Cartilha de Segurança para Internet

Parte IV: Fraudes na Internet

Versão 3.0
Setembro de 2005
http://cartilha.cert.br/

CERT.br – Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

Cartilha de Segurança para Internet

Parte IV: Fraudes na Internet

Esta parte da cartilha aborda questões relacionadas a fraudes na Internet. São apresentadas algumas maneiras de prevenção contra ataques de engenharia social, situações envolvendo fraudes comerciais e bancárias via Internet, bem como medidas preventivas que um usuário deve adotar ao acessar *sites* de comércio eletrônico ou *Internet Banking*. Também é apresentado o conceito de boato (*hoax*) e são discutidas algumas implicações de segurança e formas para se evitar sua distribuição.

Versão 3.0 – Setembro de 2005
http://cartilha.cert.br/

Sumário

1 Engenharia Social

Nos ataques de engenharia social, normalmente, o atacante se faz passar por outra pessoa e utiliza meios, como uma ligação telefônica ou *e-mail*, para persuadir o usuário a fornecer informações ou realizar determinadas ações. Exemplos destas ações são: executar um programa, acessar uma página falsa de comércio eletrônico ou *Internet Banking* através de um *link* em um *e-mail* ou em uma página, etc.

O conceito de engenharia social, bem como alguns exemplos deste tipo de ataque, podem ser encontrados na parte I: Conceitos de Segurança. Exemplos específicos destes ataques, envolvendo diversos tipos de fraude, são abordados nas seções 2.1 e 2.2.

1.1 Como me protejo deste tipo de abordagem?

Em casos de engenharia social o bom senso é essencial. Fique atento para qualquer abordagem, seja via telefone, seja através de um *e-mail*, onde uma pessoa (em muitos casos falando em nome de uma instituição) solicita informações (principalmente confidenciais) a seu respeito.

Procure não fornecer muita informação e **não** forneça, sob hipótese alguma, informações sensíveis, como senhas ou números de cartões de crédito.

Nestes casos e nos casos em que receber mensagens, procurando lhe induzir a executar programas ou clicar em um *link* contido em um *e-mail* ou página *Web*, é extremamente importante que você, **antes de realizar qualquer ação**, procure identificar e entrar em contato com a instituição envolvida, para certificar-se sobre o caso.

2 Fraudes via Internet

Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial. Então, atacantes têm concentrado seus esforços na exploração de fragilidades dos usuários, para realizar fraudes comerciais e bancárias através da Internet.

Para obter vantagens, os fraudadores têm utilizado amplamente *e-mails* com discursos que, na maioria dos casos, envolvem engenharia social e que tentam persuadir o usuário a fornecer seus dados pessoais e financeiros. Em muitos casos, o usuário é induzido a instalar algum código malicioso ou acessar uma página fraudulenta, para que dados pessoais e sensíveis, como senhas bancárias e números de cartões de crédito, possam ser furtados. Desta forma, é muito importante que usuários de Internet tenham certos cuidados com os *e-mails* que recebem e ao utilizarem serviços de comércio eletrônico ou *Internet Banking*.

A seções 2.1 e 2.2 ilustram algumas situações envolvendo estes tipos de fraudes. A seção 2.3 descreve alguns cuidados a serem tomados pelos usuários de Internet, ao acessarem *sites* de comércio eletrônico ou *Internet Banking*. As seções 2.4, 2.5 e 2.6 apresentam alguns procedimentos para verificar a legitimidade de um *site*. E a seção 2.7 recomenda o que o usuário deve fazer se perceber que seus dados financeiros podem estar sendo usados por terceiros.

2.1 O que é *scam* e que situações podem ser citadas sobre este tipo de fraude?

O *scam* (ou "golpe") é qualquer esquema ou ação enganosa e/ou fraudulenta que, normalmente, tem como finalidade obter vantagens financeiras.

As subseções 2.1.1 e 2.1.2 apresentam duas situações envolvendo este tipo de fraude, sendo que a primeira situação se dá através de páginas disponibilizadas na Internet e a segunda através do recebimento de *e-mails*. Observe que existem variantes para as situações apresentadas e outros tipos de *scam*. Além disso, novas formas de *scam* podem surgir, portanto é muito importante que você se mantenha informado sobre os tipos de *scam* que vêm sendo utilizados pelos fraudadores, através dos veículos de comunicação, como jornais, revistas e *sites* especializados.

2.1.1 *Sites* de leilões e de produtos com preços "muito atrativos"

Você acessa um *site* de leilão ou de venda de produtos, onde os produtos ofertados têm preços muito abaixo dos praticados pelo mercado.

