



DOCUMENT TECHNIQUE

SÉCURITÉ ET CONFIANCE : LES DEUX PILIERS DU COMMERCE EN LIGNE

SOMMAIRE

- 3 INTRODUCTION
- 3 TECHNOLOGIE DE CRYPTAGE ET CERTIFICATS SSL
- 6 VERISIGN® SEAL-IN-SEARCH™ : LA CONFIANCE EN AMONT
- 6 CERTIFICAT SSL EXTENDED VALIDATION (EV) : UN GAGE DE CONFIANCE
- 7 VERISIGN : LEADER DE LA SÉCURITÉ ET DE LA CONFIANCE SUR INTERNET
- 8 CONCLUSION
- 8 EN SAVOIR PLUS
- 8 L'ENTREPRISE VERISIGN



SÉCURITÉ ET CONFIANCE : LES DEUX PILIERS DU COMMERCE EN LIGNE

INTRODUCTION

Toute entreprise amenée à échanger des informations sensibles sur Internet doit faire de la confiance clients une priorité absolue. À l'époque du shopping en ligne, le consommateur craint, entre autres, de voir son identité usurpée et se montre, à juste titre, méfiant à l'idée de communiquer des renseignements personnels sur des sites perçus comme non fiables. La communication d'informations de type carte de crédit, numéro de sécurité sociale, mot de passe, dossier médical et autres données confidentielles suscite généralement de grandes réticences. Outre la crainte de voir ces données interceptées en cours de transfert, l'exploitation de sites falsifiés par des fraudeurs aux buts non avouables alimente la majorité des peurs.

Principale conséquence : l'abandon de panier – véritable plaie du commerce en ligne. D'après une étude sur le sujet, 21 % des utilisateurs n'auraient pas concrétisé un achat en ligne par crainte d'une protection insuffisante de leur numéro de carte de crédit.¹ Les autres se contentent d'opérations modestes et plafonnent le montant de leurs transactions par peur d'une arnaque.

Or ces inquiétudes sont parfaitement fondées. D'après le 11^{ème} rapport annuel sur la fraude en ligne, le montant des pertes des cybermarchands nord-américains imputables à la fraude s'élevait à 3,3 milliards US\$ en 2009.² Quant au nombre total d'attaques de phishing signalées au Groupe de travail anti-phishing (APWG), il se chiffrait à 46 190 pour le seul mois de décembre 2009.³

Les cybermarchands ont tout à gagner à apaiser les inquiétudes des consommateurs. Comme nous venons de l'évoquer, les craintes de cyberfraude constituent un facteur de dissuasion majeur pour la vente en ligne. Une enquête TNS réalisée en mars 2010 révélait à ce propos que 73 % des internautes américains se sentaient particulièrement menacés par les usurpations d'identité.⁴ Les craintes de consommateurs limitant non seulement le nombre mais également le volume des transactions, on saisit toute l'importance de gagner la confiance du client pour développer son activité sur Internet. Mais les consommateurs ont également beaucoup à y gagner. Car côté pratique et

financier, la vente en ligne reste plus qu'avantageuse. Pour faire son shopping, le cyberconsommateur surfe à travers plusieurs sites dont les niveaux de fiabilité perçue varient de manière très sensible. Plus la confiance règnera sur la planète e-commerce, plus le consommateur aura de chances d'effectuer le meilleur choix possible, sans risque pour la confidentialité de ses données.

Heureusement, plusieurs technologies permettent aux cybermarchands de protéger les données sensibles de leurs clients, d'authentifier leurs sites Web et d'instaurer une relation de confiance avec le consommateur. Grâce à ces technologies, l'internaute est capable de distinguer un site fiable d'un clone créé de toutes pièces par les professionnels de l'arnaque en ligne.

