WORLDLINE

Payments to grow your world

Le migliori pratiche 3-D Secure

7 consigli per i commercianti dell'e-commerce

Nell'ambito della seconda direttiva europea sui servizi di pagamento PSD2, le organizzazioni delle carte di credito richiedono a tutti i commercianti online dell'UE e della Svizzera di conformarsi allo standard di sicurezza 3-D Secure (3DS) per l'elaborazione dei pagamenti nel commercio elettronico. Seguite i nostri 7 consigli & trucchi per prevenire le frodi, aumentare i tassi di conversione e ridurre i costi.

#1 Richiedere le esenzioni tramite 3DS Server per saltare i passi di sicurezza aggiuntivi

Ecco come funziona	A volte, è possibile saltare il controllo di sicurezza supplementare quando i clienti effettuano un acquisto. Questa azione è chiamata esenzione. È possibile richiedere queste esenzioni tramite il server 3-D Secure, che consente di determinare quali transazioni sono sufficientemente sicure da non richiedere ulteriori passi di sicurezza.
Esempio tratto dalla vita reale	Immaginate che un cliente ordini online il pranzo. Invece di richiedere l'inserimento di un codice speciale o una password, il sistema può riconoscere che si tratta di un acquisto a basso rischio e consente di effettuarlo senza ulteriori problemi.
Vantaggi	**Aumento delle vendite:** Con meno attriti, più persone saranno disposte a effettuare gli acquisti. **Risparmio sui costi:** Un minor numero di controlli di sicurezza può ridurre i costi delle transazioni. **Pagamenti più veloci:** I clienti effettuano i loro acquisti più velocemente, si offre un'esperienza di acquisto senza problemi e si migliorano le prestazioni aziendali.
Disponibilità	Mastercard e Visa

#2 Utilizzare le richieste "Solo informazioni" per Mastercard Insights

Ecco come funziona	Inviate una richiesta 3DS a Mastercard con tutti i soliti dettagli di pagamento, ma invece di richiedere l'autenticazione completa, richiedete solo informazioni. Mastercard fornisce quindi una valutazione del rischio che aiuta la banca a decidere se la transazione è sicura, senza costi aggiuntivi.
Esempio tratto dalla vita reale	Immaginate che un cliente stia acquistando un libro nel vostro negozio online. Invece di eseguire un controllo di sicurezza completo, si chiede a Mastercard un punteggio di rischio basato sui dettagli della transazione. Mastercard invia un punteggio che la banca utilizza per approvare o rifiutare il pagamento.
Vantaggi	**Decisioni informate:** La banca riceve informazioni utili per prendere decisioni migliori sull'approvazione delle transazioni. **Flessibilità:** Utilizzate questo approccio per le transazioni che non richiedono controlli di sicurezza rigorosi. **Costi inferiori:** Evitate le spese aggiuntive saltando l'intero controllo di sicurezza.
Disponibilità	Mastercard

#3 Utilizzare 3DS per le transazioni avviate dall'esercente (MIT)

Ecco come funziona	Quando un cliente effettua un primo acquisto, salvate i dettagli di autenticazione come l'importo, la marca temporale e l'ID della transazione. Per i pagamenti futuri, inviate questi dati al vostro server 3DS. Se il pagamento viene approvato, si ottiene un codice speciale da aggiungere alla richiesta di pagamento.
Esempio tratto dalla vita reale	Immaginate che un cliente si abboni a un servizio mensile del vostro sito. Per il primo pagamento, si salvano i dati di sicurezza. Per i pagamenti mensili successivi, si utilizzano questi dati salvati per assicurarsi che i pagamenti siano sicuri e per trasferire la responsabilità alla banca.
Vantaggi	**Protezione extra:** Ottenete una protezione da responsabilità per i pagamenti futuri. **Risparmio sui costi:** Evitate spese aggiuntive utilizzando i dati di sicurezza memorizzati. **Pagamenti facilitati:** Garantite l'elaborazione senza problemi dei pagamenti futuri senza dover effettuare nuovamente l'autenticazione del cliente.
Disponibilità	Mastercard

#4 Migliorare la qualità dei dati

Ecco come funziona	EMV 3DS consente di inviare molte informazioni dettagliate sul cliente e sulla transazione. Quanto più questi dati sono accurati e completi, tanto meglio la banca può valutare il rischio della transazione.
Esempio tratto dalla vita reale	Immaginate che un cliente stia acquistando un computer portatile nel vostro negozio online. Inviando informazioni dettagliate come il nome, l'indirizzo, l'e-mail e lo storico degli acquisti del cliente, la banca può valutare meglio il rischio e probabilmente approvare la transazione senza richiedere ulteriori controlli di sicurezza.
Vantaggi	**Checkout fluido:** I clienti subiscono meno interruzioni, il che li rende più soddisfatti. **Protezione da responsabilità:** Dati migliori aiutano a trasferire la responsabilità alla banca, proteggendovi dalle frodi. **Tassi di approvazione più elevati:** Le banche possono prendere decisioni migliori, con conseguente aumento del numero di transazioni approvate.
Disponibilità	Mastercard e Visa

