



RÉSIST

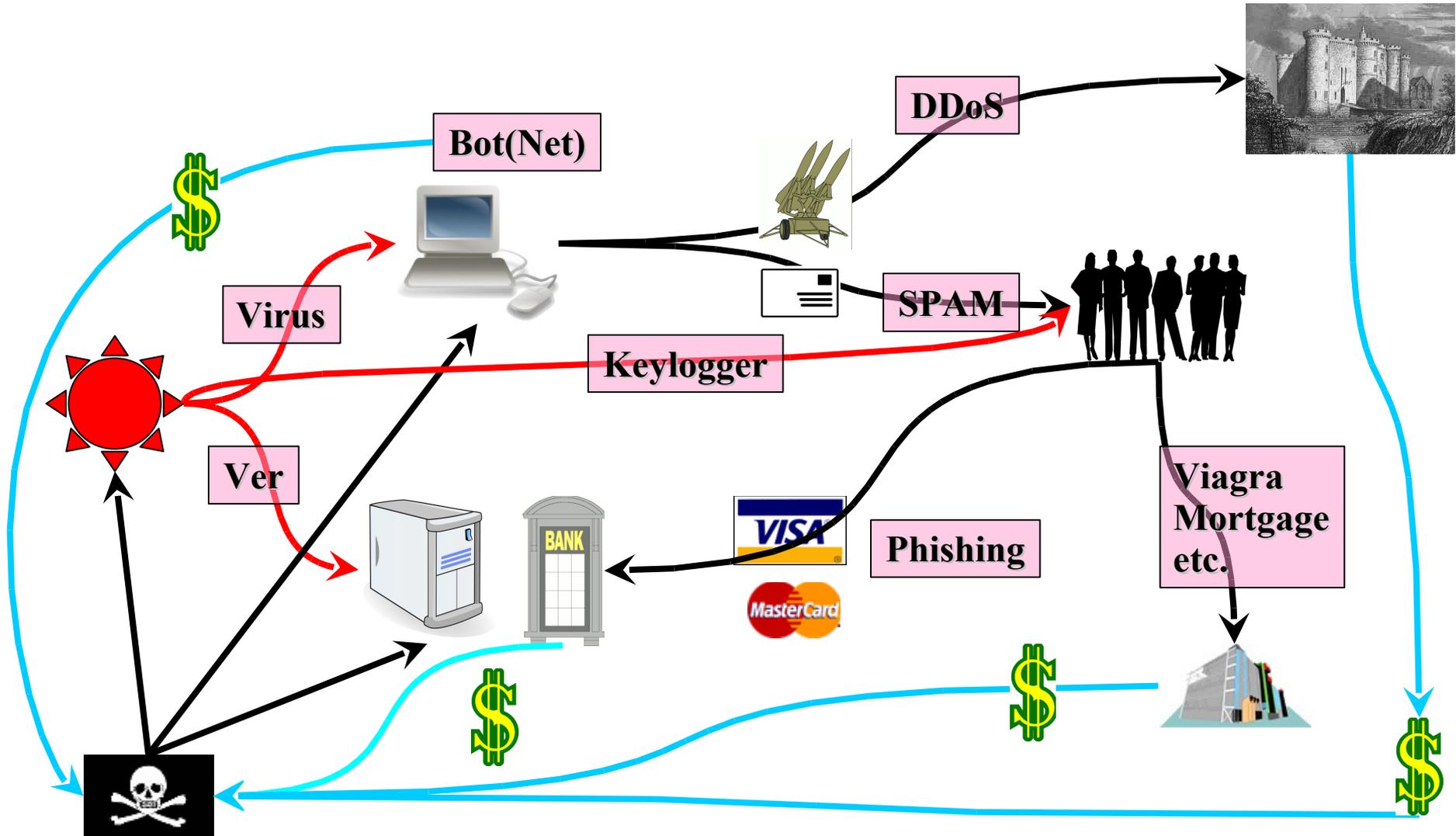
Le phishing

Etat des lieux

- Internet est à l' image du monde dit réel
 - avec ses gens « bien »
 - avec ses délinquants
- A la différence que pour les délinquants
 - les actions se font à distance
 - sur une très large population
 - avec une très grande rapidité
 - sans implication psychologique
 - par des procédés techniques incompréhensibles

