Linha Defensiva

www.linhadefensiva.org

Como evitar fraudes na Internet

Altieres Rohr e Fábio Assolini

Dia Internacional da Segurança em Informática

Linha Defensiva

- Online desde 28 de janeiro de 2005
- Parceira do UOL: maio/2005 - setembro/2008
- Mais de 18.000 casos resolvidos no Fórum
- Mais de 3 milhões de downloads de ferramentas
- Atualmente conta com 17 voluntários

“Defendendo seu PC contra os perigos da Internet”

Áreas de Atuação

1. Repasse de informação
2. Prevenção
3. Monitoramento
4. Remoção e auxílio

Áreas de Atuação

1. Repasse de informação
2. **Prevenção**
3. Monitoramento
4. Remoção e auxílio

ARIS/LD

- Grupo de Análise e Resposta a Incidentes de Segurança
- Realiza análise de fraudes, publicação de alertas e monitoramento de ataques

  http://twitter.com/linhadefensiva
- Trabalha com provedores usados por criminosos para tirar fraudes do ar

O que é uma 'fraude'?

No Brasil, chama-se “fraude” qualquer e-mail cujo objetivo é enganar o internauta e incentivá-lo a acessar um site ou realizar uma tarefa que irá prejudicá-lo. Geralmente é enviada em massa, para milhares de destinatários.

Por que criam-se fraudes?

Para roubar informações como credenciais de acesso a **bancos**, sites de **redes sociais**, **mensageiros** instantâneos, caixas de **e-mail** e até **jogos**.

Como são roubadas as senhas?

- O e-mail fraudulento contém um link
- Ao ser acessado, ele tentará instalar códigos maliciosos no computador da vítima. Este código irá roubar as senhas.
- Ou então ele apresenta uma página falsa em que o internauta digitará suas credenciais
- É um exemplo de **engenharia social**

Classificação de Fraudes

- **Sementes de trojan** – buscam a instalação de um vírus (trojan) no computador da vítima
- **Phishing** – Apresentam uma página falsa, clonada do site legítimo, em que é solicitada a informação. Os criminosos 'pescam'.
- **419** – Oferece uma grande oferta em dinheiro, mas necessita de um 'pagamento adiantado'. O dinheiro jamais chega.

Você acaba de receber um Vale Presente no valor de **R$ 100,00**. Um presente com milhões de opções para pessoas muito especiais.

Com o Vale Presente Americanas.com, você escolhe qualquer produto do site da Americanas. Ao concluir as compras, basta digitar o código do seu vale.

Para visualizar seu Vale Presente **clique aqui** ou na imagem abaixo.
Após abrir digite o código **31278032**

Vale Presente de R$100

- Golpe usa o nome do Americanas.com
- Promete ao internauta um prêmio de R$100
- E pede o acesso ao link para recebê-lo

Agora você pode ter seu NokiaNserie pela metade do valor e ainda indicar um amigo para ter as mesmas vantagens, graças à queima de estoque da nokia. É só gerar o seu código e acessar o site da LojaVirtual Nokia ,escolher e comprar seu NokiaNserie usando o código promocional. Mais corra mesmo, são apenas 9.800 aparelhos na promoçao!

Gerar Código Promocional

Obs: Esta promoção é limitada e será validado apenas (01) um aparelho por código até o término da promoção ou liquidação de estoque.

Celular em Oferta

- Golpe usa o nome da Nokia
- Promete ao internauta um aparelho em oferta desde que seja gerado um código
- E pede o acesso ao link para gerá-lo

Saraiva.com.br

PARABÉNS

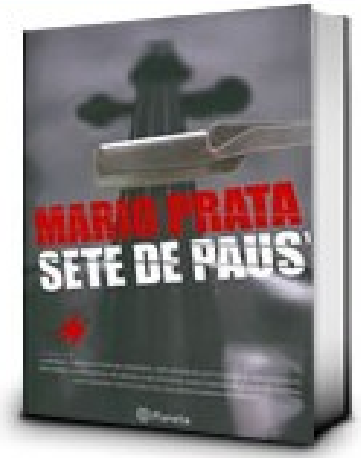
VOCÊ CLIENTE SARAIVA FOI UM DOS 500 SORTEADOS A GANHAR UM VALE COMPRAS NO VALOR DE :

