Le contrôle du certificat

Les certificats numériques sont utilisés pour chiffrer les connexions, de manière à ce que les utilisateurs aient la certitude d'être connectés au bon site web. Mais étant donné que les sites piratés en font également usage, il importe de vérifier leur authenticité, surtout lors des opérations d'e-banking.

Pour vous protéger,

- tapez toujours **manuellement l'adresse web (URL) de votre institut financier** dans la barre d'adresse du navigateur.
- accordez la juste attention aux **alertes** et aux **messages d'erreur** qui s'affichent lors de l'établissement de la connexion et n'hésitez pas à l'interrompre si nécessaire.
- assurez-vous que la barre d'adresse (URL) contient bien le symbole du **cadenas**.
- contrôlez que le certificat a effectivement été établi au **nom de l'institut financier** (celui-ci s'affiche en cliquant sur le cadenas, dans la fenêtre sous « Certificat émis pour : »).
- vérifiez que l'adresse web (URL) contient le nom de domaine correct de l'institut financier et qu'il est correctement orthographié (vous trouverez ici (https://www.ebas.ch/fr/structure-et-verification-dune-adresse-web/) de plus amples explications sur la manière dont est structurée une adresse web).
- ne saisissez vos **identifiants personnels de connexion** qu'une fois le contrôle du certificat terminé et s'il s'est avéré positif.

Les certificats : protection et danger

Lors de l'établissement de la connexion à un site donné, le navigateur contrôle automatiquement l'authenticité et la validité du certificat TLS/SSL. Si le test est positif, le site-cible s'affichera correctement et sans messages.

Or, il faut savoir que parmi les faux sites d'instituts bancaires utilisés par les hackers pour leurs attaques de phishing, de plus en plus sont dotés d'un certificat TLS/SSL valide. La procédure de vérification effectuée par le navigateur n'est donc pas suffisante pour pouvoir affirmer avec certitude que l'on a atterri sur le bon site.

D'où l'intérêt de toujours taper manuellement l'adresse web (URL) de l'institut financier dans la barre d'adresse du navigateur et de contrôler le certificat vous-même avant d'ouvrir une session d'e-banking !

Contrôle du certificat dans le navigateur

En règle générale, le navigateur ne doit afficher aucun message d'erreur lors du passage à une connexion sécurisée. Dans le cas contraire, cela signifie qu'il y a un problème de certificat ou de connexion et la connexion doit être immédiatement interrompue.

Ne forcez donc jamais manuellement l'établissement de la connexion en cas d'alertes ou de messages

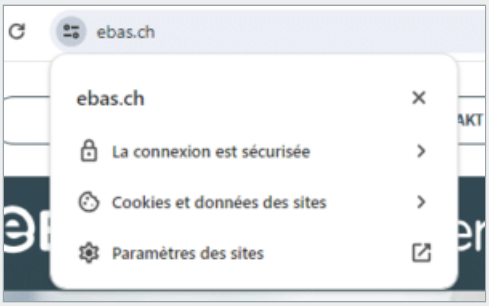
Copyright © 2024 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

d'erreur !

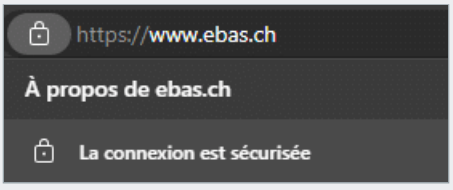
Une connexion TLS/SSL correctement établie – soit une connexion sécurisée – menant au site web souhaité, et basée sur un certificat valide et authentique, se reconnait grâce à la présence des trois éléments suivants :

1. **Symbole du cadenas dans la barre d'adresse**
   La connexion a été chiffrée à l'aide d'un certificat TLS/SSL valide.
2. **Nom de l'institut financier correct (il peut être affiché en cliquant sur le cadenas dans la fenêtre qui apparaît sous « Certificat émis pour : »)**
   L'identité du titulaire du certificat (la banque) est ainsi confirmée.
3. **L'adresse web (URL) porte le bon nom de domaine et ce dernier est correctement orthographié**
   Vous êtes bien sur le site web de l'institut financier.
   Pour plus d'informations sur la structure d'une adresse web (URL), cliquez ici (https://www.ebas.ch/fr/structure-et-verification-dune-adresse-web/) .

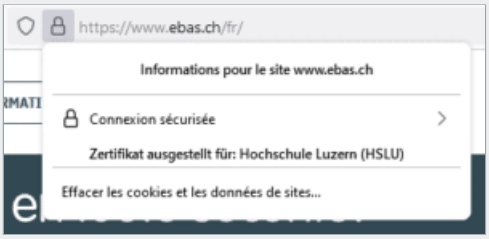
Google Chrome:



Microsoft Edge:

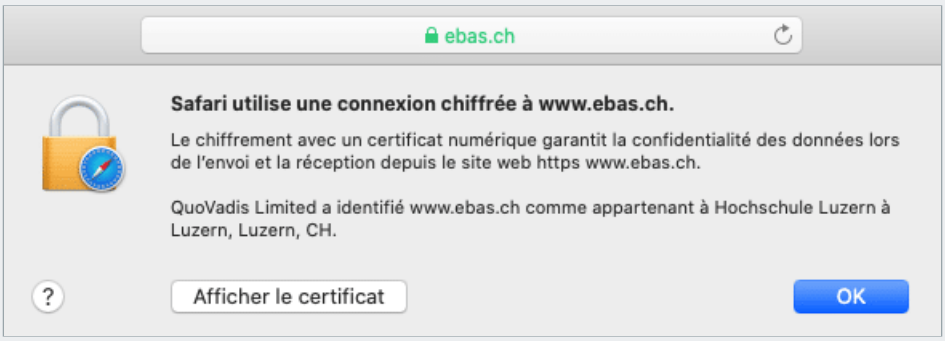


Mozilla Firefox:



Apple Safari:

Copyright © 2024 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique



La représentation graphique de ces éléments peut être légèrement différente d'un navigateur à l'autre. Consultez nos modes d'emploi (https://www.ebas.ch/fr/controle-du-certificat-du-navigateur/) pour retrouver ces éléments dans les principaux navigateurs.

