

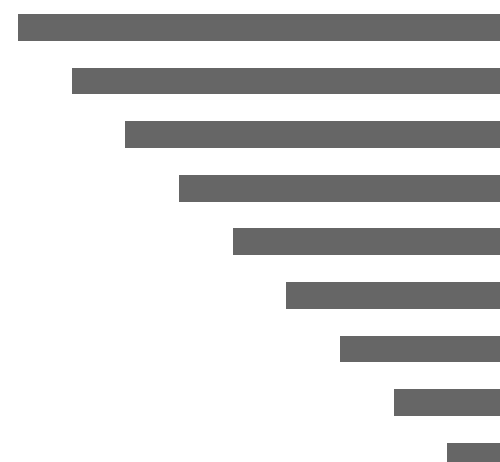
# Phishing: Por favor atualize seus dados!

RNP - Rede Nacional de Ensino e Pesquisa  
CAIS - Centro de Atendimento a Incidentes de Segurança

2 de Setembro de 2004, Workshop PoP-MG

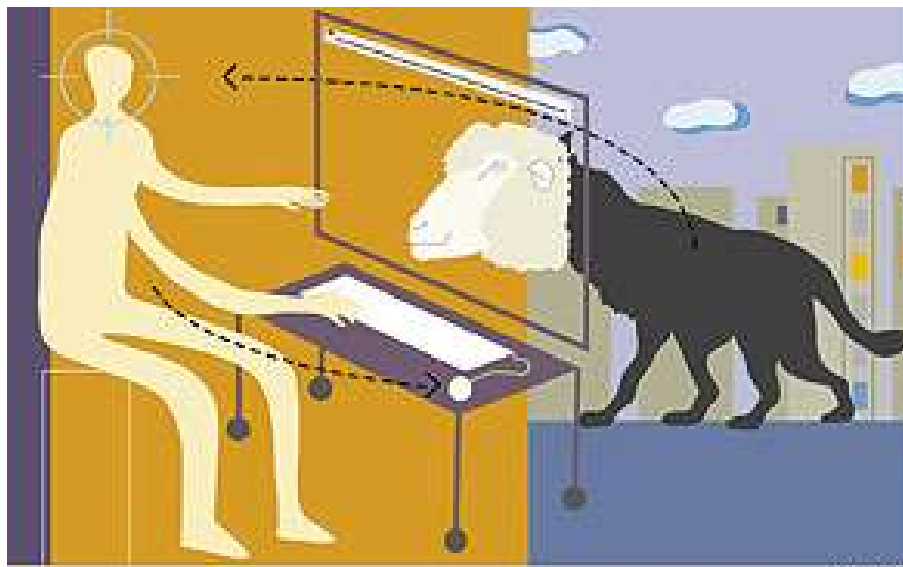


**Ronaldo Vasconcellos**



## Sumário

- Phishing?
- Características
- Amostras
- Prevenção
- Reação
- Soluções
- Estatísticas
- Artigos e Notícias Recentes
- Teste seu Q.I. de Phishing



NOVA BRUNSWICK

# Phishing: Por favor atualize seus dados!



## Phishing?

- **F**ishing se transformou em **Ph**ishing assim como no passado **F**reaking se transformou em **Ph**reaking, a exploração da rede telefônica
- Analogia com pescaria (de senhas e dados financeiros)
- A primeira menção ao termo data de Janeiro de 1996, no newsgroup *alt.2600*. O termo foi cunhado por crackers que roubavam contas da AOL.
- “Phish” - produto da fraude phishing bem sucedida: nomes de usuários, senhas e outros dados sensíveis

# Phishing: Por favor atualize seus dados!



## Características

- Engenharia Social - confiança na marca, apelativa
- Convence pela aparência, seja da mensagem ou pelo próprio site falso
- E-mail de origem forjada que aparenta ser de um instituição de crédito ou financeira de boa reputação
- uso de nomes de domínio semelhantes ao das vítimas