- Gagner de l'argent rapidement
 - Vendre n'importe quoi (SPAMs)
 - Vendre des réseaux de vente (Botnet) : « 10000 infected pc's for 25\$ », avec l'aide de « mules »
 - Racketter (DDoS)
 - Escroquerie
 - SCAM
 - Revendre des objets virtuels (MMORPG)

Schéma « financier »



- Obtenir des informations directement ou indirectement moneyables
- Mélange de fishing (pêche) et phreaking (piratage téléphonique)
- Aussi appelé « hameçonnage »

- Envoi d 'un mail « piègeur »
- Présentation d 'un site web d 'apparence connue
- Mécanismes psychologiques
 - Paresse intellectuelle
 - Peur
 - Envie
- Mécanismes techniques (en appui de mécanismes psychologiques)

- Clients de banques
 - d 'abord américaines
 - puis européennes
- Clients de sites monnayables
 - Site d'enchères (eBay, Yahoo, etc.)
 - Site de paiement en ligne (Paypal)
- Plus récemment : le trésor public américain



Cher client de **BNP Paribas**,

Le département technique de BNP Paribas procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

<http://www.secure.bnpparibas.net/banque/portail/confprocedure.asp>

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.



Cher client de **SOCIÉTÉ GÉNÉRALE**

Le département technique de Société Générale procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

<http://www.societegenerale.fr/customercare/banque/confprocedure.asp>

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

© Société Générale 2000-2006

www.societegenerale.fr.customercare.banque.xxx.com/r1/sg/

The screenshot displays the Société Générale online banking interface. The browser window title is "Société Générale : produits et services pour la clientèle de particuliers, gestion de compte en ligne via Logiciel Net - Mozilla Firefox". The address bar shows the URL "http://www.societegenerale.fr.customercare.banque.ngincorps.com/r1/sg/". The main header features the Société Générale logo and the slogan "Toute votre banque en ligne". Below the header, there is a navigation bar with links for "Contactez un Conseiller", "Trouver une Agence", and "Trouver dans le site". The main content area is titled "Page de confirmation de détails de client" and contains a form for client details. The form includes fields for "VOTRE CODE CLIENT" and "VOTRE CODE SECRET", and an "OK" button. The page also features several promotional banners and a sidebar with various services. The footer contains the text "© SOCIÉTÉ GÉNÉRALE", "Configuration et (re)chargé | Nos engagements | Marchés régulés et contrôlés généralement | Société Générale 2008", and "Terminé".

RÉSIST

Mais l'Europe entière est touchée

GRUPO BANCO POPULAR Identificación

Acceso al Servicio de Banca por Internet

Por motivos de seguridad que hemos mejorado le pedimos que introduzca su firma de transferencias para entrar en su oficina internet

FIRMA:

Demo

- Información sobre el servicio
- Solicitud de Contratación
- Tarifas

AVISO IMPORTANTE DE SEGURIDAD

Les informamos que **NUNCA** le enviaremos un correo solicitándole sus claves. Igualmente, los recordamos que no debe facilitar sus claves a nadie, ni por correo electrónico, ni por teléfono, ni en persona, aunque manifieste hacerlo en nombre del propio Banco. **Saber más**

Para cualquier duda llame al 902 365 111 o info@bancopopular.es

Servicio de Atención: 902 365 111 o info@bancopopular.es

© 2004 Grupo Banco Popular. Todos los derechos reservados. [800x600] [IE Explorer 5.5 o superior] [Netscape 6.2]

Dresdner Bank - Privatkundenportal - Microsoft Internet Explorer

Adresse <http://219.144.194.158:8081/secure.dresdner-privat.de/tb/privat/login/login.htm>

Home Inhalt Kontakt GuidedTour Sicherheit Hilfe Wichtige Hinweise Dresdner Bank

Dresdner Bank
Die Beraterbank

Login

Suche

Login mittels PIN

Banking-ID / Alias

PIN

TAN 1

TAN 2

TAN 3

Zugang zum Testkonto und Testdepot

So erhalten Sie Ihre Banking-ID und PIN

Sie erhalten beide in Verbindung mit einer Anmeldung zum [Dresdner MultikanalBanking](#). Den [Antrag zum MultikanalBanking](#) (PDF 153 KB) können Sie gleich am Bildschirm **ausfüllen, ausdrucken** und uns unterschrieben **zusenden**. Oder wenden Sie sich an eine [Dresdner Bank-Filiale](#) in Ihrer Nähe.

