



LA VALEUR COMMERCIALE DE LA CONFIANCE

ENTREPRISES : COMMENT JOUER LA CARTE DE LA CONFIANCE
POUR RASSURER LE CYBERCONSOMMATEUR ET MAXIMISER VOS
VENTES EN LIGNE






LA VALEUR COMMERCIALE DE LA CONFIANCE

Vous cherchez à booster votre taux de conversion, à faire décoller vos ventes et à réduire le taux d'abandons de paniers sur votre site ? Pour VeriSign, la confiance du consommateur est l'enjeu central du web marchand. Aussi, découvrez les solutions concrètes adoptées par de nombreux responsables informatiques pour rassurer et mettre les cyberconsommateurs en confiance.

L'exploitation d'un site marchand est loin d'être aisée. Non seulement il faut s'adapter aux évolutions métier de l'entreprise - nouveaux produits, nouveaux visuels et nouvelles fonctionnalités - mais il faut également veiller à la bonne marche du site. Entre les correctifs à appliquer ou les bugs à réparer, ce n'est pas le travail qui manque. Mais au final, quel est l'objectif de votre site web marchand ? La réponse est évidente : vendre.

Plus un site d'e-commerce inspire confiance, plus les internautes sont susceptibles d'y faire leurs achats. Parmi les responsables informatiques interrogés pour les besoins de cette étude, quatre sur cinq affirment l'importance pour eux « de renforcer la confiance ». Or, malgré ce constat, nombre de cybermarchands négligent encore bien souvent les solutions simples, éprouvées et économiques de mise en confiance du client¹.

Ce rapport d'étude se penche sur le rôle du facteur confiance dans le web marchand et passe en revue les moyens mis en œuvre par les entreprises pour bâtir cette confiance (ou dans certains cas, la négliger). Dans une seconde partie, nous vous proposons un tour d'horizon des solutions VeriSign à même d'instaurer rapidement un cadre d'achat rassurant, sans vous ruiner.



DE L'IMPORTANCE DE LA CONFIANCE

65 %

des Européens se
déclaraient inquiets à
l'idée que des
données
confidentielles
transmises sur Internet
puissent être perdues.

L'importance de la confiance s'explique par la multiplication des expériences malheureuses sur la Toile. D'après la campagne Get Safe Online orchestrée par le gouvernement britannique, en 2008, un tiers (34 %) de la population britannique avait fait la douloureuse expérience d'une infection par virus informatique, un cinquième (22 %) avait fait l'objet d'arnaques de type phishing, tandis que 21 % avaient été victime d'une usurpation d'identité. Résultat : près d'un tiers des internautes n'achètent jamais en ligne, soit par crainte pour leur sécurité personnelle, soit par manque de confiance à l'égard des sites marchandsⁱⁱ.

Si la cybercriminalité touche un nombre défini de personnes, elle contribue à alimenter les craintes collectives. D'après une étude récente, 65 % des Européens se déclaraient inquiets à l'idée que des données confidentielles transmises sur Internet puissent être perduesⁱⁱⁱ. Pour vaincre la psychose, les sites web doivent rassurer les internautes sur la sécurité des achats en ligne^{iv}.

La bonne nouvelle est que les cyberconsommateurs sont de plus en plus avertis sur les questions de sécurité sur Internet. D'après

l'enquête VeriSign, une grande majorité sait reconnaître les différentes marques de sécurité d'un site - protocole https, symbole du cadenas, barre d'adresse verte et autres marques de confiance comme le sceau VeriSign Secured® Seal. Un certificat périmé peut fortement entamer la confiance de l'internaute. Les clients veulent également qu'on les conseille sur les méthodes de protection, et qu'on les rassure sur le sérieux du site visité en matière de confidentialité et de sécurité. Il est tout simplement inconcevable de faire ses achats sur un site qui prendrait ces questions à la légère.

