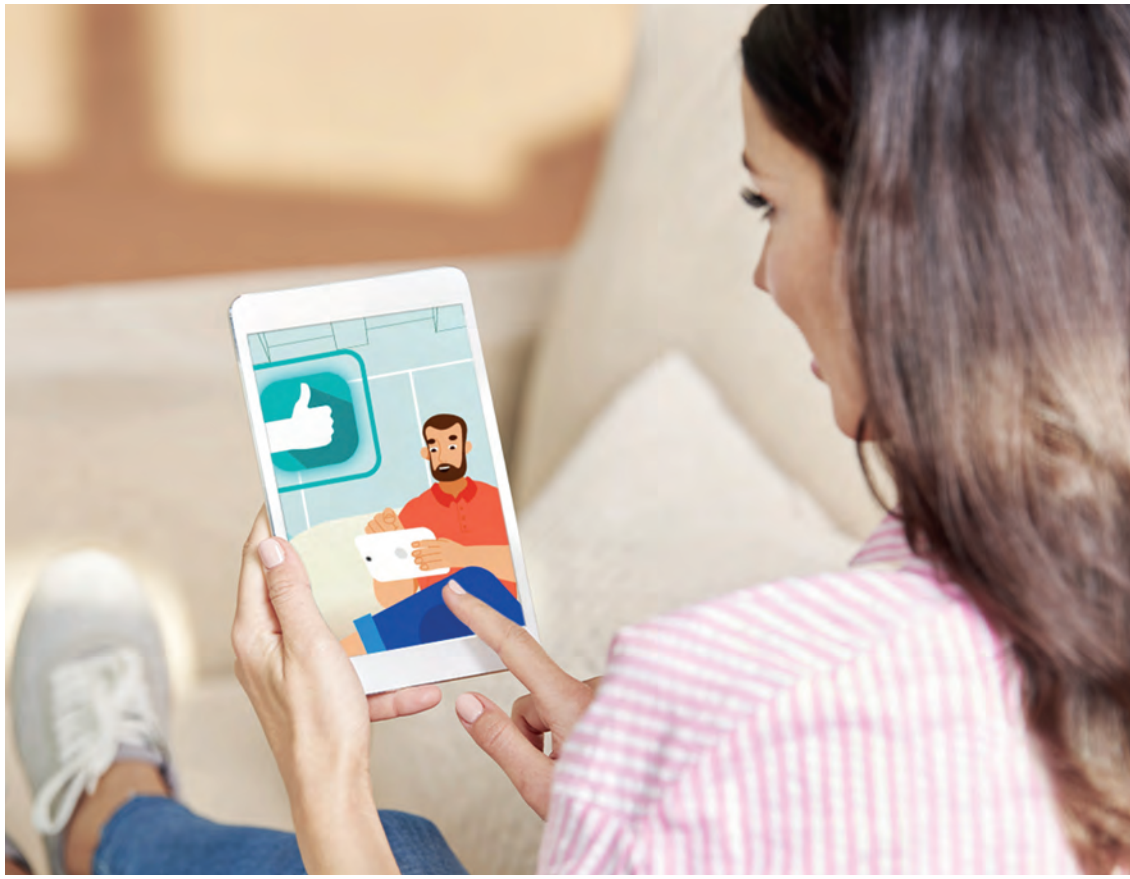
LEGÁLITAS FUNDACIÓN

SI NO ES SEGURO NO ES COMERCIO

POLICÍA NACIONAL

Si no es seguro no es comercio

Infórmate de tus derechos y, si eres víctima o testigo de un delito, acude a la Policía Nacional.



LEGÁLITAS FUNDACIÓN

SI NO ES SEGURO NO ES COMERCIO

POLICÍA NACIONAL

Si no es seguro no es comercio

Campaña de concienciación realizada por la Fundación Legálitas y la Policía Nacional.

"Si no es seguro, no es comercio" es una iniciativa de la Fundación Legálitas y la Policía Nacional para que todos podamos conocer los peligros que pueden surgir a la hora de realizar nuestras compras.

Algunos tips para comprar y navegar seguro

- Comprar en páginas que inspiren confianza, que incluyan el icono en forma de candado y que su URL empiece por HTTPS.
- Evitar comprar utilizando redes wifi públicas, o bien mediante el uso de ordenadores, tablets o teléfonos públicos o compartidos.
- Asegurar que la tienda online está plenamente identificada en la web, así como su ubicación y la existencia de una política de tratamiento de datos personales.
- Si es posible, utilizar una tarjeta de uso exclusivo para realizar pagos online.
- Comprobar cuál es el importe final de la operación y no enviar nunca dinero en efectivo para completar una compra.
- Verificar los términos de la transacción y las fechas de entrega, conservando los registros y los recibos de que se disponga.
- Utilizar contraseñas fuertes, que no resulten fácilmente deducibles (como las fechas de cumpleaños) y que integren letras, números y caracteres especiales.

Es importante saber que se puede desistir de una compra online en los 14 días posteriores, sin tener que dar explicaciones y sin que conlleve coste alguno para el comprador.

Alerta ante fraudes y estafas

El phishing es el método más extendido para obtener datos bancarios, números de tarjetas de crédito y pin o CVV asociados, así como cualquier otra información sensible de la víctima.

Los delincuentes suplantan la identidad de una entidad pública o privada a través del envío de un SMS (smishing), e-mail (spear phishing), página web (typosquatting) o llamada telefónica (vishing), para generar "confianza" en la víctima y que acceda a aportar sus datos personales y/o bancarios, con el pretexto de corte de suministro, bloqueo de cuenta o promociones especiales de venta, entre otros.

El uso fraudulento de tarjetas de crédito (carding) tiene varios modus operandi: el skimming (clonación de tarjetas), pharming (manipulación de sitio web), spyware y malware (programas para el robo de datos), entre otros.

Falsos pagos utilizando plataformas de envío de dinero instantáneo. Creyendo recibir dinero, en ocasiones se podría recibir una solicitud de "envío". Al aceptar esa solicitud, se estará enviando el dinero al delincuente en lugar de recibirlo.

Viviendas vacacionales falsas. En ocasiones se publicitan y no existen, pidiendo ingresar dinero por adelantado para realizar reservas.

Desconfía de chollos y gangas, de anuncios mal escritos o con faltas de ortografía y de quienes tengan mucha prisa por vender o alquilar en sus ofertas.