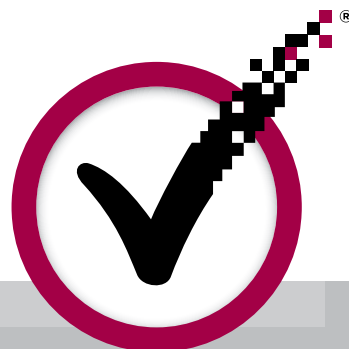




RAPPORT



❑ COMMENT SÉDUIRE ET METTRE EN CONFIANCE LE CYBERCONSOMMATEUR

PANORAMA DES MESURES ADOPTÉES PAR DES
ENTREPRISES AVISÉES POUR BÂTIR ET EXPLOITER
LEUR CAPITAL CONFIANCE DANS LA COURSE À
LA CONCURRENCE SUR INTERNET.

➤ COMMENT SÉDUIRE ET METTRE EN CONFIANCE LE CYBERCONSOMMATEUR

Panorama des mesures adoptées par des entreprises avisées pour bâtir et exploiter leur capital confiance dans la course à la concurrence sur Internet.

Toute entreprise possédant un site Web doit gagner la confiance de ses clients. Si l'élaboration d'un bon site Web coûte cher, la création d'une marque et sa publicité représentent un investissement encore plus lourd. Or la moindre fausse note se paie comptant. Ainsi, lorsque par manque de confiance vos clients quittent votre site juste avant d'avoir validé leur achat, on peut même parler de véritable gâchis. Un peu comme un coureur de marathon qui s'arrêterait quelques mètres avant la ligne d'arrivée.

PERCEPTIONS DU RISQUE

Amplement relayés par les médias, les problèmes de sécurité sur la Toile ont un effet anxiogène sur le consommateur. Conséquence pour les entreprises : une partie de la population n'effectue aucune transaction en ligne. Pour les autres, il s'agit avant tout d'écartier les sites qui n'inspirent aucune confiance. Enfin, il arrive souvent que des internautes aillent quasiment au bout de la transaction, mais abandonnent leur panier s'ils considèrent la protection de leurs données personnelles insuffisante.

Parrainé par VeriSign, le site public britannique de sensibilisation Get Safe Online publie une série de statistiques révélatrices de la propension des consommateurs à effectuer leurs transactions en ligne. Malgré une majorité d'internautes prêts à effectuer leurs achats, gérer leurs comptes bancaires et réserver leurs vacances sur Internet, près d'un tiers de la population évite encore les transactions en ligne¹.

On comprend mieux leurs réticences au vu du nombre de personnes ayant un jour été victimes d'une attaque sur Internet : virus informatique (34 %), phishing (22 %), arnaque (15 %) et usurpation d'identité (21 %).

LA CONFIANCE : UNE ARME CONCURRENTIELLE

Réduction du taux d'abandons, augmentation de la valeur du panier d'achat, protection des marges, optimisation du retour sur investissement publicitaire ou compétitivité accrue face aux grandes marques... tous les objectifs prioritaires des responsables e-commerce reposent sur un facteur : la confiance. Dans les autres secteurs que le Web marchand, la confiance joue un rôle encore plus crucial. Ainsi, sur les sites bancaires ou d'assurances, la quantité d'informations à fournir dépasse largement celle des sites marchands. Et que dire des sites publics en libre-service mis en place par les différentes administrations. Qui serait disposé à remplir sa déclaration d'impôts ou à accéder à son dossier médical en ligne sur un site qui n'inspirerait pas confiance?

Pour transformer ces problèmes en opportunité, il vous faut jouer à fond la carte de la confiance – un formidable vecteur de compétitivité sur Internet.

34 %

des cyberconsommateurs ont un jour été victimes d'un virus informatique.

¹ Rapport « Get Safe Online 2009 » : http://www.getsafeonline.org/nqcontent.cfm?a_id=1517

❖ DONNÉES FACTUELLES POUR ENTREPRISES BIEN RÉELLES

Nous avons récemment interrogé 103 responsables informatiques en France. Objectif : mieux cerner les préoccupations des entreprises et identifier leurs actions pour séduire les clients et gagner leur confiance sur le Web.

