

# Incident Handling and Internet Security in Brazil

Cristine Hoepers  
<[cristine@cert.br](mailto:cristine@cert.br)>

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil  
*Computer Emergency Response Team Brazil*  
<http://www.cert.br/>

Comitê Gestor da Internet no Brasil  
*Brazilian Internet Steering Committee*  
<http://www.cgi.br/>

## Agenda

- CERT.br
  - Mission
  - CGI.br Structure
- History of Incident Response in Brazil
- CERT.br Activities
  - Training, Early Warning, Awareness, Partnerships, etc
- Other Initiatives Related to Security
- References

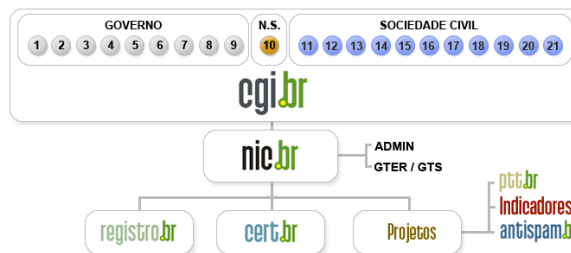
## CERT.br

- Created in 1997 to *receive, review and respond to computer security incident reports and activities related to networks connected to the Internet in Brazil.*
  - National focal point for reporting security incidents
  - Establish collaborative relationships with other entities
  - Help new CSIRTs to establish their activities
  - Provide training in incident handling
  - Produce best practices' documents
  - Help raise the security awareness in the country
  - Forum of Incident Response and Security Teams (FIRST) Full member (<http://www.first.org/membership/>)

<http://www.cert.br/mission.html>

LACNIC IX - Network Security Event - May 2006

## The Brazilian Internet Steering Committee (CGI.br)



- 1 – Ministry of Science and Technology (Coordination)
- 2 – Ministry of Communications
- 3 – Presidential Cabinet
- 4 – Ministry of Defense
- 5 – Ministry of Development, Industry and Foreign Trade
- 6 – Ministry of Planning, Budget and Management
- 7 – National Telecommunications Agency
- 8 – National Council of Scientific and Technological Development
- 9 – National Forum of Estate Science and Technology Secretaries
- 10 – Internet Expert

- 11 – Internet Service Providers
- 12 – Telecommunication Infrastructure Providers
- 13 – Hardware and Software Industries
- 14 – General Business Sector Users
- 15 – Non-governmental Entity
- 16 – Non-governmental Entity
- 17 – Non-governmental Entity
- 18 – Non-governmental Entity
- 19 – Academia
- 20 – Academia
- 21 – Academia

<http://www.cgi.br/internacional/>

LACNIC IX - Network Security Event - May 2006

## History of CSIRTs in Brazil

- **August/1996:** CGI.br released the document: "Towards the Creation of a Security Coordination Center for the Brazilian Internet."<sup>1</sup>
- **June/1997:** CGI.br created CERT.br (at that time called NBSO - NIC BR Security Office), based on the report's recommendation<sup>2</sup>
- **August/1997:** the Brazilian Research Network (RNP) created it's own CSIRT (CAIS)<sup>3</sup>, followed by the *Rio Grande do Sul* State, that created CERT-RS<sup>4</sup>
- **1999:** other institutions, including Universities and Telecommunication Companies announced their CSIRTs
- **2003:** more than 20 CSIRTs formed
- **2004:** CTIR Gov was created, with the Brazilian Federal Government Administration as their constituency<sup>5</sup>

<sup>1</sup><http://www.nic.br/grupo/historico-gts.htm>

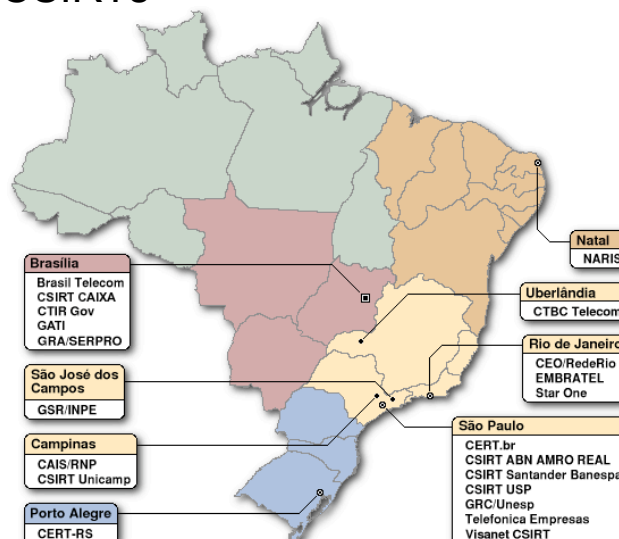
<sup>2</sup><http://www.nic.br/grupo/gts.htm>

