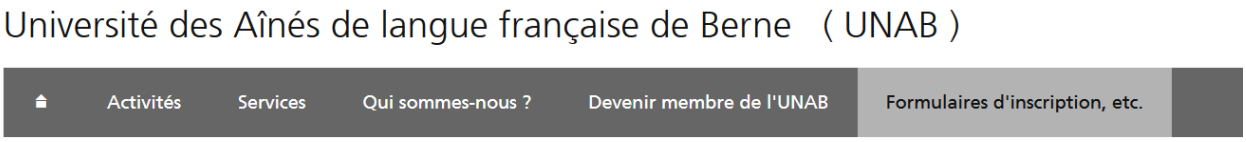
Problème d'accès à un formulaire UNAB

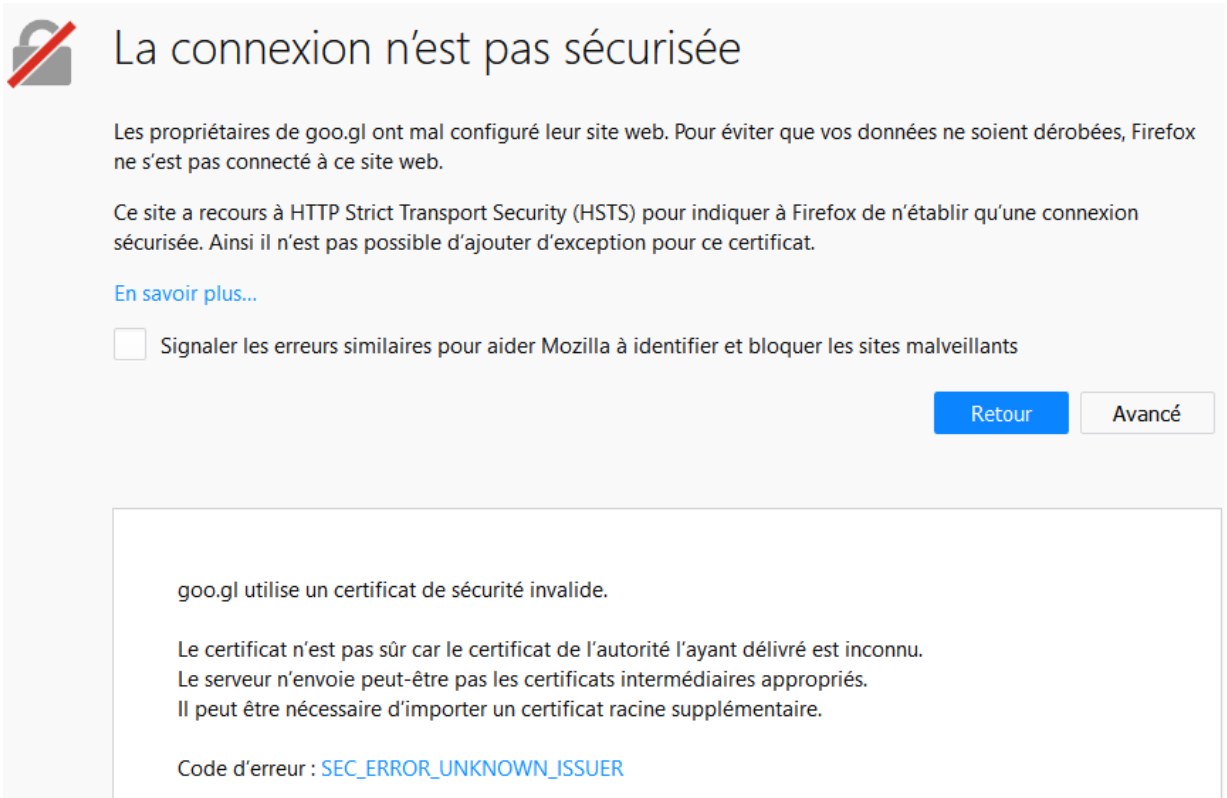
Par exemple à l'appel d'un formulaire par clic sur le bouton tout à droite du menu principal du site, à savoir :



Sous

N.B. : Que **Firefox** Quantum soit en version 32 bits ou 64 bits ne change rien au contenu de cette note.