Risco: ao efetivar uma compra, na melhor das hipóteses, você receberá um produto que não condiz com o que realmente foi solicitado. Na maioria dos casos, você não receberá nenhum produto, perderá o dinheiro e poderá ter seus dados pessoais e financeiros furtados, caso a transação tenha envolvido, por exemplo, o número do seu cartão de crédito.

Como identificar: faça uma pesquisa de mercado sobre preço do produto desejado e compare com os preços oferecidos. Então, você deve se perguntar por que estão oferecendo um produto com preço tão abaixo do praticado pelo mercado.

É importante ressaltar que existem muitos *sites* confiáveis de leilões e de vendas de produtos, mas nesta situação a intenção é ilustrar casos de *sites* especificamente projetados para realizar atividades ilícitas.

2.1.2 O golpe da Nigéria (*Nigerian 4-1-9 Scam*)

Você recebe um *e-mail* em nome de uma instituição governamental da Nigéria (por exemplo, o Banco Central), onde é solicitado que você atue como intermediário em uma transferência internacional de fundos. O valor mencionado na mensagem normalmente corresponde a dezenas ou centenas de milhões de dólares.

Como recompensa, você terá direito de ficar com uma porcentagem (que é normalmente alta) do valor mencionado na mensagem. Para completar a transação é solicitado que você pague antecipadamente uma quantia, normalmente bem elevada, para arcar com taxas de transferência de fundos, custos com advogados, entre outros.

Este tipo de golpe também é conhecido como *Advance Fee Fraud*, ou "a fraude de antecipação de pagamentos", e já foram registrados casos originados ou que mencionavam a África do Sul, Angola, Etiópia, Libéria, Marrocos, Serra Leoa, Tanzânia, Zaire, Zimbábue, Holanda, Iugoslávia, Austrália, Japão, Malásia e Taiwan, entre outros.

No nome dado a este tipo de fraude, *Nigerian 4-1-9 Scam*, o número "419" refere-se à seção do código penal da Nigéria que é violada por este golpe. É equivalente ao artigo 171 do código penal brasileiro, ou seja, **estelionato**.

Risco: ao responder a este tipo de mensagem e efetivar o pagamento antecipado, você não só perderá o dinheiro investido, mas também nunca verá os milhares ou milhões de dólares prometidos como recompensa.

Como identificar: normalmente, estas mensagens apresentam quantias astronômicas e abusam da utilização de palavras capitalizadas (todas as letras maiúsculas) para chamar a atenção do usuário. Palavras como "URGENT" (urgente) e "CONFIDENTIAL" (confidencial) também são comumente usadas no assunto da mensagem para chamar a atenção do usuário.

Você deve se perguntar por que foi escolhido para receber estes "milhares ou milhões" de dólares, entre os inúmeros usuários que utilizam a Internet.

2.2 O que é *phishing* e que situações podem ser citadas sobre este tipo de fraude?

Phishing, também conhecido como *phishing scam* ou *phishing/scam*, foi um termo originalmente criado para descrever o tipo de fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários.

A palavra *phishing* (de "*fishing*") vem de uma analogia criada pelos fraudadores, onde "iscas" (*e-mails*) são usadas para "pescar" senhas e dados financeiros de usuários da Internet.

Atualmente, este termo vêm sendo utilizado também para se referir aos seguintes casos:

- mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros;
- mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

A subseções a seguir apresentam cinco situações envolvendo *phishing*, que vêm sendo utilizadas por fraudadores na Internet. Observe que existem variantes para as situações apresentadas. Além disso, novas formas de *phishing* podem surgir, portanto é muito importante que você se mantenha informado sobre os tipos de *phishing* que vêm sendo utilizados pelos fraudadores, através dos veículos de comunicação, como jornais, revistas e *sites* especializados.

Também é muito importante que você, ao identificar um caso de fraude via Internet, notifique a instituição envolvida, para que ela possa tomar as providências cabíveis[1].

2.2.1 Mensagens que contêm *links* para programas maliciosos

Você recebe uma mensagem por *e-mail* ou via serviço de troca instantânea de mensagens, onde o texto procura atrair sua atenção, seja por curiosidade, por caridade, pela possibilidade de obter alguma vantagem (normalmente financeira), entre outras. O texto da mensagem também pode indicar que a não execução dos procedimentos descritos acarretarão conseqüências mais sérias, como, por exemplo,

[1] Veja detalhes sobre como realizar a notificação na parte VII: Incidentes de Segurança e Uso Abusivo da Rede.

a inclusão do seu nome no SPC/SERASA, o cancelamento de um cadastro, da sua conta bancária ou do seu cartão de crédito, etc. A mensagem, então, procura induzí-lo a clicar em um *link*, para baixar e abrir/executar um arquivo.