Haben Sie weitere Fragen?

Sie finden hier **Antworten** auf die am häufigsten gestellten Fragen zum **Thema MultikanalBanking**. Darüber hinaus steht Ihnen unsere **Hotline** zur Verfügung: per **Telefon** unter 0 18 03/366-966* oder per **E-Mail**: dresdner-privat@dresdner-bank.com. Oder Sie schauen sich unsere [Guided Tour MultikanalBanking](#) an.

Sie haben Ihre Zugangsdaten vergessen?

- Wenn Sie Ihre **PIN** nicht mehr wissen oder diese gesperrt haben, wenden Sie sich bitte an Ihre [Dresdner Bank-Filiale](#).
- Haben Sie Ihre **Banking-ID** vergessen, hilft Ihnen unsere Hotline gerne weiter. Wählen Sie 0 18 03/366-966*.

Dresdner Bank - Die Beraterbank

CHI SIMMO LA BANCA COME VUOI TU LAVORARE CON NOI IL GRUPPO RAS SERVIZIO CLIENTI

RAS BANK Investimenti e risparmio | Previdenza | Protezione | Conti correnti | Mutui | Prestiti personali

Sintesi Gennaio 2006
Crescita e protezione insieme

Puoi sottoscrivere la nuova linea di gestione.

Mobile banking
La tua banca ovunque con te...

Scopri i dettagli!

Accedi all'area clienti

Codice Utente:

Numero Personale:

Parola Chiave:

numero verde 800.22.33.44

Altri contatti

Diventa cliente

SCOPRI I VANTAGGI UNO SPECIALISTA AL TUO RANCO

Altri contatti

Incontra promotore
Trova il tuo promotore locale per discutere le tue esigenze.

RasBank aderisce a PattiChiaro

Di cosa hai bisogno?

- Preparare la pensione
- Dare solidità alla mia famiglia
- Semplificarmi la vita
- Realizzare un mio progetto
- Far crescere il mio patrimonio
- Acquistare casa

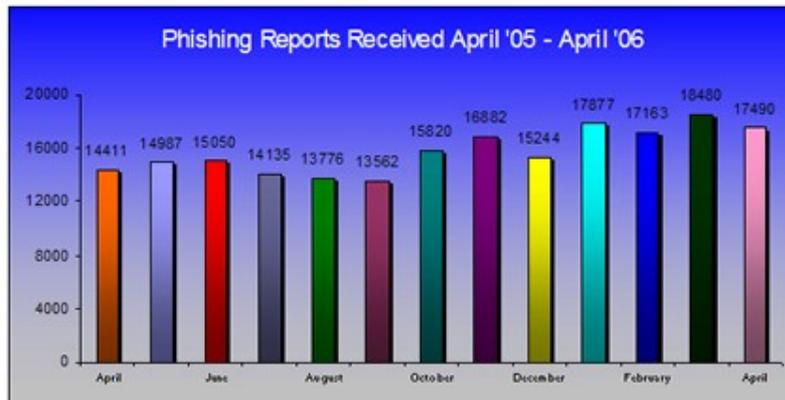
Quotazioni prodotti RasBank

Scegli il prodotto

Continua il Concorso Previdenza e Finanza
Prova a vincere i premi che RasBank mette in palio!

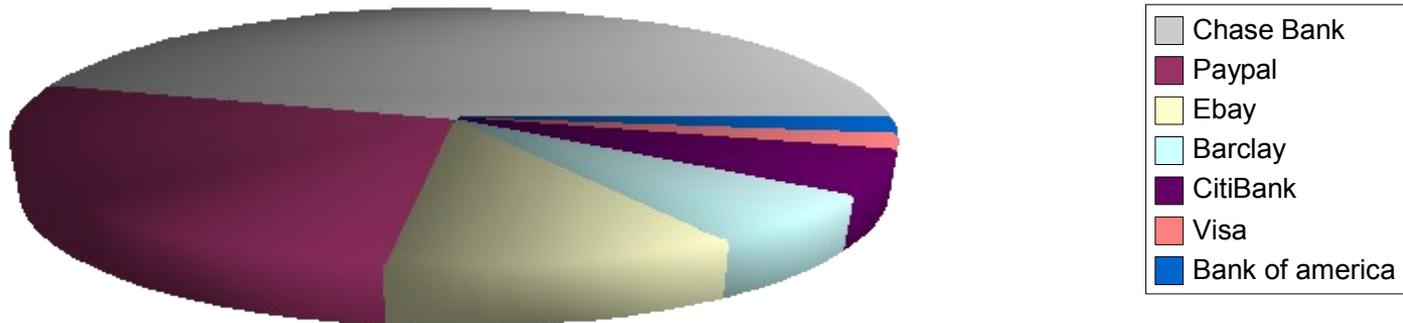
Cerca | Mappa | Guida al sito | Glossario | Privacy | Sicurezza | Area clienti istituzionali | **Accesso Promotori**