Ce document propose donc un tour d'horizon de la sécurité du Web et du rôle majeur de VeriSign dans la protection des données sensibles et la mise en confiance des clients. Nous débuterons par le cryptage SSL (*Secure Sockets Layer*), technologie permettant de lutter contre le risque connu – mais ô combien d'actualité – d'interception des données en cours de transmission. Nous nous pencherons ensuite sur la nécessité de mettre en place un cryptage des données, notamment par SSL, et d'autres mesures permettant l'authentification d'un site Web et l'instauration d'une relation de confiance avec le client.

TECHNOLOGIE DE CRYPTAGE ET CERTIFICATS SSL

Toute information transmise sur un site Web non sécurisé est potentiellement en danger. Les clients l'ont bien compris. L'utilisation de certificats SSL pour le cryptage et la protection des données clients sensibles est devenue indispensable à la survie de tout site marchand.

Le cryptage désigne le processus qui consiste à transformer des données pour les rendre inintelligibles à toute personne autre que leur destinataire. Il s'agit là du fondement même de l'intégrité et de la confidentialité des données indispensables à la pratique du commerce en ligne. Aucun client ou partenaire ne s'aventurera à transmettre des données sensibles ou à

1. "Security Concerns Hinder Online Shopping, Survey Finds," juin 2009. www.eweek.com/c/a/Midmarket/Security-Concerns-Hinder-Online-Shopping-Survey-Finds-288359/

2. www.marketingcharts.com/direct/e-commerce-fraud-losses-drop-12308/cybersource-online-revenue-loss-fraud-mar-2010.jpg

3. Groupe de travail anti-phishing, décembre 2009, www.apwg.org

4. VeriSign Trust Index Report, mars 2010. https://www.trustthecheck.com/assets/VeriSign_Internet_Trust_Index_March_2010.pdf



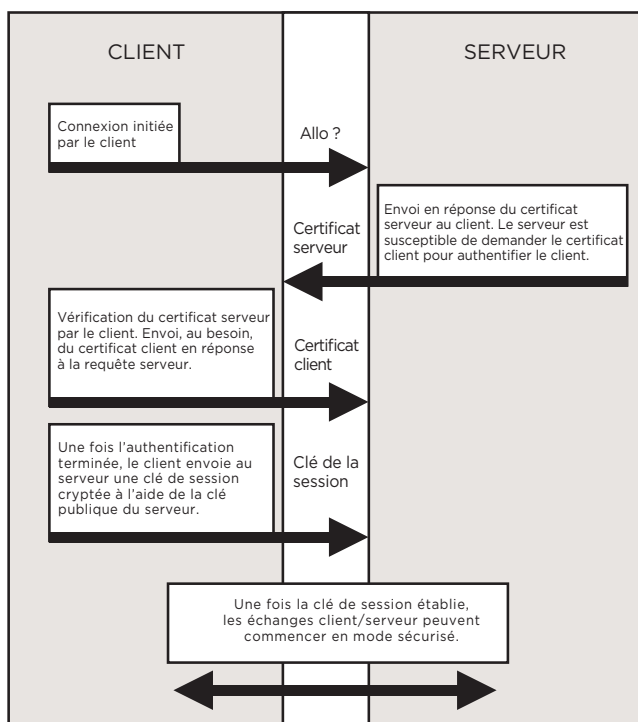


effectuer des transactions en ligne sur un site où la sécurité semble aléatoire. Aussi toute entreprise prenant très au sérieux sa politique de développement sur le Net aura à cœur de mettre en place une infrastructure fiable adossée à une technologie de cryptage.

Norme internationale de la sécurité en ligne, la technologie SSL (Secure Sockets Layer) sert à crypter et protéger les informations transmises sur la Toile en HTTP – le protocole de référence. SSL protège les données en cours de transfert contre tout risque d'interception et de modification susceptible de survenir en l'absence de cryptage. La plupart des systèmes d'exploitation, navigateurs Web, applications Web et serveurs physiques sont compatibles SSL.

Un certificat SSL est un fichier électronique identifiant de manière ciblée des individus et des sites Web. Il permet par ailleurs de crypter les transferts de données. Un certificat SSL fait office de « passeport numérique » ou de support d'authentification. Généralement, le « signataire » d'un certificat SSL est une autorité de certification (AC) indépendante. Avec plus d'un million de serveurs Web sécurisés aux quatre coins du globe, VeriSign est l'autorité de certification leader dans le monde.⁵

Le schéma suivant illustre le processus permettant d'assurer la protection des communications entre un serveur Web et un client. Tous les échanges de certificats SSL s'effectuent en quelques secondes, sans aucune intervention côté utilisateur.



5. Y compris filiales et revendeurs VeriSign.

Cryptage standard ou cryptage SGC

Le niveau de cryptage des données dépend du nombre de bits utilisés par l'algorithme de cryptage. À l'heure actuelle, le standard minimum s'élève à 128 bits. Ce cryptage est réputé inviolable aux niveaux de puissance actuelle des ordinateurs les plus récents. L'utilisation conjointe d'anciennes versions de systèmes d'exploitation et de navigateurs interdit la prise en charge d'une puissance de cryptage supérieure à 40 ou 56 bits. Or avec un niveau de cryptage aussi faible, les utilisateurs sont à la merci d'attaques et autres actes de piratage informatique.

Intégrée à certains certificats VeriSign SSL, la technologie SGC (*Server-Gated Cryptography*) est la parade idéale dans 99,9 % des cas. Les sites Web intégrant la fonction SGC montent à 128 bits le niveau de cryptage de toute communication avec des systèmes généralement plafonnés à 40 ou 56 bits.* Les entreprises munies de certificats SSL SGC peuvent ainsi garantir à leurs clients un niveau de cryptage suffisant. Les certificats VeriSign Secure Site Pro et Secure Site Pro avec EV proposent le cryptage SGC 128 bits. Les certificats VeriSign SSL permettent tous un cryptage atteignant 256 bits dès lors que le serveur et le poste client prennent en charge un tel niveau de cryptage.

* Les utilisateurs des versions de navigateurs et de systèmes d'exploitation suivantes bénéficieront temporairement du cryptage SSL 128 bits lorsqu'ils consultent un site Web intégrant un certificat SSL SGC : versions export d'Internet Explorer comprises entre 3.02 et 5.5 ; versions export de Netscape comprises entre 4.02 et 4.72 ; systèmes Windows 2000 vendus avant mars 2001 sans installation du pack High Encryption de Microsoft ou du Service Pack 2, et utilisés avec Internet Explorer. Les versions d'Internet Explorer antérieures aux versions 3.02, et les versions Netscape antérieures à 4.02 ne sont pas compatibles 128 bits, et ce, quel que soit le certificat SSL.



Niveaux d'authentification et de confiance

Les certificats SSL visent essentiellement à rassurer le cyberconsommateur sur l'authenticité des sites Web consultés. En effet, ce dispositif d'authentification par un tiers de confiance garantit à l'internaute que le site sur lequel il se trouve est vraiment le site en question. On distingue généralement trois catégories d'authentification SSL :

- Authentification de l'entreprise
- Validation renforcée ou Extended Validation (EV)

Les différences de niveaux de sécurité – et de capital confiance généré – sont d'une importance cruciale. Aussi, pour un même niveau d'authentification, le processus peut varier d'une AC à l'autre – d'où l'intérêt de faire appel à une autorité de certification réputée et digne de confiance. Aucune autre AC ne jouit de la confiance et de la notoriété de VeriSign.

Authentification du domaine

Les certificats procédant à l'authentification du domaine représentent le plus bas niveau d'authentification disponible. Pour ce type de validation, les AC vérifient que l'entité candidate à un certificat SSL d'authentification de domaine possède bien le domaine en question ou, du moins, les droits d'utilisation de ce nom de domaine. L'AC peut également être amenée à vérifier que l'adresse e-mail de la personne requérant le certificat figure dans l'annuaire WHOIS ou répond aux règles d'alias prédéfinies. Les sites Web sécurisés à l'aide de certificats VeriSign® sont soumis à un niveau d'authentification supérieur à une simple authentification du domaine.