Nous les avons tout d'abord sondés sur leur perception des préoccupations de leurs clients – un sujet révélateur des types de menaces dont les sociétés cherchent à se prémunir.

Principal risque perçu : les pertes financières ou les fraudes, suivies de près par les sites marchands frauduleux. Ces résultats présentent une certaine cohérence avec le traitement médiatique de la cybercriminalité et la publication des résultats de sondages d'internautes, comme le rapport annuel « Get Safe Online » commandité par le gouvernement britannique. Derrière cette première question se dessine en filigrane la nécessité pour les responsables informatiques de crédibiliser leur site Web et de rassurer leur clientèle sur la sécurité de leur site, notamment sur les mesures prises pour prévenir toute interception malveillante des numéros de cartes de crédit.

Lorsque nous avons interrogé ces responsables informatiques sur leurs préoccupations à eux, le scénario était sensiblement différent. Les problèmes d'usurpation d'identité ou les arnaques de type *phishing* ne constituaient pas la priorité des professionnels. Leur principal souci était, de manière fort compréhensible, de créer un sentiment de sécurité chez leurs clients, sans pour autant occulter les problèmes pratiques. La crainte de voir les certificats SSL expirer à leur insu constitue, en ce sens, un exemple symptomatique de leurs préoccupations majeures.

Toutes ces inquiétudes sont parfaitement légitimes. L'usurpation d'adresse IP (également appelée *spoofing*) constitue une menace bien réelle. Au dernier trimestre 2009, près de 911 marques ont ainsi été les victimes de ce fléau². Quant au *phishing*, une arnaque montée à base de faux e-mails et sites Web, il peut gravement nuire à la réputation d'une marque, aussi forte soit-elle. L'ensemble de ces points met en évidence la nécessité pour les entreprises de légitimer leur site afin d'éviter toute méprise avec de faux sites ou des impostures. À l'origine de la friilosité des internautes sur la Toile, on retrouve la crainte d'usurpation d'identité³; d'où la nécessité pour les propriétaires de sites Web de justifier d'un niveau de protection des données personnelles adéquat, notamment par le biais d'un dispositif de cryptage.

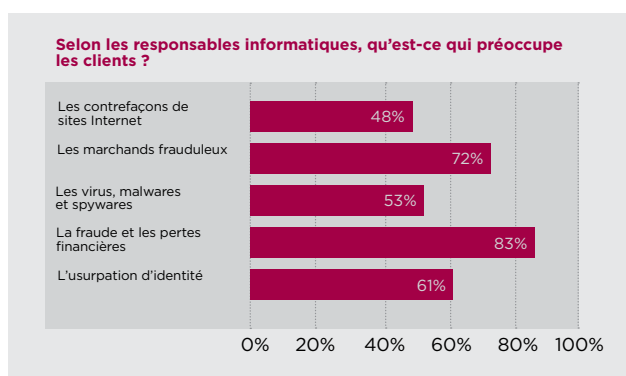
Un certificat SSL expiré peut sérieusement entacher le capital confiance d'un site, notamment à cause des messages d'erreur alarmistes (et terriblement techniques) qui s'affichent alors dans les navigateurs Web. Et pour les entreprises ayant une pléthore de certificats SSL à gérer, les responsables

informatiques peinent parfois à maîtriser l'échéancier des renouvellements. Or, la mise en place d'une gestion efficace des certificats et l'adoption de mesures permettant d'éviter leur expiration « surprise » relèvent bel et bien de leurs attributions.