# Phishing: Por favor atualize seus dados!



## Amostras - Brasil



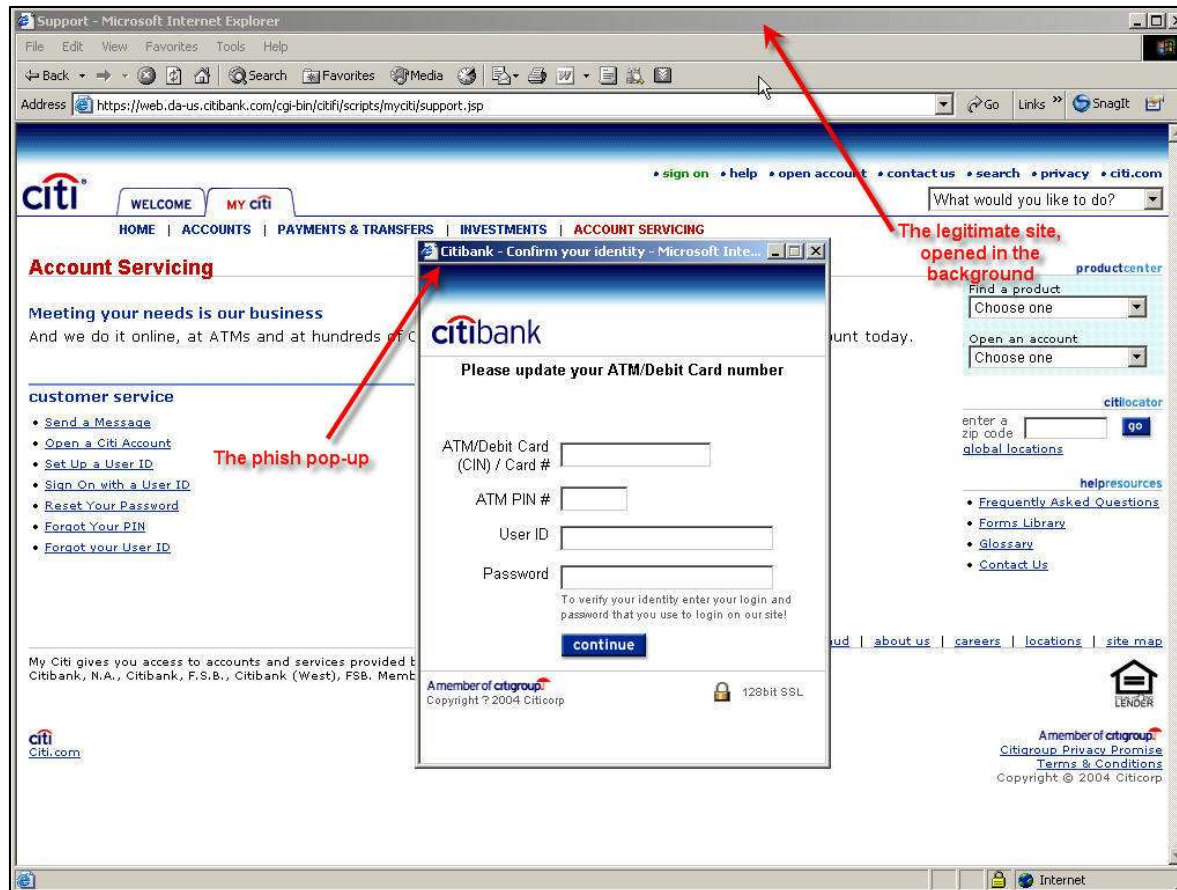
# Phishing: Por favor atualize seus dados!

