

1. Le message, son aspect général :



2. Identification du site hostile :

Ce cas de phishing est basé un lien à cliquer dont le code html associé est rudimentaire :

```
<body bgcolor="#000000">
```

```
...
<a href=http://creditmutuei.com><font color=#ff9c00><b>Appuyez ce lien pour vous
faire enregistrer</b></font></a>
```

```
...
</body>
```

L'utilitaire nslookup permet de repérer l'IP du site Web hostile :

```
C:\Documents and Settings\Administrator>nslookup
Default Server: associatedwinners.com
Address: 10.0.0.2

> set type=ALL
> creditmutuei.com
Server: associatedwinners.com
Address: 10.0.0.2

Non-authoritative answer:
creditmutuei.com nameserver = ns7428.creditmutuei.com
creditmutuei.com nameserver = ns5192.creditmutuei.com
creditmutuei.com internet address = 60.208.91.65
>
```

Whois 60.208.91.65 ?

```

inetnum: 60.208.0.0 - 60.217.255.255
netname: CNCGROUP-SD
descr: CNCGROUP Shandong province network
descr: China Network Communications Group Corporation
descr: No.156,Fu-Xing-Men-Nei Street,
descr: Beijing 100031
country: CN
admin-c: CH455-AP
tech-c: XZ14-AP
mnt-by: APNIC-HM
mnt-lower: MAINT-CNCGROUP-SD
mnt-routes: MAINT-CNCGROUP-SD
status: ALLOCATED PORTABLE
source: APNIC

role: CNCGroup Hostmaster
e-mail: abuse@cnc-noc.net
address: No.156,Fu-Xing-Men-Nei Street,
address: Beijing,100031,P.R.China
nic-hdl: CH455-AP
phone: +86-10-82993155
fax-no: +86-10-82993102
country: CN
admin-c: CH444-AP
tech-c: CH444-AP
changed: abuse@cnc-noc.net 20041119
mnt-by: MAINT-CNCGROUP
source: APNIC

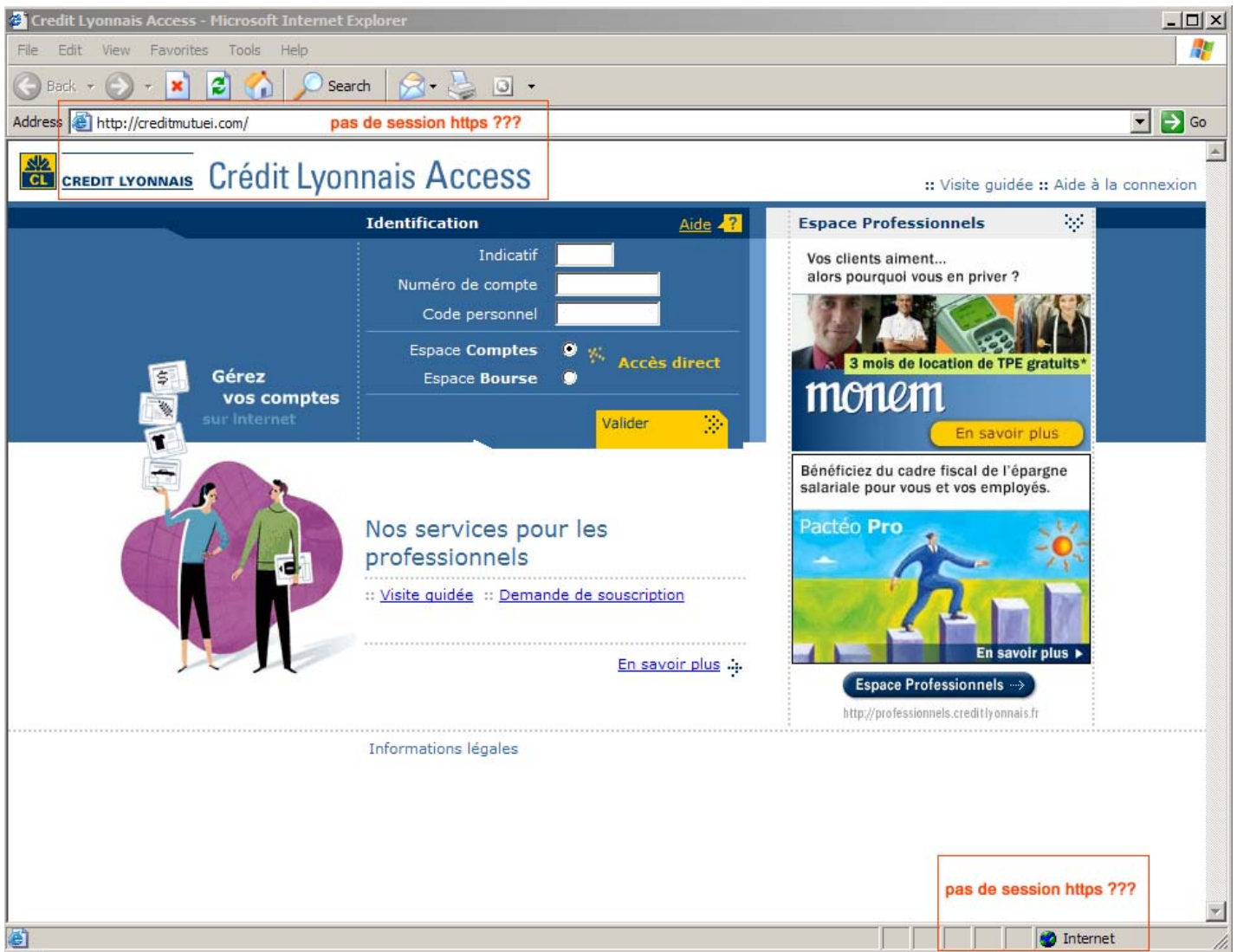
```