Car l'enjeu est de taille. D'après eMarketer, le chiffre d'affaires de l'e-commerce en Europe atteindra les 275 milliards de livres Sterling d'ici 2011^v. Plus de deux tiers (70 %) de la population britannique achète en ligne^{vi} - un chiffre qui atteint 93 % en période de Noël^{vii}.





LE WEB MARCHAND DE PLUS EN PLUS PRIS POUR CIBLE

Les craintes des consommateurs sont parfaitement fondées au regard de l'ingéniosité et de la détermination dont les cybercriminels font preuve. Dans une certaine mesure, la cybercriminalité brasse davantage que le trafic de drogue international – avec moins de risques de se faire prendre ou de succomber à une mort violente. Particulièrement bien organisée, l'économie souterraine favorise, à cet égard, la spécialisation et la course à l'innovation. Les pirates y vendent leurs produits et services, à savoir leurs logiciels malveillants et leur savoir-faire, à des intermédiaires qui sous-traitent à leur tour la revente de marchandises volées, le blanchiment d'argent et le piratage de cartes bancaires.

La cybercriminalité est un problème croissant. Ainsi, d'après l'APACS, une agence rattachée au Ministère de l'Intérieur britannique, la fraude en ligne et la fraude aux cartes téléphoniques ont augmenté de 13 % entre 2007 et 2008. Au premier semestre 2009, le montant total de la fraude s'élevait à 134 millions de livres Sterling pour le seul Royaume-Uni^{viii}, soit trois fois plus qu'en 2000 – alors que le montant total des achats en ligne n'avait fait que doubler sur la même période^{ix}.

Mais les consommateurs ne sont pas les seuls visés. Les entreprises sont également la cible d'attaques en tous genres – intrusions, usurpations d'adresse IP, attaques par déni de service, logiciels espions et vol de données. D'après une récente enquête du Department for Business, Innovation and Skills (BIS) britannique consacrée aux failles de sécurité informatique^x, près de la moitié (45 %) des petites entreprises auraient été victimes d'une violation de sécurité en 2008. Coût moyen par incident : entre 10 000 £ et 20 000 £. Le problème est encore plus patent dans les grandes entreprises (72 %) pour lesquelles l'addition peut atteindre entre 90 000 et 170 000 £ par incident. Sur l'ensemble des crimes et délits perpétrés, deux types de menaces impactent directement la confiance du cyberclient : le vol de données et l'usurpation d'adresses

IP de sites web (ou spoofing). La moindre défaillance de l'entreprise sur ces deux points peut se solder par une perte d'image et de réputation catastrophique.

Ces préoccupations sont palpables chez les informaticiens interrogés pour les besoins de l'enquête VeriSign. Ils sont en effet 71 % à partager les inquiétudes des clients, en qualifiant notamment les risques suivants de « très importants » :

- Usurpation d'adresse IP (44 %)
- Phishing (40 %)
- Usurpation d'identité (63 %)

À ceci viennent s'ajouter les problèmes de gestion des certificats, plus précisément sur les questions d'expiration ou d'obsolescence des informations contenues dans ces certificats. Pour 36 % des personnes interrogées, la gestion multi-certificats posait problème et 53 % avouaient leur inquiétude à l'idée que leurs certificats puissent arriver à expiration à leur insu.

En clair, pour les responsables informatiques comme pour les clients, ces problèmes de fond freinent sérieusement le développement du commerce en ligne. Heureusement, il existe des solutions simples et éprouvées que les entreprises peuvent aisément se procurer pour rassurer leurs clients et protéger leurs données.



45 %

des petites entreprises
auraient été victimes
d'une violation de
sécurité en 2008.

VERISIGN À LA RESCOUSSE

VeriSign intervient à deux niveaux. D'un côté, VeriSign crypte les données personnelles de vos clients et prouve l'authenticité de votre site. De l'autre, VeriSign vous permet de mettre en avant le sérieux de votre politique de confidentialité

et de sécurisation des données de vos clients. Dans le cadre de cette étude, nous avons pu identifier les objectifs de certains sites marchands que nous avons croisés avec les technologies VeriSign existantes les mieux adaptées.



