GLOSSÁRIO

- **Firewall:** Ferramenta cuja finalidade é filtrar o tráfego de rede que entra e sai do sistema.
- **URL:** Uniform Resource Locator. É o endereço de um recurso (site, arquivo, etc) disponível na rede. Exemplos comuns de URL são endereços de internet do tipo http://www.rnp.br.
- **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 a fornecer dados sigilosos para golpistas.
- **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 Identier é uma sequência de letras ou números utilizada como nome de uma rede sem fio.
- **WEP:** Wired Equivalency Privacy. Trata-se de um protocolo de segurança para redes sem fio, mas com vulnerabilidades conhecidas.
- **WPA:** Wi-Fi Protected Access. É um outro padrão de segurança para redes sem fio, mais seguro que o WEP.
- **WPA2:** É o protocolo mais seguro para redes sem fio atualmente, sendo recomendada a sua utilização.

INTERESSADO EM MAIS INFORMAÇÕES?

- CAIS – Centro de Atendimento a Incidentes de Segurança: http://www.rnp.br/cais/
- DISI – Dia Internacional de Segurança em Informática: http://www.disi.rnp.br/
- Catálogo de fraudes do CAIS http://www.rnp.br/cais/fraudes.php

'11 DISI

DIA INTERNACIONAL DE SEGURANÇA EM INFORMÁTICA

Realização

CAIS

Apoio

UFPR 100 Anos 1912 • 2012

Patrocínio

Trustwave SpiderLabs

Parceria

RedCLARA + Red + Ciencia

Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

RNP

Ministério da **Educação**

Ministério da **Cultura**

Ministério da **Ciência e Tecnologia**

GOVERNO FEDERAL BRASIL PAÍS RICO É PAÍS SEM POBREZA

'11 DISI

DIA INTERNACIONAL DE SEGURANÇA EM INFORMÁTICA

CONSCIENTIZAÇÃO EM SEGURANÇA UM DEVER DE TODOS

31.AGO.2011
CURITIBA

NAVEGANDO DE FORMA SEGURA

- Acostume-se a sempre digitar manualmente no seu navegador 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 navegador.
- Aprenda como funcionam os certificados digitais no seu navegador: http://cartilha.cert.br/conceitos/sec9.html
- Desative a execução de Java, Javascript, ActiveX, pop-ups e o recebimento de cookies no seu navegador. 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 (cibercafés, por exemplo).
- Habilite a verificação de phishing no seu navegador e instale ferramentas que ajudem a verificar a confiabilidade das URLs acessadas, como o Anti-Phishing Toolbar, da NetCraft (toolbar.netcraft.com/).

SENHAS, COMO ESCOLHÊ-LAS

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

MANTENDO O 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 software original.

LIDANDO COM E-MAILS

- 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 abri-los.
- Habilite os filtros anti-spam e anti-vírus do 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.

UTILIZANDO REDES SEM FIO

- Utilize WPA/WPA2 sempre que possível (WEP em último caso).
- 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.
- Lembre-se que, em redes abertas (sem segurança), o tráfego não é protegido. Ou seja, todos os acessos à Internet podem ser capturados por terceiros.
- Não crie conexões Ad-hoc (micro-a-micro) com computadores que você não conhece.
- Desabilite sempre o Bluetooth ou Infravermelho 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.

CONTRIBUA E PARTICIPE

- Envie e-mails de fraudes 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 em RSS http://www.rnp.br/cais/alertas/rss.xml
- Utilize o servidor de Sincronismo de Hora do CAIS: ntp.cais.rnp.br