## Amostras - Brasil



# Phishing: Por favor atualize seus dados!

## Amostras - Exterior



# Phishing: Por favor atualize seus dados!



## Amostras - Exterior

The screenshot shows a web browser window with the address bar containing the URL `https://www.paypal.com/cgi-bin/webscr?cmd=_login-run`. The page content is a PayPal login form. At the top, the PayPal logo is on the left, and links for [Sign Up](#), [Log In](#), and [Help](#) are on the right. Below these are navigation buttons for [Welcome](#), [Send Money](#), [Request Money](#), [Merchant Tools](#), and [Auction Tools](#). The main heading is **Member Log In**, with a [Secure Log in](#) link and a small icon. The text below reads: "Registered users log in here. Be sure to [protect your password](#)." There are two input fields: "Email Address:" and "Password:". A [Forget your password?](#) link is next to the password field. Below the fields, it says "New users [sign up here!](#) It only takes a minute." A "Log In" button is at the bottom right of the form area. At the very bottom of the page, there is a footer with links for [About](#), [Accounts](#), [Fees](#), [Privacy](#), [Security Center](#), [Contact Us](#), [User Agreement](#), [Developers](#), [Referrals](#), [Shops](#), and [Mass Pay](#), followed by the text "an eBay company" and copyright information: "Copyright © 1999-2004 PayPal. All rights reserved. [Information about FDIC pass-through insurance](#)".

A red arrow points to the address bar with the text "The entire address bar is overwritten".

**Phishing: Por favor atualize seus dados!**



## **Amostras - Exterior**

APWG - Phishing Archive

[http://antiphishing.org/phishing\\_archive.html](http://antiphishing.org/phishing_archive.html)

# Phishing: Por favor atualize seus dados!



## Estatísticas - APWG Junho de 2004

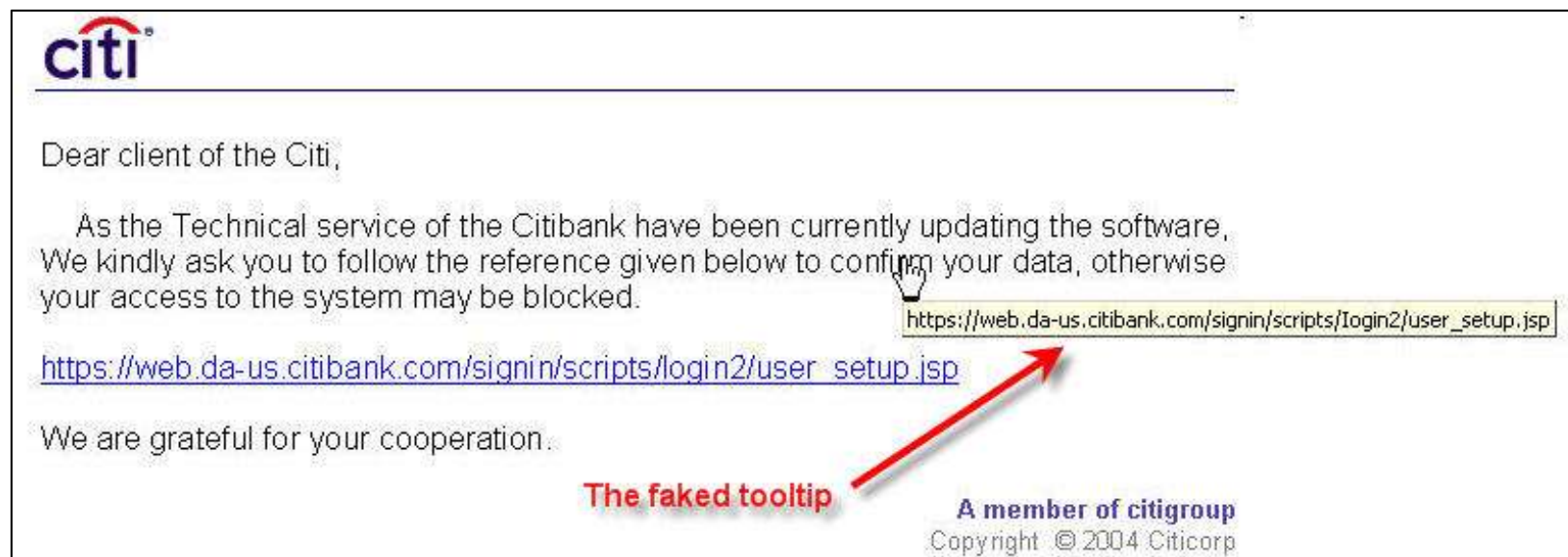
- Efetividade de marketing direto: 2%  
Efetividade de phishing: **5%**
- **54 horas** tempo médio de vida médio de um site de phishing. Alguns chegam a viver por 2 semanas
- 1422 ataques únicos - 19% de aumento em relação a Maio

