

INTERESSADO EM OUTRAS REFERÊNCIAS ?

- **CAIS – Centro de Atendimento a Incidentes de Segurança**
<http://www.rnp.br/cais/>
- **Internet Storm Center**
www.isc.sans.org
- **The Twenty Most Critical Internet Security Vulnerabilities**
<http://www.sans.org/top20/>
- **VirusTotal**
www.virustotal.com
- **US-CERT**
<http://www.us-cert.gov/>
- **Microsoft Security Brasil**
<http://www.microsoft.com/brasil/security/default.aspx>
- **Guide to Information Security 2005 – 2006**
http://www.upenn.edu/computing/security/brochure/brochure_current.html
- **Computer Security Day**
<http://www.computersecurityday.org/>

GLOSSÁRIO:

- **Bot:** Programa malicioso instalado em um computador, capaz de receber ordens, executar ações ou roubar dados de usuários através de comandos em canais de IRC.
- **IRC:** *Internet Relay Chat*, é uma forma de comunicador instantâneo, no qual os usuários se encontram dentro de canais (salas de bate-papo) para conversar.
- **Malware:** Todo tipo de programa cuja finalidade é executar alguma atividade maliciosa ou não solicitada pelo usuário.
- **Phishing Scam:** Golpe de engenharia social no qual o usuário é induzido a acessar páginas falsas na Internet e fornecer dados sigilosos

para golpistas despercebidamente.

- **Spywares:** Programas instalados no sistema sem o consentimento do usuário, cuja finalidade é capturar informações pessoais, fazer propaganda ou mesmo oferecer serviços.
- **SSID:** *Service Set Identifier*, é uma sequência de letras ou números que identifica uma rede sem fio.
- **WEP:** *Wired Equivalency Privacy*, sendo um protocolo de segurança para redes sem fio, mas com vulnerabilidades conhecidas.
- **WPA:** *Wi-Fi Protected Access*, um outro padrão de segurança para redes sem fio, mas mais seguro que o WEP.

CONTRIBUA E PARTICIPE:

- Envie e-mails de Phishing Scam para phishing@cais.rnp.br
- Envie e-mails contendo malware anexados ou links para malware para artefatos@cais.rnp.br
- Receba gratuitamente os alertas de segurança divulgados pelo CAIS:
<http://www.rnp.br/cais/alertas/> ou RSS em <http://www.rnp.br/cais/alertas/rss.xml>

CAIS / RNP Campinas
Prédio da Embrapa/Unicamp
Av. André Tosello, 209
Cidade Universitaria Zeferino Vaz
13083-886 – Campinas,SP

Tel.: +55 19 3787-3300
Fax: +55 19 3787-3301
INOC-DBA: 1916*800

cais@cais.rnp.br
www.rnp.br/cais



DISI 2005

Dia Internacional de Segurança em Informática

SEGURANÇA RESPONSÁVEL:
Dicas e boas práticas para
manter-se seguro.

Em Comemoração ao
30 de Novembro, Dia Internacional de Segurança em
Informática (DISI 2005), uma iniciativa de Computer
Security Day

MANTENDO SEU MICRO SEGURO

- Utilize um anti-vírus e anti-spyware atualizados diariamente, bem como um firewall pessoal.
- Atualize rotineiramente seu sistema operacional e aplicativos.
- Instale as correções de segurança disponibilizadas pelos fabricantes dos programas que você utiliza.
- Desabilite compartilhamentos e serviços que você não utiliza no micro.
- Utilize sempre softwares originais.

LIDANDO COM E-MAILS Spams, Fraudes e Vírus

- Jamais clique em programas recebidos por e-mail cuja origem você desconhece.
- Verifique com anti-vírus atualizado os arquivos recebidos por e-mail antes de executá-los.
- Habilite filtros anti-spam de seu webmail (muitos provedores hoje fornecem estes serviços).
- A menos que você solicite, bancos nunca entram em contato com clientes através de e-mail, muito menos operadoras de cartões de crédito.
- Desconfie de TODAS as mensagens recebidas por e-mail cujo conteúdo solicite informações ou atualizações de dados pessoais.
- Não clique em URLs de bancos recebidas por e-mail. Elas normalmente direcionam usuários para sites fraudulentos.

NAVEGANDO NA INTERNET DE FORMA SEGURA

- Acostume-se a sempre digitar manualmente no seu browser o endereço (URL) do seu banco.
- Em acessos a páginas da Internet que peçam login e senha, sempre verifique a presença do cadeado fechado no canto inferior direito do seu browser.
- Desative a execução de Java, Javascript, ActiveX, pop-ups e o recebimento de cookies no seu browser. Ative a execução destes somente para sites confiáveis.
- Não divulgue informações pessoais como telefone ou endereço em sites de relacionamentos pessoais, blogs ou mesmo em comunicadores instantâneos (Icq, Msn, etc).
- Não acesse páginas bancárias ou que necessitem de informações confidenciais em computadores que você não confia (Cyber-Cafés, por exemplo).
- Instale ferramentas que ajudem a verificar a confiabilidade das URLs acessadas, como o "Anti-Phishing Toolbar", da NetCraft (www.netcraft.com)



SENHAS, COMO ESCOLHÊ-LAS CORRETAMENTE

- Não utilize senhas baseadas em informações pessoais, sequências de números (123456) ou palavras de dicionários.
- Utilize pelo menos 6 caracteres em senhas, misturando letras, números e caracteres especiais (, . @ # % * , etc).
- Construa senhas baseadas em frases: Frase: "Segurança.*é*. importante!" Senha: S.*e*.i!
- Caso desconfie que sua senha foi violada, modifique-a e avise a instituição envolvida imediatamente .

UTILIZANDO REDES SEM FIO

- Utilize WEP ou WPA sempre que possível.
- Tente obter informações sobre o SSID da rede que pretende acessar antes de conectar-se.
- Em redes Wi-Fi públicas, evite acessar sites de bancos, webmails ou outros que necessitem de informações pessoais.
- Não crie conexões Ad-hoc (micro-a-micro) com computadores que você não conhece.
- Desabilite sempre o Bluetooth ou Infra-vermelho de seus aparelhos (laptop, celular, PDA) quando não estiver usando tais serviços.

DESCONFIE E DENUNCIE !

- Caso note diferenças, mesmo que sutis, no acesso pela Internet ao seu banco, entre em contato imediatamente com sua agência.
- Envie possíveis e-mails de Phishing Scam (fraude) que você venha a receber para o grupo de segurança da instituição envolvida.
- Em caso de dúvidas sobre como proceder, contate sempre o grupo de segurança da instituição envolvida.