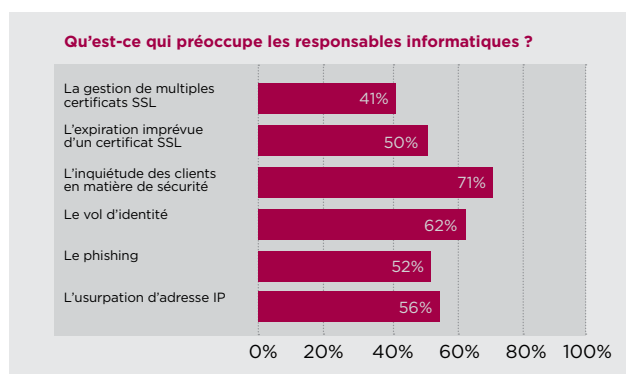
Nous avons également interrogé notre panel de responsables informatiques sur les mesures adoptées pour rassurer les internautes et accroître la sécurité en ligne. L'utilisation de certificats SSL permettant le cryptage de données confidentielles

constitue manifestement la méthode la plus répandue. Toutefois, il est surprenant de constater que seule une minorité a recours à la forme de certificat SSL la plus sécurisée et la plus visible – à savoir les certificats SSL Extended Validation (EV). Peu de sites affichent des rubriques consacrées à l'explication de la politique de sécurité du site. Quant aux marques de confiance comme le sceau VeriSign Secured® Seal, elles sont encore plus rares. Il semble donc que les responsables de sites Web ne profitent pas de tous les outils à leur disposition.

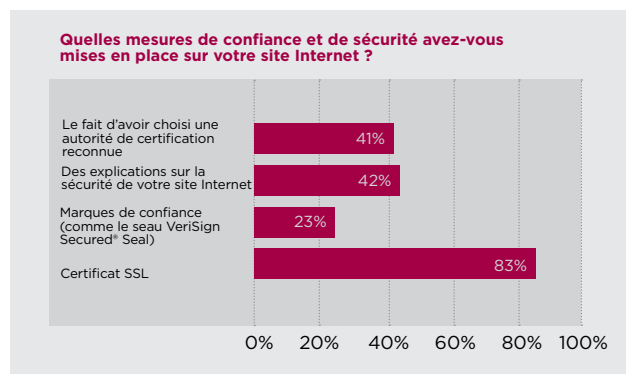
(i)



(ii)



(iii)



² Groupe de travail anti-phishing, décembre 2009, www.apwg.org

³ Étude Synovate/GMI 2009

LES ATOUTS DES CERTIFICATS SSL EXTENDED VALIDATION

Qu'implique précisément la notion de « confiance » dans ce contexte ? Il s'agit d'abord d'un sentiment et d'une réaction par rapport à une menace de cybercriminalité perçue, comme notamment l'usurpation d'identité. De fait, l'enjeu consiste à changer la perception de sécurité des clients. Nous avons divisé ces points en quatre thématiques :

- Authentification du vendeur (« nous sommes ce que nous affirmons être »)
- Protection et cryptage des données (« nous protégeons vos données »)
- Renforcement du capital marque (« nous respectons votre vie privée »)
- Mise en confiance (« vous pouvez faire vos achats ici en toute sécurité »)

Gage d'un niveau de sécurité supplémentaire par rapport aux certificats SSL classiques, les certificats SSL Extended Validation (EV) affichent le nom de la société et une barre d'adresse verte dans les versions récentes des navigateurs les plus courants (Internet Explorer 7 et Firefox 3.0 et leurs versions ultérieures, ainsi que les navigateurs des smartphones dernier cri). Les utilisateurs ont alors la preuve tangible de l'authenticité et de la sécurité du site sur lequel ils surfent.

Ces certificats répondent aux quatre points cités plus haut :