2005 RASBANK Una società di Allianz Group



- 10000 sites
- 5 jours de vie
- Vol de x Milliards \$
- Défense 800 millions \$ en 2008

Proportion de Phishing



- Chiffres de septembre 2006
 - 154 marques
 - 23 670 campagnes de phishing
 - 14 191 sites de phishing

- Rapide
- Peu de risque
- Taux de rentabilité excellent (0,01 %)
 - En 2004 : 20% ont cliqué
 - En 2004 : 1,3% ont donner des informations
- Large audience

- Educative
- Administrative
- Technique

- On explique aux utilisateurs les risques
- On explique ce à quoi il faut faire attention
 - Les banques font beaucoup d'effort

- Marcus J Ranum : les 6 plus idiotes idées de la sécurité
- Les techniques changent
 - Regardez le cadenas => contourné
 - Regardez l'url (IP) => contourné
 - Regardez le nom de domaine => contourné
 - Les banques n'envoient jamais de mail => faux

- Jouons sur la psychologie
 - <https://www.mabanque.cm@site.dupirate.com>
 - <https://www.lc1.fr> (le second L est le chiffre 1)
 - <https://www.mabanque.tg.lite.dupirate.com>
- Jouons avec la technique
 - les pop-up
 - les frames et Iframes
 - <http://cri.univ-tlse1.fr/demonstrations/phishing>

- Non !
- Culture du doute : Est-ce normal ?
 - Fautes d 'orthographe
 - Banque qui perde des identifiants
 - Recevoir
- Information sur l 'arnaque en question

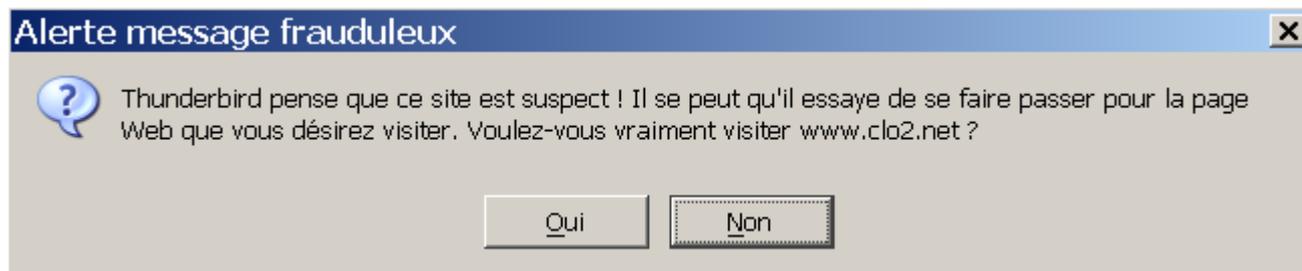
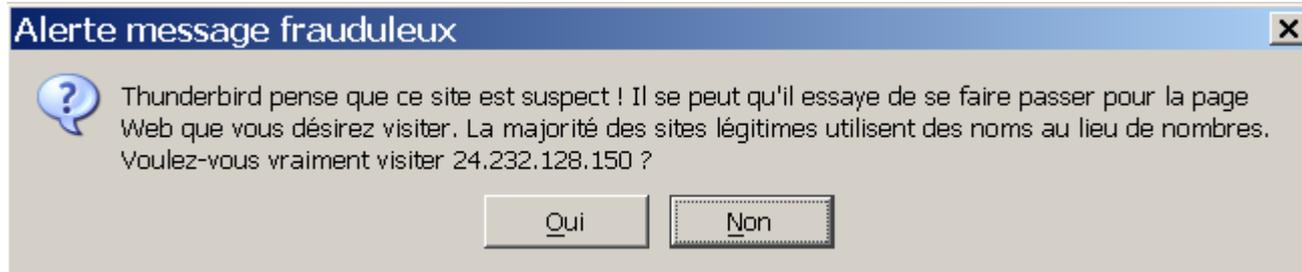
- Les registrars vérifient les demandes de domaines (AFNIC)
- Les NIC bloquent les domaines « pathogènes »
- Les FAI bloquent les IP « pathogènes »

