WORLDLINE

Payments to grow your world

3-D Secure Best Practices

7 Tipps für E-Commerce-Händler

Im Rahmen der zweiten europäischen Zahlungsdienste-Richtlinie PSD2 verlangen die Kartenorganisationen von allen Online-Händlern in der EU und der Schweiz die Einhaltung des Sicherheitsstandards 3-D Secure (3DS) für die Zahlungsabwicklung im E-Commerce. Befolgen Sie unsere 7 Tipps & Tricks, um Betrug zu verhindern, Ihre Conversion Rate zu steigern und Kosten zu senken.

#1 Beantragen Sie über den 3DS-Server Ausnahmen, um zusätzliche Sicherheitsschritte zu überspringen

So geht's	Manchmal können Sie die zusätzliche Sicherheitsprüfung überspringen, wenn Kunden einen Kauf tätigen. Dieses Vorgehen wird als Ausnahme bezeichnet. Sie beantragen diese Ausnahmen über Ihren 3-D Secure-Server, mit dessen Hilfe Sie feststellen können, welche Transaktionen sicher genug sind, um zusätzliche Sicherheitsschritte überspringen zu können.
Praxis-Beispiel	Stellen Sie sich vor, ein Kunde bestellt online eine Pizza. Anstatt den Kunden zur Eingabe eines speziellen Codes oder Passworts aufzufordern, kann Ihr System diesen Kauf als risikoarm erkennen und ihn problemlos genehmigen.
Vorteile	**Höhere Umsätze:** Gibt es weniger Reibungsverluste, dann sind mehr Kunden bereit, ihre Einkäufe auch abzuschliessen. **Kosteneinsparungen:** Weniger Sicherheitsprüfungen können die Transaktionskosten senken. **Schnellerer Bestellabschluss:** Kunden schliessen ihre Einkäufe schneller ab, haben ein reibungsloseres Kundenerlebnis und Sie steigern Ihren Umsatz.
Verfügbarkeit	Mastercard und Visa

#2 Nutzen Sie „Information Only"-Anfragen für Mastercard Insights

So geht's	Senden Sie eine 3DS-Anfrage mit allen üblichen Zahlungsdaten an Mastercard, aber fordern Sie statt einer kompletten Authentifizierung nur Informationen („information only") an. Mastercard gibt dann eine Risikobewertung ab, anhand derer die Bank entscheiden kann, ob die Transaktion ohne zusätzliche Kosten sicher ist.
Praxis-Beispiel	Stellen Sie sich vor, ein Kunde kauft ein Buch in Ihrem Online-Shop. Anstatt eine vollständige Sicherheitsprüfung durchzuführen, fragen Sie Mastercard nach einer Risikobewertung auf Grundlage der Transaktionsdetails. Mastercard sendet eine Bewertung zurück, anhand derer die Bank die Zahlung genehmigt oder ablehnt.
Vorteile	**Sachgerechte Entscheidungen:** Die Bank erhält hilfreiche Informationen, um Entscheidungen über die Genehmigung von Transaktionen besser treffen zu können. **Flexibilität:** Nutzen Sie diese Vorgehensweise für Transaktionen, die keine strengen Sicherheitsprüfungen erfordern. **Geringere Kosten:** Vermeiden Sie zusätzliche Gebühren, indem Sie die vollständige Sicherheitsprüfung überspringen.
Verfügbarkeit	Mastercard

#3 Nutzen Sie 3DS für Händler-initiierte Transaktionen (MIT)

So geht's	Speichern Sie beim erstmaligen Kauf eines Kunden die Authentifizierungsdetails, wie Betrag, Zeitstempel und Transaktions-ID. Bei zukünftigen Zahlungen senden Sie diese Angaben immer an Ihren 3DS-Server. Wird die Zahlung genehmigt, so erhalten Sie einen speziellen Code, den Sie in die Zahlungsanforderung einfügen.
Praxis-Beispiel	Stellen Sie sich vor, ein Kunde abonniert eine monatliche Dienstleistung auf Ihrer Website. Bei der ersten Zahlung speichern Sie die Sicherheitsdaten. Für die folgenden monatlichen Zahlungen verwenden Sie diese gespeicherten Daten, um die Sicherheit der Zahlungen zu gewährleisten und die Haftung auf die Bank zu verlagern (Liability Shift).
Vorteile	**Zusätzlicher Schutz:** Sie erhalten einen Haftungsschutz für zukünftige Zahlungen. **Kosteneinsparungen:** Sie vermeiden zusätzliche Gebühren, indem Sie die gespeicherten Sicherheitsdaten verwenden. **Reibungslose Zahlungen:** Sie stellen die reibungslose Abwicklung künftiger Zahlungen sicher, ohne den Kunden erneut authentifizieren zu müssen.
Verfügbarkeit	Mastercard

