Especialização em **Gestão das Tecnologias na Educação Básica**

Disciplina: **Informática Aplicada a Educação**

Prof. Walteno Martins Parreira Júnior

Segurança em Informática

Inicialmente, responda o questionário abaixo.

1- Possui e utiliza computador em casa?	
( ) Sim / Com acesso à internet	( ) Sim / Sem acesso à internet
( ) Não tenho nenhum tipo de contato	( ) Acesso em outros espaços (lan house, trabalho, cursos etc.)

2- Sabe o que é e qual a função de um antivírus?
( ) Sim ( ) Possuo / Qual? _____ ( ) Não possuo ( ) Faço atualizações ou ocorrem atualizações automáticas / com a freqüência de _____ dias ( ) Não faço atualizações
( ) Não

3- Sabe o que é e qual a função de um Firewall?
( ) Sim ( ) Possuo / Qual? _____ ( ) Não possuo
( ) Não

4- Já teve algum problema relacionado a vírus em seu equipamento?	
( ) Sim	( ) Não

5- Realiza ou já realizou algum tipo de compra pela internet?	
( ) Sim	( ) Não

6- Costuma <u>receber</u> e-mails em massa com apresentações/imagens/mensagens em anexo que foram enviados para uma lista de pessoas?	
( ) Sim	( ) Não

7- Costuma <u>enviar</u> e-mails em massa com apresentações/imagens/mensagens em anexo destinados a uma lista de pessoas?	
( ) Sim	( ) Não

Segundo o Comitê Gestor da Internet no Brasil (cgi.br), é necessário que cada usuário da Internet observe um conjunto de atitudes para se defender dos problemas advindos do acesso aos serviços disponíveis.

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

- Mantenha o programa leitor de *e-mails* sempre atualizado.
- Desative a visualização de *e-mails* em HTML.
- Desative as opções de execução automática de arquivos anexados.
- Desative a execução de *JavaScript* e *Java*.

Proteja sua privacidade

- Use senhas com letras, números e símbolos.
- Nunca use como senha dados pessoais ou palavras de dicionários.
- Não coloque dados pessoais em páginas *Web*, *blogs* ou *sites* de redes de relacionamentos.

Use celulares e PDAs com segurança

- Habilite *bluetooth* só quando for utilizá-lo.
- Consulte o fabricante sobre atualizações para seu aparelho.
- Não aceite qualquer arquivo enviado para seu aparelho. Cheque a procedência.

Dicas para quem usa banda larga

- Use antivírus e *firewall* pessoal.
- Desligue o compartilhamento de recursos.
- Mantenha os programas que você usa sempre atualizados.
- Instale todas as correções de segurança.

Dicas para quem usa redes sem fio

- Use antivírus e *firewall* pessoal.
- Use WEP ou WPA sempre que possível.
- Use somente serviços com conexão segura.
- Implemente também as dicas para quem usa banda larga.

No site do cgi.br tem disponível para leitura a Cartilha de Segurança para Internet (http://cartilha.cert.br/download/). Para visualizar estes arquivos é necessário que tenha instalado no computador o *software Acrobat Reader*.

Exemplos de email recebidos e que são do tipo Engenharia Social. Pode-se observar que tem todas as características descritas na literatura.

Email 1:

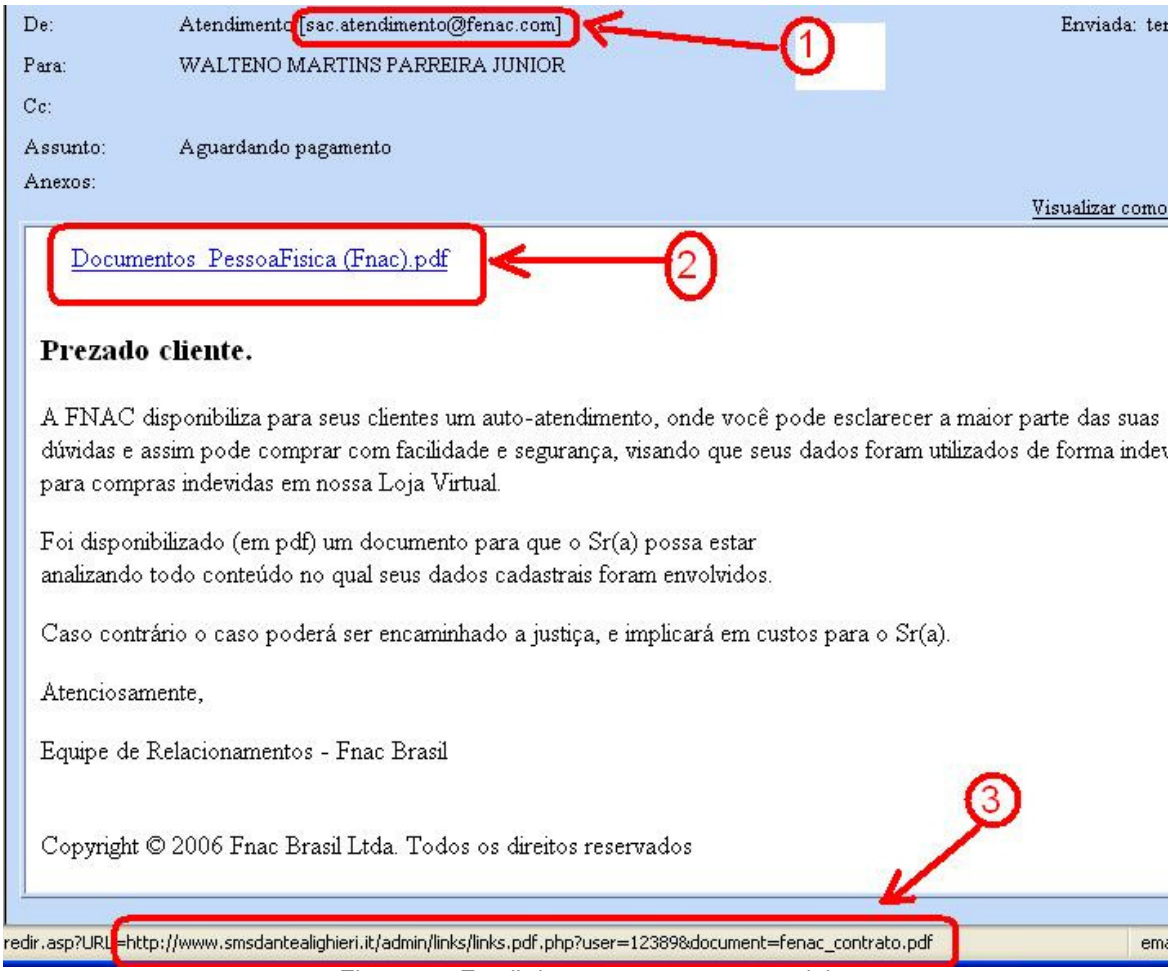

Figura 1 – Email de uma empresa comercial

Item 1 - Falsa Identidade – um endereço de email de um provedor estrangeiro e de livre utilização para mandar suposta correspondência de um órgão público brasileiro.

Item 2 - Arquivo Anexo – não existe arquivo anexado e sim um link para um endereço. Colocando o ponteiro do mouse sobre o texto (destaque 2), pode-se observar o endereço na barra de status (destaque 3). Provavelmente, ao clicar sobre o link, um código malicioso será instalado na maquina.

Item 3 – Endereço real do link – é um endereço diferente do apresentado no corpo do email, pode ser observado a partir da sobreposição do ponteiro do mouse sobre o link em que é solicitado que seja executado e visualizado na área de status do navegador.

Email 2:

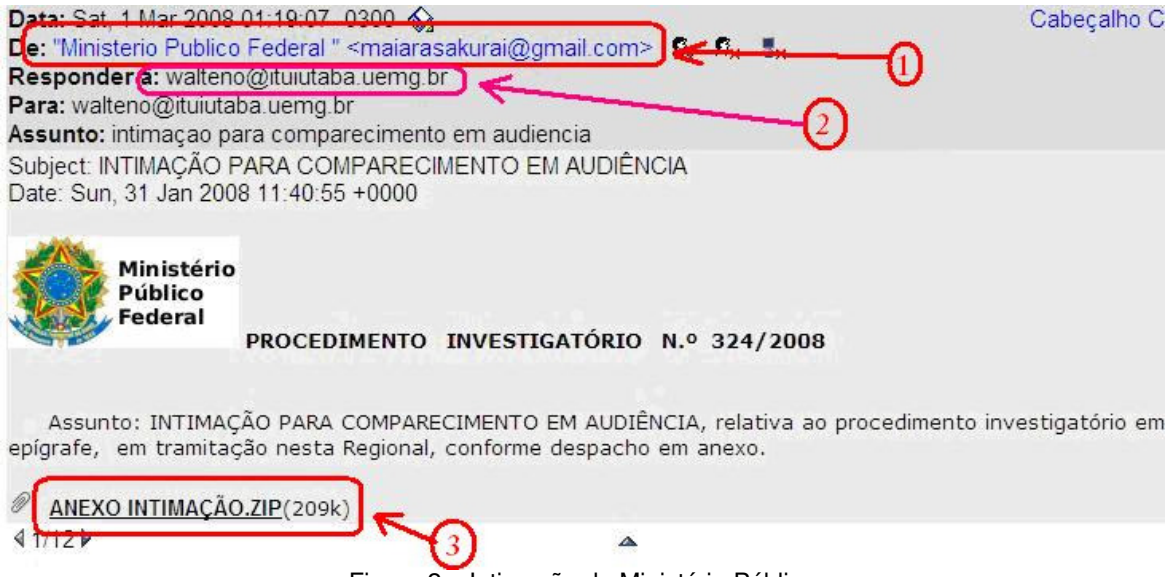

Figura 2 – Intimação do Ministério Público

Item 1 - Falsa Identidade – uso de um endereço de email de um provedor estrangeiro e de livre utilização para mandar suposta correspondência de um órgão público brasileiro.

Item 2 - Email para Resposta – é o seu próprio email, então se você responder o email ele volta para a sua própria caixa postal.

Item 3 - Arquivo Anexo – não existe arquivo anexado e sim um link para um endereço. Colocando o ponteiro do mouse sobre o texto, pode-se observar o endereço na barra de status. Provavelmente, ao clicar sobre o link, um código malicioso será instalado na maquina.

Email 3:

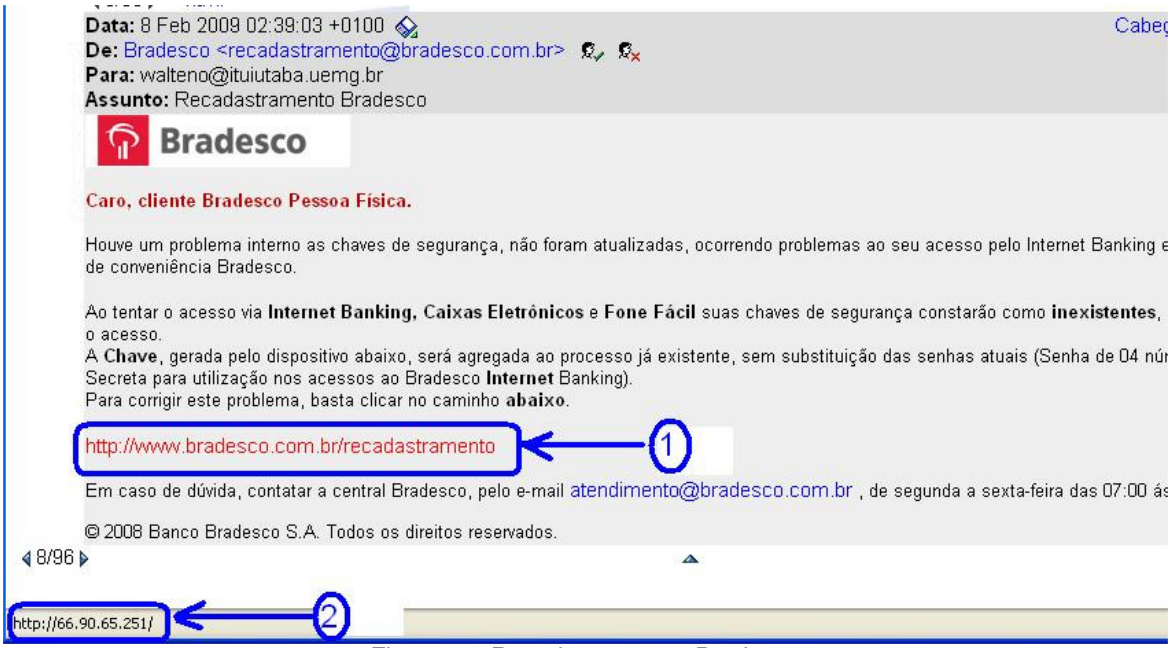

Figura 3 – Recadastramento Bradesco

Email 4:

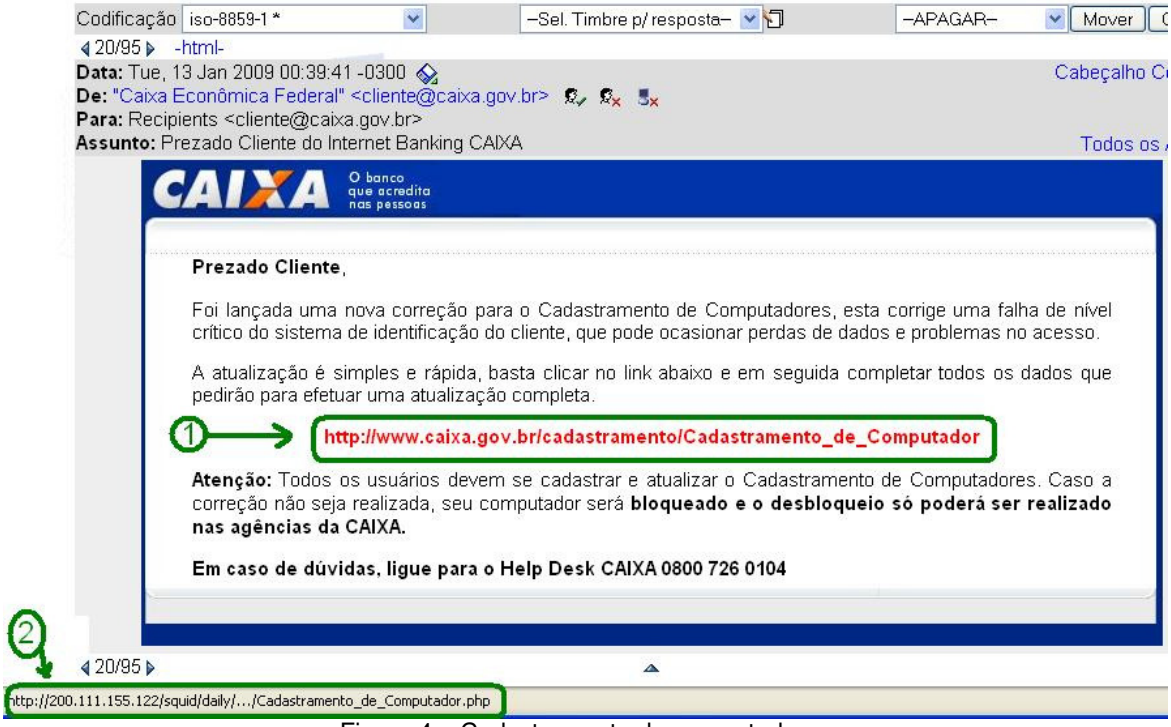

Figura 4 – Cadastramento de computadores

Na figura 4, posicionando (sem clicar) o ponteiro do mouse sobre o link que foi solicitado (destaque 1) que seja executado, aparece o endereço real do link na barra de status (destaque 2), observe que no endereço não aparece o nome da empresa. Copiando o endereço aparente e mandando buscar (ver figura 5), descobrimos que o endereço (destaque 1) não existe no site do banco, conforme a figura 5.

Figura 5 – Acessando o endereço solicitado

Email 5:

Figura 6 – Correspondência dos Correios

Este email é enviado, informando que tenho um telegrama on-line e um link para ler. Buscando no site dos Correios, tem-se a seguinte mensagem:

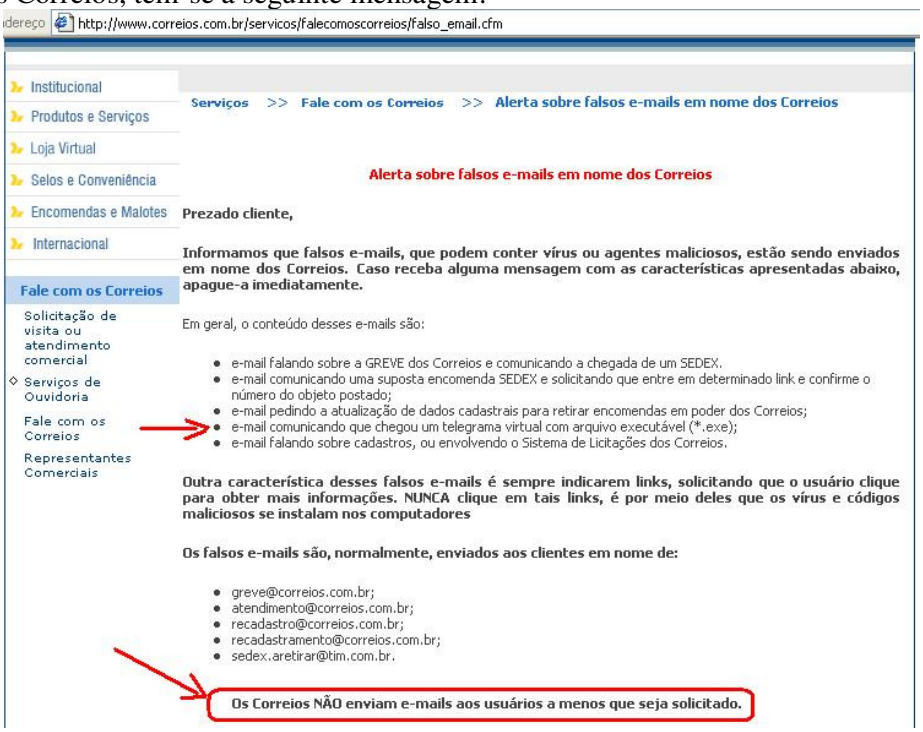

Figura 7 – Alerta no site dos Correios

Email 6:

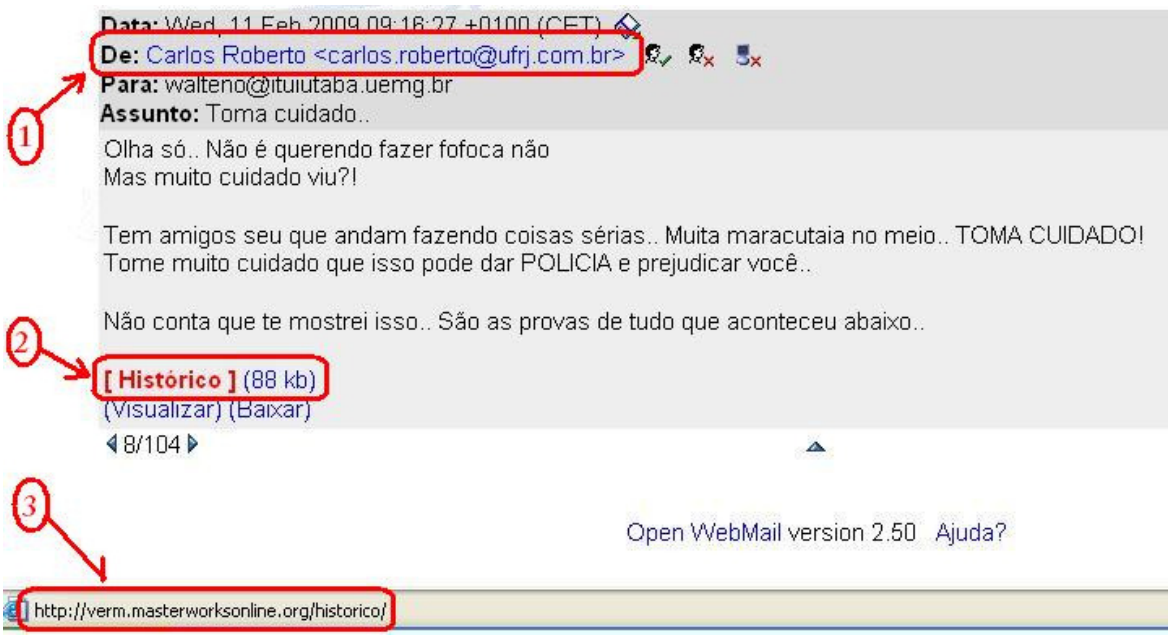

Figura 8 – Fofoca

Estes são alguns exemplos da utilização de email para invadir os nossos computadores. Muitos outros estão circulando pela Internet. Quando tiver dúvida, não faça o que é solicitado e pesquise o suposto remetente.