300 R$ (TREZENTOS REAIS)

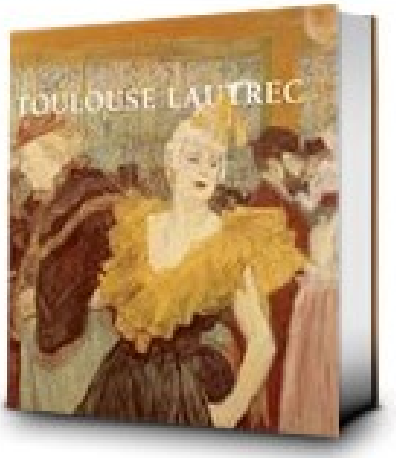
PARA PEGAR O VALE COMPRAS CLIQUE AQUI, IMPRIMA O VALE COMPRAS E COMPAREÇA EM UMA DE NOSSA LOJAS.

A SARAIVA AGRADECE SUA PARTICIPAÇÃO

A Essência do Mal
Sebastian Faulks



Sete de Paus
Mario Prata



Toulouse Lautrec
Importado

Vale-compra de R$300

- Golpe usa o nome da loja Saraiva
- Diz que o internauta recebeu um vale compra no valor de R$300
- Porém é necessário imprimi-lo – o código não está já no e-mail
- É necessário uma visita a um link para ver o tal 'vale'

Caro cliente,

Informamos que desde 30/10/2008, o sistema de segurança do Itaú Bankline foi atualizado para melhor interagir com o nosso novo sistema de identificação digital, prevenindo assim, atos fraudulentos de quaisquer natureza.

Neste caso, será necessário que você acesse sua conta em nosso site, e após o acesso, verifique se os seus dados estão corretos. Acesse agora nosso site clicando aqui: www.itau.com.br

Informamos que o Itáu Bankline, NÃO usa NENHUM tipo de software que seja necessário instalação no computador para acessar sua conta. Nosso sistema online funciona SOMENTE através de nosso site, 24 horas por dia, 7 dias por semana, pelo endereço: www.itau.com.br

Caso você receba qualquer tipo de e-mail orientando você á fazer download de algum software para instalação em seu computador, DENÚNCIE através de nosso site: www.itau.com.br

Agradecemos a cooperação.

Atualização Itaú

- Este golpe usa o nome do Itaú, mas é comum também com Caixa, Bradesco e BB
- Diz que o usuário precisa atualizar os dados
- Inclui até mesmo dicas de segurança
- Apresenta uma página falsa, clonada do banco, quando o link é clicado

:: Bradesco Pessoa Física :: - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

http://services-onlines.com/Bradescompleto/Recadastramento/PessoaFisica/

:: Bradesco Pessoa Física ::

Acesse aqui o seu Bradesco Internet Banking
Acessível aos Deficientes Visuais

Agência Conta OK COMO USAR MAPA DO SITE

Bradesco

Bradesco Pessoa Física | Bradesco Prime | Bradesco Private | Pessoa Jurídica

Sexta-feira, 28 de Novembro de 2008
11:38 horário de Brasília

- Governança Corporativa
- Relações com Investidores
- Responsabilidade Socioambiental
- Segurança da Informação
- Conteúdo RSS

MEDIA CENTER

MERCADO FINANCEIRO

SEGURANÇA

GOODPRIV@CY

ISO 9001

Fone Fácil Bradesco
4002-0022
Capitais e Regiões Metropolitanas
Para demais localidades, clique aqui.

Abra sua Conta

Saiba Tudo Sobre

- Bradesco Celular
- Câmbio
- Capitalização
- Cartões
- Comércio Eletrônico
- Consórcios
- Contas
- Deficientes Visuais
- Despachante e CFC
- Empréstimos e Financiamentos
- Investimentos
- Nikkei
- Poder Público
- Produtos e Serviços
- Seguros
- Universitários
- Vida e Previdência

Conveniência

Banco24Horas
Realize saques e consulte saldos e extratos também nestes terminais.

Crédito Imobiliário

Ao seu alcance
Clique aqui, confira todas as vantagens e realize seu sonho.

Extrato em Braille

Ser um banco completo significa ser para todos. Confira.