Objectif de l'entreprise	Pourcentage des personnes interrogées qualifiant cet objectif de 'très important'	Rôle de VeriSign
Rassurer davantage le client et renforcer sa confiance	80 %	Dans la mesure où vous pouvez choisir votre fournisseur de certificats SSL, il est logique de sélectionner celui qui vous permettra d'inspirer la plus grande confiance chez les visiteurs de votre site. Une récente étude révélait que 81 % des cyberconsommateurs britanniques reconnaissent le sceau VeriSign Secured Seal, soit un pourcentage nettement supérieur aux autres marques de confiance ^{xi} . En Europe, 78 % des acheteurs en ligne considèrent VeriSign comme l'entreprise « digne de confiance » par excellence ^{xii} . L'affichage du sceau VeriSign Secured Seal permet aux clients de vérifier la validité du certificat SSL et affiche de manière visible que le site visité confie la protection de ses données à une société sérieuse. De même, les certificats SSL Extended Validation de VeriSign affichent le nom du propriétaire du site ainsi qu'une barre de navigation verte (sur les navigateurs récents) – un témoin visuel qui garantit le sérieux et l'authenticité du site, ainsi que l'utilisation du cryptage SSL.
Renforcer la sécurité	64 %	Les certificats SGC (Server-Gated Cryptography) de VeriSign permettent de crypter les données de plus de 99,9 % des internautes à l'aide du protocole SSL 128 ou 256 bits (selon le navigateur, le système d'exploitation et le serveur d'hébergement) – soit le système de cryptage SSL le plus puissant du marché à l'heure actuelle ^{xiii} . Ce système offre aux internautes une garantie de sécurité optimale lors des transferts de données entre leur navigateur et votre serveur.
Valoriser votre image de marque	54 %	La grande majorité (84 %) des cyberconsommateurs britanniques savent reconnaître les différentes marques de sécurité d'un site Web (protocole https, symbole du cadenas, barre de navigation verte et marques de confiance ^{xiv}). A vous de miser sur ces outils pour mettre en avant le sérieux de votre enseigne et de votre site. Côté gestion, VeriSign met à votre disposition des systèmes d'administration centralisée des certificats, comme le VeriSign® Certificate Center ou le VeriSign® Managed PKI for SSL pour les grandes entreprises. L'avantage ? Éviter que l'expiration des certificats ne passe inaperçue – avec les risques que cela entraîne en termes de sécurité et d'image de l'entreprise.
Augmenter le taux de conversion	44 %	Attirer des visiteurs sur votre site est une chose, déclencher l'acte d'achat en est une autre. Si les actions marketing et publicitaires génèrent du trafic, une fois l'internaute sur le site, tout est une affaire de conversion. En fait, plus de deux tiers des internautes (68 %) font part de leurs hésitations à passer commande sur un site d'e-commerce qui n'affiche aucune marque de confiance ou label de sécurité ^{xv} . L'utilisation de certificats SSL Extended Validation et de marques de confiance comme le sceau VeriSign Secured Seal permet de rassurer les clients, surtout lors du passage à l'achat ou la saisie d'informations personnelles. Enfin, pour appuyer votre message, pensez à informer vos visiteurs sur les mesures de protection et la charte de confidentialité en vigueur sur votre site.
Augmenter le montant du panier par commande	34 %	Jouez la carte de la confiance et de la sécurité pour doper vos ventes de produits et services. Si votre site n'inspire que faiblement confiance, les liens vers les offres d'extension de garanties ou autres produits associés s'apparenteront davantage à du spam ou des publicités intrusives qu'à des offres sérieuses. En revanche, un client qui surfe en confiance sera curieux d'en savoir plus. De même, un site aura tout intérêt à mettre ses internautes en confiance avant de leur demander des informations personnelles. C'est notamment le cas des compagnies d'assurance qui auront besoin de recueillir un certain nombre de renseignements personnels avant de pouvoir établir un devis. D'expérience, si les internautes ne se sentent pas en sécurité, les abandons de paniers sont élevés et les inscriptions au site en chute libre.

