



DOCUMENT TECHNIQUE

LES CERTIFICATS SSL EXTENDED VALIDATION DOPENT LES VENTES ET LES TRANSACTIONS EN LIGNE — PREUVES À L'APPUI

SOMMAIRE

- 1 INTRODUCTION
- 1 LE DÉFICIT DE CONFIANCE, UN FREIN À LA CROISSANCE DE L'E-COMMERCE
- 2 EXTENDED VALIDATION RESTAURE LA CONFIANCE
- 4 LA VALEUR DE SSL EV, PREUVES À L'APPUI
- 6 CONCLUSION
- 6 EN SAVOIR PLUS
- 6 L'ENTREPRISE VERISIGN



LES CERTIFICATS SSL EXTENDED VALIDATION DOPENT LES VENTES ET LES TRANSACTIONS EN LIGNE – PREUVES À L'APPUI

INTRODUCTION

Achats, échanges d'informations, transactions bancaires, consultations de compte : à l'heure où Internet bouleverse les habitudes de consommation, les clients sont de plus en plus attentifs à la notion de sécurité en ligne. Toutefois, leurs inquiétudes concernant l'usurpation d'identité et la fraude dissuadent encore de nombreux internautes à effectuer leurs transactions en ligne. Pour endiguer le phénomène, il faut pouvoir rassurer le cyberconsommateur sur la protection de ses informations confidentielles contre tout détournement malveillant.

En ce sens, les certificats SSL Extended Validation (EV) œuvrent en faveur d'une mise en confiance du client pour effectuer des opérations en ligne. 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).¹

Dans les navigateurs sécurisés, VeriSign SSL EV se matérialise par une barre d'adresse verte témoignant d'une couche de sécurité supplémentaire sur le site Web. Objectif : rassurer le client. Ce document propose donc un tour d'horizon des méthodes utilisées par des entreprises pour booster le volume de leurs opérations en ligne, réduire les abandons de paniers et doper le nombre de conversions de visiteurs/abonnés... le tout grâce aux certificats VeriSign SSL EV.

VeriSign SSL EV : des résultats concrets

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

CRSHotels.com : conversions en hausse de 30 %.

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

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

CreditKarma.com : progression des conversions de 26 %.

Consultez www.verisign.com/ssl/ssl-information-center/ssl-case-studies/index.html pour plus d'informations.

DÉFICIT DE CONFIANCE : UN FREIN À LA CROISSANCE DE L'E-COMMERCE

Aujourd'hui, le grand public peut accéder à Internet et passer du temps en ligne comme jamais auparavant. En 2008, malgré la crise économique mondiale, les 500 plus grandes enseignes du Web ont enregistré une hausse de 11,7 % de leurs ventes.² De même, d'après les spécialistes du secteur financier, la banque en ligne est appelée à constituer le principal point de contact clientèle au cours de la prochaine décennie. Le taux de pénétration d'Internet continue de croître et la navigation se popularise sur les terminaux mobiles. Résultat : les entreprises développent de nouveaux relais de croissance avec la vente en ligne et autres services par abonnement. Seul bémol, les internautes éprouvent encore certaines réticences à effectuer des transactions sur la Toile, principalement en raison des inquiétudes qu'ils nourrissent à l'égard de la protection de leurs informations confidentielles.

Même si l'usurpation d'identité se produit plus souvent hors du cadre d'Internet, en France, les internautes ont pointé du doigt les pirates et les virus comme les principales raisons de leur manque de confiance dans les activités en ligne.³ Ces craintes se vérifient tous les jours sur l'économie du Web :

- L'abandon des paniers d'achat se traduit par un manque à gagner et une perte de chiffre d'affaires.
- Le suivi du taux de clics montre que les clients potentiels atteignent les formulaires d'inscription, mais ne les remplissent pas.
- Les outils d'analyse des recherches et les alertes montrent l'ampleur des détournements de marques et de noms d'entreprise visant à dérouter les clients des sites légitimes.