Alguns exemplos de temas e respectivas descrições dos textos encontrados em mensagens deste tipo são apresentados na tabela 1.

Tabela 1: Exemplos de temas de mensagens de *phishing*.

Tema	**Texto da mensagem**
Cartões virtuais	UOL, *Voxcards*, Humor Tadela, O Carteiro, *Emotioncard*, Criança Esperança, AACD/Teleton.
SERASA e SPC	débitos, restrições ou pendências financeiras.
Serviços de governo eletrônico	CPF/CNPJ pendente ou cancelado, Imposto de Renda (nova versão ou correção para o programa de declaração, consulta da restituição, dados incorretos ou incompletos na declaração), eleições (título eleitoral cancelado, simulação da urna eletrônica).
Álbuns de fotos	pessoa supostamente conhecida, celebridades, relacionado a algum fato noticiado (em jornais, revistas, televisão), traição, nudez ou pornografia, serviço de acompanhantes.
Serviço de telefonia	pendências de débito, aviso de bloqueio de serviços, detalhamento de fatura, créditos gratuitos para o celular.
Antivírus	a melhor opção do mercado, nova versão, atualização de vacinas, novas funcionalidades, eliminação de vírus do seu computador.
Notícias/boatos	fatos amplamente noticiados (ataques terroristas, *tsunami*, terremotos, etc), boatos envolvendo pessoas conhecidas (morte, acidentes ou outras situações chocantes).
Reality shows	BigBrother, Casa dos Artistas, etc – fotos ou vídeos envolvendo cenas de nudez ou eróticas, discadores.
Programas ou arquivos diversos	novas versões de *softwares*, correções para o sistema operacional Windows, músicas, vídeos, jogos, acesso gratuito a canais de TV a cabo no computador, cadastro ou atualização de currículos, recorra das multas de trânsito.
Pedidos	orçamento, cotação de preços, lista de produtos.
Discadores	para conexão Internet gratuita, para acessar imagens ou vídeos restritos.
Sites de comércio eletrônico	atualização de cadastro, devolução de produtos, cobrança de débitos, confirmação de compra.
Convites	convites para participação em *sites* de relacionamento (como o orkut) e outros serviços gratuitos.
Dinheiro fácil	descubra como ganhar dinheiro na Internet.
Promoções	diversos.
Prêmios	loterias, instituições financeiras.
Propaganda	produtos, cursos, treinamentos, concursos.
FEBRABAN	cartilha de segurança, avisos de fraude.
IBGE	censo.

Cabe ressaltar que a lista de temas na tabela 1 não é exaustiva, nem tampouco se aplica a todos os casos. Existem outros temas e novos temas podem surgir.

Risco: ao clicar no *link*, será apresentada uma janela, solicitando que você salve o arquivo. Depois de salvo, se você abrí-lo ou executá-lo, será instalado um programa malicioso (*malware*) em seu computador, por exemplo, um cavalo de tróia ou outro tipo de *spyware*, projetado para furtar seus dados pessoais e financeiros, como senhas bancárias ou números de cartões de crédito[2]. Caso o seu programa leitor de *e-mails* esteja configurado para exibir mensagens em HTML, a janela solicitando que você salve o arquivo poderá aparecer automaticamente, sem que você clique no *link*.

Ainda existe a possibilidade do arquivo/programa malicioso ser baixado e executado no computador automaticamente, ou seja, sem a sua intervenção, caso seu programa leitor de *e-mails* possua vulnerabilidades.

Esse tipo de programa malicioso pode utilizar diversas formas para furtar dados de um usuário, dentre elas: capturar teclas digitadas no teclado; capturar a posição do cursor e a tela ou regiões da tela, no momento em que o *mouse* é clicado; sobrepor a janela do *browser* do usuário com uma janela falsa, onde os dados serão inseridos; ou espionar o teclado do usuário através da *Webcam* (caso o usuário a possua e ela esteja apontada para o teclado). Mais detalhes sobre algumas destas técnicas podem ser vistos na seção de *keyloggers*, na parte VIII: Códigos Maliciosos (*Malware*).

Depois de capturados, seus dados pessoais e financeiros serão enviados para os fraudadores. A partir daí, os fraudadores poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros, ou utilização dos seus dados financeiros para efetuar pagamentos, transferir valores para outras contas, etc.