ENTREPRISES : LES SOLUTIONS POUR SE PROTÉGER

VeriSign préconise l'utilisation de certificats SSL Extended Validation (EV), l'affichage de marques de confiance (sceau VeriSign Secured Seal) et davantage de communication sur les mesures de sécurité adoptées sur le site, indices visuels à l'appui - des conseils suivis par une majorité d'entreprises éclairées. Pourtant, de telles mesures restent encore lettre morte dans un grand nombre d'entreprises. En fait, seules 40 % des entreprises interrogées pour notre étude utilisent des certificats SSL EV, et à peine 32 % ont recours aux marques de confiance.

Enfin, elles ne sont que 30 % à gérer leurs certificats de manière centralisée. Or, sans de tels outils, vous risquez de vous faire damer

le pion par une concurrence consciente de l'avantage compétitif qu'ils procurent.

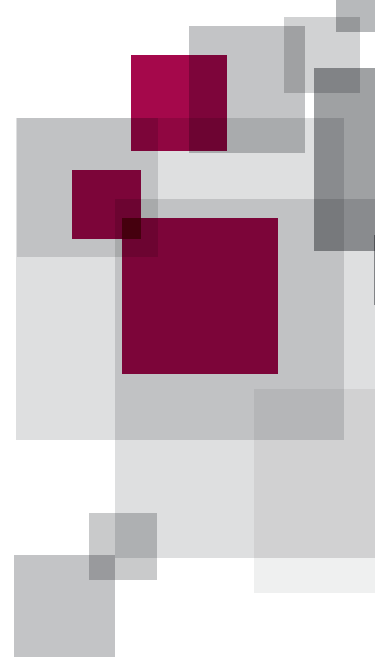
Qu'exige la mise en œuvre de ces outils ? A vrai dire pas grand chose car le processus est à la fois simple et économique. Sur le plan technique, le passage d'un certificat SSL standard à un certificat SSL avec Extended Validation n'a rien de compliqué, d'autant que VeriSign offre un support complet. Les modifications à apporter à un site pour afficher une marque de confiance et des conseils sur la sécurité en ligne sont, somme toute, mineures. Enfin, la gestion centralisée des certificats permet de garder en permanence un œil sur leurs dates d'expiration afin d'éviter les mauvaises surprises.

Tableau : Stratégie de confiance des entreprises

Certificats SSL	84 %
Certificats SSL Extended Validation	40 %
Marque de confiance (ex : sceau VeriSign Secured)	32 %
Explication des fonctions de sécurité du site	25 %

Source : Enquête VeriSign auprès de responsables informatiques, janvier 2010

PRÉCONISATIONS DE VERISIGN



Les craintes des clients en matière de sécurité apparaissent comme la principale préoccupation des responsables informatiques.

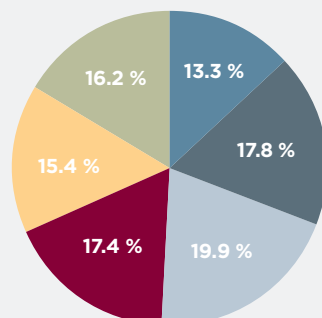
Les clients qui déploient la technologie VeriSign font état d'augmentations significatives des taux de conversion et des ventes, assorties d'une réduction du nombre d'abandons de paniers. Ainsi, le déploiement de certificats SSL Extended Validation* a permis au site Misco de réduire de 5 % le nombre d'abandons de paniers. Quant au voyageur Directline Holidays, il a vu son taux de conversion grimper de 8 %*. Enfin, avec l'installation de certificats SSL Extended Validation et du sceau VeriSign Secured Seal, QuickRooms.com a enregistré une augmentation de près de 7 %* de son chiffre d'affaires.

