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 :

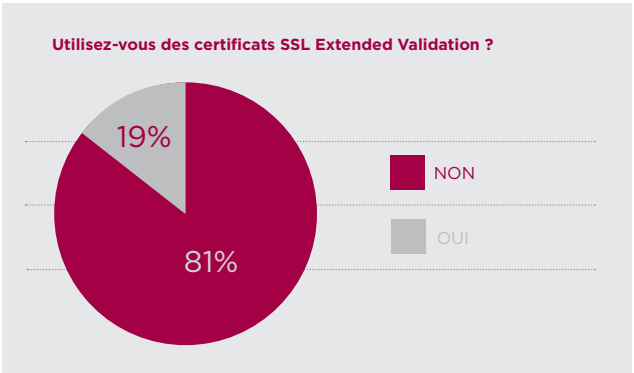
- **Authentification du vendeur.** La rigueur des procédures d'authentification appliquées par VeriSign en amont de la délivrance d'un certificat offre aux internautes toutes les garanties d'authenticité du site consulté.
- **Protection et cryptage des données.** Les certificats SSL EV offrent le niveau 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.



Source : http://www.verisign.com/ssl/ssl-information-center/extended-validation-ssl-certificates/index.html

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 transactions[4]. Les résultats des études menées récemment auprès de clients VeriSign SSL EV sont éloquents* :

- Réduction de 5 % du nombre d'abandons de paniers sur le site e-commerce de Misco
- Augmentation de 8 % du taux de conversion du voyagiste 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 position[5].
- **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.
- **Informer 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