Les arnaques Internet sont mieux coordonnées et plus sophistiquées que par le passé, ce qui mine la confiance des internautes. Or pour une entreprise en ligne, cette confiance est un facteur indispensable. Les chiffres sont alarmants : en octobre 2009, le nombre de marques détournées a atteint un sommet historique de 356, soit 4,4 % de progression par rapport au précédent record de 341 en août 2009.⁴

1. Consultez www.verisign.fr/ssl/ssl-information-center/ssl-case-studies/index.html pour en savoir plus sur les résultats obtenus par nos clients.

2. Internet Retailer, 2009 www.top500guide.com

3. Etude Synovate/GMI 2009

4. www.antiphishing.org



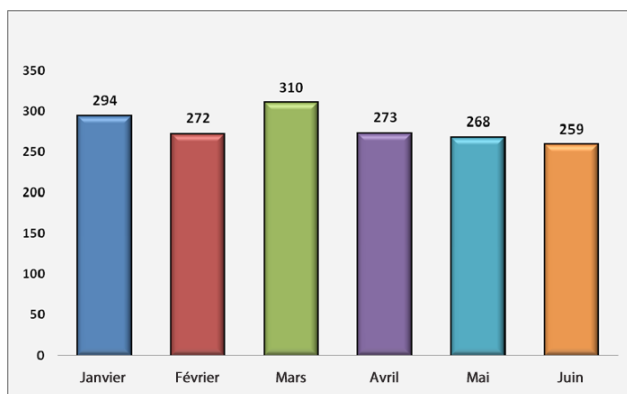


Le phishing utilise quant à lui des e-mails et des sites Web qui semblent authentiques pour inciter les internautes à communiquer des informations personnelles. Autre attaque en vogue, le SSL stripping procède par interception (man-in-the-middle) pour rediriger les utilisateurs vers des sites Web « sécurisés », qui sont en réalité des contrefaçons (certaines mesures de sécurité ont été prises et sont affichées, mais le site Web n'est pas celui que l'internaute pense visiter). Ce type d'attaque cible souvent les applications de Webmail, les sites sécurisés et les intranets.

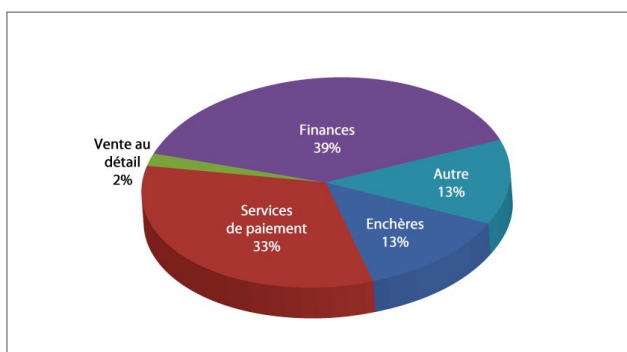
Définition du phishing

Type d'attaque par laquelle des fraudeurs fabriquent des e-mails et des sites Web falsifiés imitant ceux d'une marque connue, le but de la manœuvre étant de recueillir des informations personnelles à des fins d'usurpation d'identité.

Marques piratées par mois Premier semestre 2009



Principaux secteurs ciblés - Troisième trimestre 2009



Source : Anti-Phishing Working Group, mai 2009

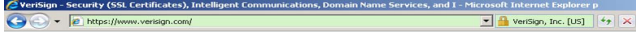
EXTENDED VALIDATION RESTAURE LA CONFIANCE

