

Tus clientes, el próximo objetivo

Ciberdelincuencia y suplantación de marca en el retail de moda

Pablo Molina Borchert

Socio Responsable del Área Penal, Litigación y Arbitraje

1. Previo

En mayo de 2026 han saltado a los medios diversas noticias sobre filtración de datos de toda clase de entidades públicas o privadas. En lo que ahora nos ocupa lo que persiguen estos ataques son los datos de nuestros clientes y los detalles de sus transacciones. Lo que persiguen estos piratas es la venta a terceros de datos precisos sobre nuestros clientes para que, a través de datos muy específicos, crear estafas muy actualizadas, sofisticadas y en tiempo real, es decir, simultáneas a las operaciones que realizan con nosotros. Imaginad un cliente esperando un pedido en su casa que recibe una notificación con sus datos específicos y número de pedido que le deriva a una página web falsa donde este cliente volcará de nuevo sus datos bancarios, de tarjeta etc.

2. El contexto en cifras

- **INCIBE (2025):** gestionó 122.223 incidentes, un 26 % más que el año anterior. De ellos, 45.445 fueron fraude online y 25.133 phishing.
- **Línea 017:** recibió 142.767 consultas, un 45 % más. El phishing fue el primer motivo, con un 28 %.

3. Los peligros más reales hoy.

1. **La puerta de atrás; el proveedor.** Hablamos de la plataforma de e-commerce, el CRM, la agencia de email marketing, el servicio de atención al cliente externalizado o un proveedor antiguo que conserva una copia de la base de datos. Hoy el retailer rara vez es el eslabón débil; lo es quien trabaja para él.
2. **La estafa a tus clientes en tu nombre, con datos reales.** Los formatos más habituales son:
 - un SMS de «incidencia con tu pedido n°...» con enlace de pago;
 - un correo de «reembolso pendiente»;
 - una llamada de un falso servicio de atención al cliente que pide verificar la tarjeta o un código SMS.El cliente no distingue entre la marca y el estafador, así que el daño reputacional lo paga la marca.
3. **Tiendas clonadas y anuncios falsos.** Son webs copia de la marca con «outlet 70 %» o «cierre de tienda», promocionadas con anuncios en redes sociales. No necesitan robarte datos: usan tu logo y tus fotos. Es especialmente típico en moda.
4. **Perfiles falsos de atención al cliente.** Cuando un cliente se queja en redes, aparece en minutos una cuenta clonada de la marca que le escribe por privado para «resolverlo» y le pide datos o un pago.

4. Qué hacer, en clave práctica.

Prevención:

- Hacer un inventario de quién tiene datos de clientes y borrarlos cuando acaba la relación con un proveedor.
- Incluir en los contratos con proveedores cláusulas de seguridad, auditoría y aviso inmediato de incidentes (art. 28 RGPD).
- Pedir solo los datos necesarios y conservarlos solo el tiempo necesario.
- **Comunicación preventiva con el cliente:** dejar claro, por escrito y de forma repetida, que «nunca te pediremos pagos ni códigos por SMS ni teléfono». Es la vacuna más barata.
- **Vigilancia de marca:** monitorizar dominios parecidos y perfiles falsos, y pedir su retirada a las plataformas y registradores.

Si ocurre:

- Notificar a la AEPD en un máximo de 72 horas y, si hay alto riesgo, avisar a los afectados (arts. 33 y 34 RGPD).
- Presentar denuncia y conservar las evidencias.
- Avisar a los clientes antes de que lo hagan los estafadores.

Ángulo jurídico; el retailer responde como responsable del tratamiento, aunque la brecha la cause un proveedor; sanciones de la AEPD y posibles reclamaciones de clientes.

5. Cierre

Dos preguntas para llevarse a la empresa mañana:

1. ¿Sabemos qué proveedores tienen datos de nuestros clientes? ¿podemos confiar en ellos?
2. ¿Saben nuestros clientes qué no les pediremos nunca?

Fuentes

- [INCIBE gestiona un 26 % más de incidentes en 2025 – Red Seguridad](#)
- [Balance de Ciberseguridad 2025 – INCIBE \(PDF\)](#)
- [Principales ciberataques en España en 2026 – Channel Partner](#)
- [Fraude online 2025-2026 en tiendas digitales – Ciphersafety](#)