Authentification de l'entreprise

L'authentification de l'entreprise est le processus de validation conjointement utilisé par VeriSign et les autres AC pour les certificats SSL classiques (c'est-à-dire sans EV). L'AC commence par vérifier l'existence de l'entité dans les registres de l'administration. Cela consiste généralement à interroger les bases de données du public et du privé. L'AC peut, au besoin, demander la production des statuts de l'entreprise, de son inscription au registre du commerce et des différentes marques et enseignes utilisées par une même société. Avant d'émettre un certificat SSL avec authentification de l'entreprise, l'AC vérifie l'identité de l'entreprise et confirme son statut de personne morale. Elle procède alors à une double vérification pour s'assurer, d'une part, que l'entreprise est autorisée à utiliser le nom de domaine figurant dans le certificat et, d'autre part, que l'individu requérant le certificat SSL pour le compte de l'entreprise est dûment habilité à le faire.

Extended Validation (EV)

L'Extended Validation (EV) constitue le plus haut niveau d'authentification disponible pour un certificat SSL. L'authentification EV renforce la structure et les contrôles du processus d'authentification. Ainsi, la validation approfondie de l'authenticité d'une entité commence par la production d'une reconnaissance contractuelle (*Acknowledgement of Agreement*) dûment signée par l'interlocuteur officiel de l'entreprise. Un document attestant de l'inscription de la société au registre du commerce ou à la chambre des métiers pourra être demandé si la consultation des bases de données publiques ne permet pas à l'AC de s'en assurer. Une référence juridique écrite (*legal opinion letter*) pourra être requise pour confirmer les informations suivantes sur l'entreprise :

- Adresse physique du lieu d'activité
- Numéro de téléphone
- Confirmation du droit exclusif à utiliser le domaine
- Confirmation supplémentaire de l'existence de la société (pour les sociétés de moins de 3 ans)
- Vérification de l'embauche de la personne désignée comme interlocuteur officiel de la société

Peu contraignant pour les entreprises exerçant dans la légalité, le processus constitue un obstacle de taille pour les entreprises frauduleuses.

Marques de confiance

Pour gagner la confiance de leurs clients et maximiser leurs ventes en ligne, les sites marchands doivent joindre la parole au geste. Outre la protection des transmissions électroniques de leurs clients, ils doivent également communiquer clairement sur les mesures prises pour assurer un niveau de sécurité satisfaisant. Pour prouver cet investissement sécurité et accroître le capital confiance des clients, les autorités de certification proposent des sceaux de confiance affichables sur les sites Web concernés.

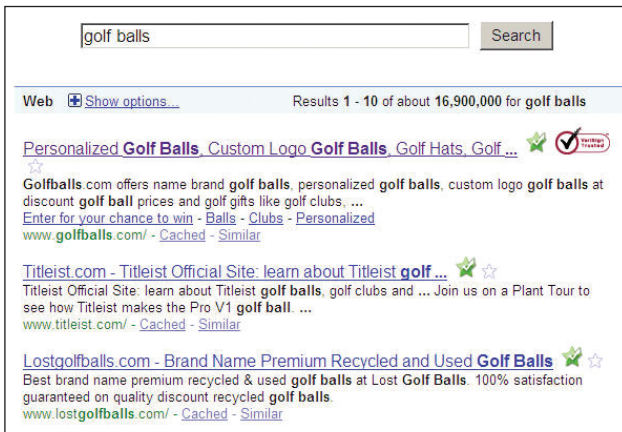
Le sceau VeriSign s'impose comme la marque de sécurité la plus répandue et la plus reconnue dans le monde. Un clic sur ce sceau, et une page s'affiche pour indiquer le nom du propriétaire du certificat, sa période de validité, les niveaux de sécurité du site ainsi que toute autre information relative à la procédure de validation du propriétaire menée par VeriSign en amont de l'émission du certificat. Dans une étude sur la notoriété de la marque VeriSign réalisée en 2009, 11 % des personnes interrogées expliquaient leur choix d'interrompre leur achat ou transaction en ligne par l'absence du sceau VeriSign.⁶