#5 Utilizzare il reindirizzamento fuori banda

Ecco come funziona	Quando è necessario un controllo di sicurezza 3DS, la vostra app può reindirizzare automaticamente il cliente all'app della sua banca per l'autenticazione. Questo semplifica il processo per il cliente.
Esempio tratto dalla vita reale	Immaginate che un cliente stia acquistando delle scarpe nel vostro negozio online. Quando i clienti raggiungono la fase di pagamento e devono verificare la loro identità, la vostra app apre automaticamente l'app della loro banca, dove possono approvare la transazione. Dopo l'approvazione, i clienti vengono riportati alla vostra app per completare l'acquisto.
Vantaggi	**Tasso di successo più elevato:** Un maggior numero di clienti porta a termine i propri acquisti senza errori. **Migliore esperienza del cliente:** Il processo è più fluido e meno confuso, soprattutto per chi ha poca familiarità con i pagamenti online. **Minor numero di insuccessi:** Riduce i problemi, come l'autenticazione non riuscita o i timeout, rendendo più affidabile il processo di checkout.
Disponibilità	EMV 3DS 2.2

#6 Utilizzare Method URL per la raccolta dei dati

Ecco come funziona	Prima della fase di autenticazione, il sistema ACS (il sistema di sicurezza della banca) fornisce tramite il 3DS Server un URL che raccoglie in modo trasparente ulteriori dati dal browser del consumatore. Questa fase aiuta a raccogliere le informazioni necessarie per valutare il rischio della transazione.
Esempio tratto dalla vita reale	Immaginate che un cliente stia acquistando un nuovo gadget online. Prima di dover autenticare un acquisto, tramite un passo nascosto si raccolgono i dati dal browser. Questi dati aiutano la banca a decidere che l'acquisto è sicuro e, pertanto, il cliente non deve fare ulteriori passi.
Vantaggi	**Esperienza utente senza soluzione di continuità:** I consumatori sperimentano un processo di checkout fluido senza essere soggetti a ulteriori richieste di sicurezza. **Valutazione del rischio potenziata:** Gli emittenti di carte possono eseguire valutazioni del rischio più accurate utilizzando i dati raccolti, con conseguente riduzione di complicazioni inutili. **Aumento dei tassi di conversione:** Riducendo il numero di richieste di autenticazione, si ottiene un numero maggiore di transazioni completate con successo, con conseguente incremento delle vendite.
Disponibilità	Emittenti Mastercard e Visa per il flusso nel browser 3DS

#7a Utilizzare il autenticazione forte del cliente (Strong Customer Authentication SCA) dell'esercente – opzione Mastercard

Ecco come funziona	Con la delega SCA, se la vostra azienda dispone di una soluzione SCA conforme, potete bypassare il processo 3DS. Ciò significa che l'autenticazione è gestita dall'esercente e non dall'emittente. Tuttavia, poiché l'emittente della carta non effettua la SCA, non vi è alcun trasferimento di responsabilità. La delega SCA deve essere richiesta per ogni autorizzazione attraverso il Servizio Token di Rete ed è applicabile ai clienti conosciuti, non al checkout degli ospiti.
Esempio tratto dalla vita reale	Immaginate che un cliente abituale acquisti un abbonamento mensile sul vostro sito web. Poiché disponete di un sistema SCA conforme, potete gestire voi stessi l'autenticazione, offrendo al cliente un processo fluido. Si richiede la delega SCA per questa transazione e l'emittente la autorizza, saltando il passo 3DS. Il cliente completa l'acquisto rapidamente senza ulteriori controlli di sicurezza.
Vantaggi	**Checkout fluido:** I clienti hanno il beneficio di un'esperienza di checkout rapida e senza ulteriori passi di autenticazione. **Relazioni di fiducia:** Per i clienti conosciuti, il processo è più rapido ed efficiente. **Miglioramento della soddisfazione dei clienti:** Un processo di esperienza senza soluzione di continuità per i clienti conosciuti, che offre un'esperienza di acquisto più rapida ed efficiente.
Disponibilità	Mastercard

#7b Utilizzare il autenticazione forte del cliente (Strong Customer Authentication SCA) dell'esercente – opzione Visa

Come funziona il Digital Authentication Framework (DAF)	Il DAF autentica una credenziale di pagamento specifica per un esercente, anziché autenticare l'autorizzazione stessa. Se l'esercente dispone di una soluzione SCA conforme, può richiedere di utilizzare il DAF per ogni transazione. Questa richiesta può essere effettuata attraverso il Servizio Tokens di Rete o il server 3DS, in genere dopo l'autenticazione iniziale da parte dell'emittente della carta. Il DAF può essere applicato per i clienti noti, ma non per gli ospiti.
Esempio tratto dalla vita reale	Un cliente abituale effettua un acquisto nel vostro negozio online utilizzando le credenziali di pagamento salvate. La vostra app gestisce l'autenticazione senza problemi all'interno dell'ambiente esercenti utilizzando il DAF, saltando ulteriori passi 3DS e garantendo una transazione rapida e sicura.
Vantaggi	**Esperienza di checkout senza attriti:** Se la vostra app supporta la SCA, potete saltare il 3DS per le transazioni idonee, garantendo ai clienti un processo di checkout più fluido. **Potenziale trasferimento di responsabilità:** A differenza della delega SCA, il DAF offre la possibilità di un trasferimento di responsabilità a determinate condizioni, aumentando la protezione finanziaria per gli esercenti. **Applicabilità alle MIT:** A partire dal 2024, il DAF sarà disponibile anche per le Merchant Initiated Transactions (MIT), semplificando ulteriormente le transazioni sicure.
Disponibilità	Visa

Parlate di queste opzioni con il vostro partner PSP. In caso di ulteriori domande, non esitate a contattare il nostro Servizio Clienti tramite e-mail:
cs.ecom@worldline.com

Il punto di contatto locale è disponibile all'indirizzo: **worldline.com/merchant-services/contacts**

110.1159.04 INT_IT/09.2024