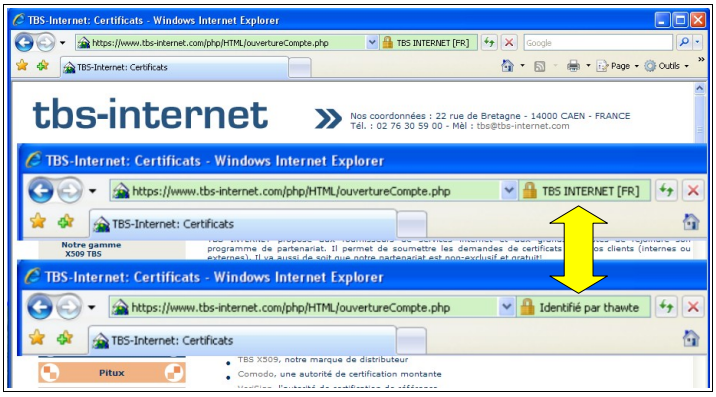
Le phishing est une technique qui vise à amener un utilisateur à communiquer des informations personnelles ou confidentielles sur un site internet imitant un site réputé fiable (banque, administration, etc.)

Problématique : comment vérifier que le site affiché est bien le site officiel ?	**Solution** : consulter la carte d'identité du site (=> le certificat électronique) avant de saisir quoi que ce soit !

Ce qu'il faut vérifier (a minima) : – Qui est le propriétaire du certificat – Qui a identifié le site (autorité de certification de confiance)	**Ce qu'il ne faut PAS faire :** – Saisir des informations sur un site sans SSL (https) – Poursuivre une connexion malgré un message d'avertissement

Avec Internet Explorer 7 :



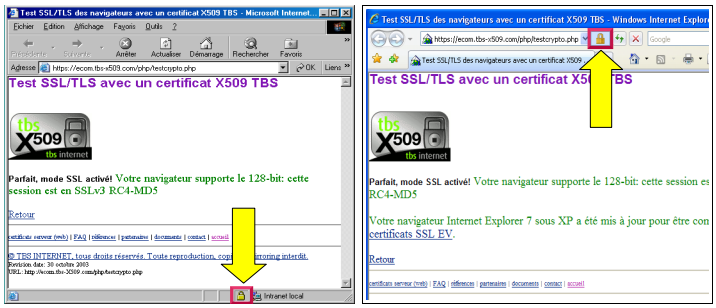
Avec Internet Explorer 7, **les sites hautement sécurisés affichent une barre d'URL verte** et un volet défilant comportant un cadenas doré contenant le propriétaire du site et l'autorité de certification. Le **certificat EV** active la barre verte ; c'est le plus haut niveau de sécurité SSL.

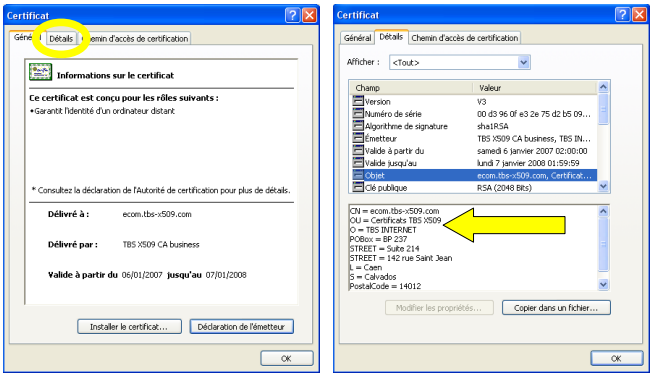
Si la barre verte apparaît, le site est sûr.

Avec Internet Explorer 5, 6, ou 7 :

Lorsque la barre d'URL reste blanche, **il faut vérifier le certificat représenté par le cadenas**. Avec IE7, il se trouve à coté de l'URL, cliquez dessus puis sur « afficher les certificats ».
Avec IE5 ou IE6, double-cliquez sur le cadenas qui se trouve en bas à droite.

Si vous ne trouvez pas le cadenas, le site n'est pas sécurisé, passez votre chemin !



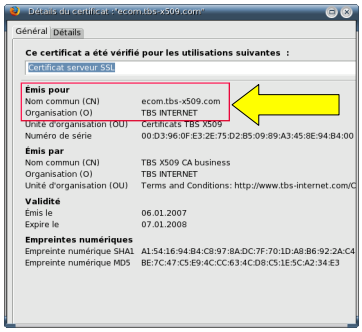


Il est nécessaire de vérifier que l'autorité de certification a bien certifié le propriétaire, en allant voir dans l'onglet « Détail » puis cliquer sur « Objet ». Vous devez vérifier le champ O.

Si le champ O contient le nom du site au lieu du nom du propriétaire, ou si le champ OU contient « domain validated », le propriétaire est inconnu, abandonnez votre connexion !

Avec Firefox :

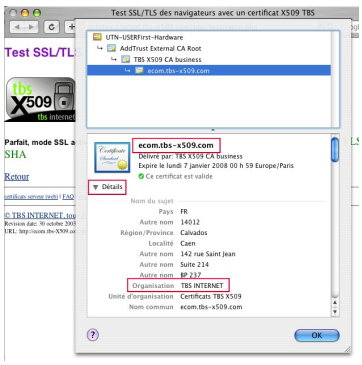
il faut vérifier le certificat représenté par le cadenas. Un double clic sur le cadenas (qui peut se trouver en bas de la fenêtre ou à la fin de l'URL), puis bouton « Afficher ».
Si vous ne trouvez pas le cadenas, le site n'est pas sécurisé, passez votre chemin !



Le propriétaire du site doit être l'entité affichée dans « Organisation (O) ».
Si le champ « Nom commun (CN) » et « Organisation (O) » sont identiques, le propriétaire est inconnu, abandonnez votre connexion !

Avec Safari :

Lors d'un accès sécurisé, un cadenas apparaît en haut à droite de la fenêtre . **Il faut cliquer sur le certificat** puis déplier la section « Détails ».
Si vous ne trouvez pas le cadenas, le site n'est pas sécurisé, passez votre chemin !



Le propriétaire du site doit être l'entité affichée dans « Organisation ».
Si le champ « Nom commun » (titre) et « Organisation » sont identiques, le propriétaire est inconnu, abandonnez votre connexion !

Quelle autorité de certification a délivré le certificat ?

Le phishing peut être efficacement combattu en développant les réflexes de vérification des utilisateurs et l'utilisation d'autorité de certification efficaces. **Mais toutes les autorités de certification ne se valent pas !**

TBS INTERNET, spécialiste des certificats électroniques avec plus de 10 ans d'expérience, commercialise et recommande l'utilisation des autorités ci-dessous, parce qu'elles appliquent des procédures de vérification strictes, qui garantissent que le propriétaire affiché dans le certificat a bien été audité.

VeriSign	Thawte	Comodo	TBS X509
VeriSign Secured VÉRIFIER	thawte it's a trust thing	C·O·M·O·D·O Creating Trust Online™	tbs X509 tbs internet

Pour évaluer vos besoins et mettre en place un certificat SSL de ces grandes marques sur vos sites, contactez TBS INTERNET sur http://www.tbs-certificats.com/ ou par téléphone au 02 76 30 59 00.