Como identificar: seguem algumas dicas para identificar este tipo de mensagem fraudulenta:

- leia atentamente a mensagem. Normalmente, ela conterá diversos erros gramaticais e de ortografia;
- os fraudadores utilizam técnicas para ofuscar o real *link* para o arquivo malicioso, apresentando o que parece ser um *link* relacionado à instituição mencionada na mensagem. Ao passar o cursor do *mouse* sobre o *link*, será possível ver o real endereço do arquivo malicioso na barra de *status* do programa leitor de *e-mails*, ou *browser*, caso esteja atualizado e não possua vulnerabilidades. Normalmente, este *link* será diferente do apresentado na mensagem;
- qualquer extensão pode ser utilizada nos nomes dos arquivos maliciosos, mas fique particularmente atento aos arquivos com extensões ".exe", ".zip" e ".scr", pois estas são as mais utilizadas. Outras extensões freqüentemente utilizadas por fraudadores são ".com", ".rar" e ".dll";
- fique atento às mensagens que solicitam a instalação/execução de qualquer tipo de arquivo/programa;
- acesse a página da instituição que supostamente enviou a mensagem, seguindo os cuidados apresentados na seção 2.3, e procure por informações relacionadas com a mensagem que você recebeu. Em muitos casos, você vai observar que não é política da instituição enviar *e-mails* para usuários da Internet, de forma indiscriminada, principalmente contendo arquivos anexados.

[2] O conceito de *malware* pode ser encontrado na parte I: Conceitos de Segurança. Os conceitos de cavalo de tróia e *spyware* estão disponíveis na parte VIII: Códigos Maliciosos (*Malware*).

Recomendações:

- no caso de mensagem recebida por *e-mail*, o remetente **nunca** deve ser utilizado como parâmetro para atestar a veracidade de uma mensagem, pois pode ser facilmente forjado pelos fraudadores;
- se você ainda tiver alguma dúvida e acreditar que a mensagem pode ser verdadeira, entre em contato com a instituição para certificar-se sobre o caso, antes de enviar qualquer dado, principalmente informações sensíveis, como senhas e números de cartões de crédito.

2.2.2 Páginas de comércio eletrônico ou *Internet Banking* falsificadas

Você recebe uma mensagem por *e-mail* ou via serviço de troca instantânea de mensagens, em nome de um *site* de comércio eletrônico ou de uma instituição financeira, por exemplo, um banco. Textos comuns neste tipo de mensagem envolvem o recadastramento ou confirmação dos dados do usuário, a participação em uma nova promoção, etc. A mensagem, então, tenta persuadí-lo a clicar em um *link* contido no texto, em uma imagem, ou em uma página de terceiros.

Risco: o *link* pode direcioná-lo para uma página *Web* falsificada, semelhante ao *site* que você realmente deseja acessar. Nesta página serão solicitados dados pessoais e financeiros, como o número, data de expiração e código de segurança do seu cartão de crédito, ou os números da sua agência e conta bancária, senha do cartão do banco e senha de acesso ao *Internet Banking*.

Ao preencher os campos disponíveis na página falsificada e clicar no botão de confirmação (em muitos casos o botão apresentará o texto “Confirm”, “OK”, “Submit”, etc), os dados serão enviados para os fraudadores.

A partir daí, os fraudadores poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros, ou utilização dos seus dados financeiros para efetuar pagamentos, transferir valores para outras contas, etc.

Como identificar: seguem algumas dicas para identificar este tipo de mensagem fraudulenta:

- os fraudadores utilizam técnicas para ofuscar o real *link* para a página falsificada, apresentando o que parece ser um *link* relacionado à instituição mencionada na mensagem. Ao passar o cursor do *mouse* sobre o *link*, será possível ver o real endereço da página falsificada na barra de *status* do programa leitor de *e-mails*, ou *browser*, caso esteja atualizado e não possua vulnerabilidades. Normalmente, este *link* será diferente do apresentado na mensagem;
- acesse a página da instituição que supostamente enviou a mensagem, seguindo os cuidados apresentados na seção 2.3, e procure por informações relacionadas com a mensagem que você recebeu;
- *sites* de comércio eletrônico ou *Internet Banking* confiáveis **sempre** utilizam conexões seguras (vide seção 2.4) quando dados pessoais e financeiros de usuários são solicitados. Caso a página não utilize conexão segura, desconfie imediatamente. Caso a página falsificada utilize conexão segura, um novo certificado (que não corresponde ao *site* verdadeiro) será apresentado e, possivelmente, o endereço mostrado no *browser* será diferente do endereço correspondente ao *site* verdadeiro.

