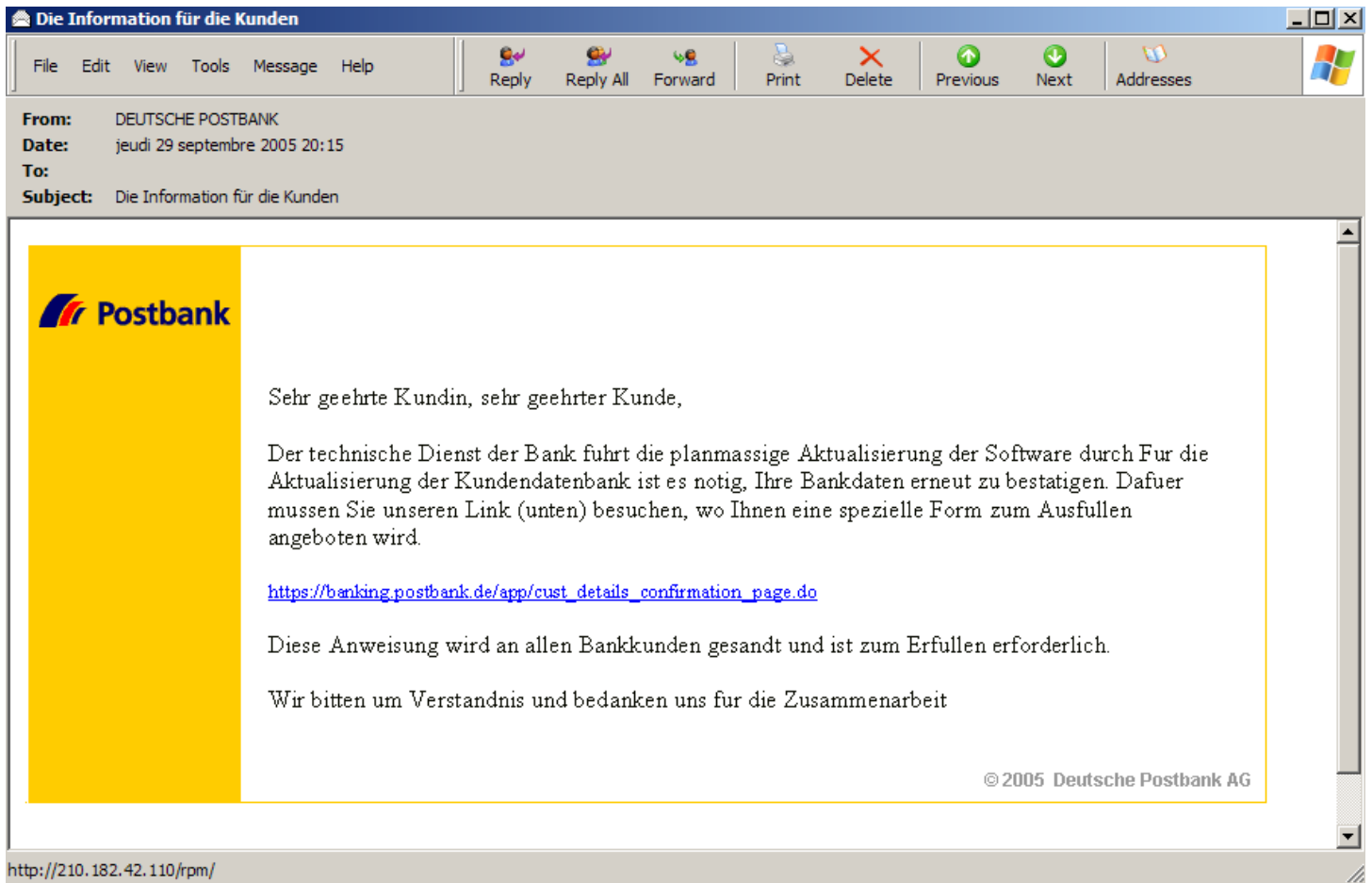


## 1. Le message, son aspect général :

Le message ne devrait interpellé qu'un internaute comprenant l'Allemand mais la signature <http://210.182.42.110/rpm/> est caractéristique d'un essai de phishing :



On peut en effet se demander pourquoi une structure telle que Postbank n'utilise pas les mécanismes usuelles de DNS ?