De nombreux propriétaires de sites Web reconnaissent un site protégé par SSL, notamment au vu d'indices connus comme le cadenas fermé et « https » dans la barre d'adresse. Avant SSL Extended Validation, les internautes ne pouvaient qu'espérer que seuls des sites légitimes puissent utiliser SSL. Mais profitant du laxisme des processus de validation de certaines autorités de certification de second rang, les fraudeurs se sont engouffrés dans la brèche en achetant des certificats SSL pour des domaines falsifiés. À l'aide de ces certificats SSL, ils ont créé des sites « sécurisés » comme rampe de lancement d'attaques de phishing et de SSL stripping, érodant par là même la confiance globale des consommateurs. Les certificats VeriSign® SSL EV apportent une réponse forte à cette utilisation frauduleuse de la technologie SSL. Ses missions : réduire les taux d'abandons et doper les conversions grâce à des transactions en ligne plus sûres, garantes d'une meilleure protection des informations d'identification personnelle et d'une réduction des coûts.

Mode de fonctionnement de l'authentification EV

Extended Validation, ou « EV », constitue le niveau d'authentification le plus élevé d'un certificat SSL. Les certificats SSL EV appliquent un niveau de protection supplémentaire pour les consommateurs et propriétaires de sites Web. Leur spécificité : les candidats doivent suivre une procédure d'obtention très stricte définie par le CA/Browser Forum. L'authentification SSL EV est devenue une fonction de sécurité standard intégrée aux principaux navigateurs, comme Internet Explorer® ou Firefox®, et sur les terminaux mobiles tels que l'iPhone® ou Droid. Ainsi les navigateurs reconnaissent les sites Web sécurisés par EV et l'indiquent visuellement pour informer les internautes que le site Web est digne de confiance. Lorsque les consommateurs visitent une page Web sécurisée par un certificat SSL EV, la barre d'adresse s'affiche en vert (dans les navigateurs compatibles) et un champ spécial indique tour à tour le nom du propriétaire légitime du site et celui de l'autorité de certification. Cet indice visuel contribue à renforcer la confiance des consommateurs envers le Web marchand.





« Dès qu'ils voient la barre verte, les clients de 1-800-FLOWERS.COM savent qu'ils ont atteint un site Web authentique, auquel ils peuvent se fier », explique Steve Bozzo, DSI chez 1-800-FLOWERS.COM. « Le déploiement des certificats VeriSign SSL EV représente un investissement rentable dans notre stratégie de fidélisation de nos clients - un atout inestimable sur le Web marchand. »

Tout le poids du nom de confiance sur Internet SSL EV aide aussi les utilisateurs à vérifier à qui ils ont affaire et qui a validé le site Web en question. En effet, la barre d'adresse des navigateurs compatibles SSL EV affiche les noms de l'entité détentrice du certificat SSL EV et de l'autorité qui l'a émis.

Marque de confiance la plus reconnue sur Internet, le sceau VeriSign® est présent sur plus de 90 000 sites Web dans 160 pays. Il est affiché jusqu'à 250 millions de fois par jour. D'après une étude, 68 % des cyberconsommateurs européens reconnaissent le sceau VeriSign Secured Seal plus que toute autre marque de confiance.⁵ Un certificat VeriSign® SSL EV renforce la notion de marque et de sécurité d'un site en plaçant dans la barre d'adresse le nom VeriSign à côté de celui de l'e-entreprise.

Certificats VeriSign SSL : gage de sécurité et de confiance

Premier fournisseur mondial de certificats SSL, VeriSign est également le numéro un des certificats SSL EV, avec plus de 70 % de parts de marché. VeriSign compte parmi ses clients SSL EV les plus grands noms du commerce électronique et du secteur bancaire.⁶ 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.⁷ 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.

Retour sur investissement en capital confiance

Même une légère hausse des conversions peut produire un effet notable sur le chiffre d'affaires et les inscriptions en ligne. Les entreprises qui utilisent un certificat VeriSign SSL EV pour sécuriser leur site Web font état d'une augmentation moyenne de 17,8 % du volume de leurs transactions.⁸ En d'autres termes, sans certificat VeriSign SSL EV, une entreprise dont le chiffre d'affaires atteint 100 millions d'euros peut tabler sur un manque à gagner annuel de 17 800 000 d'euros dû aux préoccupations sécuritaires de ses visiteurs. De même, un site Web possédant 100 000 clients en ligne peut perdre jusqu'à 17 800 nouveaux comptes en raison d'un manque de confiance.