Recomendações:

- no caso de mensagem recebida por *e-mail*, o remetente **nunca** deve ser utilizado como parâmetro para atestar a veracidade de uma mensagem, pois pode ser facilmente forjado pelos fraudadores;
- se você ainda tiver alguma dúvida e acreditar que a mensagem pode ser verdadeira, entre em contato com a instituição para certificar-se sobre o caso, antes de enviar qualquer dado, principalmente informações sensíveis, como senhas e números de cartões de crédito.

2.2.3 *E-mails* contendo formulários para o fornecimento de informações sensíveis

Você recebe um *e-mail* em nome de um *site* de comércio eletrônico ou de uma instituição bancária. O conteúdo da mensagem envolve o recadastramento ou confirmação de seus dados, a participação em uma nova promoção, etc.

A mensagem apresenta um formulário, com campos para a digitação de informações envolvendo dados pessoais e financeiros, como o número, data de expiração e código de segurança do seu cartão de crédito, ou os números da sua agência e conta bancária, senha do cartão do banco e senha de acesso ao *Internet Banking*. A mensagem, então, solicita que você preencha o formulário e apresenta um botão para confirmar o envio das informações preenchidas.

Risco: ao preencher os dados e confirmar o envio, suas informações pessoais e financeiras serão transmitidas para fraudadores, que, a partir daí, poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros, ou utilização dos seus dados financeiros para efetuar pagamentos, transferir valores para outras contas, etc.

Como identificar: o serviço de *e-mail* convencional não fornece qualquer mecanismo de criptografia, ou seja, as informações, ao serem submetidas, trafegarão em claro pela Internet. Qualquer instituição confiável **não** utilizaria este meio para o envio de informações pessoais e sensíveis de seus usuários.

2.2.4 Comprometimento do serviço de resolução de nomes

Ao tentar acessar um *site* de comércio eletrônico ou *Internet Banking*, mesmo digitando o endereço diretamente no seu *browser*, você é redirecionado para uma página falsificada, semelhante ao *site* verdadeiro.

Duas possíveis causas para este caso de *phishing* são:

- o atacante comprometeu o servidor de nomes do seu provedor (DNS), de modo que todos os acessos a determinados *sites* passaram a ser redirecionados para páginas falsificadas;
- o atacante o induziu a instalar um *malware*, por exemplo, através de uma mensagem recebida por *e-mail* (como mostrado na seção 2.2.1), e este *malware* foi especificamente projetado para alterar o comportamento do serviço de resolução de nomes do seu computador, redirecionando os acessos a determinados *sites* para páginas falsificadas.

Apesar de não ter uma definição consolidada na data de publicação desta Cartilha, os veículos de comunicação têm utilizado o termo ***pharming*** para se referir a casos específicos de *phishing*, que envolvem algum tipo de redireção da vítima para *sites* fraudulentos, através de alterações nos serviços de resolução de nomes.

Risco: ao preencher os campos disponíveis na página falsificada e confirmar o envio dos dados, suas informações pessoais e financeiras serão transmitidas para fraudadores, que, a partir daí, poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros, ou utilização dos seus dados financeiros para efetuar pagamentos, transferir valores para outras contas, etc.

Como identificar: neste caso, onde fraudadores alteram o comportamento do serviço de resolução de nomes, para redirecionar acessos para páginas falsificadas, não são válidas dicas como digitar o endereço diretamente no seu *browser*, ou observar o endereço apresentado na barra de *status* do *browser*.

Deste modo, a melhor forma de identificar este tipo de fraude é estar atento para o fato de que *sites* de comércio eletrônico ou *Internet Banking* confiáveis **sempre** utilizam conexões seguras quando dados pessoais e financeiros de usuários são solicitados. Caso a página não utilize conexão segura, desconfie imediatamente. Caso a página falsificada utilize conexão segura, um novo certificado, que não corresponde ao *site* verdadeiro, será apresentado (mais detalhes sobre verificação de certificados na seção 2.6).

Recomendação: se você ainda tiver alguma dúvida e acreditar que a página pode ser verdadeira, mesmo não utilizando conexão segura, ou apresentando um certificado não compatível, entre em contato com a instituição para certificar-se sobre o caso, antes de enviar qualquer dado, principalmente informações sensíveis, como senhas e números de cartões de crédito.

2.2.5 Utilização de computadores de terceiros

Você utiliza um computador de terceiros, por exemplo, em uma *LAN house*, *cybercafe* ou *stand* de um evento, para acessar um *site* de comércio eletrônico ou *Internet Banking*.