6. VeriSign Brand Tracking Research, 2009



VERISIGN® SEAL-IN-SEARCH™ : LA CONFIANCE EN AMONT

Si le protocole SSL permet de rassurer sur le niveau de sécurité des transactions et l'authenticité des sites Web visités, d'autres solutions contribuent à instaurer la confiance du client à divers points du processus d'achat en ligne. Plus l'affichage des marques de confiance intervient en amont, plus le site est gagnant. Aussi, pour inspirer confiance à toutes les phases du processus d'achat, VeriSign associe le cryptage SSL à d'autres outils de mise en confiance : à savoir des fonctions de recherche de malwares sur les sites Web consultés et l'affichage de la marque de confiance à côté des liens dans les moteurs de recherche.



Baptisée VeriSign® Seal-in-Search™, cette fonctionnalité permet aux sites marchands de rassurer le consommateur avant même qu'il ne clique sur le lien du site Web. La transmission d'une image positive et rassurante très tôt dans l'acte d'achat représente un précieux facteur de différenciation concurrentielle. En misant sur VeriSign® Seal-in-Search™, une e-entreprise se distinguera de ses concurrents utilisant d'autres marques de certificats SSL ne proposant ni service de détection de malwares, ni dispositif d'affichage de marques de confiance dans les moteurs de recherche.

CERTIFICAT SSL EXTENDED VALIDATION (EV) : UN GAGE DE CONFIANCE

Autrefois, la simple mention « https » évoquant la présence d'une session SSL sécurisée ou l'affichage d'un cadenas doré au bas de l'écran suffisaient à balayer les craintes des internautes. Inquiets à l'idée d'être la cible d'actes de cybermalveillance, les internautes trouvaient dans ces mesures un gage de confiance suffisant quant au niveau

de cryptage et de protection de leurs données sensibles. Aujourd'hui, le problème dépasse la simple question du niveau de cryptage. Principal responsable : le phishing. Les fraudeurs sont passés maîtres dans l'art d'endosser le costume d'un cybermarchand respectable. Ils achètent des certificats SSL – trop facilement accessibles auprès d'AC peu scrupuleuses sur la qualité des procédures d'authentification – et s'en servent pour duper les clients et leur soustraire des informations sensibles. Si le cryptage reste nécessaire, il s'avère désormais insuffisant. À quoi bon, si le destinataire de la transmission cryptée est une société malhonnête cherchant à exploiter des données confidentielles pour l'usurpation d'identité ou tout autre acte délictueux ? Établir une relation de confiance représente donc un défi de taille. Car si un site présente toutes les caractéristiques d'un site marchand connu et réputé, comment être certain qu'il ne s'agit pas d'un clone derrière lequel se cache un imposteur mal intentionné ? Une enquête YouGov réalisée pour VeriSign révèle que 88 % des internautes américains représentent une victime potentielle des cyberfraudeurs. La raison ? Leur incapacité à identifier les différentes formes de phishing actuellement en pratique sur le Net.⁷

Pour gagner la confiance des internautes, une entreprise doit non seulement démontrer clairement que les transactions sur son site sont sécurisées, mais également visiblement afficher la légitimité et l'authenticité de son identité. Le standard Extended Validation (EV) est né de ce besoin. En unissant leurs forces, les éditeurs de solutions de sécurité et les développeurs de navigateurs Internet ont ainsi effectué le premier changement majeur en plus de dix ans dans le domaine de la sécurité du commerce en ligne. Les certificats SSL Extended Validation témoignent de l'adhésion de VeriSign à ce standard.