Normes d'authentification plus strictes

Avant d'émettre un certificat SSL EV, l'autorité émettrice doit :

- vérifier l'existence juridique, physique et opérationnelle de l'entité ;
- vérifier que son identité correspond aux registres officiels ;
- vérifier qu'elle dispose du droit exclusif d'exploitation des domaines spécifiés dans le certificat SSL EV ;
- vérifier qu'elle a correctement autorisé l'émission du certificat SSL EV.

5. Etude Synovate/GMI 2009

6. Rapport Netcraft, mars 2010

7. Comprend les filiales et revendeurs VeriSign.

8. Résultats basés sur les mesures effectuées chez 30 clients. Pour plus d'informations, consultez www.verisign.com/ssl/ssl-information-center/ssl-case-studies/index.html





LA VALEUR DE SSL EV, PREUVES À L'APPUI

À mesure que les certificats SSL EV se généralisent sur Internet, la barre d'adresse verte s'impose comme un élément indispensable dans tout un ensemble de secteurs opérant en ligne. Le tracking des impressions, des clics et des interactions permet de mesurer le retour sur investissement des certificats SSL EV et de quantifier l'impact positif d'un renforcement de la sécurité sur les résultats d'une entreprise. À ce jour, plus de 23 000 sites Web ont déployé des certificats SSL EV et VeriSign est le fournisseur privilégié de plus de 16 000 d'entre eux (enquête Netcraft, mars 2009).

Réduction des abandons de paniers

Le meilleur moyen d'améliorer le résultat d'une entreprise reste encore d'augmenter son chiffre d'affaires. Dans le cas des grandes enseignes Internet, l'abandon de transactions en cours de route représente des clients potentiels non matérialisés, qui ont pris le temps de chercher un produit avant de renoncer à l'acheter. Or lorsque les clients voient la barre d'adresse verte, ils sont davantage disposés à aller au bout de la transaction.

- **E-détaillants.** « Avec Extended Validation nous offrons à nos clients un niveau de sécurité maximum, particulièrement pour ceux utilisant les nouveaux navigateurs tels qu'IE7 avec le système d'affichage de la barre d'adresse en vert. Quand nous avons décidé d'héberger notre plateforme de paiements en interne, nous avons pensé qu'y associer les certificats VeriSign était le meilleur moyen de soutenir la croissance de Cdiscount. » a déclaré Aurélien Fauré, Responsable d'exploitation chez Cdiscount.

« Nous avons abordé EV comme une nouvelle étape de notre sécurité, une évolution naturelle dans le renforcement de notre relation avec VeriSign », explique Luke Barlow, directeur de Fitness Footwear. « De plus, il est tout à fait naturel que les clients, lorsqu'ils voient la barre d'adresse en vert pendant leur achat, poursuivent le processus avec plus de sérénité. EV représente un excellent investissement », poursuit Jonathan Dicks, responsable couleurs et formes.

Premier site marchand indépendant de chaussures au Royaume-Uni, Fitness Footwear a constaté un recul de 13,3 % des abandons de paniers et une hausse de 16,9 % des conversions.⁹

- **Tourisme et hôtellerie.** Pour lutter contre un taux élevé d'abandons, le service de réservation d'hôtels Central Reservation Service (CRShotels.com) a adopté les

certificats VeriSign SSL EV[®]. Des tests ont ainsi révélé *un taux de conversion de 30 % supérieur sur les pages affichant la barre verte symbolisant SSL EV.*⁹ Un résultat qui a largement dépassé les attentes de l'entreprise.

