Barre de confiance

Présentation

Complément indispensable de l'identification renforcée, la **Barre de confiance** est une barre d'outils destinée à combattre le risque de piratage sur Internet en vous indiquant de façon visible si vous vous trouvez sur un site du groupe Crédit Mutuel-CIC.
Elle est disponible pour Internet Explorer sous Windows et pour Firefox sous Windows, Macintosh et Linux.

Ainsi, avant de vous identifier, vous prendrez l'habitude de vérifier que la barre vous en donne le feu vert.

La barre de confiance se présente sous la forme d'une zone de texte et d'un bouton déroulant un menu. L'icône présente sur ce bouton diffère selon le site sur lequel vous vous trouvez.


Vous êtes sur un site Crédit Mutuel


Vous êtes sur un site CIC


Vous êtes sur un site CM - CIC


Vous êtes sur un site faisant partie de vos domaines de confiance *(Internet Explorer uniquement)*


Vous êtes sur Internet ou sur un fichier local de votre ordinateur


Vous êtes sur une page suspecte


La page demandée est en cours de chargement

Comme illustré ci-dessus, si vous êtes sur un site sécurisé (http**s** au lieu de http), un cadenas figure à droite du bouton de la barre de confiance.

À la droite de l'icône figure le nom de domaine du site sur lequel vous vous trouvez.
Si celui-ci fait partie des domaines de confiance, il apparaît sur fond vert ou bleu.
Si la page affichée a été déterminée comme suspecte ou si des éléments suspects ont été détectés sur votre ordinateur, un message clignotant sur fond rouge vous en informe et une icône « Sens Interdit » figure à sa gauche. Ceci ne concerne que nos sites de banque à distance.

Le domaine ne fait pas partie des domaines de confiance.

Le domaine fait partie des domaines de confiance.

La page affichée est considérée comme suspecte.

Certains éléments présents sur votre ordinateur sont considérés comme suspects.

QUE FAIRE EN CAS DE PAGE SUSPECTE ?	Au cours de votre navigation sur nos sites bancaires, si la barre vous affiche le message clignotant ci-dessus accompagné de l'icône « Sens Interdit », votre ordinateur est vraisemblablement victime d'un virus ayant corrompu le code de la page. 1. Si ce n'est déjà fait, installez un anti-virus. 2. Faites une mise à jour de la base de données de votre anti-virus.

	3. Lancez une vérification de votre disque dur. **En aucun cas vous ne devez saisir d'information (identifiant, codes de votre carte de clés personnelles…) ou valider une telle page.**

IMPORTANT	**Les contrôles effectués par la barre de confiance ne concernent que la page affichée dans la fenêtre du navigateur liée à la barre. En aucun cas, ces contrôles ne concernent les éventuelles fenêtres surgissantes (ou *pop-up*) ouvertes par la page principale.** Avec Internet Explorer, si une fenêtre surgissante est affichée sans que les différentes barres d'outils soient visibles, vous devez visualiser ces dernières en mode « Plein écran », accessible en appuyant sur la touche F11 du clavier.

À SAVOIR	**La barre de confiance ne s'affiche pas sous Internet Explorer ?** Allez dans le menu « Affichage > Barres d'outils » d'Internet Explorer et sélectionnez « Barre de confiance ». **Avec Internet Explorer 7** Allez dans le menu « Outils > Gérer les modules complémentaires > Activer ou désactiver les modules complémentaires ». Dans la fenêtre affichée, activez les extensions « Barre de confiance » et « BHO Barre de confiance » en cliquant dessus puis sur le bouton-radio « Activer » de la rubrique « Paramètres ». Allez dans le menu « Outils > Barre d'outils », à droite des onglets, et sélectionnez « Barre de confiance ».

Qu'est-ce que le « *phishing* » ?

Le « *phishing* » est une technique utilisée par des pirates qui consiste à envoyer au hasard un courrier électronique frauduleux en se faisant passer pour une banque ou une société de commerce électronique réputée. Ce courriel vous invite à vous identifier ou à faire un achat en cliquant sur un lien qui vous route sur un site « pirate » identique au site de cette banque ou de cette société dans le but de subtiliser vos informations personnelles (codes d'accès, numéro de carte bancaire…).

La **Barre de confiance** vous permettra de détecter que vous vous trouvez sur un site ne faisant pas partie du groupe Crédit Mutuel – CIC ou, si vous utilisez Internet Explorer, ne figurant pas dans la liste de vos sites de confiance.

Si vous êtes un jour victime d'une tentative de « *phishing* » ne saisissez aucune information personnelle et n'hésitez pas à nous le signaler.

En outre, certains virus informatiques espionnent les touches de votre clavier ou, cachés en amont de votre navigateur Internet, injectent du code dans la page Web que vous avez demandée. Il est donc primordial de disposer d'un anti-virus actif et régulièrement mis à jour.