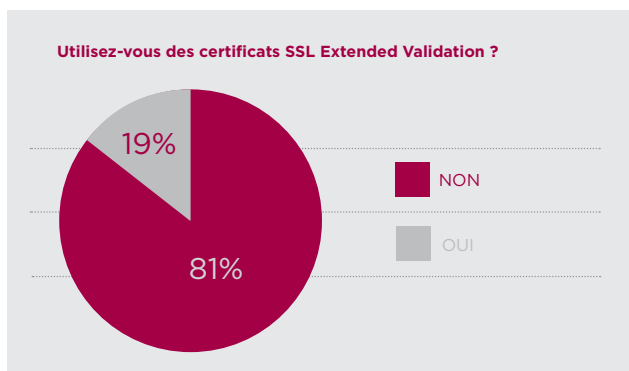
- **Authentification du vendeur.** La rigueur des procédures d'authentification appliquées par VeriSign en amont de la délivrance d'un certificat offre aux internautes toutes les garanties d'authenticité du site consulté.
- **Protection et cryptage des données.** Les certificats SSL EV offrent le niveau de cryptage maximum actuellement possible sur un certificat SSL, avec à la clé un cryptage haute sécurité des données utilisateurs entre le navigateur et le site visité.
- **Renforcement du capital de la marque.** A condition d'utiliser un navigateur compatible, les certificats SSL EV affichent le nom de la société dans la barre d'adresse du navigateur. Objectif : rassurer les internautes sur l'authenticité du site visité.
- **Mise en confiance.** La barre d'adresse verte d'un site protégé par un certificat SSL EV constitue un signe fort et rassurant du niveau de sécurité renforcée du site.

À PROPOS DES CERTIFICATS SSL EXTENDED VALIDATION

Les certificats SSL Extended Validation ont été créés pour faire face à l'augmentation de la fraude en ligne, elle-même à l'origine d'une érosion de la confiance des cyberconsommateurs. Offrant un niveau de vérification supplémentaire par rapport aux certificats SSL classiques, le standard SSL Extended Validation commande l'affichage de repères visuels dans les navigateurs sécurisés.

En 2006, un groupement d'autorités de certification (AC) SSL leaders et d'éditeurs de navigateurs se sont accordés sur un nouveau standard de validation et d'affichage de certificats - standard baptisé « Extended Validation ». Pour pouvoir émettre un certificat SSL conforme à ce standard, l'autorité de certification doit adopter une pratique de validation étendue du certificat et se soumettre à un audit Webtrust. Le processus de validation exige que l'AC authentifie le propriétaire du domaine et l'identité de la société du demandeur, ainsi que le statut d'employé du demandeur auprès de la société en question et son habilitation à demander le certificat SSL Extended Validation.

Les certificats SSL Extended Validation transmettent aux navigateurs Web sécurisés des informations permettant d'identifier clairement l'identité de l'entreprise propriétaire d'un site Web. Ainsi, si vous utilisez Microsoft® Internet Explorer 7 pour vous rendre sur un site Web sécurisé par un certificat SSL conforme au standard Extended Validation, IE7 affichera une barre d'adresse verte. Un panneau situé à gauche de la barre verte affichera tour à tour le nom de l'organisation listée dans le certificat et l'autorité de certification (VeriSign, par exemple). Firefox 3 prend également en charge le protocole SSL Extended Validation.



DES RÉSULTATS TANGIBLES

Augmentation de la valeur du panier d'achat, réduction du taux d'abandon et chiffre d'affaires en hausse... notre enquête aura permis de mettre en lumière l'impact positif des certificats SSL EV pour les entreprises utilisatrices. Mais le principal avantage reste, sans aucun doute, l'amélioration de la perception de sécurité du site aux yeux des clients. C'est du moins ce que révèle une majorité écrasante des personnes interrogées (74 %) :

Nous obtenons invariablement les mêmes résultats avec nos clients. Les entreprises qui utilisent un certificat VeriSign SSL EV pour sécuriser leur site Web font état d'une augmentation de plus de 20 % de leur volume de transactions⁴. Les résultats des études menées récemment auprès de clients VeriSign SSL EV sont éloquentes* :

- Réduction de 5 % du nombre d'abandons de paniers sur le site e-commerce de Misco
- Augmentation de 8 % du taux de conversion du voyageur Directline Holidays
- Hausse de près de 7 % du chiffre d'affaires du site QuickRooms.com
- Quasi doublement (hausse de 87 %) des inscriptions en ligne sur Papercheck.com
- Augmentation de 18 % des inscriptions en ligne sur CarInsurance.com
- Augmentation de 16,9 % du taux de conversion et réduction de 13,3 % du nombre d'abandons de paniers sur le site de Fitness Footwear
- Hausse spectaculaire de 26 % du taux de conversion de CreditKarma.com

PRÉCONISATIONS DE VERISIGN

Cinq mesures très simples permettent de rassurer et de mettre en confiance vos visiteurs :

- **Monter en gamme vers le SSL EV.** Si le protocole SSL est efficace, le SSL Extended Validation l'est encore plus. Les certificats SSL EV remplacent les certificats SSL classiques, sont guère plus onéreux et nécessitent peu de procédures de déploiement supplémentaires.

