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.
* *BotNet:* Redes de computadores infectados com Bot e controlados através de canais 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 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 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.

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.rnp.br/eventos/disi/
* Computer Security Day
  http://www.computersecurityday.org/
* SaferNet Brasil
  http://www.safernet.org.br/site/prevencao
* Microsoft Security Brasil
  http://www.microsoft.com/brasil/security/
* Centro de Tratamento de Incidentes de Segurança em Rede de Computadores da Administração Pública Federal
  http://www.ctir.gov.br

CONTRIBUA E PARTICIPE

* Envie e-mails de fraudes para:
  phishing@cais.rnp.br
* Acesse o Catálogo de fraudes do CAIS
  http://www.rnp.br/cais/fraudes.php
* 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

Apoio:

Realização:

CAIS Centro de Atendimento a Incidentes de Segurança

RNP

Ministério da Educação

Ministério da Ciência e Tecnologia

BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

2008 DISI

Prevenção: a melhor forma de defesa contra ameaças

http://www.rnp.br/eventos/disi/2008/

Em comemoração ao Dia Internacional de Segurança em Informática (DISI).

Uma iniciativa de Computer Security Day (http://www.computersecurityday.org)

CAIS

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

Spam, 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* 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.

NAVEGANDO NA INTERNET 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 (www.netcraft.com).

SENHAS, COMO ESCOLHÊ-LAS CORRETAMENTE

* 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 .

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.

segurança*prevenção