Recarga Direta

Recarregue seu celular a qualquer hora, em qualquer lugar.

Second Life

Cursos e oficinas on-line na Ilha Bradesco. Saiba mais.

Bradesco Notícias | Fale Conosco | Oportunidade de Carreira | Política de Qualidade | Política de RH | Rede de Atendimento

Recebendo dados de services-onlines.com...

Adblock

Página falsa Bradesco

- É referenciada por uma fraude que também solicita atualização de dados
- A página é idêntica a do banco. Neste caso, é possível ver que o endereço é diferente. Os links na página não estavam operantes.

Carta de Amor

Amar é...

""Amar é enlouquecer, ou simplesmente sentir um brisa no olhar... um olhar que penetra e chega onde quer e conquista... amar é envolver-se, é deixar-se conquistar... é simplesmente viver o momento...""

Para ler sua carta e saber quem lhe enviou clique em

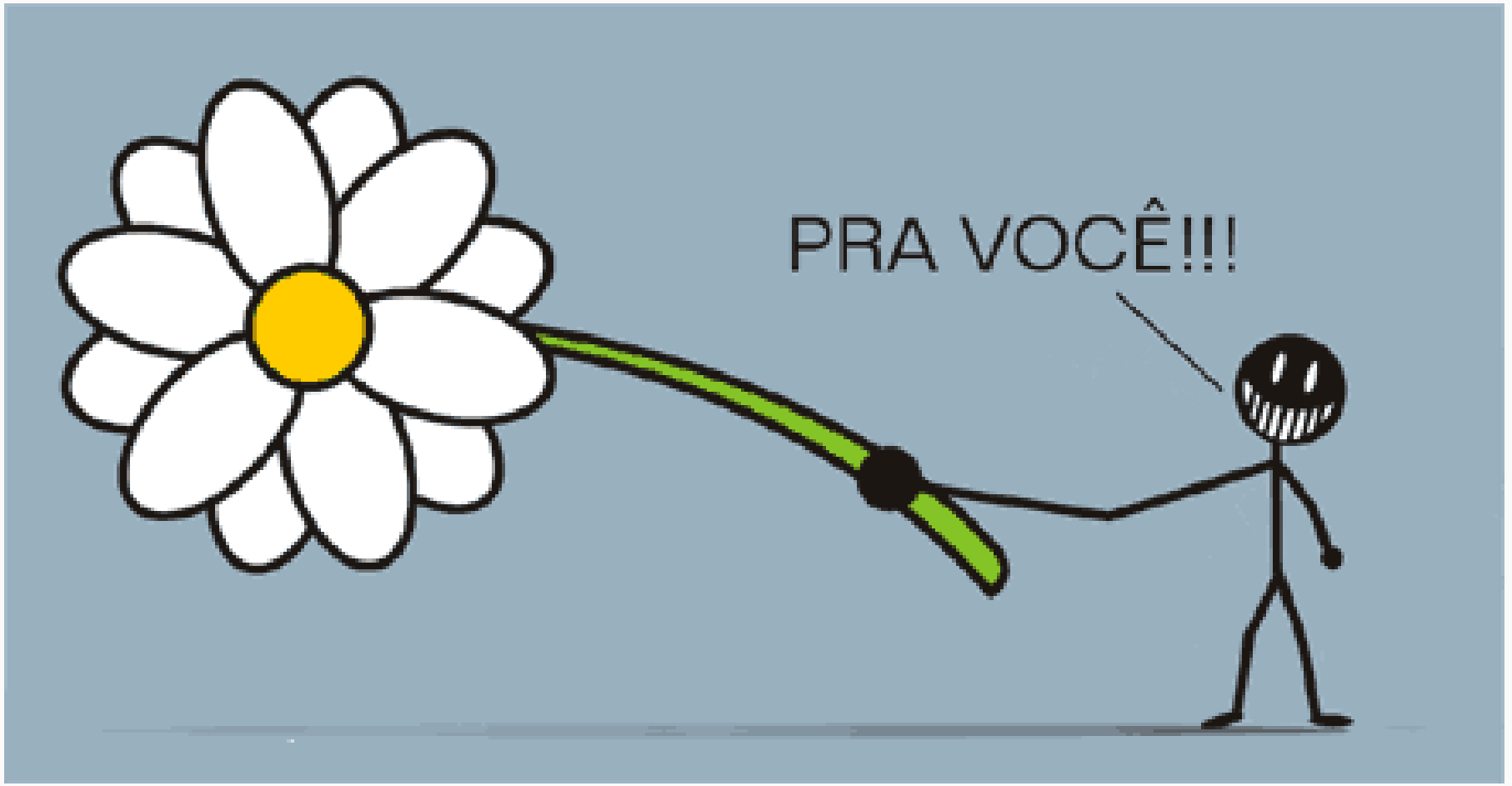
"Ler minha Carta de Amor"