Risco: como estes computadores são utilizados por muitas pessoas, você pode ter todas as suas ações monitoradas (incluindo a digitação de senhas ou número de cartões de crédito), através de programas especificamente projetados para este fim (como visto na seção 2.2.1) e que podem ter sido instalados previamente.

Recomendação: não utilize computadores de terceiros em operações que necessitem de seus dados pessoais e financeiros, incluindo qualquer uma de suas senhas.

2.3 Quais são os cuidados que devo ter ao acessar *sites* de comércio eletrônico ou *Internet Banking*?

Existem diversos cuidados que um usuário deve ter ao acessar *sites* de comércio eletrônico ou *Internet Banking*. Dentre eles, podem-se citar:

- realizar transações somente em *sites* de instituições que você considere confiáveis;
- procurar sempre digitar em seu *browser* o endereço desejado. Não utilize *links* em páginas de terceiros ou recebidos por *e-mail*;

- certificar-se de que o endereço apresentado em seu *browser* corresponde ao *site* que você realmente quer acessar, antes de realizar qualquer ação;
- certificar-se que o *site* faz uso de conexão segura (ou seja, que os dados transmitidos entre seu *browser* e o *site* serão criptografados) e utiliza um tamanho de chave considerado seguro (vide seção 2.4);
- antes de aceitar um novo certificado, verificar junto à instituição que mantém o *site* sobre sua emissão e quais são os dados nele contidos. Então, verificar o certificado do *site* antes de iniciar qualquer transação, para assegurar-se que ele foi emitido para a instituição que se deseja acessar e está dentro do prazo de validade (vide seção 2.6);
- estar atento e prevenir-se dos ataques de engenharia social (como visto na seção 1.1);
- não acessar *sites* de comércio eletrônico ou *Internet Banking* através de computadores de terceiros;
- desligar sua *Webcam* (caso você possua alguma), ao acessar um *site* de comércio eletrônico ou *Internet Banking*.

Além dos cuidados apresentados anteriormente é muito importante que você tenha alguns cuidados adicionais, tais como:

- manter o seu *browser* sempre atualizado e com todas as correções (*patches*) aplicadas;
- alterar a configuração do seu *browser* para restringir a execução de *JavaScript* e de programas *Java* ou *ActiveX*, exceto para casos específicos;
- configurar seu *browser* para bloquear *pop-up windows* e permití-las apenas para *sites* conhecidos e confiáveis, onde forem realmente necessárias;
- configurar seu programa leitor de *e-mails* para não abrir arquivos ou executar programas automaticamente;
- não executar programas obtidos pela Internet, ou recebidos por *e-mail*.

Com estes cuidados adicionais você pode evitar que seu *browser* contenha alguma vulnerabilidade, e que programas maliciosos (como os cavalos de tróia e outros tipos de *malware*) sejam instalados em seu computador para, dentre outras finalidades, furtar dados sensíveis e fraudar seus acessos a *sites* de comércio eletrônico ou *Internet Banking*. Maiores detalhes sobre estes cuidados podem ser obtidos nas partes II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção e VIII: Códigos Maliciosos (*Malware*).

2.4 Como verificar se a conexão é segura (criptografada)?

Existem pelo menos dois itens que podem ser visualizados na janela do seu *browser*, e que significam que as informações transmitidas entre o *browser* e o *site* visitado estão sendo criptografadas.

O primeiro pode ser visualizado no local onde o endereço do *site* é digitado. O endereço deve começar com `https://` (diferente do `http://` nas conexões normais), onde o **s** antes do sinal de

dois-pontos indica que o endereço em questão é de um *site* com conexão segura e, portanto, os dados serão criptografados antes de serem enviados. A figura 1 apresenta o primeiro item, indicando uma conexão segura, observado nos *browsers Firefox* e *Internet Explorer*, respectivamente.

Alguns *browsers* podem incluir outros sinais na barra de digitação do endereço do *site*, que indicam que a conexão é segura. No *Firefox*, por exemplo, o local onde o endereço do *site* é digitado muda de cor, ficando amarelo, e apresenta um cadeado fechado do lado direito.