- Connaître toutes les spécificités d'un pays
 - Nom de société,
 - Vocables
 - Clavier !
- Délai pour le blocage
 - Détection
 - Vérification
 - Propagation des blocages

- Réception
- Utilisation
- Serveurs

- Phishing => SPAM
- Même technique que les SPAMs
 - Greylisting
 - RBL (et SURBL)
 - Bayésien / Chaines markoviennes
 - Détection d 'incohérence URL

- Empêcher l'utilisation des sites façade
- RBL pour l'utilisation web
 - Proxy filtrant
 - Détecteurs intégrés
- Le blocage des popups



The screenshot shows a web browser window with the following elements:

- Menu bar:** Fichier, Edition, Affichage, Aller à, Marque-pages, Outils, ?
- Address bar:** http://www.afnic.fr/
- Bookmark bar:** grenouille, Ratiatum, freshmeat, Free, Clubic, Da Linux, Freenews, UT1
- Netcraft toolbar:** Services, Risk Rating (green bar), Since: Mar 2002, Rank: 22591, Site Report, [FR] AFNIC
- Proxy settings:** Proxy: ssh, Utiliser (checked), Modifier, Supprimer, Ajouter, Statut: Utilisation
- AFNIC website header:** Logo (fr in a circle) and text AFNIC
- Navigation tabs:** L'association, Noms de domaine, Enregistrement.fr, Outils
- Main content:** L'AFNIC est le centre d'information et de gestion des noms de domaine internet .fr (France) et .re (Île de la Réunion).
- Footer:** Dernières nouvelles (orange banner)

The screenshot shows a web browser window with the following elements:

- Menu Bar:** Fichier, Edition, Affichage, Aller à, Marque-pages, Outils, ?
- Address Bar:** http://www.postcard.0catch.com/postcard.exe
- Bookmarks Bar:** grenouille, Ratiatum, freshmeat, Free, Clubic, Da Linux, Freenews, UT1 : Rech Perso
- Netcraft Toolbar:** Includes the Netcraft logo, a 'Services' dropdown, a 'Risk Rating' indicator (a red and green bar), and links for 'New Site Rank: - Site Report' and 'Electric Lightwave Inc'.
- Proxy Settings:** Proxy: Aucun (dropdown), Utiliser (checked), Modifier (pencil icon), Supprimer (trash icon), Ajouter (plus icon). Statut: Aucun proxy utilis
- Browser Tabs:** AFNIC - centre de gestion des noms..., FILE NOT FOUND! - web hosting, ...
- Page Content:** A large blue banner with a green circular logo for 'Zero Catch'. To the right of the logo is a search result snippet for 'cross flower funeral' with a URL 'www.agen-expo.fr'. Below the banner are links for 'LOGIN CONTACT US TECH SUPPORT UPGRADE YOUR'.
- Error Message:** 'File Not Found!' is displayed at the bottom of the page.

refox

Affichage Aller à Marque-pages Outils ?

http://www.brennano.com/members/index.htm

Ratiatum freshmeat Free Clubic Da Linux Freenews UT1 : Rech Perso INTRINsec Cit@delle - ...