3. Un cas de phishing assez visible :

Les observations habituelles permettent de reconnaître la fraude :

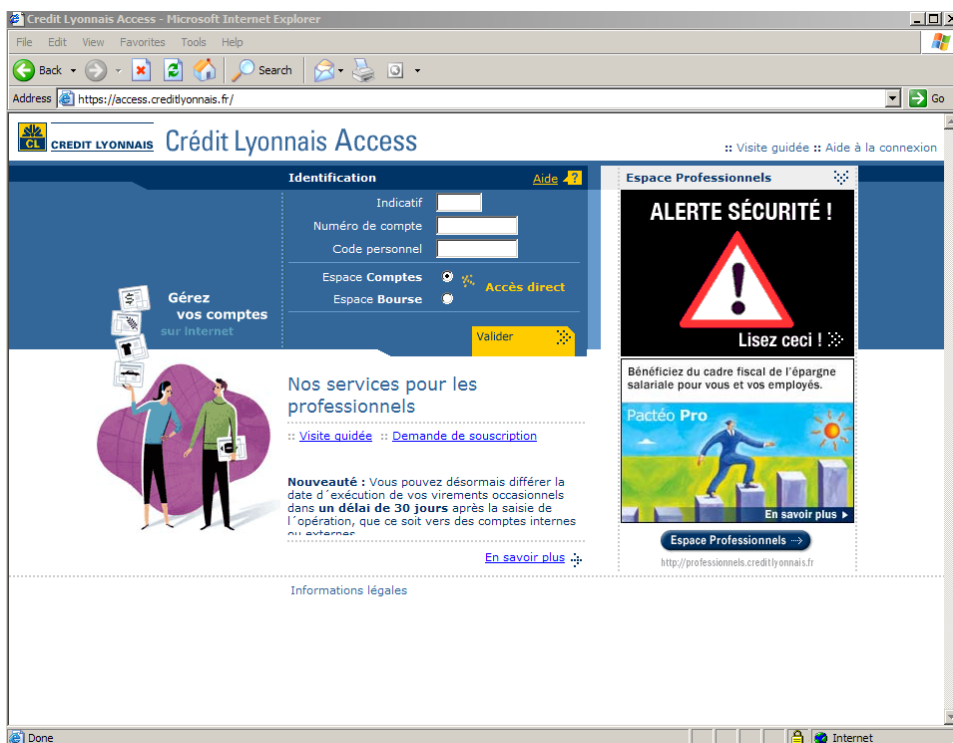
- URL ne correspondant pas à la source. La confusion entre « Crédit Mutuel » (voir l'objet du message) et « Crédit Lyonnais » (voir le site plagié) ne peut qu'attirer l'attention de l'internaute. Le seul piège possible est le remplacement du « l » final du « creditmutuel.com » par un « i » via l'url «creditmutuei.com ».
- Absence de clé SSL (icône zone sécurisée) pour un site HTTPS affiché.