<sup>3</sup>[http://www.rnp.br/\\_arquivo/documentos/rel-mp98.pdf](http://www.rnp.br/_arquivo/documentos/rel-mp98.pdf)

<sup>4</sup><http://www.cert-rs.tcche.br/cert-rs.html>

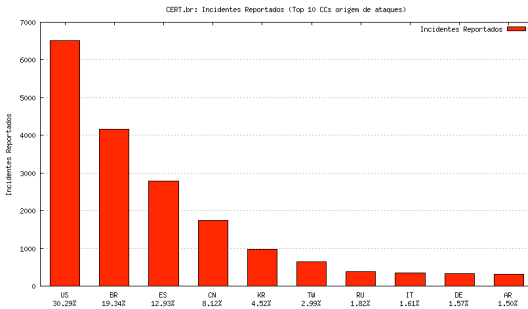
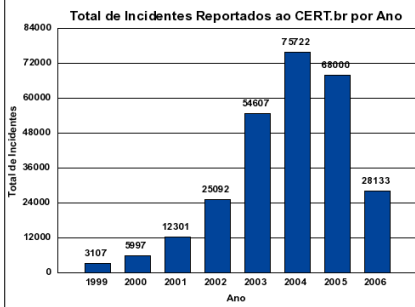
<sup>5</sup><http://www.ctir.gov.br>

## Brazilian CSIRTs



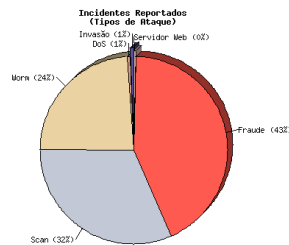
# CERT.br Activities

## Incident Handling and Statistics



<http://www.cert.br/stats/incidentes/>

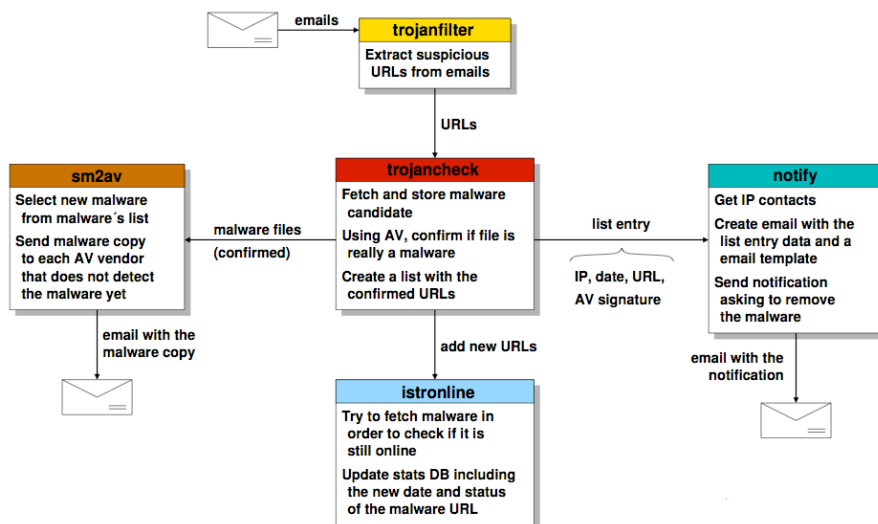
<http://www.cert.br/stats/spam/>



## Anti-Fraud Activities

- In Brazil fraud is almost all based on malicious codes disseminated through social engineering
- CERT.br and Financial Institutions:
  - Share technical details about crimeware, new social engineering techniques, malicious codes, etc
  - CERT.br:
    - Notifies sites hosting crimeware related to frauds
    - Coordinates with international sites and CSIRTs to take down the crimeware sites
    - Send new crimeware (trojans, keyloggers, etc) to 24 anti-virus vendors
    - Anti-Phishing Working Group (APWG) Research Partner <http://www.antiphishing.org/>