Rechercher PageRank ABC Orthographe S'abonner Options

Usurpation d'identité sur Internet

Il semblerait que cette page ait été créée à des fins frauduleuses en vue d'obtenir des informations confidentielles (d'ordre personnel ou financier) de la part des utilisateurs. Si vous saisissez des informations confidentielles sur cette page, vous risquez d'être victime d'une usurpation d'identité ou d'une escroquerie. [Plus d'infos »](#)

[Quitter ce site et retourner à ma page d'accueil](#) [Ne pas tenir compte de cet avertissement](#)

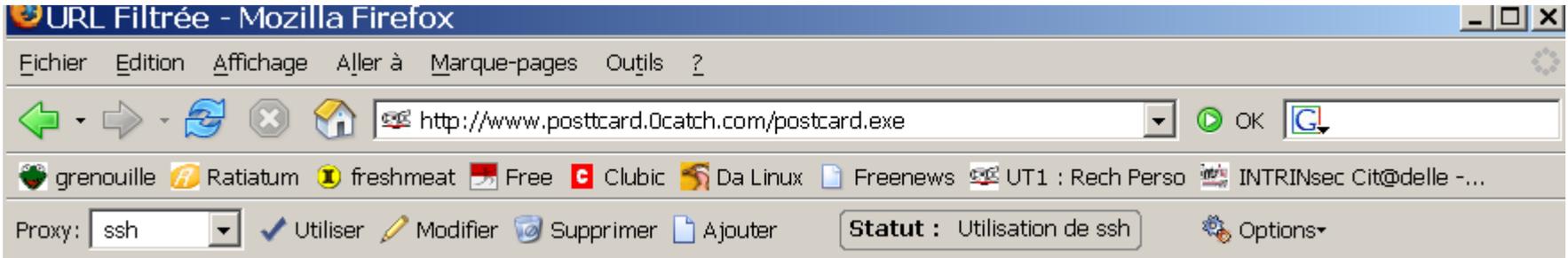
Google [\[Envoyer un rapport à Google\]](#)

me related websites for: brennano.com

Search

Related Categories

- [Norway](#)
- [Stavanger Hotels](#)
- [Norsk Hydro](#)
- [Blomster Trondheim](#)



Le site auquel vous tentez d'accéder est référencé comme site de **phishing**, c'est à dire qu'il tente de vous escroquer d'une manière ou d'une autre (faux site bancaire, faux site d'enchères, etc...).

Si vous pensez qu'il s'agit d'une erreur, veuillez contacter cachemaster@univ-tlse1.fr en sachant que l'url : <http://www.postcard.0catch.com/postcard.exe>, sera automatiquement précisée.

- Serveurs peuvent être utilisés
 - Intrusion
 - Failles XSS, IFRAME
- Serveurs DNS peuvent être empoisonnés
 - Pharming
- Programmation correcte des applications web
- Paramétrage correct des serveurs DNS

- Délai de mise à jour des RBLs
 - Et mise à jour des RBLs
- Les SPAMs s'améliorent
 - mots cachés, décompilation de message
 - réexpédition de messages (greylisting)

The screenshot shows a Mozilla Firefox browser window titled "Think Federal Credit Union - Better Banking - Mozilla Firefox". The address bar contains the URL "http://24.232.128.150/r/index.htm". The browser's menu bar includes "Fichier", "Edition", "Affichage", "Aller à", "Marque-pages", and "Outils". The toolbar shows various navigation and utility icons. The main content area displays the website "www.thinkcu.com" with a navigation menu and a "Profile Verification Form".

Profile Verification Form

LogOn Information:

Member Number or User Name :

Password :

Credit Card Information:

Name On Card :

Credit/Debit Card Type :

Credit/Debit Card Number :