# Phishing: Por favor atualize seus dados!



## Estatísticas - APWG Junho de 2004

- Técnicas de Spam
  - Assuntos
  - Contorna filtros



The screenshot shows a phishing email from Citi. The email body contains the following text:

**citi**

---

Dear client of the Citi,

As the Technical service of the Citibank have been currently updating the software, We kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.

[https://web.da-us.citibank.com/signin/scripts/login2/user\\_setup.jsp](https://web.da-us.citibank.com/signin/scripts/login2/user_setup.jsp)

We are grateful for your cooperation.

**The faked tooltip** (indicated by a red arrow) points to a tooltip that displays the URL: `https://web.da-us.citibank.com/signin/scripts/login2/user_setup.jsp`. This tooltip is a redaction of the actual URL used in the phishing attempt.

A member of citigroup  
Copyright © 2004 Citicorp

# Phishing: Por favor atualize seus dados!



## Estatísticas - APWG Junho de 2004

- Maiores Alvos nos EUA: Citibank, eBay, U.S. Bank, PayPal
- Setores da indústria mais atacados:
  - Financeiro
  - Vendas
  - Provedores de acesso a Internet
- 92% das mensagens de e-mail partem de endereços forjados

## Estatísticas - APWG Junho de 2004

- Os 5 países que mais hospedam phishing sites:
  - EUA (27%)
  - Coréia do Sul (20%)
  - China (16%)
  - Taiwan (7%)
- Para onde os dados capturados vão?
  - Mesmo Site por HTTP POST (94%)
  - Site diferente por HTTP POST (1%)
  - SMTP Mailto (1%)
  - Desconhecido (4%)

## Estatísticas - CAIS

- Maiores alvos de phishing (filtros em Agosto/04)
  - Itaú (38)
  - Banco do Brasil (11)
  - Banco Real (6)
  - Banco Safra (1)
- Renovação é freqüente



# Phishing: Por favor atualize seus dados!



## Prevenção - Usuário

- Suspeitar de mensagens com solicitações urgentes de dados particulares como nomes de usuário, número de conta, senhas, RG ou CPF
- Não fornecer os dados solicitados ou seguir URLs fornecidas em uma mensagem suspeita
- Phishers normalmente não enviam mensagens personalizadas enquanto mensagens autênticas de seu banco ou site de e-commerce são
- Verificar regularmente suas contas e extratos, atento a qualquer anomalia

# Phishing: Por favor atualize seus dados!



## Prevenção - Usuário

- Ações no cliente (browser)
  - Mantê-lo sempre atualizado
  - Instalar uma barra de ferramentas que bloqueie sites fraudulentos (disponível apenas para EUA)

### **EarthLink Toolbar - ScamBlocker**

<http://www.earthlink.net/earthlinktoolbar>

- Personal Firewall, Anti-Virus, Filtro de Spam

# Phishing: Por favor atualize seus dados!



## Prevenção - Usuário

- Se alguém **telefonasse** para você solicitando RG, CPF, número da agência e conta, data de nascimento e senha você forneceria sem questionar?
- Orientação de funcionários quanto a boas práticas de segurança
- Posição do Brasil em número de hosts 3.163.349, oitavo lugar (Network Wizards 2004) – sempre haverá um usuário que acabou de conhecer a Internet!

