***SÃ©curitÃ© : Certificats SSL, une explication simple et explicite by Symantec***
**Internet**
PostÃ© par : JPilo
PubliÃ©e le : 26/4/2013 13:30:00

Sur Internet les menaces sont courantes. Cheval de Troie, hameÃ§onnage, piratage,Â dÃ©tournement de domaine, logiciels espion, pourriels, rÃ©seau zombie ouÂ programmes malveillants sont autant de menaces lorsque vous naviguez surÂ internet.

Ces menaces suppriment des fichiers, se servent de votre ordinateur pour en pirater dâ□□autres, enregistrent vos mots de passe, noms dâ□□utilisateurs et autres informations personnelles, modifient le fonctionnement de votre ordinateur Ã votre insu, vous inondent de messages publicitaires ou vous redirigent vers des pages indÃ©sirables.

**De trÃ¨s grands rÃ©seaux ont d â□□ailleurs Ã©tÃ© piratÃ©s.**

â□¢ En 2001-2002, Gary Mc Kinnon sâ□□infiltre dans des ordinateurs de lâ□□US Army et de la NASA. Il sâ□□agirait du plus grand piratage informatique de tous les temps, avec des dÃ©gÃ¢ts qui sâ□□Ã©lÃ¨veraient Ã 1000 milliards de dollars.

â□¢ En 2008, le fabricant de cartes de crÃ©dit amÃ©ricain Heartland est piratÃ© et des donnÃ©es liÃ©es aux cartes de crÃ©dit de 134 millions de personnes sont volÃ©es.

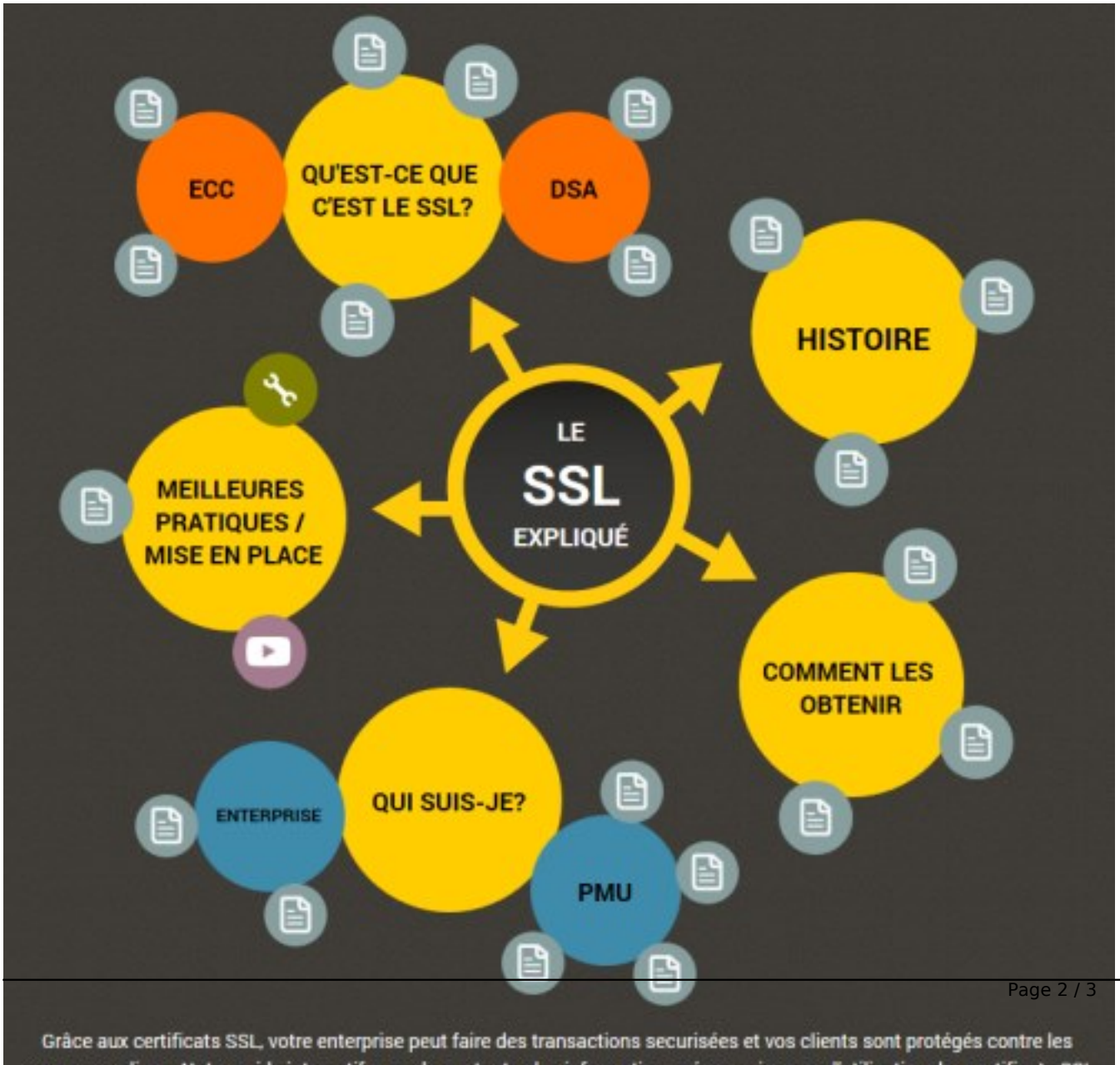
â□¢ En 2011, les donnÃ©es et identifiants de quelque 77 millions dâ□□utilisateurs utilisant le Playstation Network sont volÃ©s et Sony dÃ©cide dâ□□interrompre le rÃ©seau pendant quelques mois.