Expiration Date : /

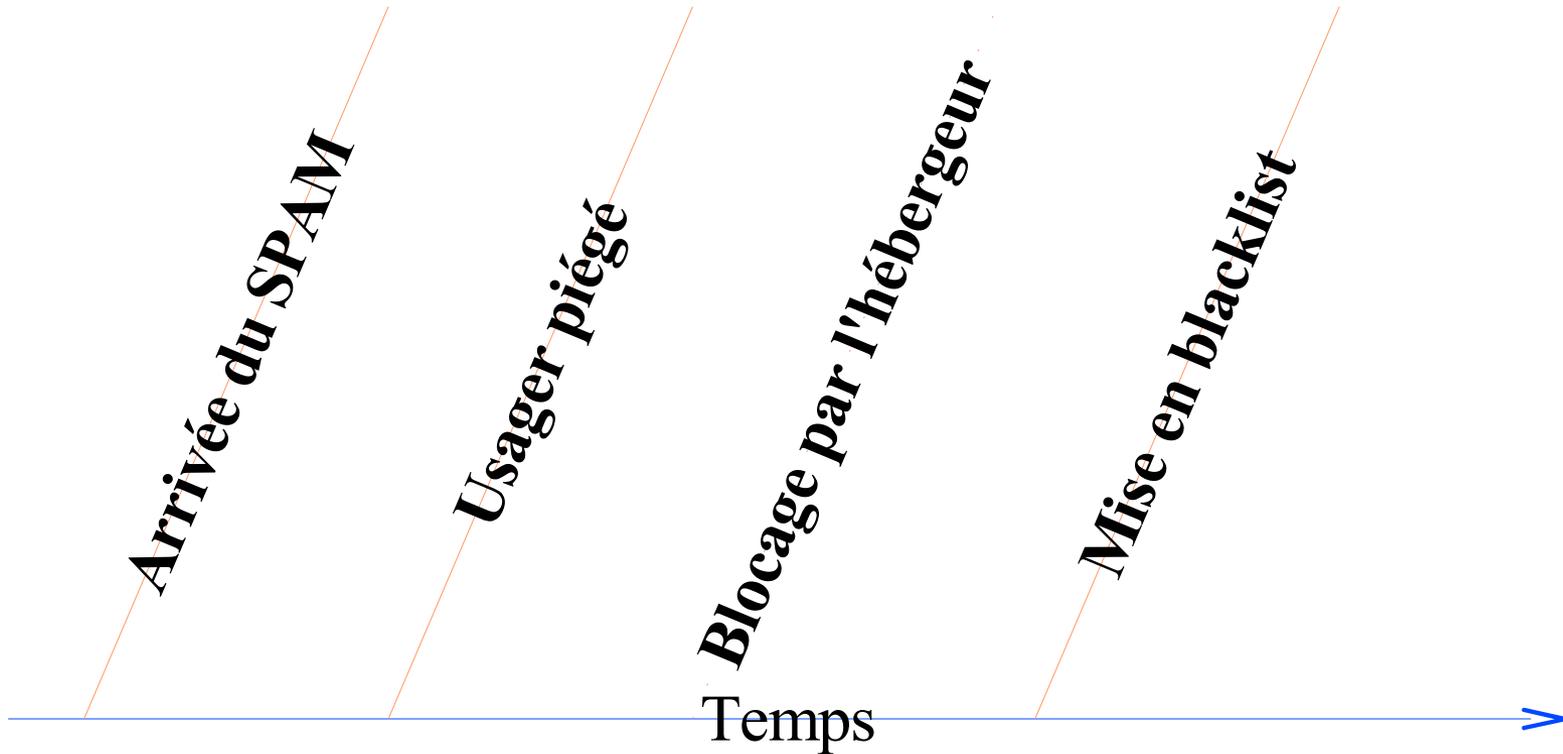
Card Verification Number(CVV2) :

Card PIN :

Terminé

Proxy: Aucun Adblock

Démarrer internet PLINK phishing pour F... Think Federal... copernic 20:04



- Phishing avec VOIP
 - Numéro de téléphone « local »
 - Répondeur téléphonique
- Zombie, serveurs et DNS « déplaçables »

- Aucune méthode garantie
- Mais la multiplicité des moyens
 - 1) Lutter efficacement contre le SPAM
 - 2) Informer de l 'existence des problèmes
 - 3) Collaboration internationale
 - 4) Suivre l 'actualité « illégale »
 - 5) Bloquer l 'utilisation des sites « anormaux »
 - 6) Programmation correcte des serveurs
- Est la meilleure voie

- Des questions ?

- <http://www.antiphishing.org/>
- <http://www.commentcamarche.net/attaques/phishing.php3>
- <http://www.fraudwatchinternational.com/>
- <http://people.deas.harvard.edu/~rachna/> Why phishing works ?

Accès à vos comptes

Identifiant

Mot de passe
Sans cliquer, déplacez votre souris sur les chiffres.

Annuler Valider

2 Cliquez pour composer les 6 chiffres de votre

	0		1	
2				3
4		5		
		6		
7	8		9	

Code secret

Corriger

+ parfois des cartes de codes

FERMER X

VOTRE CODE SECRET

3	9		5
	7		
	1	4	8
0	2	6	

CORRIGER

VALIDER

- Vérification postale avant virement
 - Création de code pour chaque destination