Abraços,
Turma do Carta de Amor
Carta de Amor

Ler minha Carta de Amor

Carta de Amor

- Diz ao internauta que ele recebeu uma declaração de amor
- Não identifica o remetente, ou não identifica pelo nome completo
- Requer uma visita ao link para ver a 'carta'



Um abrao vale mil palavras. Um amigo muito mais.

to passando pra d um "OI".... e deixar uma mensagem....

Baixar mensagem....

Mensagem de Amizade

- Diz ao internauta que ele recebeu uma mensagem de um amigo
- Mais uma vez, não identifica o remetente, ou não identifica pelo nome completo
- Português péssimo
- Requer uma visita ao link para ver a 'mensagem'

ParabÃ©ns! O pedido abaixo acaba de ser expedido de nossa Central de DistribuiÃ§Ã£o e possui entrega prevista com prazo mÃximo para o dia **15/11/2008**, atÃ© Ã s **17 horas**. Lembramos que, para recebimento do seu pedido, Ã© necessÃirio que alguÃ©m autorizado esteja presente no local solicitado para a entrega.

NÂº do seu pedido: **24267890**

Para visualizar seu pedido por inteiro: SEU PEDIDO AQUI

Atenciosamente,
ServiÃ§o de Atendimento ao Cliente
Grupos Comprafacil.com

Pedido confirmado

- O exemplo usa as Casas Bahia, mas qualquer loja ou instituição pode ser usada
- Diz que o internauta fez uma compra. Às vezes, também informa o valor da mesma
- Requer uma visita ao link para ver o 'pedido' ou, em outros casos, cancelá-lo por ter um valor muito alto



SERASA - CNPJ 62173620/0001- 80 - Av. Paulista nº 2178 - centro - São Paulo - SP - BR. Cep. 02021- 021.

São Paulo - SP, 05 de novembro de 2008.

RFS14 - CONFIDENCIAL PARA: 7384391027498-5092/2008

NOTIFICAÇÃO DE DÍVIDA

Prezado(a) Senhor(a),

Informamos que por várias vezes tentamos fazer contato para alertá-lo(a) de Dívida que V.Sª. possui em aberto com 1 (Hum) de nossos clientes, porém sem sucesso. Estamos enviando que este e-mail como ultimo aviso antes que medidas legais sejam tomadas e consequentemente, seu CPF/CNPJ e Nome serão Protestado em Cartórios, assim como também será incluso em nossa base de Dados de Inadimplentes, todavia, algumas Empresas estão renegociando dívidas em atraso, solicitamos que V.Sª. verifique na Relação de Dividas a Empresa cuja sua dívida encontra-se ativa e vencida, e em contato com a mesma, negocie a melhor forma de estar quitando o seu Débito, e consequentemente mantendo o seu CPF/CNPJ e Nome Adimplentes e livres de restrições no mercado consumidor. Segue abaixo na integra, o comunicado que se encontra registrado no cartório de Registros e Protesto de São Paulo -SP, local cuja a sede de nossa empresa se encontra, sob os números: L219, FLS 1314/1315.

Dia 02/10/2008 Valor de R$ 9.873,65 > Fatura Detalhada em arquivo PDF 

Dívida SPC/Serasa

- Um dos golpes mais antigos. Se ainda é enviado, é porque funciona
- Afirma que o internauta possui uma dívida pendente
- Pede uma visita ao link para normalizar a situação

---------- Forwarded message ----------
From: **G1 Noticias** <noticias@g1.com>
Date: 07/11/2008 11:22
Subject: A Verdade por Tras de Barack Obama
To:

Olá Usuário

G1 NOTÍCIAS > NO MUNDO

Barack Obama: a verdade por trás do novo presidente dos E.U.A.