« Aucune entreprise en ligne qui cherche à développer sa base de clients ne peut sous-estimer la valeur de la confiance, surtout maintenant que les clients sont parfaitement conscients des risques d'usurpation d'identité et sont encore plus tournés vers les prix. Choisir SSL EV (Extended Validation) de VeriSign nous permet d'instaurer la confiance chez nos clients. De plus, ce choix montre notre détermination à investir dans la meilleure sécurité SSL disponible » a déclaré Keith Taylor, Directeur des achats chez Omodo.

- **Courtiers d'assurances.** L'abandon de transactions touche également des courtiers tels que CarInsurance.com. L'entreprise propose des devis d'assurance automobile de différentes compagnies en fonction des informations personnelles saisies en ligne. Une étude menée par CarInsurance.com a révélé *une hausse de 18 %⁹ du nombre de propositions tarifaires acceptées en présence de certificats VeriSign SSL EV.*

Des taux de conversion en hausse

Pour convertir les internautes en acheteurs et les visiteurs en abonnés, un site Web doit susciter confiance et crédibilité. Dans les secteurs où la fraude et les arnaques sont monnaie courante, la rigueur du processus d'authentification sous-jacent à SSL EV démarque clairement les entreprises les plus sérieuses. Beaucoup ont constaté qu'un certificat VeriSign SSL EV les aide à asseoir leur présence en ligne, grâce à la confiance qu'accordent les internautes au nom VeriSign. Résultat final : un taux de conversions plus important, des transactions d'un montant supérieur et une hausse du chiffre d'affaires.

- **Pharmacie en ligne.** CanadaDrugs.com a amorti sa licence SSL EV en quelques jours seulement. Brock Gunter-Smith, Directeur du commerce électronique, témoigne : « Nos clients nous achètent des produits parce qu'ils ont un besoin souvent pressant de médicaments. Et nombre d'entre eux n'ont tout simplement pas les moyens de se les payer à la pharmacie du quartier. On pourrait penser que la couleur de la barre d'adresse leur importerait peu. Pourtant, VeriSign SSL EV fait une différence considérable, même auprès de personnes avec des motivations d'achats aussi élevées. »

9. Chaque étude a été directement menée par l'entreprise citée. Pour plus d'informations sur cette étude, rendez-vous sur www.verisign.com/sslcasestudies



CanadaDrugs.com a opté pour les certificats VeriSign SSL EV. Constat : un bond de 33 % des conversions et une hausse de 27 % du panier d'achat moyen⁹ chez les acheteurs qui voient la barre d'adresse verte EV.

- **Services financiers.** Credit Karma a déployé VeriSign® SSL EV pour gagner la confiance des clients dans un domaine très exposé à l'usurpation d'identité. *Le site Credit Karma a, quant à lui, mesuré un taux de conversion 26 % plus élevé⁹ chez les utilisateurs qui voient la barre d'adresse verte EV.* « La confiance est la pierre angulaire de notre offre de service et de notre business model », déclare Ken Lin, PDG de Credit Karma. « Nous nous efforçons d'inciter les consommateurs à rationaliser leurs dépenses, mais ils doivent d'abord nous faire confiance pour communiquer leurs informations personnelles. Le nom VeriSign est un facteur qui contribue nettement à cet objectif. »
- **Éducation.** Pour les nouvelles entreprises qui cherchent à augmenter leur nombre d'adhérents et à établir une présence en ligne, le taux de conversions constitue l'un des principaux leviers de croissance. PaperCheck.com, un service de correction et de relecture de documents en ligne destiné à un public d'universitaires, considère les certificats VeriSign SSL EV comme indispensables.