## Trojan Notification System



# Best Practices for Internet Users

The screenshot shows the main page of the 'Cartilha de Segurança para Internet' (Internet Security Handbook) on the CERT.br website. The page is titled 'Cartilha de Segurança para Internet' and includes a navigation menu with links for 'Início da Cartilha', 'Dicas', 'Download', 'Checklist', 'Glossário', and 'Sobre o CERT.br'. The main content area lists the following sections:

- ATENÇÃO:** Veja o aviso sobre a fraude envolvendo o nome do CERT.br e da Cartilha de Segurança para Internet
- A Cartilha de Segurança para Internet contém recomendações e dicas sobre como o usuário deve se comportar para aumentar a sua segurança e se proteger das ameaças na Internet. Além disso, apresenta o significado de diversos termos e conceitos utilizados na Internet e fornece uma série de procedimentos que visam melhorar a segurança de um computador.
- Parte I: Conceitos de Segurança**
- Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção**
- Parte III: Privacidade**
- Parte IV: Fraudes na Internet**
- Parte V: Redes de Banda Larga e Redes Sem Fio (Wireless)**
- Parte VI: Spam**
- Parte VII: Incidentes de Segurança e Uso Abusivo da Rede**
- Parte VIII: Códigos Maliciosos (Malware)**
- Checklist**
- Glossário**

On the right side of the page, there are several widgets: 'Dica do Dia' (Daily Tip) with a link to 'Saber mais', 'Copyright', 'Contato', 'Agradecimentos', and 'Revisões'. At the bottom of the page, it says 'LACNIC IX - Network Security Event - May 2006' and features logos for 'cgi.br' and 'nic.br'.

# Best Practices for Internet Users - Tips

The screenshot shows the 'Dicas' (Tips) page of the 'Cartilha de Segurança para Internet' on the CERT.br website. The page is titled 'Cartilha de Segurança para Internet' and includes a navigation menu with links for 'Início da Cartilha', 'Dicas', 'Download', 'Checklist', 'Glossário', and 'Sobre o CERT.br'. The main content area provides the following information:

Nesta página está disponível uma compilação de dicas básicas de segurança. Estas dicas também estão em 2 folhetos disponíveis para download. Para visualizá-los você precisa ter instalado em seu computador o software [Acrobat Reader](#).

- Proteja-se de fraudes**
  - Atualize seu antivírus diariamente.
  - Não clique em *links* recebidos por e-mail.
  - Não execute arquivos recebidos por e-mail ou via serviços de mensagem instantânea.
- Proteja-se de vírus, cavalos de tróia, spywares, worms e bots**
  - Mantenha todos os programas que você usa sempre atualizados.
  - Instale todas as correções de segurança.
  - Use antivírus, *firewall* pessoal e anti-spyware.
- Navegue com segurança**
  - Mantenha seu navegador sempre atualizado.
  - Desative Java e ActiveX. Use-os apenas se for estritamente necessário.
  - Só habilite JavaScript, cookies e pop-up windows ao acessar sites confiáveis.
- Cuide-se ao ler e-mails**

On the right side of the page, there are two download options:

- Folheto com dicas de segurança, formato A4. (102 KB)**
- Folder com dicas de segurança, formato A4. (1.1 MB)**

At the bottom of the page, it says 'LACNIC IX - Network Security Event - May 2006' and features logos for 'cgi.br' and 'nic.br'.

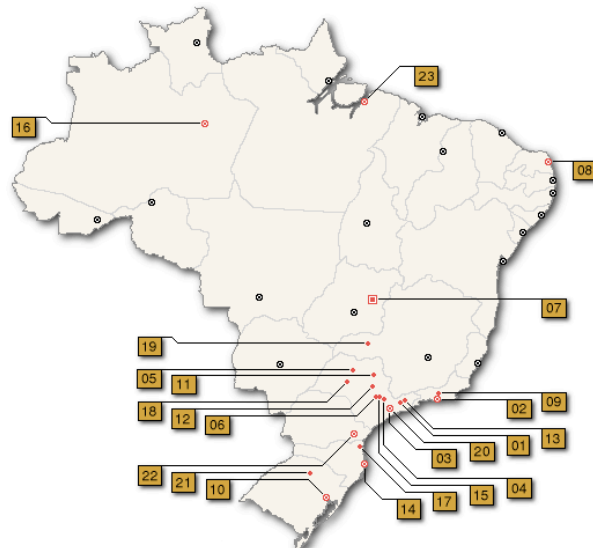
## Trend Analysis and Early Warning

### Brazilian Honeypots Alliance - Distributed Honeypots Project

**Objective:** to increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet

- Joint Coordination: CERT.br and CenPRA/MCT
- 35 partner's institutions:
  - Academic, government, industry, telecom and military networks
- Widely distributed across the country
- Based on voluntary work
- Maintain public statistics
- <http://www.honeypots-alliance.org.br/>
- Honeynet Research Alliance Member since June 2002  
<http://honeynet.org/alliance/>

