Diez consejos para que el Black Friday no salga caro

26/11/2025



Este viernes habrá numerosas ofertas en las redes sociales | Marta Maestre.

Ante el previsible aumento de compras de cara al *Black Friday*, expertos de la Policía Nacional han elaborado un decálogo para evitar posibles fraudes que se pueden producir durante estos días. Los especialistas en ciberdelincuencia recomiendan utilizar tarjetas virtuales o el monedero de crédito como opciones preferibles para una protección antifraude, además de no tomar decisiones rápidas de forma impulsiva ante mensajes del estilo "última oportunidad" o "descuento 48 horas".

No se debe olvidar que los ciberdelincuentes han variado su modus operandi y realizan campañas de *phishing y smishing* indicando a las víctimas que llamen a teléfonos que ellos mismos facilitan.

Los diez consejos para comprar con seguridad

Desconfiar de las ofertas "demasiado buenas para ser verdad"

Si hay un producto carísimo rebajado a precio de ganga, sospechar de un posible timo diseñado para robar los datos o el dinero. Compara precios en varios sitios: una

diferencia abismal respecto a la media suele ser señal de alarma.

Priorizar las webs oficiales de las marcas o de tiendas de confianza

Comprobar la URL en el navegador, debe empezar por "https://" y corresponder exactamente al dominio legítimo de la tienda.

Fijarse en las señales de alerta en la página

Una web fraudulenta suele delatarse por los detalles: diseño descuidado, imágenes de mala calidad, textos mal traducidos o con falta de ortografía evidentes.

Utilizar métodos de pago seguros.

Las tarjetas de prepago o virtuales son muy recomendables para compras *online*, ya que se recargan con el importe exacto limitan la cantidad en caso de estafa. También es preferible pagar con tarjeta de crédito antes que con transferencia bancaria directo.

No hacer clic en enlaces sospechosos

Mucho ojo con los mensajes no solicitados que te llegan por email, SMS o redes sociales con enlaces a ofertas o promociones exclusivas. Si te interesa una oferta en concreto accede de forma manual al sitio oficial tecleando la dirección en el ordenador o mediante la *app* oficial.

No compartir datos confidenciales por canales no seguros

Desconfíar de cualquier mensaje o llamada que te pida datos sensibles: contraseñas, números de tarjeta, PINs o códigos de verificación.

Cuidado con llamadas o mensajes de suplantación

Los ciberdelincuentes no solo crean webs falsas, también pueden llamar o enviar *WhatsApps* haciéndose pasar por una entidad o por alguien de confianza.

Evitar las redes Wi-Fi públicas al hacer compras

Si es necesario conectarse en un sitio público, considerar una VPN que cifre la conexión. En cualquier caso, no introducir contraseñas ni números de tarjeta cuando estés en una Wi-Fi pública no cifrada.

Mantener los dispositivos y cuentas protegidos

Actualizar el sistema operativo de tu móvil y ordenador, y utilizar un *software* antivirus fiable.

Actuar rápido si algo sale mal

Si se sufre una estafa o se percibe movimientos extraños en la cuenta, no esperar. Contactar con el banco, bloquear las tarjetas o las transferencias y denunciar el hecho a la policía.