Lorsqu'un client utilise un navigateur récent pour surfer sur un site Web sécurisé par un certificat SSL EV, la barre d'adresse s'affiche en vert, à côté de laquelle se trouve un champ affichant tour à tour le nom du propriétaire officiel du site et le nom de l'autorité ayant émis le certificat SSL EV. Le navigateur et le partenaire sécurité contrôlent l'affichage pour empêcher les arnaqueurs et autres faussaires de pirater la marque du site et subtiliser les données des clients. Les fraudeurs sont devenus de véritables experts en contrefaçon de sites Web. Or, sans certificat SSL EV de la société légitime, il leur est impossible de faire apparaître le nom de l'entreprise dans la barre d'adresse, car ils n'ont aucun contrôle sur l'affichage de ces informations. Toute personne autre que le propriétaire légitime d'un site Web ne

7. https://press.verisign.com/easyir/customrel.do?easyirid=AFC0FF0DB5C560D3&verson=live&prid=510420&releasejsp=custom_97





peut obtenir le certificat SSL EV dudit propriétaire en raison de la rigueur des processus d'authentification mis en œuvre par l'AC.

Certificats SSL EV : un outil rassurant pour le client

- ° En visualisant le nom du propriétaire du certificat dans la barre d'adresse, le cyberconsommateur peut ainsi vérifier que le site est mis en ligne par son véritable propriétaire, et non un imposteur
- ° En ajoutant plusieurs niveaux de vérification de la légitimité et de l'authenticité d'une société avant l'émission d'un certificat SSL EV, l'autorité de certification entend éviter qu'un imposteur ne se fasse passer pour un site d'e-commerce légitime.
- ° Pour obtenir le droit d'émettre des certificats SSL EV, les AC doivent remplir des critères d'une rigueur exemplaire. Elles doivent en effet se soumettre régulièrement à un audit Webtrust réalisé par une entité externe. Objectif : valider la conformité des processus de l'AC aux normes prescrites par le forum CA/Browser – un consortium d'autorités de certification et d'éditeurs de navigateurs. La procédure élimine ainsi les méthodes laxistes de certaines AC qui permettent à des imposteurs d'opérer en toute impunité. Les certificats SSL EV offrent aux clients toutes les garanties d'une vérification en bonne et due forme de la légitimité et de l'authenticité des sociétés opérant les sites Web concernés.
- ° L'affichage de la barre de navigation en vert semble avoir un impact positif sur le consommateur. Car même s'il ignore le détail des atouts d'EV, le consommateur est davantage enclin à effectuer des achats, pour des montants plus importants, dès lors que la barre de navigation passe au vert.

L'efficacité des certificats SSL EV n'est plus à démontrer. Pour preuve, des dizaines de tests menés par des entreprises du monde entier depuis avril 2010 démontrent que l'utilisation de certificats VeriSign® SSL EV fait grimper le nombre de transactions de 17,8 % en moyenne (sur plus de 30 tests).⁸

Ce type d'études réalisées par nos clients eux-mêmes illustrent parfaitement les avantages de l'association des certificats SSL EV et du nom VeriSign en termes de reconnaissance, de confiance et de préférences.

De plus, avec l'intégration systématique du sceau VeriSign à l'ensemble des certificats VeriSign SSL, les sociétés clientes ont la possibilité d'afficher sur leur site la marque de confiance numéro un sur Internet. Toujours selon l'étude de notoriété de la marque VeriSign, 86 % des personnes interrogées reconnaissent le sceau VeriSign – un pourcentage nettement supérieur aux autres marques de confiance.⁹ Le sceau VeriSign permet également aux internautes de vérifier les données et le statut du certificat SSL en temps réel – un gage de confiance supplémentaire pour les cyberconsommateurs.

VeriSign SSL EV : des résultats concrets

Papercheck.com : bond de 87 % des inscriptions en ligne.

CRSHotels.com : conversions en hausse de 30 %.