Il se peut que l'on obtienne :



Comment régler le problème quand on reçoit le message d'erreur "SEC_ERROR_UNKNOWN_ISSUER" après avoir cliqué sur le bouton « Avancé »
https://support.mozilla.org/fr/kb/comment-regler-probleme-quand-message-erreur-sites-securises?as=u&utm_source=inproduct

Sur les sites web qui sont censés être sécurisés (c'est-à-dire quand l'adresse commence par « https:// »), Firefox doit vérifier que le certificat de sécurité présenté par le site web est valide. Si le certificat ne peut pas être validé, Firefox suspendra la connexion au site web et affichera ce message d'erreur : « La connexion n'est pas sécurisée ». La suite de cet article explique pourquoi le message d'erreur « SEC_ERROR_UNKNOWN_ISSUER » s'affiche sur certains sites web et comment résoudre le problème.

Table des matières

Que signifie ce message d'erreur ?
Au cours d'une connexion sécurisée, un site web doit présenter un certificat fourni par une autorité de certification authentifiée pour prouver que l'utilisateur est bien connecté à la page cible désirée et que la connexion est chiffrée. Si la page d'erreur « Votre connexion n'est pas sûre » apparaît et que vous voyez le message « SEC_ERROR_UNKNOWN_ISSUER » après avoir cliqué sur Avancé, cela signifie que le certificat a été fourni par une autorité de certification inconnue et que Firefox ne peut pas l'authentifier.

La même erreur se produit sur plusieurs sites sécurisés
Si vous rencontrez ce problème sur plusieurs sites HTTPS sans lien entre eux, cela signifie que votre connexion est interceptée et reçoit des certificats refusés par Firefox. L'interception vient souvent de logiciels analysant les connexions chiffrées ou de logiciels malveillants qui remplacent les certificats des sites légitimes par les leurs.

Logiciels antivirus
Un logiciel antivirus propose généralement une fonction d'analyse de connexions chiffrées. Le réinstaller pourra lui permettre de réinscrire ses certificats dans le magasin de certificats de confiance de Firefox. Vous pouvez également essayer les démarches suivantes pour ces logiciels particuliers :

Avast
Vous pouvez désactiver l'interception des connexions sécurisées :
1. Ouvrez le tableau de bord d'Avast.
2. Allez à Paramètres > Protection active et cliquez sur Personnaliser à côté d'Agent Web
3. Désélectionnez Autoriser l'analyse HTTPS puis confirmez en cliquant sur OK
Pour plus d'informations à propos de cette fonctionnalité, consultez cette page du blog Avast.

Bitdefender
Vous pouvez désactiver l'interception des connexions sécurisées :
1. Ouvrez le tableau de bord de Bitdefender.
2. Pour la version *2016*, cliquez sur Modules. Pour la version *2015*, cliquez sur Protection
3. Cliquez sur Protection Web
4. Désactivez Scan SSL
Pour tous les produits Bitdefender, consultez la page d'assistance de Bitdefender.

Bullguard

Avec les logiciels de sécurité Bullguard, vous pouvez désactiver l'interception de connexions sécurisées sur certains sites particuliers (par exemple les sites web majeurs tels que Google, Yahoo et Facebook) :

1. Ouvrez le tableau de bord de votre application Bullguard.
2. Cliquez sur Paramètres antivirus > Navigation
3. Décochez l'option Afficher les résultats sans risque pour les sites web qui affichent ce message d'erreur.

ESET

Avec les produits de sécurité ESET, vous pouvez essayer de désactiver et réactiver le filtrage du protocole *SSL/TLS* ou de désactiver l'interception des connexions sécurisées, comme il est décrit dans l'article d'assistance d'ESET.

Kaspersky

Dans les produits de sécurité Kaspersky, vous pouvez désactiver l'interception des connexions sécurisées :

1. Ouvrez le panneau de contrôle de votre logiciel Kaspersky.
2. Cliquez en bas à gauche sur « Configuration ».
3. Cliquez dans le menu de gauche sur « Avancé », puis à droite sur « Réseau ».
4. Si vous utilisez une version *2016* des produits de sécurité Kaspersky : dans la section « Analyse des connexions chiffrées (HTTPS) », cochez l'option « Ne pas analyser les connexions chiffrées » et confirmez ce changement en cliquant sur « Continuer ».
   Autrement, vous pouvez aussi cliquer sur Paramètres avancés pour essayer de déclencher une réinstallation du certificat de Kaspersky. Dans la fenêtre de dialogue qui s'ouvre, cliquez sur Installer le certificat… et suivez les instructions à l'écran.
   Pour la version 2015*, décochez l'option Scanner les connexions chiffrées.*
5. Enfin, fermez correctement Kaspersky et redémarrez votre système pour que les modifications prennent effet.