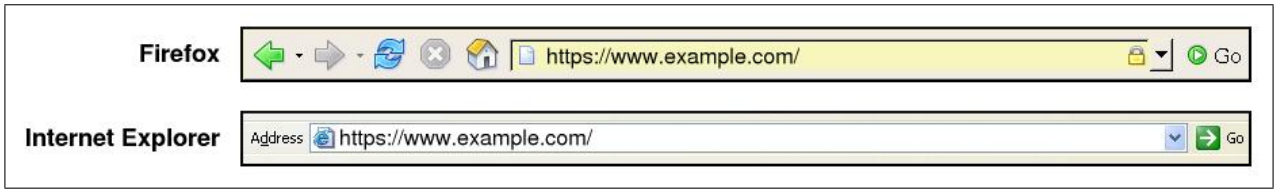

Figura 1: **https** - identificando site com conexão segura.

O segundo item a ser visualizado corresponde a algum desenho ou sinal, indicando que a conexão é segura. Normalmente, o desenho mais adotado nos *browsers* recentes é de um "**cadeado fechado**", apresentado na barra de *status*, na parte inferior da janela do *browser* (se o cadeado estiver aberto, a conexão não é segura).

A figura 2 apresenta desenhos dos cadeados fechados, indicando conexões seguras, observados nas barras de *status* nos *browsers Firefox* e *Internet Explorer*, respectivamente.

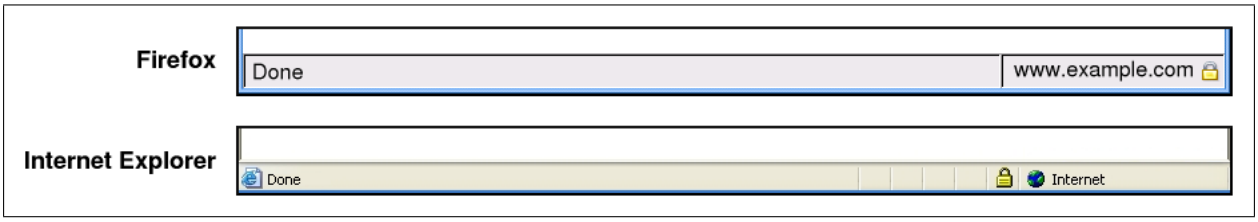

Figura 2: **Cadeado** – identificando site com conexão segura.

Ao clicar sobre o cadeado, será exibida uma tela que permite verificar as informações referentes ao certificado emitido para a instituição que mantém o *site* (veja seção 2.6), bem como informações sobre o tamanho da chave utilizada para criptografar os dados.

É muito importante que você verifique se a chave utilizada para criptografar as informações a serem transmitidas entre seu *browser* e o *site* é de no mínimo 128 bits. Chaves menores podem comprometer a segurança dos dados a serem transmitidos. Maiores detalhes sobre criptografia e tamanho de chaves podem ser obtidos na parte I: Conceitos de Segurança.

Outro fator muito importante é que a verificação das informações do certificado deve ser feita clicando única e exclusivamente no cadeado exibido na barra *status* do *browser*. Atacantes podem tentar forjar certificados, incluindo o desenho de um cadeado fechado no conteúdo da página. A figura 3 ilustra esta situação no *browser Firefox*.

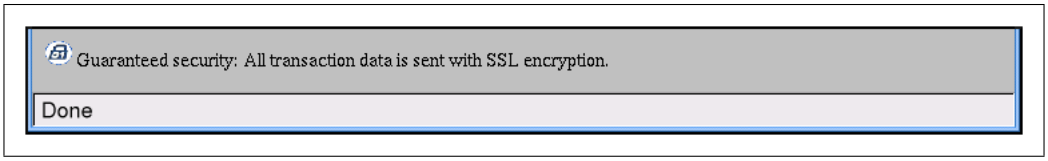

Figura 3: Cadeado forjado.

Compare as barras de *status* do *browser Firefox* nas figuras 2 e 3. Observe que na figura 3 **não** é apresentado um cadeado fechado dentro da barra de *status*, indicando que a conexão **não** é segura.

2.5 Como posso saber se o *site* que estou acessando não foi falsificado?

Existem alguns cuidados que um usuário deve ter para certificar-se que um *site* não foi falsificado.

O primeiro cuidado é checar se o endereço digitado permanece inalterado no momento em que o conteúdo do *site* é apresentado no *browser* do usuário. Existem algumas situações, como visto na seção 2.2, onde o acesso a um *site* pode ser redirecionado para uma página falsificada, mas normalmente nestes casos o endereço apresentado pelo *browser* é diferente daquele que o usuário quer realmente acessar.

E um outro cuidado muito importante é verificar as informações contidas no certificado emitido para a instituição que mantém o *site*. Estas informações podem dizer se o certificado é ou não legítimo e, conseqüentemente, se o *site* é ou não falsificado (vide seção 2.6).