Tous les ans le rapport Internet Security Threat Report publie les chiffres ayant trait au piratage. Câ□□est dans lâ□□objectif de lutter contre ces menaces que la SSI (sÃ©curitÃ© des systÃ¨mes dâ□□information) a Ã©tÃ© Ã©laborÃ©e. La SSI garanti que les donnÃ©es matÃ©rielles ou logicielles sont utilisÃ©es Ã bon escient. Ainsi les donnÃ©es doivent Ãªtre intÃ¨gres, confidentielles et doivent pouvoir Ãªtre authentifiÃ©es. Dâ□□oÃ¹ les certificats SSL.

### Quâ□□est-ce quâ□□un certificat SSL et comment fonctionne-t-il ?

Le SSL ou Secure Socket Layer est la norme internationale en matiÃ¨re de sÃ©curitÃ© de site web qui permet de procÃ©der Ã  des transactions sur internet en toute sÃ©curitÃ©. Lâ□□objectif est dâ□□assurer Ã  lâ□□utilisateur quâ□□il est connectÃ© Ã  un site lÃ©gitime et de confiance, que les donnÃ©es Ã©changÃ©es nâ□□ont pas Ã©tÃ© interceptÃ©es par un tiers, ni corrompues et que le site ne pourra nier Ãªtre lâ□□Ã©metteur des messages reÃ§us. Ces objectifs sont tenus grÃ¢ce Ã  lâ□□utilisation de cryptage pour lâ□□Ã©change de donnÃ©es, ainsi que par lâ□□utilisation de certificats servant Ã  authentifier le site internet.