CarlInsurance.com : augmentation de 18 % des souscriptions en ligne.

Flagstarbank.com : croissance de 10 % des ouvertures de comptes.

CreditKarma.com : progression des conversions de 26 %.

Pour plus d'informations, consultez www.verisign.fr/ssl/ssl-information-center/sslcase-studies/index.html

VERISIGN : LEADER DE LA SÉCURITÉ ET DE LA CONFIANCE SUR INTERNET

Premier fournisseur mondial de certificats SSL, VeriSign est également le numéro un des certificats SSL EV. Avec plus de 70 % de parts de marché¹¹, l'entreprise compte parmi ses clients SSL EV les plus grands noms du commerce électronique et du secteur bancaire.¹⁰ Les chiffres parlent d'eux-mêmes : 97 des 100 premières banques mondiales et 93 % des sociétés du Fortune 500 utilisent des certificats SSL émis par VeriSign.¹¹ Sans oublier plus de 90 000 domaines à travers 160 pays affichant le sceau VeriSign, la marque de confiance la plus reconnue du Web. Les internautes sont donc habitués à voir les sites d'e-commerce arborer le sceau VeriSign. Le symbole y est en effet affiché de manière visible, pour rassurer l'internaute sur l'authenticité de la cyberentreprise et sur sa capacité à préserver la confidentialité des informations grâce au cryptage SSL.

8. Pour plus d'informations, consultez www.verisign.fr/ssl/ssl-information-center/sslcase-studies/index.html.

9. VeriSign Brand Tracking Research, 2009

10. Rapport Netcraft, avril 2010

11. Comprend les filiales et revendeurs VeriSign.



CONCLUSION

Avec l'explosion de la fraude sur Internet, la sécurité des transmissions de données personnelles est devenue un enjeu majeur pour le commerce en ligne. Tristement célèbre pour sa récurrence et ses conséquences, l'usurpation d'identité fait l'objet de toutes les craintes et de toutes les attentions. À l'heure où prolifèrent les vols de données sur Internet, les clients potentiels font donc preuve d'un scepticisme et d'un discernement accrus. Les clients demandent à être protégés, comme le démontre une enquête selon laquelle 83 % des personnes interrogées disent vouloir être davantage rassurées sur la sécurité de leurs données.¹²

La mise en confiance du client permet de faire toute la différence. Et sur le plan strictement financier, l'investissement technologique dans la protection et l'instauration de la confiance des clients reste, somme toute, tout à fait dérisoire, comparé au coût global d'une activité d'e-commerce. L'investissement s'avérant minime au regard des gains potentiels, l'engagement d'une démarche visant à renforcer la sécurité d'un site d'e-commerce, à l'aide de technologies comme le SSL, s'impose comme une évidence pour les cybermarchands cherchant à mettre toutes les chances de leur côté.

Et pour rassurer pleinement vos clients actuels et futurs sur les investissements réalisés pour la sécurisation de votre site marchand, ne prenez aucun risque : faites appel à l'éditeur de solutions de sécurité le plus connu et reconnu du Web. Si VeriSign est aujourd'hui la marque de confiance No1 sur Internet, c'est parce qu'elle a su gagner la confiance des internautes grâce à ses solutions de pointe dans le domaine de la sécurité sur le Net.

EN SAVOIR PLUS

Pour plus d'informations sur les certificats VeriSign SSL, composez le 0800 90 43 51, ou écrivez-nous à l'adresse : ventes@verisign.fr

L'ENTREPRISE VERISIGN

VeriSign est le fournisseur de services d'infrastructures Internet de confiance du monde en réseau. Chaque jour, l'infrastructure Internet VeriSign permet aux entreprises et aux particuliers de réaliser des milliards d'échanges et de transactions sécurisés à travers le monde.

Pour plus d'informations, rendez-vous sur www.Verisign.fr.

12. VeriSign Brand Tracking Research, 2008