À RETENIR	**Pour accéder à vos comptes, ne saisir votre identifiant et votre mot de passe que :** - si la barre de confiance affiche l'icône Crédit Mutuel ou CIC, - si le cadenas est présent, - si le nom de domaine est sur fond vert ou bleu.

Qu'est-ce qu'un "domaine de confiance" ?

Un site Internet possède un nom de domaine qui permet de l'identifier.

Par "domaine de confiance", on entend tout nom de domaine sur lequel vous pouvez saisir des informations personnelles en toute sécurité.

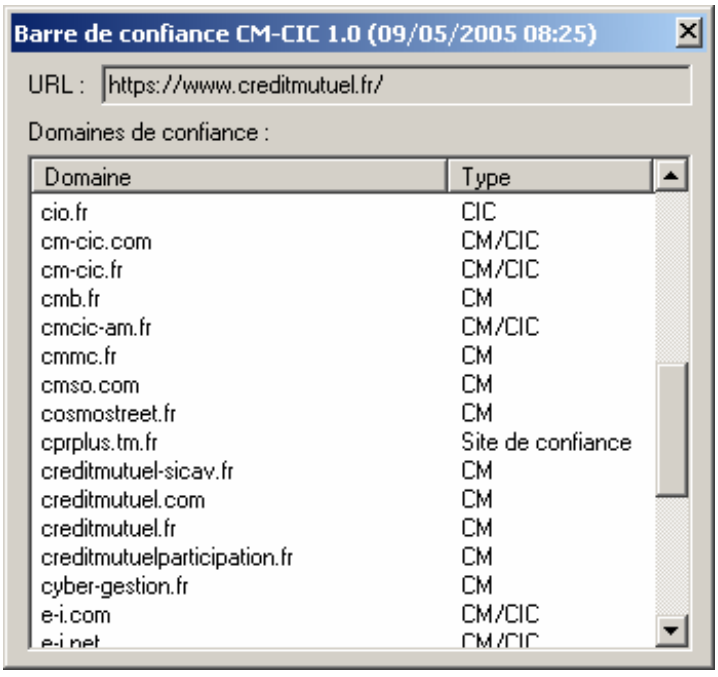
La **Barre de confiance** utilise deux types de domaines de confiance :

- plusieurs domaines intégrés à l'application : il s'agit des principaux noms de domaines des sites Crédit Mutuel et CIC. Si vous êtes sur un tel domaine, la barre l'affichera sur un fond vert.
- Avec la version dédiée à Internet Explorer, des domaines obtenus à partir de la liste de vos sites de confiance (menu "Outils > Options Internet..." puis onglet "Sécurité" et icône "Sites de confiance"). Si vous êtes sur un tel domaine, la barre l'affichera sur un fond bleu.

Avec Internet Explorer, vous pouvez facilement ajouter des noms de domaines dans la liste de confiance : par exemple vos sites de commerce électronique préférés… Ils seront alors reconnus par la **Barre de confiance**.
Cette fonctionnalité n'est pas disponible avec la version Firefox.

Bouton et menu de la Barre de confiance

Un clic sur l'icône de la barre ou la sélection du menu « Domaines de confiance… » ouvre la fenêtre qui donne la liste des sites Crédit Mutuel et CIC, intégrée à l'application :



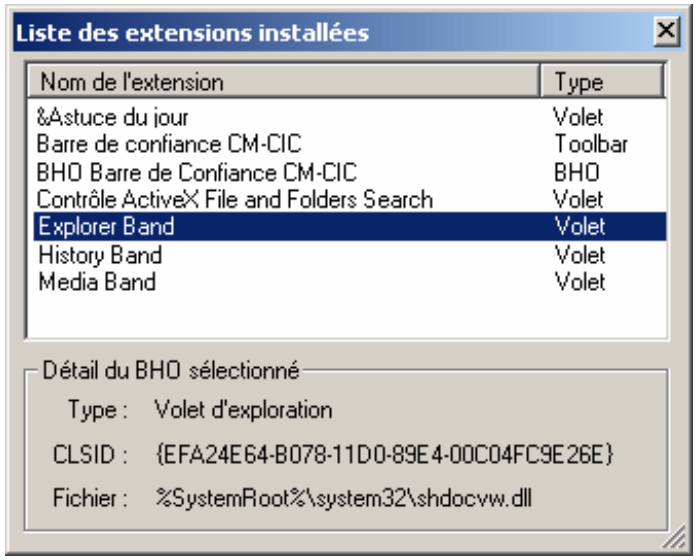
Dans la version pour Internet Explorer, l'URL affichée est l'adresse du site Internet sur lequel vous vous trouvez. Cette URL peut être différente de l'URL affichée par le navigateur suite à une redirection*.

La liste des domaines de confiance affichée sur votre ordinateur, peut différer de celle figurant sur cette copie d'écran.

** Une redirection consiste à rediriger les requêtes concernant une page Internet vers une autre page Internet.*

Le menu déroulant permet également d'afficher le certificat de sécurité du site sur lequel vous vous trouvez si celui-ci est en HTTPS.
Cette fonctionnalité n'est pas disponible dans la version Firefox.

Dans la version pour Internet Explorer uniquement, le menu "Liste des extensions installées…" vous permet d'afficher l'ensemble des extensions greffées à ce navigateur, qu'elles soient d'origine ou installées par après.
Par extension, on entend tout type de module complémentaire venant enrichir Internet Explorer, tels que les volets d'exploration (la fenêtre affichant l'historique, par exemple), les barres d'outils ou encore les BHO (*Browser Helper Object*), des greffons pas nécessairement visibles mais pouvant potentiellement espionner ce qui transite par le navigateur.



En cliquant sur l'une de ces extensions dans la liste, vous obtenez quelques informations supplémentaires, notamment le nom du fichier et son emplacement, informations pouvant se révéler utiles si vous avez des doutes concernant une extension.
Notez que la Barre de confiance installe un BHO permettant de gérer son affichage dans Internet Explorer.

Une autre ligne de menu donne accès à ce document d'aide.

Que faire en cas de courrier non sollicité de type phishing ?

- La première règle consiste à ne pas ouvrir les courriers électroniques suspects, dont l'expéditeur vous est inconnu ou dont le sujet vous paraît farfelu.
- Ne cliquez jamais dans les liens figurant dans un courrier électronique.
- Ne répondez jamais à ce type de message, y compris pour vous plaindre ou demander votre désabonnement.
- Avertissez-nous immédiatement.

Plus d'informations sur le *phishing* sont disponibles sur le site de Microsoft :

`http://www.microsoft.com/france/securite/gpublic/spam/phishing.mspx`

Rappel de quelques règles de sécurité

- Utilisez un logiciel anti-virus et un pare-feu (*firewall*).
- Mettez à jour régulièrement votre système d'exploitation, votre navigateur Internet et votre anti-virus.
- Ne cliquez jamais sur un lien figurant dans un courrier électronique.
- Déconnectez-vous de votre site bancaire en utilisant le lien adéquat.

- Ne saisissez votre identifiant et votre mot de passe que si la page est sécurisée (icône en forme de cadenas) et si la **Barre de confiance** vous en donne le feu vert.
- Ne communiquez jamais à quiconque votre mot de passe. Celui-ci ne vous sera jamais demandé par nos services, que ce soit par courrier électronique ou par téléphone.
- Changez régulièrement de mot de passe.

Comment désinstaller la Barre de Confiance ?

Pour Internet Explorer :

1. Allez dans le menu « Démarrer > Paramètres > Panneau de configuration » de Windows.
2. Choisissez « Ajout/Suppression de programmes ».
3. Cliquez sur « Barre de Confiance » puis sur le bouton « Supprimer ».

Pour Firefox :

1. Lancez Firefox.
2. Allez dans le menu « Outils > Extensions ».
3. Cliquez sur « Barre de Confiance » puis sur le bouton « Désinstaller ».

Un peu de vocabulaire…

Dans ce document, certains termes peuvent nécessiter une définition :

Phishing **:**	Il s'agit de la contraction des mots anglais « *fishing* », pêche, et « *phreaking* », signifiant piratage de lignes téléphoniques. Des sites miroirs semblables à des portails de renom (banques, sites d'enchères…) sont créés puis les internautes sont arrosés au hasard avec un courrier non sollicité (*spam*) qui reprend à son tour l'habillage graphique du portail détourné. Le but du jeu est alors d'attirer un internaute réellement client du site plagié. Ce *spam* invite l'internaute à se rendre sur le faux site pour mettre à jour certains renseignements personnels dans un questionnaire tout aussi faux. L'internaute ainsi dupé laisse ses identifiants de connexion et mots de passe, son numéro de compte bancaire et parfois de carte de crédit. Le *phishing* est aussi appelé *brand spoofing* ou *carding*. (http://www.journaldunet.com/encyclopedie/definition/591/33/21/phishing.shtml)
Domaine (ou Nom de domaine) :	C'est l'adressage d'un serveur sur Internet, géré par d'autres serveurs appelés *Domain Name Server* (DNS). Exemple : creditmutuel.fr ou cic.fr
URL :	*Uniform Ressource Locator* Il s'agit de l'adresse d'une ressource Internet (page Web ou fichier quelconque) et du chemin à suivre pour y accéder. L'URL de *Cyber*MUT est : `https://www.creditmutuel.fr/` L'URL de Filbanque est : `https://www.cic.fr/`