## Cities Where the Honeypots are Located

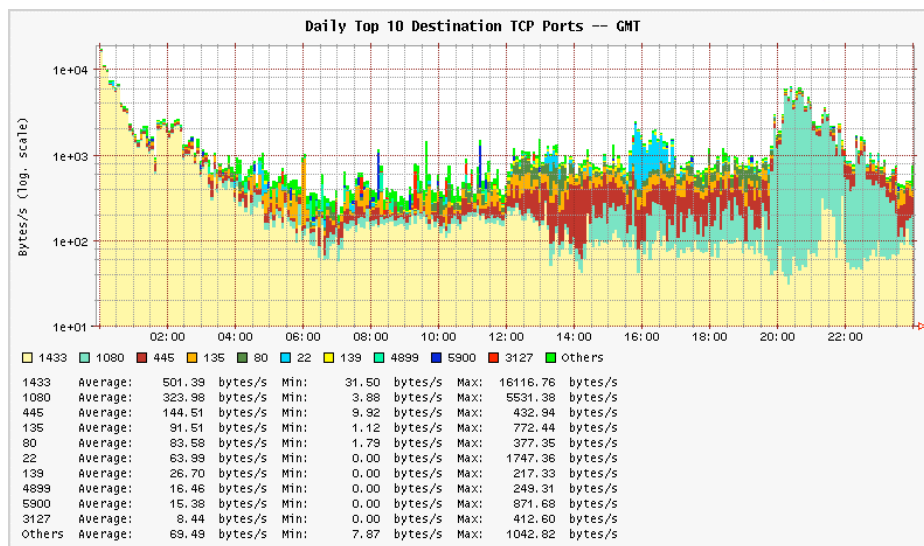


## Partners of the Brazilian Honeypots Alliance

#	City	Institutions
01	São José dos Campos	INPE, ITA
02	Rio de Janeiro	CBPF, Embratel, Fiocruz, IME, PUC-RIO, RedeRio, UFRJ
03	São Paulo	ANSP, CERT.br, Diveo, Durand, UNESP, USP
04	Campinas	CenPRA, HP Brazil, ITAL, UNICAMP, UNICAMP FEEC
05	São José do Rio Preto	UNESP
06	Piracicaba	USP
07	Brasília	Brasil Telecom, Ministry of Justice, TCU, UNB LabRedes
08	Natal	UFRN
09	Petrópolis	LNCC
10	Porto Alegre	CERT-RS
11	Ribeirão Preto	USP
12	São Carlos	USP
13	Taubaté	UNITAU
14	Florianópolis	UFSC DAS
15	Americana	VIVAX
16	Manaus	VIVAX
17	Joinville	UDESC
18	Lins	FPTE
19	Uberlândia	CTBC Telecom
20	Santo André	VIVAX
21	Passo Fundo	UPF
22	Curitiba	PoP-PR
23	Belém	UFPA

LACNIC IX - Network Security Event - May 2006

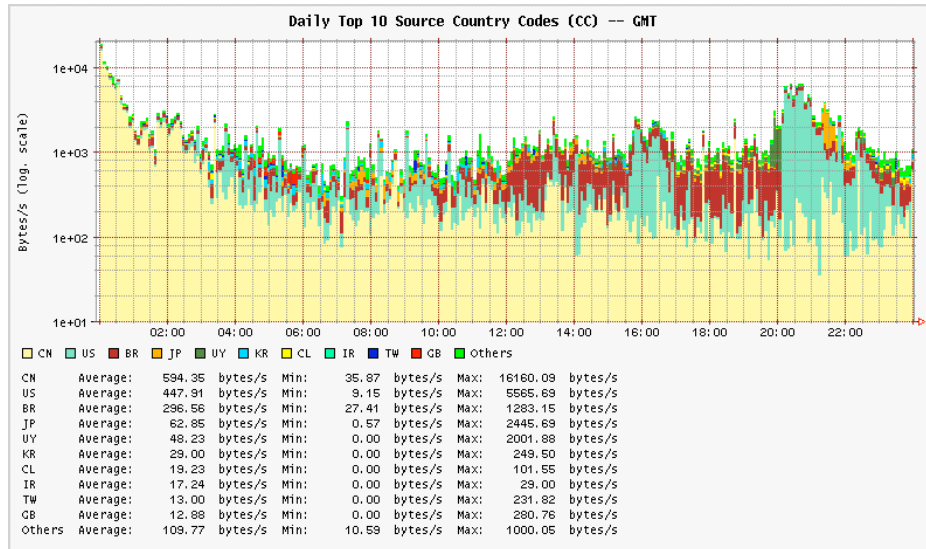
## Honeypots Flows - Top Destination TCP Ports