#4 Datenqualität erhöhen

So geht's	Mit EMV 3DS können Sie viele detaillierte Informationen über den Kunden und die Transaktion übermitteln. Je genauer und vollständiger diese Daten sind, desto besser kann die Bank das Risiko der Transaktion einschätzen.
Praxis-Beispiel	Stellen Sie sich vor, ein Kunde kauft in Ihrem Online-Shop einen Laptop. Indem Sie der Bank detaillierte Informationen, wie Name, Adresse, E-Mail und Kaufhistorie des Kunden übermitteln, kann diese das Risiko besser einschätzen und die Transaktion voraussichtlich ohne zusätzliche Sicherheitsprüfungen genehmigen.
Vorteile	**Reibungsloser Bestellabschluss:** Kunden erleben weniger Störungen und sind dadurch zufriedener. **Haftungsschutz:** Bessere Daten erleichtern die Verlagerung der Haftung auf die Bank und schützen Sie vor Betrug. **Höhere Genehmigungsquoten:** Die Banken können bessere Entscheidungen treffen, was zu mehr genehmigten Transaktionen führt.
Verfügbarkeit	Mastercard und Visa

#5 Out-of-Band-Weiterleitung verwenden

So geht's	Ist eine 3DS-Sicherheitsprüfung erforderlich, so kann Ihre App den Kunden automatisch zur Authentifizierung an seine Bank-App weiterleiten. Für den Kunden wird der Ablauf dadurch einfacher.
Praxis-Beispiel	Stellen Sie sich vor, ein Kunde kauft in Ihrem Online-Shop Schuhe. Wenn sie den Bezahlschritt erreichen und ihre Identität verifizieren müssen, öffnet Ihre App automatisch die Bank-App des Kunden, damit dieser die Transaktion genehmigen kann. Nach der Genehmigung gelangt der Kunde zurück zu Ihrer App, um den Kauf abzuschliessen.
Vorteile	**Höhere Erfolgsquote:** Mehr Kunden schliessen ihre Einkäufe erfolgreich und ohne Fehler ab. **Bessere Kundenerfahrung:** Das Verfahren ist reibungsloser und weniger verwirrend, insbesondere für diejenigen, die mit Online-Zahlungen nicht so vertraut sind. **Weniger Abbrüche:** Fehlgeschlagene Authentifizierungen oder Zeitüberschreitungen werden verringert und der Checkout-Prozess wird zuverlässiger.
Verfügbarkeit	EMV 3DS 2.2

#6 Method URL für die Datenerfassung verwenden

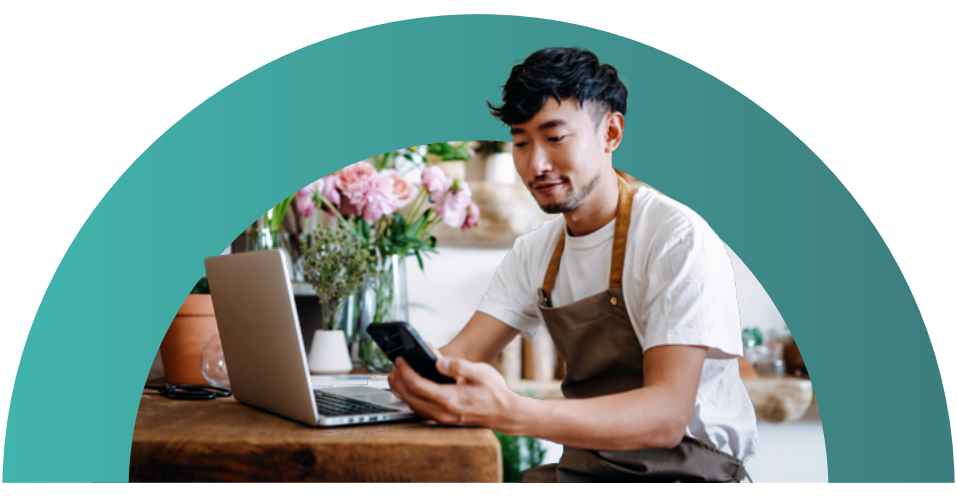
So geht's	Vor dem Schritt der Authentifizierung stellt das ACS-System (das Sicherheitssystem der Bank) über den 3DS-Server eine URL bereit, die auf transparente Weise zusätzliche Daten vom Browser des Verbrauchers erfasst. Dieser Schritt trägt dazu bei, die notwendigen Informationen zur Bewertung des Transaktionsrisikos zu sammeln.
Praxis-Beispiel	Stellen Sie sich vor, ein Kunde kauft online ein neues Gadget. Bevor ein Kauf authentisiert werden muss, werden in einem verdeckten Schritt Daten vom Browser des Kunden gesammelt. Anhand dieser Daten kann die Bank entscheiden, ob der Kauf sicher ist und der Kunde keine zusätzlichen Schritte durchlaufen muss.
Vorteile	**Nahtloses Benutzererlebnis:** Der Checkout-Prozess gestaltet sich für die Konsumenten reibungslos, ohne dass sie zusätzliche Sicherheitsabfragen erhalten. **Verbesserte Risikobewertung:** Die Kartenherausgeber können anhand der gesammelten Daten genauere Risikobewertungen vornehmen. **Höhere Conversion Rates:** Durch eine geringere Zahl von Authentifizierungsanforderungen werden mehr Transaktionen erfolgreich abgeschlossen und der Umsatz wird gesteigert.
Verfügbarkeit	Mastercard- und Visa-Kartenherausgeber für Browser Flow 3DS

