

PROUVEZ VOTRE IDENTITÉ POUR RENFORCER VOTRE CAPITAL CONFIANCE



Votre business sur Internet, c'est d'abord une stratégie, une marque et un site web qui doivent inspirer confiance. C'est d'ailleurs pour cela que vous investissez dans des certificats SSL : rassurer vos clients et les mettre en sécurité. Seulement voilà, tous les certificats SSL ne se valent pas. Au point que certains peuvent même produire un effet repoussoir. Si votre entreprise ne vit que par sa présence en ligne, il est indispensable de bien faire valider votre identité – et de l'afficher haut et fort aux yeux des internautes.

COMMENT GAGNER LA CONFIANCE DES INTERNAUTES ?

Les 3 principaux ressorts de la confiance en ligne

1

2

3

icône du cadenas https:// sceau de confiance

1

https://sitedeconance.fr

63 % des consommateurs accordent une grande importance aux sceaux de confiance. Chaque jour, les sceaux DigiCert apparaissent près d'un milliard de fois sur plus de 100 000 sites à travers 170 pays.

93 % des clients se sentent davantage disposés à saisir leur numéro de carte de paiement sur un site affichant un sceau de confiance DigiCert.

3

MAUVAIS CERTIFICAT, MAUVAIS MESSAGE

Si votre site n'affiche pas clairement les preuves de son authenticité, n'attendez pas de vos clients qu'ils achètent quoi que ce soit. Mais attention à ne pas sombrer dans la facilité en optant pour une simple validation de domaine (DV, Domain Validation). Ces certificats s'obtiennent en effet sans aucune preuve d'identité, ce qui les rend particulièrement attractifs pour les sites frauduleux. À l'inverse, les certificats de validation d'organisation (OV, Organization Validation) et de validation étendue (EV, Extended Validation) sont délivrés à l'issue de contrôles beaucoup plus stricts et s'accompagnent généralement d'un sceau de confiance – un indicateur visuel rassurant pour les cyberconsommateurs.

Extended Validation (EV)

CARACTÉRISTIQUES

- Niveau d'assurance maximal, indicateurs visuels d'authenticité les plus irréfutables
- Le certificat contient une grande quantité d'informations vérifiées et validées

L'INTERNAUTE SE DIT...

« Je sens que je peux saisir mes données personnelles les plus sensibles sur ce site sécurisé. »

VALIDE...

Le contrôle/la propriété d'un domaine

Des informations supplémentaires sur l'entreprise qui contrôle le site (nom d'inscription au registre du commerce, dénomination juridique, adresse du siège social, etc.)

Des informations d'identification détaillées (statut juridique, existence physique et opérationnelle, autorité du signataire du contrat, etc.) obtenues grâce au recoupement de données tierces

UTILISATION LA PLUS COURANTE

- Sites voués à recevoir des paiements ou traiter des données privées ou sensibles (banque, e-commerce, sites à caractère médical)
- Sites cherchant à rassurer les internautes par un indicateur visuel fort dans leur barre d'adresse

Organization Validation (OV)

CARACTÉRISTIQUES

- Haute assurance par différentes preuves visuelles de légitimité
- Le certificat contient des informations vérifiées et validées

L'INTERNAUTE SE DIT...

« Je suis sur un site sécurisé appartenant à une entreprise légitime. »

VALIDE...

Le contrôle/la propriété d'un domaine

Des informations supplémentaires sur l'entreprise qui contrôle le site (nom d'inscription au registre du commerce, dénomination juridique, adresse du siège social, etc.)

UTILISATION LA PLUS COURANTE

- Sites publics effectuant des transactions peu sensibles
- Sites d'informations avec option de recherche
- Sites éducatifs ou de services publics

Domain Validation (DV)

CARACTÉRISTIQUES

- Délais d'émission les plus courts
- Aucune information sur l'entreprise dans le certificat
- Faciles à obtenir pour les sites de phishing

L'INTERNAUTE SE DIT...

« Je suis sur un site qui a l'air d'être sûr. »

VALIDE...

Le contrôle/la propriété d'un domaine

UTILISATION LA PLUS COURANTE

- Sites internes/non destinés au public
- Applications web (non exposées au risque de fraude)
- Sites pour lesquels la sécurité des données passe avant la crédibilité

SOLUTIONS D'IDENTIFICATION – PLUS DE SÉCURITÉ, MOINS DE FRAUDES

Conformité DSP2 : la nouvelle directive sur les services de paiements (DSP2) impose aux prestataires de services de paiement européens de sécuriser les communications à l'aide de certificats numériques qualifiés (QWAC).

CERTIFICATS QUALIFIÉS D'AUTHENTIFICATION DE SITE INTERNET (QWAC) ET CERTIFICATS QUALIFIÉS DE CACHET ÉLECTRONIQUE (QSEALC)

Les certificats numériques qualifiés conformes à la DSP2 sont reconnus comme fiables par 70 % des banques européennes. DigiCert est non seulement un prestataire de services de confiance qualifié (PSCo), mais aussi le leader des fournisseurs de certificats qualifiés d'authentification de site Internet (QWAC) et de certificats qualifiés de cachet électronique (QsealC), utilisés respectivement pour sécuriser des pages web et sceller numériquement les données et les communications sensibles de vos applications.

Les deux types de certificats impliquent des processus d'identification des plus stricts (authentification en personne, identification d'entité, identifiants PSP, etc.) pour maintenir l'intégrité et la confiance de tout un marché.

PLUS D'INFOS

Pour renforcer le capital confiance de votre site, contactez notre service commercial dès aujourd'hui à contactus@digicert.com