Si d'autres facteurs sont susceptibles d'influer sur les résultats de ces sites, et si vos

résultats diffèrent légèrement, il n'en reste pas moins que le coût reste minime au regard du budget total d'un site. Par ailleurs, les gains potentiels – calculés sur la base d'un pourcentage du chiffre d'affaires réalisé en ligne – sont très alléchants. L'investissement n'est, par conséquent, pas difficile à justifier.

Les perspectives à long terme sont encore plus prometteuses. Avec l'essor du commerce électronique et l'intensification de la pression concurrentielle, la confiance constitue un levier de différenciation pour votre site. Les enjeux : une double augmentation de vos taux de conversion et de la valeur du panier d'achat. Et ce qui est bon pour les affaires est forcément bon pour vous.

Quelles sont vos principales préoccupations ?



- Gestion de multiples certificats SSL
- Prévention des expirations inattendues de certificats SSL
- Craintes des clients en matière de sécurité
- Usurpation d'identité
- Phishing par e-mail
- Usurpation d'adresse IP (spoofing)

L'ENTREPRISE VERISIGN

VeriSign, Inc. (NASDAQ : VRSN) est le fournisseur de services d'infrastructures Internet de confiance du monde en réseau. Avec ses certificats SSL, ses systèmes d'authentification et de protection des identités, et ses services de référentiels, VeriSign permet aux entreprises et aux particuliers de réaliser chaque jour, en toute confiance, des milliards d'échanges et de transactions sécurisées à travers le monde.

VeriSign est la première autorité de certification SSL (Secure Sockets Layer) garantissant la sécurité des transactions et des communications sur les sites Internet, intranets et extranets. Membre du forum CA/Browser – une association professionnelle regroupant les autorités de certification SSL EV – VeriSign poursuit sa mission de chef de file dans le domaine des certificats SSL.

➤ Rendez-vous sur www.verisign.fr pour en savoir plus.

ⁱ Étude en ligne VeriSign réalisée du 4 au 13 janvier 2010

ⁱⁱ Émission « Fear Holding Back Online Shopping », BBC News, mai 2009. Disponible sur <http://news.bbc.co.uk/2/hi/business/8043717.stm>

ⁱⁱⁱ « Data Loss Is Europe-Wide Problem Says EU Expert », SC Magazine, octobre 2008. Disponible sur <http://www.scmagazineuk.com/Data-loss-is-Europe-wide-problem-says-EU-expert/article/119969/>

^{iv} Données « Get Safe Online » : Rapport annuel GSO 2009 sur www.getsafeonline.org

^v Rapport eMarketer, mai 2008

^{vi} Données « Get Safe Online » : Rapport annuel GSO 2009 www.getsafeonline.org

^{vii} Étude IMRG : <http://www.imrg.org>

^{viii} APACS : http://www.ukpayments.org.uk/media_centre/press_releases/-/page/732/

^{ix} APACS : http://www.ukpayments.org.uk/resources_publications/key_facts_and_figures/card_fraud_facts_and_figures/

^x Enquête sur les failles de sécurité : http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html

^{xi} « VeriSign 2009 Brand Research » Synovate/GMI, mai 2009

^{xii} Synovate/GMI Ibid.

^{xiii} SGC : <http://www.verisign.com/ssl/ssl-information-center/strongest-ssl-encryption/index.html>

^{xiv} « VeriSign 2009 Brand Research » Synovate/GMI, mai 2009

^{xv} Synovate/GMI Ibid.

* Les résultats de votre entreprise sont susceptibles de varier, d'autres facteurs propres à ces clients étant susceptibles d'influer sur leurs résultats. N'hésitez pas à contacter VeriSign pour discuter des solutions de sécurité VeriSign les mieux adaptées aux besoins de votre entreprise.

