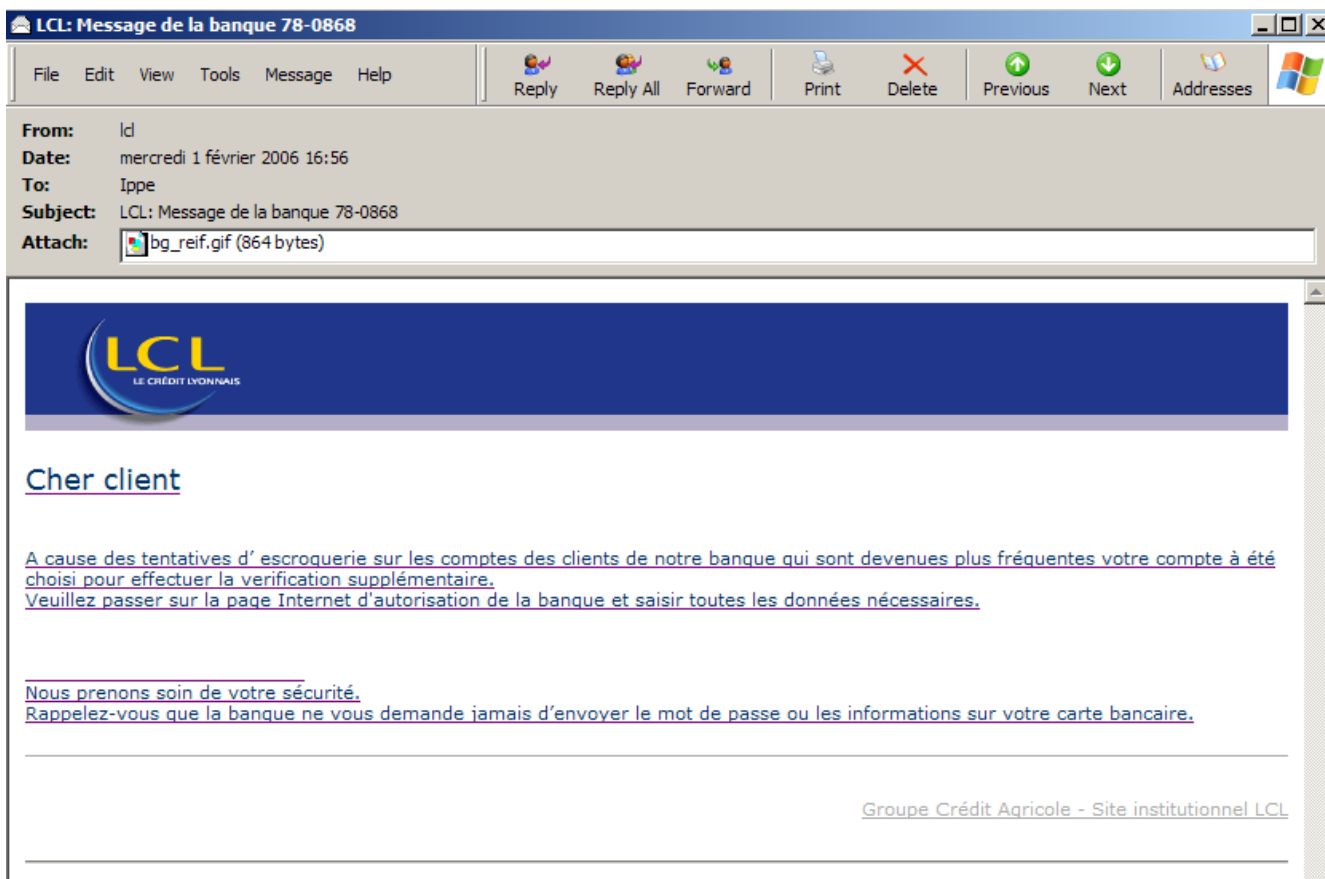


1. Le message, son aspect général :

Faisant suite à une première tentative visant les clients du Crédit Lyonnais, tentative décrite depuis le 26 janvier 2006 sur notre site Web: <http://www.associatedwinners.com/phishing/lcl.pdf>, une nouvelle tentative cherche à rebondir sur « **des tentatives d'escroquerie** » :



2. La technique utilisée :

La technique est celle du classique lien à cliquer.

Un de nos reporters sur reportphishing@antiphishing.fr signale à juste titre l'approximation du phishing :

Tentative de phishing sur le site du crédit lyonnais :

"LCL Message de la banque 78-0868.eml" mail original en pièce jointe

Le site pirate : "<http://Interactlf.credltyonnals.com/>"

à ne pas confondre avec "<http://interactif.creditlyonnais.com/>" !!

Il est à noter que le message circule déjà sous de nombreux numéros :

LCL: Message de la banque 96-8953

ou

LCL: Message de la banque 85-9489

Etc...