Novo video divulgado na internet mostra a verdade por trás do novo presidente dos EUA! Saiba tudo que as emissoras de televisão do nosso país não mostraram. Conheça toda história de crimes de Barack Obama e sua família.

Data: 06/11/08 | Duração: 10m50s|

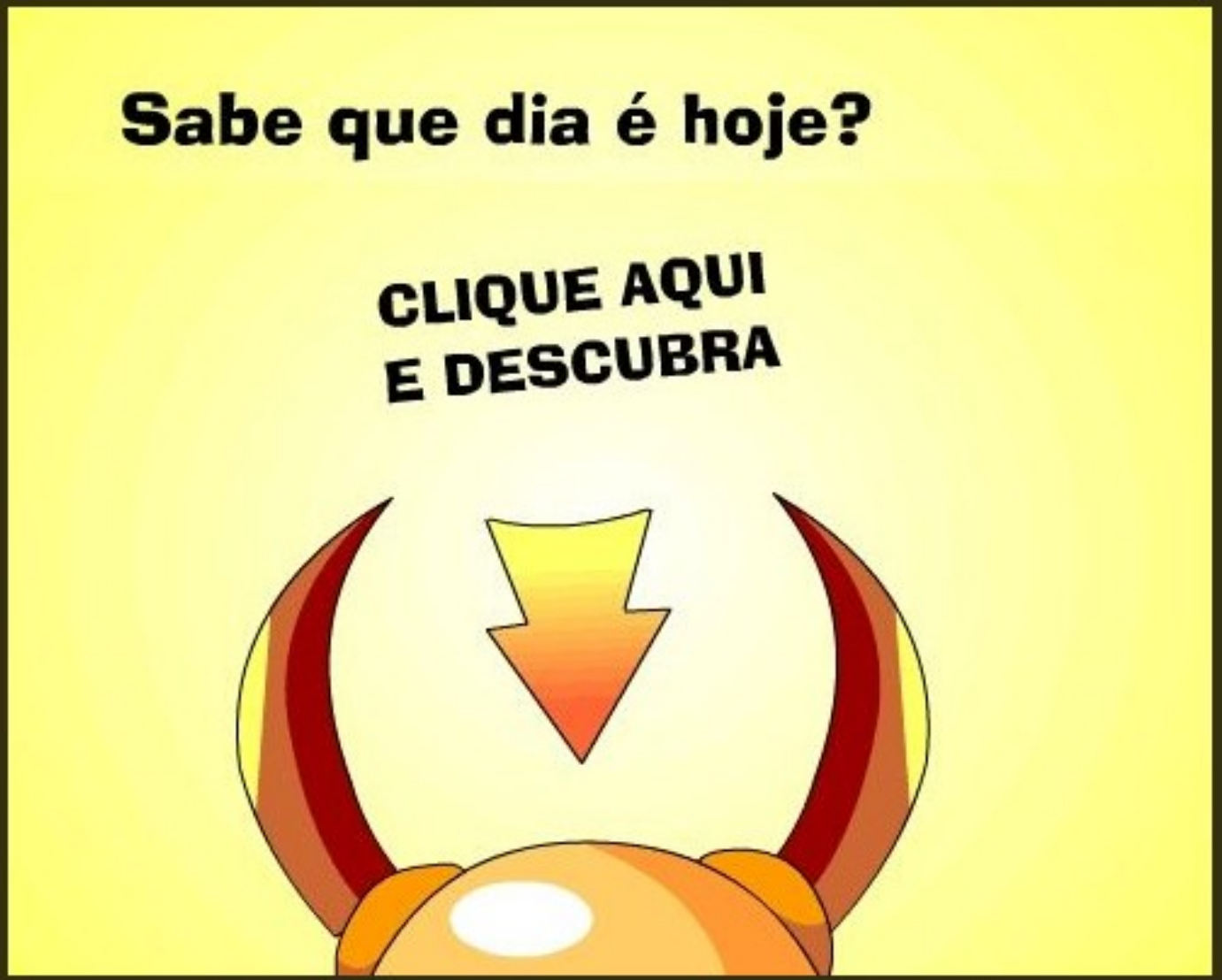
Assista aqui

Isca por fato atual

- Geralmente usa um site de notícias conhecido. No exemplo, o G1/Globo.com
- Traz vídeos ou notícias (verdadeiras ou falsas) sobre um fato corrente
- Solicita visita ao link para ver a notícia ou vídeo completo