Les donnÃ©es sensibles Ã©changÃ©es sur le site sont chiffrÃ©es ou cryptÃ©es, les rendant illisibles en cas dâ□□interception par un tiers Ã©tranger au systÃ¨me. Le cryptage utilise des algorithmes Ã  clÃ©s asymÃ©triques (clef publique et clef privÃ©e) ainsi que symÃ©trique (clef de session). Les techniques de cryptage Ã  clefs asymÃ©triques font appel notamment aux algorithmes RSA, DSA ou encore ECC (Elliptic Curve Cryptography- Cryptographie sur courbe elliptique). La clef RSA est un algorithme brevetÃ© par le gouvernement amÃ©ricain et la DSA, elle, est employÃ©e dans le mÃªme but et utilise toutefois un algorithme diffÃ©rent. Enfin lâ□□ECC est une clef plus courte qui procure des performances accrues notamment en terme de sÃ©curitÃ© et de rapiditÃ©. Lâ□□authentification du site internet passe par lâ□□utilisation de certificat SSL dÃ©livrÃ© par une autoritÃ© de certification, qui garantit aux utilisateurs que le site est lÃ©gitime.



Les Infrastructures Ã  clefs publiques (PKI) dÃ©signent lâ□□ensemble des logiciels de chiffrement ainsi que toutes les procÃ©dures gÃ©rant les certificats, qui permettent entre autres dâ□□enregistrer, identifier et authentifier les utilisateurs ainsi que de gÃ©nÃ©rer, renouveler et publier les certificats.

## Pourquoi les PME ont-elles besoin de certificats SSL ?

Les certificats SSL sont prÃ©cieux pour les entreprises lorsquâ□□il sâ□□agit dâ□□effectuer des transactions en ligne. En effet, pour les acheteurs le critÃ¨re le plus important est la sÃ©curitÃ© du site internet. Ils doivent pouvoir faire confiance au site sur lequel ils effectuent leurs achats. GrÃ¢ce aux certificats SSL, les clients peuvent transmettre leurs donnÃ©es confidentielles en sachant pertinemment que ces informations ne seront pas accessibles Ã  une tierce personne. Un client potentiel se sent rassurÃ© en voyant quâ□□une PME utilise un certificat SSL, car cela signifie que le site est authentifiÃ©, vÃ©rifiÃ© et quâ□□il utilise un logiciel de chiffrement sÃ©curisÃ© des donnÃ©es. Bien souvent les grandes entreprises ont dÃ©jÃ  la rÃ©putation nÃ©cessaire pour attirer des clients, une petite structure, elle, aura dâ□□autant plus besoin de faire ses preuves pour gagner la confiance de clients potentiels. Outre le fait dâ□□avoir une boutique en ligne, certains sites requiÃ¨rent dâ□□autres informations confidentielles telles quâ□□un numÃ©ro de sÃ©curitÃ© sociale, numÃ©ro de carte dâ□□identitÃ© ou une date de naissance, ainsi il est prÃ©fÃ©rable pour les clients de savoir que ces informations sont protÃ©gÃ©es.

## Les diffÃ©rents certificats SSL Symantec

Symantec propose 5 certificats SSL allant du plus basique au plus complexe garantissant un niveau de sÃ©curitÃ© maximal (prix variant de 450 euros Ã  1499 euros) : Secure, SSL Wildcard, Secure Site Pro, Secure Site avec Extended validation et secure site pro avec extended validation. Tous ces certificats offrent entre autres une authentification complÃ¨te de lâ□□entreprise, une prise en charge des noms de domaines internationalisÃ©s, une dÃ©tection quotidienne des logiciels malveillants sur les sites web, le sceau Norton et un service client 7/24. Les certificats les plus Ã©laborÃ©s garantissent un niveau de chiffrement entre 128 et 256 bits et dispose de lâ□□extended validation dÃ©clenchant ainsi lâ□□apparition de la barre dâ□□adresse verte dans les navigateurs les plus sÃ©curisÃ©s. Pour les acheteurs en ligne, la barre dâ□□adresse verte, le sceau Norton et la technologie Seal-in Search sont synonymes de fiabilitÃ©.

Il est possible de recevoir gratuitement et instantanÃ©ment un certificat dâ□□essai pour une pÃ©riode de 30 jours. Une version dâ□□essai est valable pour les 5 certificats proposÃ©s.

**Voir l'infographie interactive.**