May 17, 2006 - <http://www.honeypots-alliance.org.br/stats/>  
LACNIC IX - Network Security Event - May 2006

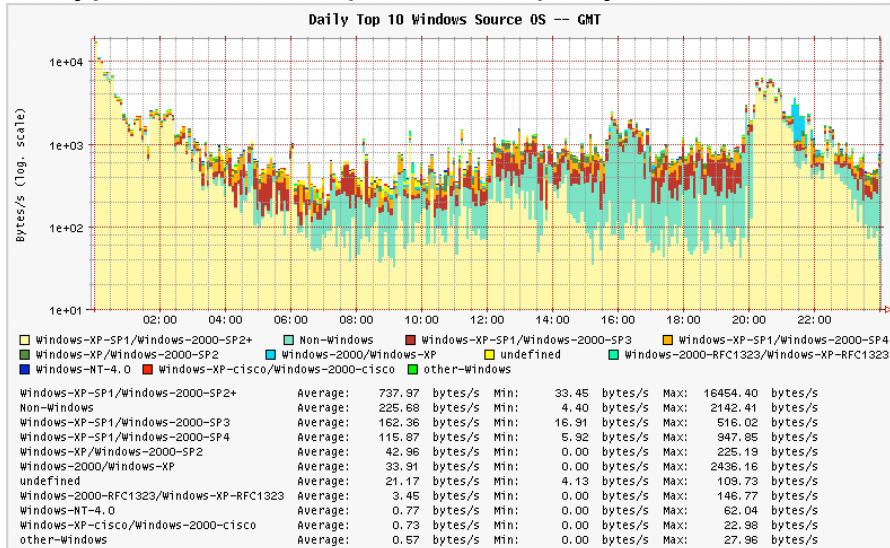


## Honeypots Flows - Top Source Country Codes



May 17, 2006 - <http://www.honeypots-alliance.org.br/stats/>  
LACNIC IX - Network Security Event - May 2006

## Honeypots Flows - Top Source Op. Systems



May 17, 2006 - <http://www.honeypots-alliance.org.br/stats/>  
LACNIC IX - Network Security Event - May 2006

## Support for new CSIRTs

- Help new CSIRTs to establish their activities
  - Meetings, presentations to C-level managers, training, etc
- SEI<sup>SM</sup>/CMU Partner, licensed to deliver CERT<sup>®</sup> Program courses in Brazil:
  - Creating a Computer Security Incident Response Team
  - Managing Computer Security Incident Response Teams
  - Fundamentals of Incident Handling
  - Advanced Incident Handling for Technical Staff
- 160+ incident handlers trained

<http://www.cert.br/cursos/>

LACNIC IX - Network Security Event - May 2006

## Other CGI.br Initiatives Related to Security

LACNIC IX - Network Security Event - May 2006

## CGI.br Anti-Spam Comission

- Created by CGI.br to articulate, with all players, viable solutions to reduce the spam problem  
<http://www.cgi.br/sobre-cg/antispam.htm>
- Produced material that include tips for preventing from security problems coming through email
  - All material available at the [www.antispam.br](http://www.antispam.br) site
- CERT.br helped to produce 2 documents
  - Technologies and Policies to Fight Spam
  - Technical Analysis of Anti-spam Legislation

## The antispam.br website

The screenshot shows the antispam.br website in a browser window. The page layout includes a top navigation bar with links like 'Sobre o NIC.br', 'Indicadores', 'Antispam.br', and 'PTT.br'. A left sidebar contains a menu with items such as 'O que é spam?', 'Problemas causados pelo spam', 'Origem e curiosidades', 'Tipos de spam', 'Como identificar', 'Prevenção', 'Boas práticas', 'Dicas', 'Como reclamar', 'FAQ', 'Links', 'Glossário', 'Créditos', and 'Mapa do site'. The main content area features a central illustration of a blue character with a magnifying glass over a globe, surrounded by papers. Text sections include 'O que é spam?' (defining spam and zombies), 'Participe da campanha' (encouraging participation), 'Como identificar' (tips for identifying spam), and 'Dicas de prevenção' (prevention tips). The footer displays logos for CGI.br, NIC.br, Registro.br, and CERT.br.

