digicert®

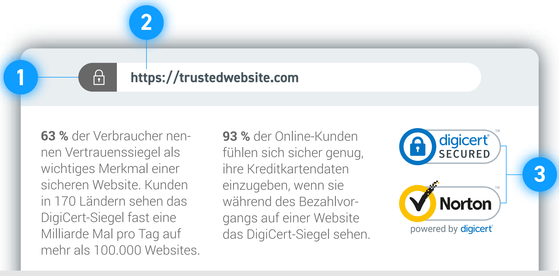
ONLINE-SIEGEL SCHAFFEN VERTRAUEN

Um erfolgreich Ihre Marke zu etablieren, eine Website einzurichten und Strategien für den Ausbau Ihrer Online-Präsenz auszuarbeiten, müssen Sie sich das Kundenvertrauen sichern. Dafür benötigen Sie eine effektive SSL-Lösung. Doch nicht alle SSL-Produkte bieten den gleichen Schutz. Unternehmen wie Ihres, die viel in ihre Online-Präsenz investieren, sollten dafür sorgen, dass sie sich vom ersten Websitebesuch an für Kunden als vertrauenswürdige Marke ausweisen.

WIE SCHAFFEN SIE ONLINE-VERTRAUEN?

Die drei wichtigsten Gründe für Online-Vertrauen:

1 Schlosssymbol
2 https://
3 Vertrauenssiegel



63 % der Verbraucher nennen Vertrauenssiegel als wichtiges Merkmal einer sicheren Website. Kunden in 170 Ländern sehen das DigiCert-Siegel fast eine Milliarde Mal pro Tag auf mehr als 100.000 Websites.

93 % der Online-Kunden fühlen sich sicher genug, ihre Kreditkartendaten einzugeben, wenn sie während des Bezahlvorgangs auf einer Website das DigiCert-Siegel sehen.

MIT DEM FALSCHEN ZERTIFIKAT SCHRECKEN SIE POTENZIELLE KUNDEN AB

Wenn Verbraucher kein identitätsbasiertes Vertrauenssiegel auf Ihrer Website sehen, ist es eher unwahrscheinlich, dass sie weiter browsen oder einen Kauf abschließen. Wie sorgen Sie dafür, dass dieses Problem gar nicht erst entsteht? Vermeiden Sie einfache DV-Zertifikate (Domain Validation), da diese ausgestellt werden, ohne die Organisation hinter der Domain zu überprüfen, und daher oft für die Erstellung betrügerischer Websites verwendet werden. Bei der Ausstellung von OV- und EV-Zertifikaten hingegen (Organization Validation bzw. Extended Validation) werden strengere Identitätschecks durchgeführt. Außerdem wird die Website des Unternehmens mit einem entsprechenden Vertrauenssiegel versehen, das für mehr Kundenvertrauen sorgt.

Extended Validation (EV)

WICHTIGE FEATURES:
- Verbraucher sehen am Vertrauenssiegel, dass sie mit dem Höchstmaß an Sicherheit geschützt sind.
- Alle Informationen zum Unternehmen werden ausführlich geprüft und im Zertifikat angezeigt.

KUNDENMEINUNG:

„Ich weiß, dass meine wertvollen persönlichen Daten auf dieser Website geschützt sind."

ÜBERPRÜFT:

Inhaber/Administrator der Domain

Zusätzliche Informationen über das Un-ternehmen, das die Website verwaltet (registrierter/offizieller Name, Standort usw.)

Weitere umfassende Details zum Unter-nehmen (Rechtsstatus, Postanschrift, Rechtspersönlichkeit, Position des Ver-tragsunterzeichners usw.), allesamt gegen Drittquellen geprüft

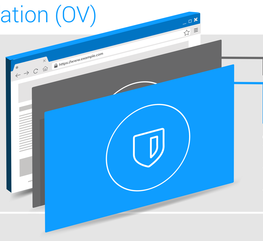
GENUTZT FÜR:
- Websites in Branchen wie E-Commerce, dem Bank- oder dem Gesundheitswesen, auf denen sich Kunden anmelden müssen, Zahlvorgänge bearbeitet oder persönliche/andere sensible Daten gespeichert werden
- Websites, die sich bereits mit einem visuellen Hinweis in der Adresszeile das Kundenvertrauen sichern wollen

Organization Validation (OV)

WICHTIGE FEATURES:
- Bietet strikte Authentifizierung und mehrere visuelle Möglichkeiten, sich als sichere Website auszuweisen.
- Alle Informationen zum Unternehmen werden geprüft und im Zertifikat angezeigt.

KUNDENMEINUNG:

„Ich weiß, dass ich eine sichere Website besuche, die einem legitimen Unternehmen gehört."



GENUTZT FÜR:

Inhaber/Administrator der Domain

Zusätzliche Informationen über das Unternehmen, das die Website verwaltet (registrierter/offizieller Name, Standort usw.)

GENUTZT FÜR:
- Öffentlich zugängliche Websites, die weniger sensible Transaktionen bearbeiten
- Websites, auf denen Anwender nach Informationen suchen und Daten einsehen können
- Von öffentlichen Dienststellen und Bildungseinrichtungen bereitgestellte Websites

Domain Validation (DV)

WICHTIGE FEATURES:
- Schnelle Ausstellung
- Keine Unternehmensangaben im Zertifikat
- Wird oft für Phishing-Websites missbraucht

KUNDENMEINUNG:

„Die Website, die ich besuche, scheint sicher zu sein."

ÜBERPRÜFT:

Inhaber/Administrator der Domain

GENUTZT FÜR:
- Intern genutzte/nicht öffentlich zugänglich Websites
- Webbasierte Anwendungen (kein Betrugs-risiko)
- Websites, auf denen die Datensicherheit wichtiger ist als ein Beweis der Vertrau-enswürdigkeit

MIT STARKER IDENTITÄTSPRÜFUNG GEGEN ONLINE-BETRUG

PSD2-konforme Zertifikate: Gemäß der Zweiten EU-Zahlungsdienstrichtlinie (PSD2) müssen Zahlungsdienstleister in Europa ihre elektronische Kommunikation mit qualifizierten Zertifikaten für die Website-Authentifizierung (QWAC) sichern.

QWAC UND QSEALC

Als qualifizierter TSP (Qualified Trust Service Provider, QTSP) und führender Anbieter von QWAC-Zertifikaten für effektive Websitesicherheit und qualifizierten eSeal-Zertifikaten (QSealC) zum Schutz sensibler Daten und Kommunikationen in Anwendungen kann DigiCert Ihnen helfen, das Kundenvertrauen zu sichern und zu fördern.

Beide Zertifikate basieren auf strengen, hochentwickelten Methoden zur Identitätsprüfung – darunter die Überprüfung durch persönliche Validierung und die Überprüfung des Anbieters und des Zahlungsdienstleisters – und schaffen somit branchenweites Vertrauen in die Integrität Ihres Unternehmens.

MEHR DAZU

Unser Vertriebsteam hilft Ihnen gern dabei, Ihre Website zu schützen und sich das Vertrauen Ihrer Kunden zu sichern. Wenden Sie sich einfach per E-Mail an **contactus@digicert.com**