Olá, Telespectador Premiado,
Esta reportagem foi enviada por Rede Globo (redeglobo@globo.com)

Caso não consiga visualizar seu cartão, clique (Mostrar conteúdo)



Mistério de fonte confiável

- Não apresenta muitas informações a respeito do que trata a mensagem
- Aproveita-se de fonte confiável (um site, um amigo com nome genérico)
- Deixa o internauta curioso pela falta de informação, convencendo-o a clicar no link

Trabalho
Ministério do Trabalho e Emprego

CODIN / Ministério do Trabalho e Emprego / Consulta Processual

Aguarde o processamento do arquivo em anexo, caso o mesmo não abra, por gentileza abra-o manualmente logo abaixo:

Processo n.º 40925/2008 - anexos relacionados abaixo:

Despacho_409252008

*** Para a visualização desse conteúdo é necessário aceitar o plugin do Adobe Flash Player

Processo

- Diz que o internauta está envolvido em algum processo
- No exemplo, é um e-mail totalmente falso do Ministério do Trabalho
- Para ter informações (ou se livrar) do processo, é necessário clicar no link

Nova versao do Messenger disponivel!

Windows Live Messenger 9.0 PT-BR

clique para
Baixar

Nova versão do MSN

- Circula há um bom tempo
- Promete uma versão nova do Windows Live (MSN) Messenger
- O link leva para o suposto programa. Ou seja, não esconde o fato de que será preciso o download de um programa

Aviso do Cancelamento de seu Email!

Caro usuário,
Identificamos que sua conta está tendo acesso por terceiros e enviando vírus, spam e e-mail maliciosos à outros membros da comunidade Hotmail.

Devido tal motivo nós teremos que Inabilitar sua conta caso o senhor(a) não tome as medidas de segurança abaixo:

Medidas de Segurança:

1) Faça o download e execute o aplicativo de segurança para eliminar possíveis agentes maliciosos contidos em seu computador.

DOWNLOAD.

2) Após ter feito isso seu computador estará mais protegido, mas ainda recomendamos que altere a senha de seu email.

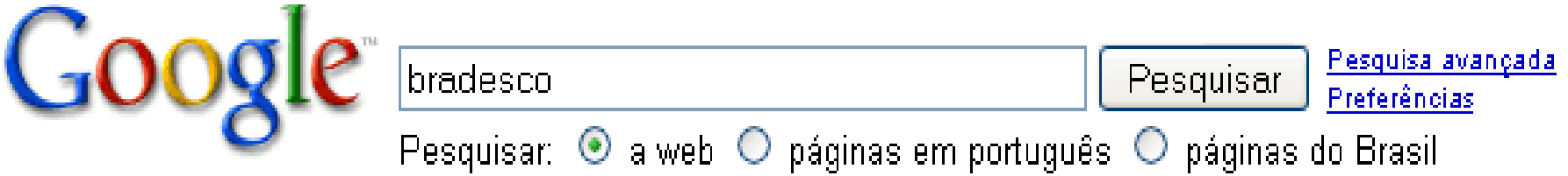
Cancelamento de Conta

- Diz ao internauta que seu acesso a um determinado serviço (e-mail, Orkut...) será cancelado
- Oferece a regularização da situação
- Mas para isso é necessário clicar em um link
- Neste exemplo o motivo é vírus: ferramentas de segurança são usadas por outros golpes