Les utilisateurs d'une **version antérieure** de Kaspersky qui ont un abonnement en cours ont la possibilité de mettre à niveau pour obtenir la toute dernière version du produit, qui est disponible au téléchargement et à l'installation sur la page des mises à jour des produits Kaspersky. Il suffira ensuite de suivre les étapes décrites plus haut.

Les paramètres du Contrôle parental avec les comptes Windows

Dans les comptes Microsoft Windows protégés par les paramètres de Contrôle parental, les connexions sécurisées sur les sites web populaires comme Google, Facebook et YouTube peuvent être interceptées et leurs certificats remplacés par un certificat fourni par Microsoft pour filtrer et enregistrer l'historique des recherches. Consultez cette page de FAQ de Microsoft pour savoir comment désactiver ces fonctions parentales pour les comptes. Dans le cas où vous souhaitez installer manuellement les certificats manquants pour les comptes concernés, référez-vous à cet article du support Microsoft.

Contrôle/filtrage sur les réseaux d'entreprise

Certains produits de contrôle/filtrage du trafic utilisés dans les environnements d'entreprise peuvent intercepter les connexions sécurisées en remplaçant un certificat de site web par le leur, ce qui déclenche en même temps des erreurs sur les sites sécurisés HTTPS. Si vous pensez que ça pourrait être le cas, veuillez contacter votre direction informatique pour obtenir la bonne configuration de Firefox pour lui permettre de fonctionner correctement dans ce type d'environnement, car le certificat nécessaire pourrait devoir être d'abord placé dans le magasin des certificats de confiance de Firefox.

Logiciel malveillant

Certains types de logiciels malveillants qui interceptent le trafic web chiffré peuvent provoquer ce message d'erreur. Référez-vous à l'article Résoudre des problèmes de Firefox causés par des logiciels malveillants pour savoir comment résoudre les problèmes dus à des logiciels malveillants.

L'erreur apparaît sur un site particulier uniquement

Dans le cas où vous rencontrez ce problème sur un site en particulier, ce type d'erreur indique en général que le serveur web n'est pas configuré correctement. Toutefois, si vous voyez cette erreur sur un site web important et légitime tel que Google ou Facebook, ou sur des sites où des transactions financières se déroulent, vous devriez poursuivre en suivant les étapes exposées ci-dessus.

Certificat émis par une autorité appartenant à Symantec
Après qu'ont été mises en lumière de nombreuses irrégularités avec des certificats émis par des autorités racines Symantec, des fournisseurs de navigateurs, parmi lesquels Mozilla, suppriment progressivement de leurs produits leur confiance en ces certificats.
Pour commencer, Firefox 60 ne se fiera plus aux certificats chaînés aux autorités racines Symantec (ce qui inclut toutes les marques de Symantec : GeoTrust, RapidSSL, Thawte et VeriSign) qui ont été émis avant le 01/06/2016. Dans Firefox 63, ce retrait de confiance sera élargi à tous les certificats émis par Symantec sans tenir compte de leur date d'émission.

MOZILLA_PKIX_ERROR_ADDITIONAL_POLICY_CONSTRAINT_FAILED sera la principale erreur, mais, avec quelques serveurs, vous pourrez voir le code d'erreur **SEC_ERROR_UNKNOWN_ISSUER** à sa place. Dans tous les cas, si vous rencontrez un tel site, vous devriez contacter les propriétaires du site web pour les informer du problème. Nous encourageons fortement les opérateurs des sites affectés de prendre immédiatement des mesures pour remplacer ces certificats.
Pour davantage d'informations sur ce problème, consultez l'article du blog de Mozilla
Retrait de la confiance envers les certificats TLS émis par Symantec (en anglais).