Contrôle du certificat par vérification de l'empreinte numérique

Il existe également une méthode manuelle, plus compliquée mais aussi plus sûre, pour vérifier l'authenticité d'un certificat. Il s'agit de vérifier que l'« empreinte » (fingerprint) affichée par le navigateur correspond à l'empreinte publiée par l'institut financier.

Quittez la page si l'empreinte numérique ne peut pas être vérifiée !

Vous trouverez sur le site de « eBanking – en toute sécurité ! » les empreintes numériques des pages de connexion e-banking (https://www.ebas.ch/fr/lempreinte-numerique-dun-certificat/) de nos banques partenaires, ainsi que des modes d'emploi (https://www.ebas.ch/fr/controle-du-certificat-du-navigateur/) détaillés pour vérifier l'empreinte numérique dans les différents navigateurs.

Dans le cadre des opérations d'e-banking, le certificat numérique sert à garantir l'authenticité du serveur auquel l'utilisateur se connecte, et à chiffrer la communication avec le serveur. Cette technologie fait appel au protocole TLS/SSL. On parle donc de certificats TLS/SSL et de connexions TLS/SSL.

En quelques clics, vous pouvez vérifier si la connexion est effectivement protégée ou non.

Copyright © 2024 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

Pour aller plus loin

Principe de fonctionnement d'une connexion TLS/SSL

Les connexions sécurisées avec un serveur web utilisent généralement le protocole TLS/SSL, une technologie de communication permettant de chiffrer les données transmises pour empêcher leur interception, tout en garantissant l'authenticité et donc l'identité du serveur de connexion.

Cette protection est assurée par ce que l'on appelle un certificat numérique. Chaque certificat est émis par une autorité de confiance appelée « autorité de certification » pour un serveur web donné.

Sachant que la sécurisation et l'identité du serveur ne peuvent être garanties que si le certificat assurant la connexion TLS/SSL est authentique et valide, on comprend bien l'importance que revêt le contrôle du certificat.

Vérification du certificat via le navigateur

À chaque fois qu'une connexion TLS/SSL est établie, le navigateur procède à une vérification du certificat et en particulier des propriétés suivantes :

- fiabilité de l'émetteur du certificat : le certificat a été établi par une autorité de certification fiable (c.a.d. signé numériquement). Cette vérification permet d'attester l'authenticité du certificat.
- validité du certificat : le certificat n'a pas expiré ou l'autorité de certification ne l'a pas révoqué avant la date d'expiration de sa validité.
- adresse du serveur web : l'adresse du serveur indiquée dans le certificat correspond effectivement à l'adresse portée dans la barre d'adresse du navigateur.

Ce n'est qu'après la vérification de ces trois éléments que le navigateur peut établir la connexion TLS/SSL sans afficher de message d'erreur.

Le contrôle des propriétés décrites plus haut par le navigateur offre un niveau élevé de sécurité. Toutefois, le système ne permet pas d'identifier les certificats qu'une autorité de certification aurait délivré à un cybercriminel suite à un examen trop sommaire du dossier de demande. De rares cas de fraude de ce genre sont devenus célèbres.

Dans la mesure où le hacker choisira probablement pour son certificat une adresse différente de celle du site visé par l'attaque (par ex. un institut financier), il est possible de reconnaître ces certificats abusifs en vérifiant l'adresse web (URL) affichée dans la barre d'adresse du navigateur.

Il revient ensuite à l'utilisateur de vérifier si le nom de domaine de l'adresse appartient effectivement à l'organisme à contacter (p. ex. un institut financier). Dans de nombreux navigateurs, cette partie de l'adresse est souvent mise en évidence graphiquement afin de faciliter le contrôle (p. ex. en gras ou en noir).

Vérification du certificat par comparaison de l'empreinte numérique

Chaque utilisateur d'une connexion TLS/SSL peut contrôler manuellement l'authenticité du certificat qui lui est associé en vérifiant l'empreinte numérique du certificat.

L'empreinte numérique est une suite de caractères formée par des lettres de A à F (sans distinction entre majuscules et minuscules) et des chiffres de 0 à 9.

Pour vérifier l'empreinte numérique, on compare cette suite de caractères avec une suite de référence que l'utilisa-

Copyright © 2024 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

teur aura obtenue de l'établissement financier. Si la suite de caractères lue dans le certificat est identique à celle communiquée par l'institut financier, le certificat est authentique.

Si l'on part du principe que la chaîne de caractères annoncée par la banque est authentique, la vérification manuelle de l'empreinte numérique est le moyen le plus sûr de contrôler le certificat.

Il est également utile de contrôler l'adresse web (URL), comme décrit plus haut pour le contrôle du certificat via le navigateur.

Copyright © 2024 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique