Barre de Confiance

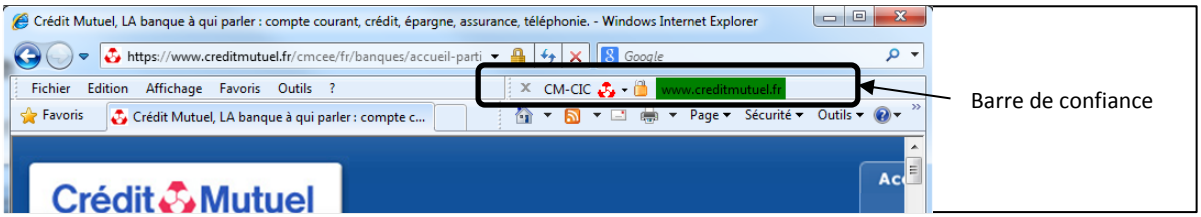
Présentation

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, pour Firefox sous Windows, Macintosh et Linux, pour Google Chrome sous Windows

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 Internet ou sur un fichier local de votre ordinateur	Vous êtes sur une page suspecte	La page demandée est en cours de chargement

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.
Si la page affichée est considérée comme une tentative de *phishing*, un message sur fond rouge vous en informe et la page est également bloquée par un message d'alerte.

CM-CIC www.creditmutuel.fr Le domaine fait partie des domaines de confiance	CM-CIC www.google.fr Le domaine ne fait pas partie des domaines de confiance	CM-CIC ATTENTION ! Tentative de phishing suspectée La page affichée est suspectée d'être une tentative de *phishing*
CM-CIC Chargement en cours... La page est en cours de chargement		

QUE FAIRE EN CAS DE TENTATIVE DE PHISHING?	Au cours de votre navigation, si la barre vous affiche le message « Tentative de phishing suspectée », **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.**

À SAVOIR	**La Barre de Confiance ne s'affiche pas sous Internet Explorer ?** Allez dans le menu « affichage » d'Internet Explorer, sélectionnez « <Barres d'outils ». Activer la ligne « Barre de Confiance CM-CIC » Si la barre de menus n'est pas affichée, appuyer sur « alt » pour la faire apparaître. Procéder de la même façon pour désactiver la barre de confiance (non recommandé).

Qu'est-ce que le « *phishing* » ?
Le « *phishing* », aussi appelé hameçonnage, 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. 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 nom de domaine est sur fond vert.

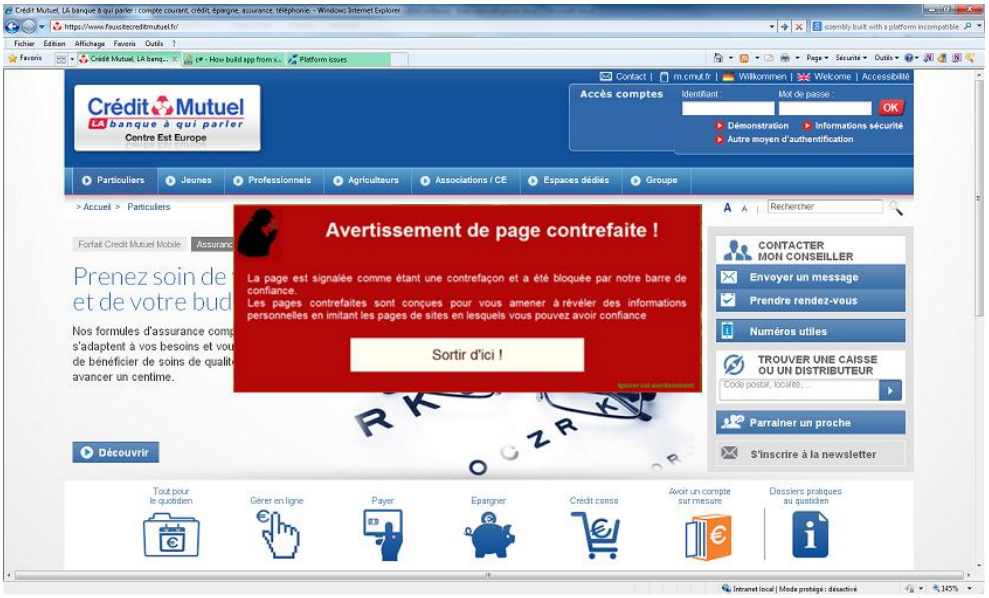
Qu'est-ce qu'un "domaine de confiance" ?
Un site Internet possède un nom de domaine qui permet de l'identifier.

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 plusieurs domaines intégrés à l'application : il s'agit des principaux noms de domaines des sites Crédit Mutuel et CIC (liste non exhaustive). Si vous êtes sur un tel domaine, la barre l'affichera sur un fond vert.

Liste noire d'adresses
À l'ouverture d'une nouvelle fenêtre Internet Explorer, la Barre de Confiance s'initialise en téléchargeant sur nos serveurs une liste d'adresses de sites connus pour être des sites de *phishing*.

Dès lors que cette liste a été chargée, une alerte vous sera affichée dans Internet Explorer si vous tentez d'accéder à l'une de ces adresses :



Si l'initialisation de la liste a échoué (blocage par votre pare-feu, indisponibilité temporaire du site de mise à jour…), la Barre de Confiance réessayera régulièrement de la télécharger. Par la suite, cette liste est régulièrement rafraichie tant que vous ne quittez pas Internet Explorer.
Si la liste n'a pas été chargée par la Barre de Confiance, celle-ci ne pourra pas vous avertir si vous tentez d'accéder à une adresse frauduleuse.

Les adresses figurant sur cette liste noire sont mises à jour par nos équipes dès lors que le site en cause a été identifié et analysé.
Cette liste n'est pas exhaustive.

Afin d'être protégé le plus efficacement possible, veillez à configurer votre pare-feu pour qu'il laisse passer les requêtes à destination d'Internet issues de la Barre de Confiance.

La Barre de Confiance n'envoie à nos serveurs bancaires aucune information personnelle vous concernant, ni aucune information sur les sites Internet visités.

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.

De plus amples informations sur le *phishing* sont disponibles sur Wikipedia :
http://fr.wikipedia.org/wiki/Hame%C3%A7onnage

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 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 ?

1. Aller dans le panneau de configuration windows
2. Allez dans le menu ajout / suppression de programme (XP) ou Programmes – Desinstaller un programme (Windows vista et ultérieurs)
3. Cliquez sur la ligne « Barre de Confiance CM-CIC», et choisissez supprimer

Un peu de vocabulaire…

Dans ce document, certains termes peuvent nécessiter une définition :

***Phishing* (ou hameçonnage)**	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/`