## Malicious codes and their relation to emails

Comitê Gestor da Internet no Brasil  
Sobre o NIC.br | Indicadores | Antispam.br | PTT.br

Início - Administradores de redes - Estatísticas - Sobre o Antispam.br

**antispam.br**

O que é spam?  
Problemas causados pelo spam  
Origem e curiosidades  
Tipos de spam  
Como identificar  
Prevenção  
Boas práticas  
Dicas  
Como reclamar  
FAQ  
Links  
Glossário  
Créditos  
Mapa do site

Busca

NIC.br Antispam.br  
CERT.br Registro  
CERT.br

**Tipos de spam**

A Balar

**Códigos maliciosos**

São programas que executam ações maliciosas em um computador. Diversos tipos de códigos maliciosos são inseridos em e-mails, contendo textos que se valem de métodos de engenharia social para convencer o usuário a executar o código malicioso em anexo. Em geral, estes códigos também são utilizados em spams enviados por fraudadores.

Dentre os códigos mais comuns enviados via spam, pode-se citar as seguintes categorias:

- **Backdoor:** Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.
- **Spyware:** Temo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.
- **Keylogger:** Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou Internet Banking, para a captura de senhas bancárias ou números de cartões de crédito.
- **Screenlogger:** Forma avançada de keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar e registrar que circunda a posição onde o mouse é clicado.
- **Cavalo de tróia:** Programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

LACNIC IX - Network Security Event - May 2006

## Frauds that come through emails

Comitê Gestor da Internet no Brasil  
Sobre o NIC.br | Indicadores | Antispam.br | PTT.br

Início - Administradores de redes - Estatísticas - Sobre o Antispam.br

**antispam.br**

O que é spam?  
Problemas causados pelo spam  
Origem e curiosidades  
Tipos de spam  
Como identificar  
Prevenção  
Boas práticas  
Dicas  
Como reclamar  
FAQ  
Links  
Glossário  
Créditos  
Mapa do site

Busca

NIC.br Antispam.br  
CERT.br Registro  
CERT.br

**Tipos de spam**

A Balar

**Fraudes**

Normalmente, não é uma tarefa simples alocar e fraudar dados em um servidor de uma instituição bancária ou comercial. Então, atacantes têm concentrado seus esforços na exploração de fragilidades dos usuários, para realizar fraudes comerciais e bancárias através da Internet.

Para obter vantagens, os fraudadores têm utilizado amplamente e-mail com discursos que, na maioria dos casos, envolvem engenharia social e que tentam persuadir o usuário a fornecer seus dados pessoais e financeiros. Em muitos casos, o usuário é induzido a instalar algum código malicioso ou acessar uma página fraudulenta, para que dados pessoais e sensíveis, como senhas bancárias e números de cartões de crédito, possam ser furtados. Desta forma, é muito importante que usuários da Internet tenham certos cuidados com os e-mails que recebem e ao utilizarem serviços de comércio eletrônico ou Internet Banking.

**Sumário**

- Golpes (Scams)
- Phishing: situações em que pode ocorrer este tipo de fraude
- Mensagens que contêm links para programas maliciosos
- Como o fraudador consegue acesso ao seu computador
- Como identificar
- Recomendações

**Golpes (Scams)**

Um dos fatos marcantes na história do spam tem sido sua utilização para disseminação de golpes. Os antigos, já praticados por meio de cartas ou ligações telefônicas, migraram para a Internet, propagados via spam. Um exemplo é o Golpe da Nigéria, também conhecido como golpe do 419 ou do 171, os famosos "contos do vigário".