La page associée au lien indiqué est la suivante :

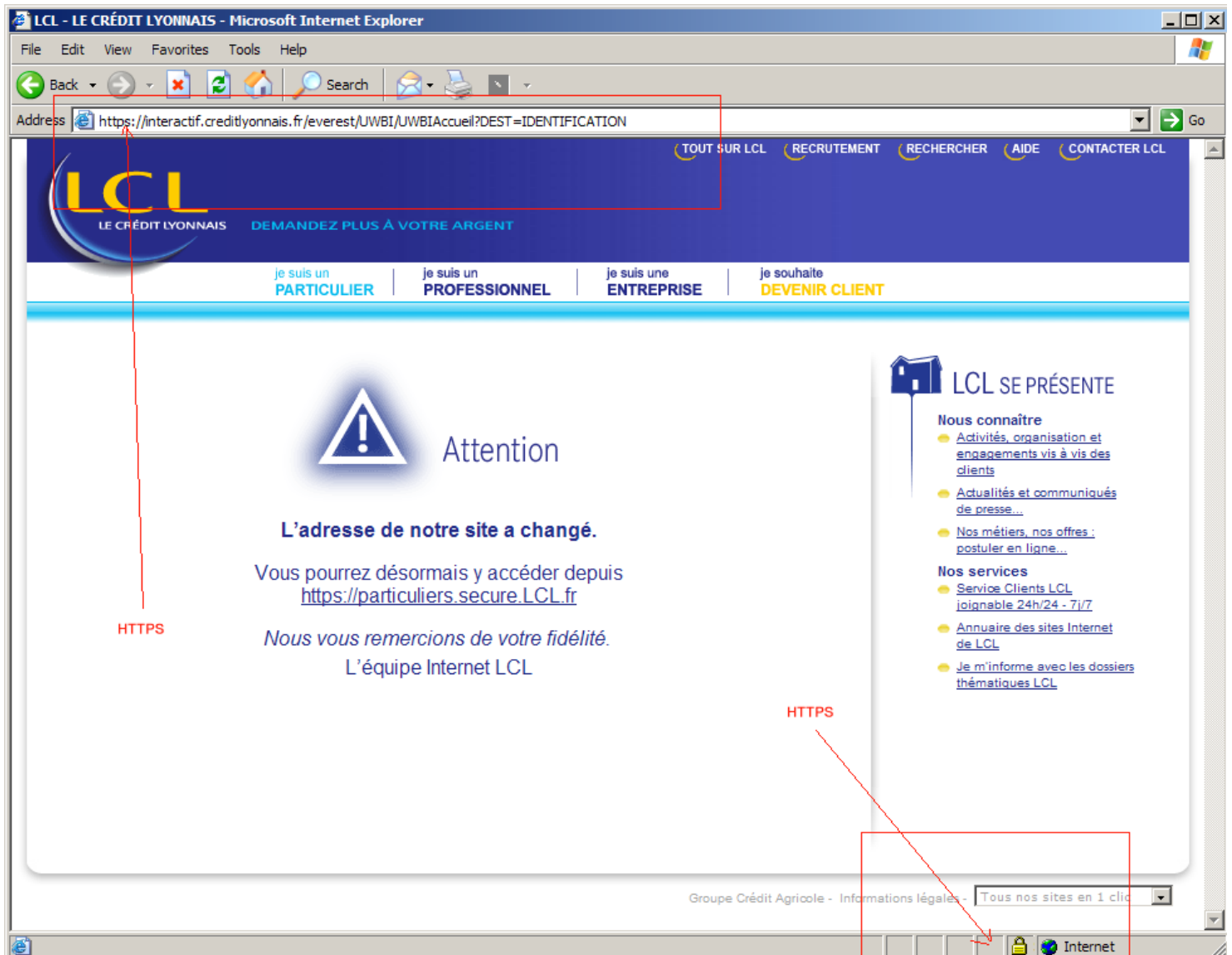
The screenshot shows the LCL website interface. At the top, there is a navigation bar with links: ANNUAIRE DES SITES, RECRUTEMENT, RECHERCHER, AIDE, and CONTACTER LCL. Below this is the LCL logo and the slogan 'LE CRÉDIT LYONNAIS DEMANDEZ PLUS À VOTRE ARGENT'. A central 'ACCÈS CLIENT' section features a login form with fields for 'Date de naissance', 'Indicateur', 'N° de compte', and 'Code personnel', and a 'VALIDER' button. Below the login form are links for 'Code oublié?', 'Visite Guidée', and 'Sécurité sur Internet'. The page is categorized by user type: 'je suis un PARTICULIER', 'je suis un PROFESSIONNEL', 'je suis une ENTREPRISE', and 'je souhaite DEVENIR CLIENT'. The main content area is divided into sections for 'PARTICULIER', 'ASSURANCES', 'CREDIT', and 'ACTUALITÉS'. A sidebar on the right contains 'MES OUTILS' and 'INFORMATIONS LCL'. The footer includes 'Offre soumise à conditions (en savoir plus)', 'Dispositions Générales de Banque - Informations légales - Guide tarifaire - Tous nos sites en 1 clic', and 'Internet'.

L'absence de session sécurisée via HTTPS et la présence d'un formulaire d'accès avec des informations confidentielles sur la page d'accueil sont caractéristiques du phishing :

This is a close-up of the 'ACCÈS CLIENT' login form. It features a blue background and contains the following elements:

- ACCÈS CLIENT** (Section Header)
- Fields for: **Date de naissance**, **Indicateur**, **N° de compte**, and **Code personnel**.
- A **VALIDER** button.
- Links below the form: [Code oublié ?](#), [Visite Guidée](#), and [Sécurité sur Internet](#).
- Below the form, the text **je souhaite DEVENIR CLIENT** is visible.

Si des informations (aléatoires !) sont fournies, le résultat est classique. Il consiste à rediriger vers une page d'erreur légitime du site officiel pour essayer de leurrer l'internaute.



3. Actions engagées

- Le Crédit Lyonnais a publié une alerte sur ce phishing en cours :

<https://particuliers.lcl.fr/CLI/phishing022006.htm>

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