## 2. La technique utilisée :

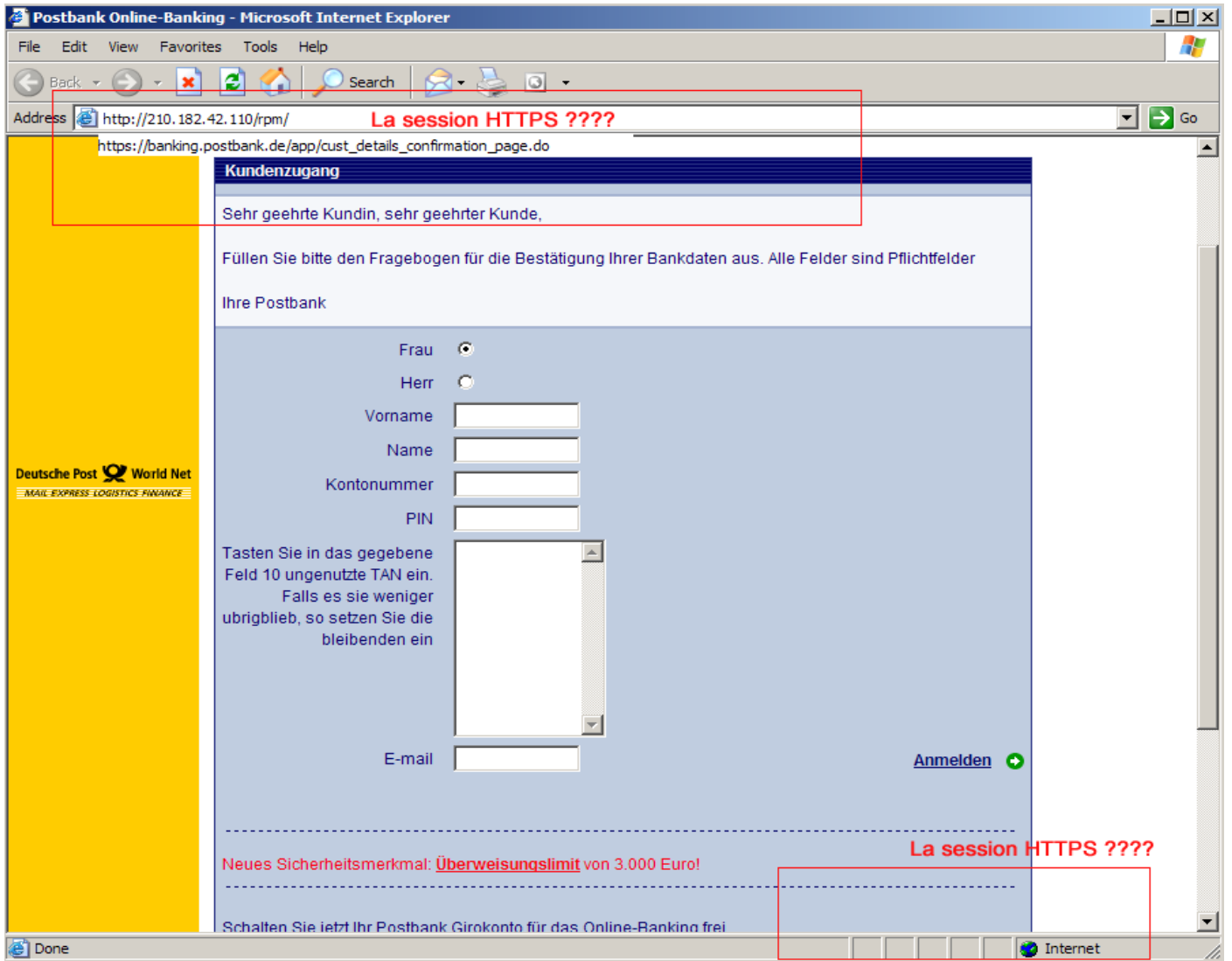
Lors de nos essais, la première IP appelée a été **210.182.42.110**. Le code html associé montre la MAP et son image « à cliquer » :

```
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=us-ascii">
<html>
<p><font face="Arial">
<A HREF="https://banking.postbank.de/app/cust_details_confirmation_page.do">
<map name="L3Klu7"><area coords="0, 0, 824, 375" shape="rect" href="http://210.182.42.110/rpm/"></map>
<img SRC="cid:part1.01020305.04020201@support_id_3283097@postbank.de" border="0"
usemap="#L3Klu7"></A></a></font></p>
```