# Phishing: Por favor atualize seus dados!



## Prevenção - Empresas de e-commerce

- Monitorar o registro de domínios buscando por nomes semelhantes ao da própria empresa. Empresas que oferecem este serviço: Name Protect e Internet Identity.
- Estabelecer contatos que possam ser acionados diante de um ataque de phishing: outras instituições do mesmo ramo, provedores de acesso à Internet
- Métodos mais sofisticados de autenticação

# Phishing: Por favor atualize seus dados!



## Prevenção - Empresas de e-commerce

- Certificar-se de que possui uma boa infra-estrutura de e-mail e monitorar mensagens retornadas, especialmente em massa
- Adoção da RFC 2142 (Mailbox Names for Common Services, Roles and Functions), um conjunto básico de nomes de caixas de e-mail, entre elas:

security@example.com

abuse@example.com

# Phishing: Por favor atualize seus dados!



## Reação

- Provedores de acesso:
  - filtro por conteúdo é impraticável no nível de backbone
  - filtro por host
- Anti-Phishing Work Group (APWG) - fundado em Novembro de 2003 conta com mais de 400 membros de mais de 250 organizações. Predominantemente ativo nos EUA.

# Phishing: Por favor atualize seus dados!

## Soluções

- Autenticação de e-mail
  - Caller ID (Microsoft),
  - SPF (Sender Policy Framework) ou
  - Domain Keys (Yahoo!)
- Endereços forjados de e-mail são um dos principais facilitadores do golpe
- Soluções baseadas em assinaturas, como algumas que tem surgido.



# Phishing: Por favor atualize seus dados!



## Artigos e Notícias Recentes

- **30.08 - Trojan Automates Phishing Scam**  
<http://www.techweb.com/wire/story/TWB20040830S0002>
- **19.08 - Do-it-yourself phishing kits found on the internet, reveals Sophos**  
<http://www.sophos.com/spaminfo/articles/diyphishing.html>
- **16.08 - New tool identifies 'phishy' Web sites**  
<http://www.infoworld.com/article/04/08/16/HNphishywebsite.html>
- **06.08 - Aluno da PUCRS chefiava quadrilha de phishers**  
<http://info.abril.com.br/aberto/infonews/082004/06082004-4.shl>

# Phishing: Por favor atualize seus dados!



## Artigos e Notícias Recentes

- **28.07 - ST04-014: Avoiding Social Engineering and Phishing Attacks**  
<http://www.us-cert.gov/cas/tips/ST04-014.html>
- **28.06 - VeriSign introduces e-mail, anti-phishing services**  
<http://www.nwfusion.com/news/2004/0628verisintro.html>
- **22.06 - APWG Phishing Attack Trends Report - May 2004**  
[http://www.antiphishing.org/APWG\\_Phishing\\_Attack\\_Report-May2004.pdf](http://www.antiphishing.org/APWG_Phishing_Attack_Report-May2004.pdf)

**Phishing: Por favor atualize seus dados!**



**Teste seu Q.I. de Phishing**

**The MailFrontier Phishing IQ Test**

<http://survey.mailfrontier.com/survey/quiztest.html>

# Phishing: Por favor atualize seus dados!



## Referências

- **APWG – <http://www.antiphishing.org>**
- **CAIS/RNP - <http://www.cais.rnp.br>**
- **US-CERT - <http://www.us-cert.gov>**
- **SANS ISC - <http://isc.sans.org>**

# Phishing: Por favor atualize seus dados!



## Contato com o CAIS

### *E-mail*

**cais@cais.rnp.br**

Chave PGP do CAIS: **<http://www.cais.rnp.br/cais-pgp.key>**

### *Web*

Formulário para Notificação de Incidentes de Segurança  
**[http://www.cais.rnp.br/atendimento\\_form.html](http://www.cais.rnp.br/atendimento_form.html)**

### *Atendimento Emergencial*

Entre em contato com a equipe do CAIS fora do horário comercial (09h00-18h00 GMT-3) para notificar eventuais incidentes de segurança utilizando o fone **+55 61 226-9465**

### *CAIS Alerta*

Assine a lista de alertas do CAIS:

**<http://www.cais.rnp.br/alertas>**

**Phishing: Por favor atualize seus dados!**



## **Sessão de Perguntas**

