

SEGURIDAD

Métodos de pago y cómo proteger



Japhet Pérez Atristain

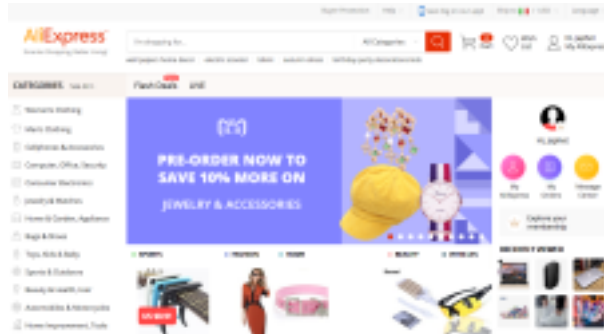
AGENDA

- **Dónde empieza**
- **Tipos de Métodos de Pago:**
 - **Agregadores.**
 - **Pasarelas.**
 - **COD.**
 - **Efectivo.**
- **Ataques Comunes:**
 - **Contracargos.**
 - **Carding.**
- **¿Qué hacer?**
 - **Prevención.**
 - **En medio de un ataque.**
 - **Aprendiendo del desastre.**
- **¿PREGUNTAS?**

DÓNDE EMPIEZA



DÓNDE EMPIEZA



DONDE EMPIEZA

Primeros indicios

¡Vamos por **MAL** camino!

    https://shoppingcart.aliexpress.com/order/confirm_order.htm?aeOrd   

¡Vamos por **BUEN** camino!

    https://shoppingcart.aliexpress.com/order/confirm_order.htm?aeOrd   

DONDE EMPIEZA

El Checkout

The screenshot shows the AliExpress checkout interface. It includes a navigation bar with the AliExpress logo and a search bar. Below the navigation, there are sections for shipping information, including a map showing the shipping route and estimated delivery date. There are also sections for payment methods and a 'Finalizar compra' button.

The screenshot shows the Oson checkout interface, divided into three main sections:

- 1. Información del Cliente:** Fields for Email, Contraseña, Nombre, Apellido, Teléfono celular, Teléfono alternativo, Complejidad, País, Código postal, Dirección, No. exterior, and Estado. A 'Enviar en la misma dirección' checkbox is also present.
- 2. Método de Pago:** Options for 'Tarjetas de Crédito y Débito' (with logos for Visa, Mastercard, etc.) and 'Método de depósito'. It includes a 'Número del titular de la tarjeta' field and a 'Vencimiento' section for card expiration.
- 3. Resumen de la Orden:** A summary of the order including shipping address, product details (e.g., 'Máscara'), and a total amount. A 'Finalizar compra' button is prominently displayed.

 At the bottom, there are logos for 'PAGO SEGURO' and 'GARANTÍA DE CALIDAD'.

TIPOS DE MÉTODOS DE PAGO



TIPOS DE MÉTODOS DE PAGO

Agregadores

- Es una compañía que ofrece sus servicios e infraestructura para procesar pagos.
- Se pueden usar Tarjetas de Crédito, Débito, Cheques, Transferencias o pagos en efectivo.
- Proporcionan seguridad, notificaciones, soporte con devoluciones o reembolsos, previenen contra cargos y/o fraudes.



TIPOS DE MÉTODOS DE PAGO

Pasarelas

- Se implementan mediante servicios (comúnmente) ofrecidos por entidades bancarias.
- Se pueden usar Tarjetas de Crédito o Débito.
- Existen versiones two-party y third-party para proporcionar confianza en el consumidor.
- Algunos de estos servicios ya integran herramientas anti fraude.



This image cannot currently be displayed.

TIPOS DE MÉTODOS DE PAGO

COD (Cash On Delivery) y Efectivo

COD:

- Se paga a la entrega de la mercancía.
- Se le da la confianza al consumidor de que pagará por su producto cuando lo tenga en sus manos.
- Se podrá aceptar Efectivo o Tarjeta de Crédito (vía terminal electrónica).

Efectivo:

- Se generará un código para su pago en alguna tienda de autoservicio, farmacia, gasolinera, etc.
- La conversión depende de que el consumidor realice el pago.

ATAQUES COMUNES



ATAQUES COMUNES

Contracargos

- Estos son el resultado de una operación fraudulenta.
- El *agregador* o el banco integrado en la *pasarela* solicitarán la devolución del dinero.
- Comúnmente son de productos entregados e irrecobrables.
- La pérdida en la operación será mayor a la venta.



ATAQUES COMUNES

Carding

- Es la generación de número de tarjetas de crédito y/o débito (falsas).
- Es también el uso de tarjeta de crédito o débito clonadas o robadas.
- Existen MILES de generadores de Tarjetas en la nube para su uso inmediato.
- Para el comercio, su rastreo comúnmente será muy difícil.



¿QUÉ HACER?



¿QUÉ HACER?

Prevención

- Aprender de los demás.
- Siempre ejecutar estos procesos detrás de una capa de seguridad SSL (HTTPS).
- Contar con listas blancas y negras de acceso.
- Contar con un sistema anti fraude que legitime el proceso.
- Integrar reglas de validación de tarjetas de crédito y/o débito.
- Integrar reglas de validación de direcciones (AVS).
- Ofrecer más de una forma de pago.
- **NUNCA GUARDAR INFORMACIÓN DEL PLÁSTICO**



¿QUÉ HACER?

En medio del ataque


- Verificar origen del ataque.
- Solicitar apoyo del equipo de infraestructura.
- Bloquear el acceso a la cuenta que está efectuando el ataque.
- Si el caso lo amerita, desactivar el medio de pago afectado.



¿QUÉ HACER?

Aprendiendo del desastre

- Implementar mejores prácticas en el checkout.
- Implementar alertas en las implementaciones de medios de pago.
- Siempre contar con un procedimiento estándar que ayude en caso de estar nuevamente bajo un ataque.
- Recuperar la mayor información de logs, bases de datos y demás para decidir la estrategia a seguir en el futuro.
- Siempre hacer rondas para intentar desestabilizar nuestro checkout o el sitio en conjunto para detectar bugs, backdoors, etc.

 This image cannot currently be displayed.

PREGUNTAS



***“TODO LO QUE NO ESTÁ PROHIBIDO,
ESTÁ PERMITIDO”***

Constitutional principle of English Law

¡Gracias!



Japhet Pérez Atristain

Email: japhet@sides-it.com / LinkedIn: japhet.perez