« Nous avons été stupéfaits de l'effet EV. 87 % d'inscriptions en plus⁹ est un chiffre formidable », déclare Darren Shafae, fondateur et Vice-président de PaperCheck.com, LLC. « Nous n'aurions jamais imaginé une telle hausse. C'est un retour sur investissement incroyable ! »

Protection renforcée

Certaines entreprises sont tenues de respecter tout un train de normes réglementaires en matière de protection des informations personnelles. Les certificats SSL EV leur permettent donc de réduire le risque de non-conformité et de communiquer sur la rigueur de leurs mesures de protection contre les menaces connues. En utilisant SSL EV et en sensibilisant leurs clients à la barre d'adresse verte, les entreprises atténuent le risque d'interception en cours de transmission et démontrent l'efficacité de leur politique de sécurité.

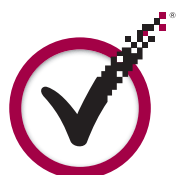
- **Banque.** « En travaillant avec VeriSign sur le déploiement SSL EV, nous avons franchi une nouvelle étape dans

la sécurisation des transactions en ligne de nos clients et nous leur apportons une confiance supplémentaire lorsqu'ils effectuent leurs opérations bancaires en ligne avec la HSBC. » déclare Jonathan Etheridge, analyste principal de sécurité informatique chez HSBC.

Plus grande banque d'épargne du Midwest américain, Flagstar a mis en œuvre les certificats VeriSign SSL EV sur ses sites dédiés aux particuliers et aux entreprises, ainsi que sur ses sites partenaires d'établissements de prêts et crédits hypothécaires. D'après Flagstar, *l'utilisation de Flagstar.com a augmenté de 49 % sur 12 mois* et la banque a enregistré *une hausse de 10 % des dossiers de demande remplis en ligne.*⁹ Dans une année de consolidation bancaire et de tourmente financière, Flagstar Bank a augmenté sa clientèle au-delà de celle des agences traditionnelles.

« La distinction entre un site Web authentique et son équivalent contrefait est un problème aigu dans notre secteur. On peut dire que VeriSign EV l'a résolu », résume Jason Dufner, Vice-président senior des Systèmes informatiques et bancaires chez Flagstar Bank.

- **Services financiers.** Lorsqu'Investors Trust s'est converti à l'utilisation des certificats VeriSign SSL EV, l'entreprise a sensibilisé ses partenaires métier et ses clients sur l'importance de la présence de la barre d'adresse verte et de l'utilisation de navigateurs sécurisés. « En matière de sécurité, VeriSign est un nom connu et réputé dans le monde entier. L'entreprise doit cette notoriété inégalée à sa capacité à fournir des solutions concrètes dans des environnements professionnels réels. Une sorte de tampon qui dirait "vous êtes en sécurité" ! », illustre Michael Valderrama, Directeur technique. « Internet est devenu une véritable jungle, et les clients doivent savoir lorsqu'ils sont en lieu sûr. Voilà pourquoi nous utilisons EV et plus particulièrement les certificats VeriSign. »
- **Courtiers d'assurances.** David Fitzgerald, DSI et Vice-président exécutif de CarInsurance.com, partage cet avis : « Nous nous devons d'assurer la sécurité des informations de nos clients. Mais il est tout aussi important de le communiquer clairement à nos clients. C'est là toute la mission du sceau VeriSign et de la barre d'adresse verte EV : la sérénité. »





CONCLUSION

Les services et la vente en ligne constituent des relais de croissance pour les entreprises de toutes tailles dans des secteurs d'activité très variés. Toutefois, un certain nombre d'exemples clients montrent que l'absence de certificats VeriSign® SSL EV peut compromettre cette opportunité de croissance. La cause ? Une réticence des consommateurs à effectuer des opérations en ligne, nourrie par la crainte de voir leurs informations personnelles tomber entre de mauvaises mains.

Les certificats VeriSign SSL EV permettent aux clients de se sentir en confiance lorsqu'ils communiquent leurs informations personnelles sur Internet. Pour les entreprises désireuses de concrétiser leur potentiel de croissance en ligne, ces certificats deviennent même incontournables.

EN SAVOIR PLUS

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

L'ENTREPRISE VERISIGN

VeriSign est le fournisseur d'infrastructure 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.