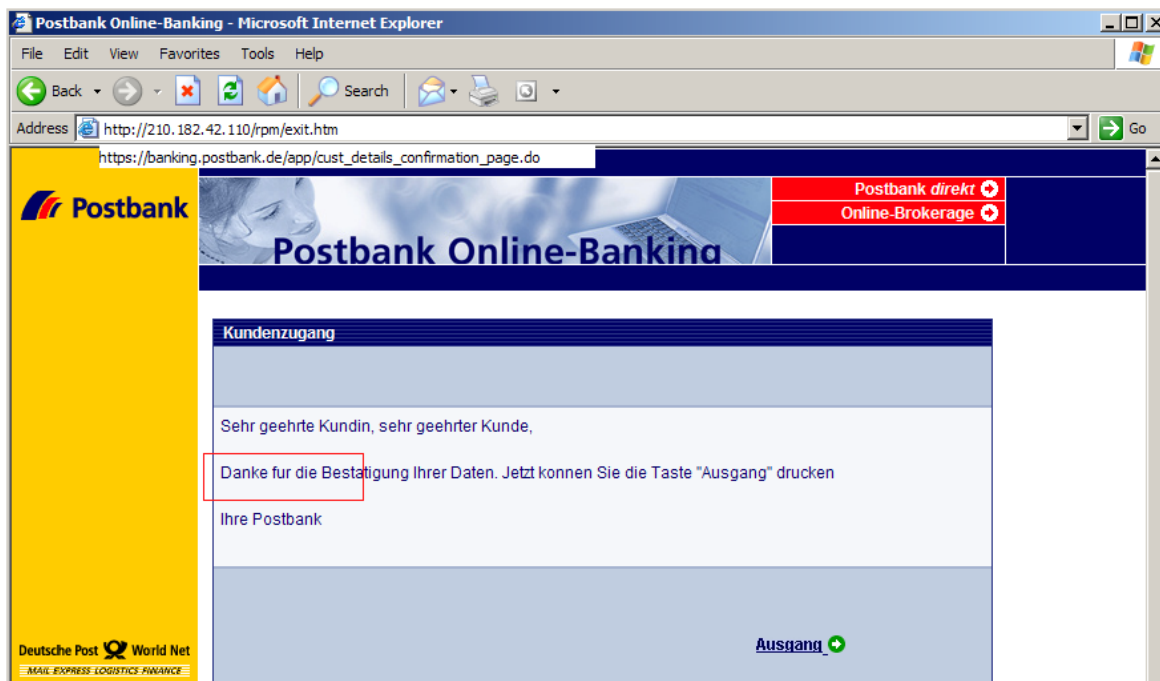
```
<p><font color="#FFFFFFD">Funny Hotmail cats and dogs Angelia Jolie I can't </font></p></html>
```

Avec sa signature farfelue !

L'écran suivant est associé au lien vers le site plagiant [www.postbank.de](http://www.postbank.de) :



La saisie d'informations (farfelues) produit un écran de confirmation :



Le dernier lien revient au site officiel. On remarquera que la charte graphique est proche du site original ce qui rend plus dangereux l'essai de phishing :



### 3. Identification du site hostile :

Le Whois définit le propriétaire suivant pour l'IP **210.182.42.110**:

```
inetnum:      210.182.0.0 - 210.182.255.255
netname:      BORANET-NET-210-182
descr:        DACOM Corp.
country:      KR
admin-c:      DB50-AP
tech-c:       DB50-AP
mnt-by:       APNIC-HM
mnt-lower:    MNT-KRNIC-AP
changed:      hm-changed@apnic.net 20021025
status:       ALLOCATED PORTABLE
source:       APNIC

role:         DACOM BORANET
address:      DACOM Bldg., 706-1, Yoeksam-dong, Kangnam-ku, Seoul
country:      KR
```

### 4. Actions engagées

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