Le lien à cliquer est associé à l'écran suivant :



Lors de notre essai, nous avons constaté un temps d'attente important lors du téléchargement des images ce qui augmente le délai de réflexion de l'internaute.

La saisie d'un numéro de compte « fantaisiste » redirige sur le site réel du Crédit Lyonnais.



Il sera évidemment trop tard pour lire l'alerte de sécurité mais cela permet de constater la réactivité de la banque qui affiche les remarques suivantes :



Plusieurs tentatives de fraude informatique de type «**phishing**» viennent d'être détectées. Elles visent les clients de différentes banques françaises dont **le Crédit Lyonnais**.

Des courriers électroniques ont été envoyés en masse aux internautes abonnés de certains fournisseurs d'accès à Internet. Ces messages prétextent d'un renforcement de la sécurité et invitent les destinataires à cliquer sur un lien. En suivant cette instruction, l'internaute est dirigé vers un **FAUX site** présentant toutes les apparences d'un site du Crédit Lyonnais. Il est alors invité à saisir ses coordonnées d'identification et code d'accès aux services Internet de gestion de comptes de la banque.

Si vous avez reçu ce mail et vous êtes identifié après avoir cliqué sur le lien qu'il contenait : **changez immédiatement** votre code personnel d'accès à votre service Internet et **vérifiez régulièrement les opérations effectuées sur vos comptes**.

Pour vous prémunir contre tout risque, respectez les conseils suivants :

- Ne répondez pas à de tels courriers électroniques, **jamais votre banque ne vous demandera ce type d'informations** d'une quelconque manière.
- **Ne cliquez sur aucun lien** contenu dans un mail non sollicité.
- **Ne communiquez jamais ni coordonnées personnelles, ni code secret.**
- **Supprimez systématiquement ce type de messages** de votre messagerie
- Avant de saisir vos coordonnées d'identification au service de gestion de vos comptes sur Internet, vérifiez toujours que vous vous trouvez bien sur les sites sécurisés du Crédit Lyonnais (présence d'un cadenas ou d'une clé sur la barre d'état de votre navigateur) dont les adresses sont :

* pour les clients Particuliers : <https://interactif.creditlyonnais.fr>

* pour les clients Professionnels : <https://access.creditlyonnais.fr>

En cas de doute sur la conduite à tenir, vous pouvez contacter votre service d'assistance du lundi au vendredi du 8h30 à 17h30 au 0 890 71 14 56 (0.15 € TTC/min, tarif France Télécom au 01/07/2005, appel depuis un poste fixe en France Métropolitaine)

Pour tout savoir sur le **phishing**, rendez vous sur l'espace sécurité du Crédit Lyonnais à l'adresse suivante :

<http://particuliers.creditlyonnais.fr/securite/internet/emails/2.html>

4. Actions engagées

- La publication de ce document,
- Ce cas a été reporté au niveau « .org »