Certificat intermédiaire manquant
Sur un site auquel il manque un certificat intermédiaire vous verrez la description d'erreur suivante après avoir cliqué sur le bouton Avancé sur la page d'erreur de « Connexion non sécurisée » :
Le certificat n'est pas sûr car l'autorité délivrant le certificat est inconnue.
Le serveur n'envoie peut-être pas les certificats intermédiaires appropriés.
Il peut être nécessaire d'importer un certificat racine supplémentaire.
Le certificat du site web pourrait ne pas avoir été émis par une autorité de certification fiable et aucune chaîne de certificat vérifiée par une autorité fiable n'a été fournie (ce que l'on appelle un « certificat intermédiaire » est manquant).

Vous pouvez tester si un site est correctement configuré en saisissant une adresse web dans un service tiers comme la page de test du SSL Labs. Si le message qui est renvoyé est : « Problèmes de chaîne : Incomplète », cela signifie qu'une certification intermédiaire fait défaut. Vous devriez contacter les propriétaires du site web et les informer de ce problème.

Certificats auto-signés
Sur un site qui utilise un certificat auto-signé vous verrez apparaître l'avertissement d'erreur suivant après avoir cliqué sur Avancé sur la page d'erreur « Connexion non sécurisée » :
Le certificat n'est pas sûr car il est auto-signé.
Un certificat auto-signé qui n'a pas été émis par une autorité de certification est considéré comme non fiable par défaut. Les certificats auto-signés peuvent sécuriser vos données par rapport aux oreilles indiscrètes, mais ne disent rien sur les destinataires des données que vous communiquez. C'est courant pour les sites web en intranet qui ne sont pas disponibles publiquement et vous pouvez ignorer l'avertissement pour de tels sites.

Ignorer l'avertissement
Attention : vous ne devriez jamais ajouter d'exception de certificat pour un site majeur légitime ou des sites qui proposent des transactions financières. Dans ce cas, un certificat invalide peut signaler que votre connexion est dangereusement compromise par une tierce partie.
Si le site web le permet, vous pouvez ajouter une exception pour visiter le site, dans le cas où son certificat n'est pas reconnu par défaut :

1. Sur la page d'avertissement, cliquez sur Avancé
2. Cliquez sur Ajouter une exception… La boîte de dialogue *Ajouter une exception* apparaît.
3. Lisez le texte décrivant les problèmes rencontrés avec le site web. Vous pouvez cliquer sur Voir… pour inspecter de plus près le certificat non reconnu.
4. Cliquez sur Confirmer l'exception de sécurité si vous êtes sûr que vous faites confiance au site.

Partagez cet article : http://mzl.la/2429Jqu
Ces formidables personnes ont aidé à écrire cet article : Goofy, Banban, Mozinet, Imen, Abbackar DIOMANDE, Macbetha, YD.
Vous pouvez également aider - découvrez comment.

++

Surprise éventuelle à l'appel d'un formulaire :

Alors que l'appel à partir d'un PC x présente le problème décrit ci-dessus,
le même appel à partir d'un PC y présente par exemple ce qui suit :

Ce même résultat apparaît chez d'autres internautes, également avec le navigateur MS Edge/Internet Explorer.
Ce résultat serait normal si l'on avait dépassé le délai d'inscription, ou alors c'est que le nombre maximum de participants a été atteint, ou que le cours/séminaire ou l'excursion a été annulé(e).

Par contre, sur les deux PC x et y,
si l'on clique sur le lien « Devenir membre de l'UNAB »,
tout le formulaire d'adhésion à l'UNAB est disponible et semble fonctionner parfaitement.

Dans un tel cas, il y a, *momentanément*, 2 problèmes distincts touchant des responsables différents :

1° Le problème de connexion qui n'est pas sécurisée sur le PC x.
Dans ce cas, il appartient à l'internaute de revoir ses réglages/paramétrages de Mozilla Firefox et/ou de l'antivirus installé sur l'appareil utilisant ce navigateur Internet (voir les solutions proposées ci-devant).

2° Celui de l'accès au formulaire d'inscription et donc l'impossibilité de répondre audit formulaire sur les 2 PC.
Dans ce cas, le problème se situe au niveau de la relation Google avec ledit formulaire ; c'est alors le créateur dudit formulaire qu'il faut contacter. Un nouveau formulaire peut devoir être créé et pour lequel une nouvelle adresse Internet devra sans doute être communiquée au webmaster du site à partir duquel ce formulaire doit pouvoir être appelé.

Juin 2018 / Chs Christen, webmaster de www.unab.unibe.ch