- **Choisir une autorité de certification de confiance.** La réputation de l'autorité de certification (comme VeriSign) est un critère important aux yeux des utilisateurs. Dans une étude récente, 88 % des participants déclaraient avoir confiance en VeriSign, contre seulement 22 % pour l'autorité arrivant en seconde position⁵.

- **Afficher une marque de confiance.** Complétez vos certificats SSL EV par des indices visuels supplémentaires attestant du sérieux de votre politique de sécurité des données de vos clients. La notoriété de ce type de marque de confiance constitue un précieux atout. Pour référence, 68 % des cyberconsommateurs à travers l'Europe reconnaissent le sceau VeriSign Secured[®] Seal, soit un pourcentage nettement supérieur aux autres marques de confiance.⁶

- **Améliorer la gestion des certificats.** Auditez votre portefeuille de certificats pour vous assurer d'être automatiquement alerté des prochaines dates d'expiration. En ce sens, il s'avère judicieux de regrouper l'ensemble de vos certificats sous un compte géré. Pour ce faire, le VeriSign Certificate Center met à votre disposition un système d'administration centralisée des certificats VeriSign. Si vous utilisez des certificats provenant de plusieurs autorités de certification, ou si vous exploitez un grand nombre de certificats, prévoyez d'investir dans un outil d'administration comme VeriSign Managed PKI pour SSL.

- **Informez les utilisateurs sur votre politique de protection des données.** Ajoutez une page à votre rubrique d'Aide, ou un menu en pied de page, explicitant votre politique de protection des données utilisateur, avec notamment une explication du rôle d'un certificat SSL. La présence de ce genre d'information aide à rassurer les internautes.

Notre étude révèle que les entreprises interrogées consacrent en moyenne 13 % de leur budget à la sécurité. Même si ce chiffre représente une part importante de leurs dépenses, de nombreuses sociétés ne prennent pas les mesures de base pour rassurer leurs internautes, ou encore améliorer la sécurité ou le capital confiance de leurs sites.

Or ces mesures impliquent un investissement en temps somme toute minime - comme pour la modification d'une page Web en vue de l'insertion d'une marque de confiance - et ne sont, dans l'absolu, pas particulièrement onéreuses au regard des budgets alloués à la cybersécurité.

La pérennité des certificats SSL EV est assurée. Déjà utilisés par des sociétés avisées, ils sont de plus en plus connus et reconnus par les consommateurs. Malgré cela, les certificats SSL EV restent les grands absents de nombreux sites - dont certains de vos concurrents - qui ne prennent aucune autre mesure pour gagner la confiance de leurs internautes. La mise en œuvre de certificats SSL EV et l'adoption de l'ensemble de nos préconisations s'imposent par conséquent comme une évidence. La confiance de vos clients est un précieux avantage concurrentiel. Vous pouvez compter sur VeriSign pour vous aider à la gagner.

68 %

des
cyberconsommateurs
à travers l'Europe
reconnaissent le sceau
VeriSign Secured[®] Seal.⁶

⁴ Depuis décembre 2009, les tests réalisés sur des dizaines de sites à travers le monde révèlent que les certificats VeriSign SSL EV ont permis d'augmenter les taux de conversions entre 5 % et 87 %, avec une moyenne établie à 20 %.

⁵ Tec-Ed, janv. 2007

⁶ Étude Synovate/GMI 2009

↳ L'ENTREPRISE VERISIGN

VeriSign, Inc. (NASDAQ : VRSN) est le fournisseur de services d'infrastructures Internet de confiance du monde en réseau. Chaque jour, nos certificats SSL, systèmes d'authentification et services de référentiels et de protection des identités permettent aux entreprises et aux particuliers de réaliser 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.

*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.