#7a Händlereigene starke Kundenauthentifizierung (SCA) nutzen – Mastercard-Option

So geht's	Mit der starken Kundenauthentifizierung (SCA) können Sie das 3DS-Verfahren umgehen, wenn Ihr Unternehmen über eine SCA-konforme Lösung verfügt. Das bedeutet, die Authentifizierung wird von Ihnen als Händler, und nicht vom Kartenherausgeber vorgenommen. Da aber der Kartenherausgeber nicht die SCA durchführt, gibt es keine Haftungsverlagerung. Die starke Kundenauthentifizierung muss für jede Autorisierung über den Network Tokens Service beantragt werden und ist nur für bekannte Kunden möglich, nicht für Checkouts als Gast.
Praxis-Beispiel	Stellen Sie sich vor, ein Stammkunde kauft ein Monatsabonnement auf Ihrer Website. Da Sie über ein SCA-konformes System verfügen, können Sie die Authentifizierung selbst vornehmen und der Prozess verläuft für den Kunden nahtlos. Sie beantragen für diese Transaktion die starke Kundenauthentifizierung und der Kartenherausgeber genehmigt diese, so dass der 3DS-Schritt übersprungen wird. Der Kunde schliesst den Kauf schnell und ohne zusätzliche Sicherheitsprüfungen ab.
Vorteile	**Reibungsloser Bestellabschluss:** Die Kunden profitieren von einer reibungslosen und schnellen Kaufabwicklung ohne zusätzliche Authentifizierungsschritte. **Vertrauensbeziehungen:** Für bekannte Kunden ist das Verfahren schneller und effizienter. **Mehr Kundenzufriedenheit:** Ein nahtloser Prozess für bekannte Kunden, der ein schnelleres und effizienteres Einkaufserlebnis bietet.
Verfügbarkeit	Mastercard

#7b Händlereigene starke Kundenauthentifizierung (SCA) nutzen – Visa-Option

So funktioniert das Digital Authentication Framework (DAF)	Über das Digital Authentication Framework (DAF) wird ein Zahlungszertifikat speziell für einen Händler und nicht die Autorisierung selbst authentifiziert. Wenn der Händler über eine SCA-konforme Lösung verfügt, kann er die Verwendung von DAF pro Transaktion anfordern. Diese Anforderung kann über den Network Tokens Service oder den 3DS-Server erfolgen, in der Regel nach der ursprünglichen Authentifizierung durch den Kartenherausgeber. DAF kann für bekannte Kunden zum Einsatz kommen, nicht für Checkouts als Gast.
Praxis-Beispiel	Ein Stammkunde kauft in Ihrem Online-Shop mit seinen gespeicherten Zahlungsdaten ein. Ihre App wickelt die Authentifizierung unter Einsatz des DAF nahtlos innerhalb der Händlerumgebung ab, überspringt zusätzliche 3DS-Schritte und gewährleistet eine schnelle und sichere Transaktion.
Vorteile	**Reibungsloser Bestellvorgang:** Wenn Ihre App eine SCA durchführen kann, können Sie 3DS für zulässige Transaktionen überspringen und so für Ihre Kunden einen reibungsloseren Checkout-Prozess ermöglichen. **Potenzielle Haftungsverlagerung:** Anders als bei der SCA bietet das DAF die Möglichkeit der Haftungsverlagerung unter bestimmten Voraussetzungen und kann so den finanziellen Schutz für den Händler erhöhen. **Anwendbarkeit auf MIT:** Ab 2024 wird DAF auch für Händler-initiierte Transaktionen (Merchant Initiated Transactions, MIT) verfügbar sein. Damit werden sichere Transaktionen weiter optimiert.
Verfügbarkeit	Visa



Bitte besprechen Sie diese Möglichkeiten mit Ihrem PSP-Partner. Weitere Fragen beantwortet Ihnen unser Kundenservice gerne unter der folgenden E-Mail-Adresse: cs.ecom@worldline.com

Ihren Ansprechpartner vor Ort finden Sie unter: **worldline.com/merchant-services/contacts**

110.1159.01 INT_DE/09.2024