LACNIC IX - Network Security Event - May 2006

## Tips to prevent spam and security problems



The screenshot shows the website <http://www.antispam.br/dicas/>. The page is titled "Dicas" (Tips) and provides several sections of advice:

- Principais dicas para ajudar o usuário a receber menos spam, preservar sua privacidade e evitar que códigos maliciosos sejam instalados em seu computador:**
  - Preserve sua privacidade:**
    - Seja cauteloso ao informar seus endereços de e-mail em cadastros, sites de relacionamentos etc.
    - Tenha e-mails diferentes para uso pessoal, trabalho, compras on-line e cadastros em sites em geral.
    - Evite utilizar e-mails simples, como aqueles formados apenas pelo primeiro nome.
    - Leia com atenção os formulários e cadastros on-line, evitando preencher ou concordar, inadvertidamente, com as opções para recebimento de e-mails de divulgação do site e de seus parceiros.
    - Não forneça dados pessoais, documentos e senhas por e-mail ou via formulários on-line.
    - Verifique a política de privacidade dos sites, onde pretende registrar seus dados.
  - Mantenha-se informado:**
    - Conhecer os tipos de spam ajuda a reconhecer e-mails suspeitos e, eventualmente, não detectados pelos softwares anti-spam.
    - Acompanhar as notícias e alertas sobre os golpes e fraudes, reduz o risco de ser enganado e/ou prejudicado financeiramente por e-mails desse gênero.
    - Procurar informações sobre fatos recebidos por e-mail, antes de repassá-los, contribui para a redução do volume de mensagens de correias, boatos e lendas urbanas, enviadas repetidas vezes na rede.
    - Procurar informações no site das empresas, ao receber e-mails sobre prêmios e promoções, reduz o risco de ser enganado em golpes propagados por e-mail.
  - Proteja-se:**
    - Utilize softwares de proteção (antivírus, anti-spam, anti-spyware e firewall pessoal) nos computadores de uso doméstico e corporativo, mantendo-os com as versões, assinaturas e configurações atualizadas.
    - Não seja um "cliqueador compulsivo". Não execute arquivos anexados em e-mails sem examiná-los previamente com antivírus, bem como, não clique em URLs incluídas em e-mails.
    - Procure informações sobre os recursos técnicos do seu software anti-spam. Configure as listas negras e listas brancas. Monitore a quarentena, se for o caso.

The page also features a sidebar with navigation links such as "O que é spam?", "Problemas causados pelo spam", "Tipos de spam", and "Como identificar". There is also a search bar and a "Busca" section with radio buttons for "NIC.br", "Antispam.br", "CERT.br", and "Registro.br".

LACNIC IX - Network Security Event - May 2006

## CGI.br Indicators

- Survey on the Use of Information and Communication Technologies In Brazil 2005
- Includes indicators about security and spam
  - **Households:** security problems encountered, security measures adopted, antivirus updating frequency, frequency they receive spam, time spent with spam, etc.
  - **Enterprises:** identified IT security problems, security measures adopted, antivirus updating frequency, technologies adopted for secure communication, etc.



<http://www.nic.br/indicadores/>

<http://www.nic.br/indicadores/indicadores.pdf>

## References

- This presentation
  - <http://www.cert.br/docs/palestras/>
  - <http://www.cert.br/docs/presentations/>
- CSIRT development references (English and Portuguese)  
<http://www.cert.br/csirts/>
- Best Practices in Portuguese:
  - Tips for home users (*Cartilha de Segurança para Internet*)  
<http://cartilha.cert.br/>
  - Security Best Practices for System and Network Administrators (*Práticas de Segurança para Administradores de Redes Internet*)  
<http://www.cert.br/seg-adm-redes/>
- SEI<sup>SM</sup>/CMU CERT<sup>®</sup> Program Courses delivered by CERT.br  
<http://www.cert.br/cursos/>
- CERT.br Statistics  
<http://www.cert.br/stats/>
- Comitê Gestor da Internet - CGI.br: <http://www.cgi.br/>
- CGI.br Indicators: <http://www.nic.br/indicadores/>

## References (cont)

### CSIRTs around the world:

- FIRST Member Teams  
<http://www.first.org/about/organization/teams/>
- National Computer Emergency Response Teams  
<http://www.cert.org/csirts/national/contact.html>
- TI Directory of European CSIRTs  
<http://www.ti.terena.nl/teams/>
- APCERT Member Teams  
<http://www.apcert.org/about/structure/members.html>
- Brazilian CSIRTs Contact Information  
<http://www.cert.br/contact-br.html>