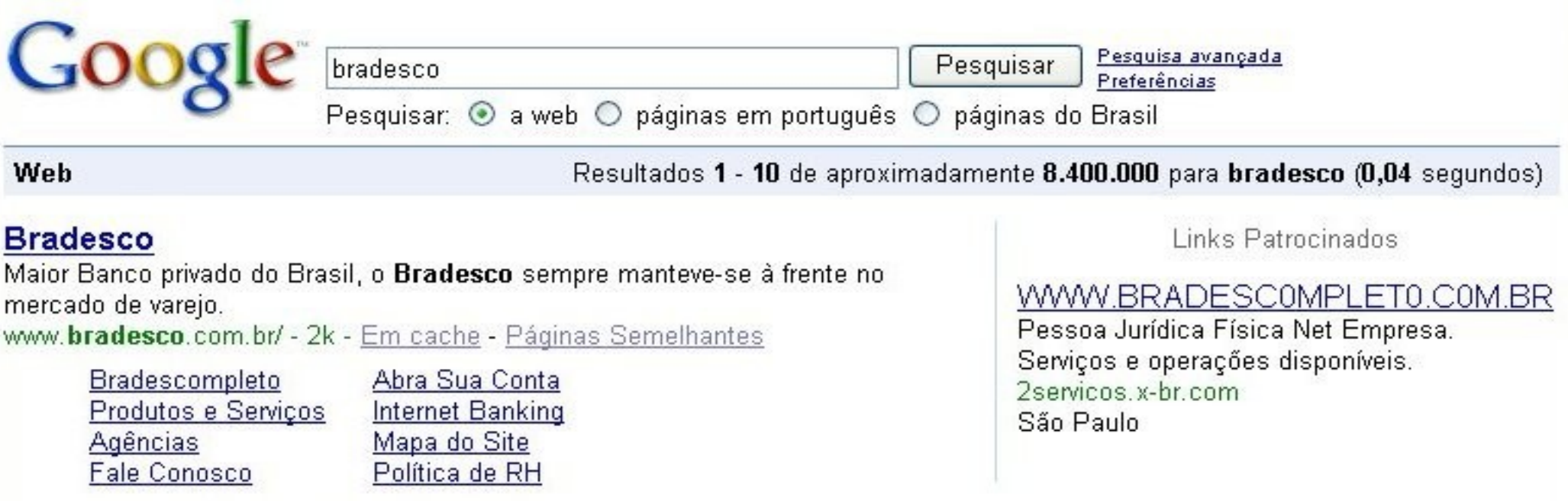
Fraudes não são só e-mails

- Contas roubadas do Orkut
- Infecções de worm (Orkut, MSN, e-mails)
- Anúncios publicitários

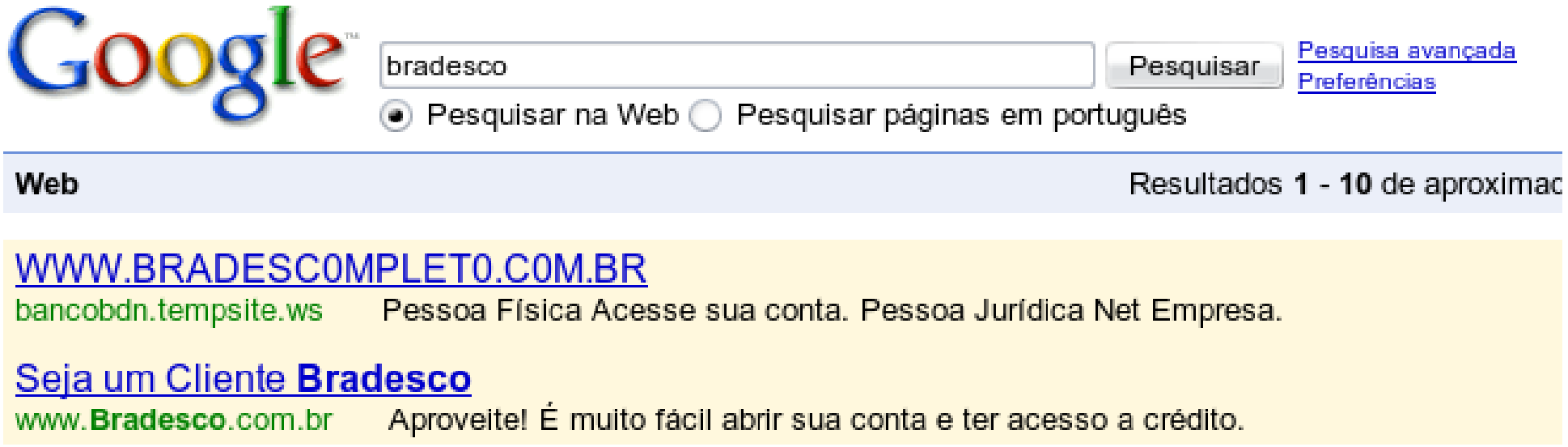
Google Adwords



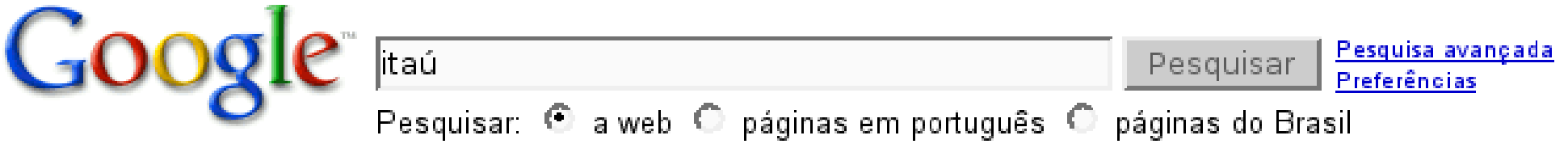
Google Adwords II



Google Adwords III



Google Adwords IV



A “fraude nigeriana” ou 419

- Varia muito. Autores ganharam o prêmio “Ignobel de literatura”
- Envolve uma história em que o internauta pode ganhar uma grande quantia em dinheiro
- Por complicações com a transferência dos fundos, ele precisa pagar antes
- No Brasil, é realizado freqüentemente por telefone

Ataque aos mal-intencionados

“Descubra senhas Hotmail” é um truque que promete ensinar o internauta a roubar uma senha do Hotmail, mas na verdade rouba as senhas

“Conta Tibia Premium grátis” ensina o jogador a obter uma conta Premium, mas na verdade rouba suas credenciais

Existem outras fraudes?

- Há muitos outros golpes além dos citados
- A existência de novos golpes depende da criatividade do criminoso. Quando truques antigos pararem de funcionar, a tendência é que novos apareçam.

- Por isso é essencial manter-se **informado**.

Como identificar uma fraude

- Tente utilizar a comunicação. Um telefonema ao banco, um ou MSN com o amigo que supostamente enviou a correspondência
- Mas não use o mesmo meio de onde veio a fraude para fazê-lo
- Existem maneiras mais técnicas, como tentar ver o link, mas avanços e falhas dificultam esse tipo de verificação

Como identificar uma fraude

- Na dúvida, não clique. Fraudes sempre parecem tratar de um assunto importante!
- Pergunte a opinião de um amigo. Pode ser que ele tenha recebido exatamente o mesmo e-mail
- Ou então...


Google™

Cliquei na fraude. E aí?

- Algumas tentam usar falhas de segurança
- Outras roubam suas credenciais na própria página
- A maioria apenas serve o download do trojan

Como se comporta o trojan

- Remove ou desativa softwares de segurança (usando softwares de segurança!)
- Instala-se na inicialização do sistema
- Monitora o acesso a bancos para criar janelas falsas ou adiciona redirecionamentos

Uma vez infectado...

- O computador é do criminoso, não mais seu
- A limpeza feita pelo antivírus nem sempre é completa

  BankerFix: www.linhadefensiva.org/bankerfix/
- Algumas pragas digitais danificam o sistema de modos imperceptíveis de imediato
- O melhor é a **prevenção**

Onde há mais informações?

- Catálogo de Fraudes do CAIS

  www.rnp.br/cais/fraudes.php
- E-Farsas - www.e-farsas.com
- Snopes - www.snopes.com
- Quatro Cantos - www.quatrocantos.com

Linha Defensiva

CONTATOS

Altieres Rohr
altieres@linhadefensiva.org
http://altieresrohr.com.br

Fábio Assolini
fabio@linhadefensiva.org

ARIS-LD
avs@linhadefensiva.org
www.linhadefensiva.org/aris-ld/

2008 DISI
Prevenção: a melhor forma de defesa contra ameaças

Informações Extras

- Esta apresentação foi elaborada para o DISI 2008, do CAIS/RNP

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

- Esta é uma versão revisada da apresentação original. A distribuição e alteração é permitida de acordo com as regras da licença CC BY-NC-SA:

  creativecommons.org/licenses/by-nc-sa/2.0/br/