2.6 Como posso saber se o certificado emitido para o *site* é legítimo?

É extremamente importante que o usuário verifique algumas informações contidas no certificado. Um exemplo de um certificado, emitido para um *site* de uma instituição é mostrado abaixo.

```
This Certificate belongs to:   This Certificate was issued by:
 www.example.org                www.examplesign.com/CPS Incorp.by Ref.
 Terms of use at                LIABILITY LTD.(c)97 ExampleSign
 www.examplesign.com/dir (c)00  ExampleSign International Server CA -
 UF Tecno                       Class 3
 Example Associados, Inc.       ExampleSign, Inc.
 Cidade, Estado, BR

Serial Number:
  70:DE:ED:0A:05:20:9C:3D:A0:A2:51:AA:CA:81:95:1A
This Certificate is valid from Sat Aug 20, 2005 to Sun
Aug 20, 2006
Certificate Fingerprint:
  92:48:09:A1:70:7A:AF:E1:30:55:EC:15:A3:0C:09:F0
```

O usuário deve, então, verificar se o certificado foi emitido para o *site* da instituição que ele deseja acessar. As seguintes informações devem ser checadas:

- o endereço do *site*;
- o nome da instituição (dona do certificado);
- o prazo de validade do certificado.

Ao entrar pela primeira vez em um *site* que usa conexão segura, seu *browser* apresentará uma janela pedindo para confirmar o recebimento de um novo certificado. Então, verifique se os dados do certificado correspondem à instituição que você realmente deseja acessar e se seu *browser* reconheceu a Autoridade Certificadora que emitiu o certificado[3].

[3] Os conceitos de Autoridade Certificadora e certificados digitais, bem como as principais informações encontradas em um certificado podem ser encontradas na parte I: Conceitos de Segurança.

Se ao entrar em um *site* com conexão segura, que você utilize com freqüência, seu *browser* apresentar uma janela pedindo para confirmar o recebimento de um novo certificado, fique atento. Uma situação possível seria que a validade do certificado do *site* tenha vencido, ou o certificado tenha sido revogado por outros motivos, e um novo certificado foi emitido para o *site*. Mas isto também pode significar que você está recebendo um certificado ilegítimo e, portanto, estará acessando um *site* falsificado.

Uma dica para reconhecer esta situação é que as informações contidas no certificado normalmente não corresponderão às da instituição que você realmente deseja acessar. Além disso, seu *browser* possivelmente informará que a Autoridade Certificadora que emitiu o certificado para o *site* não pôde ser reconhecida.

De qualquer modo, caso você receba um novo certificado ao acessar um *site* e tenha alguma dúvida ou desconfiança, não envie qualquer informação para o *site* antes de entrar em contato com a instituição que o mantém, para esclarecer o ocorrido.

2.7 O que devo fazer se perceber que meus dados financeiros estão sendo usados por terceiros?

Caso você acredite que terceiros possam estar usando suas informações pessoais e financeiras, como o número do seu cartão de crédito ou seus dados bancários (senha de acesso ao *Internet Banking* e senha do cartão de banco), entre em contato com a instituição envolvida (por exemplo, seu banco ou operadora do seu cartão de crédito), informe-os sobre o caso e siga as orientações que serão passadas por eles.

Monitore regularmente suas movimentações financeiras, por exemplo, através de extratos bancários e/ou de cartões de crédito, e procure por débitos, transferências ou cobranças inesperadas.

É recomendado que você procure uma delegacia de polícia, para registrar um boletim de ocorrência, caso tenha sido vítima de uma fraude via Internet.

3 Boatos

Boatos (*hoaxes*) são *e-mails* que possuem conteúdos alarmantes ou falsos e que, geralmente, têm como remetente ou apontam como autora da mensagem alguma instituição, empresa importante ou órgão governamental. Através de uma leitura minuciosa deste tipo de *e-mail*, normalmente, é possível identificar em seu conteúdo mensagens absurdas e muitas vezes sem sentido.

Dentre os diversos boatos típicos, que chegam às caixas postais de usuários conectados à Internet, podem-se citar as correntes, pirâmides, mensagens sobre pessoas que estão prestes a morrer de câncer, entre outras.

Histórias deste tipo são criadas não só para espalhar desinformação pela Internet, mas também para outros fins maliciosos.

3.1 Quais são os problemas de segurança relacionados aos boatos?

Normalmente, o objetivo do criador de um boato é verificar o quanto ele se propaga pela Internet e por quanto tempo permanece se propagando. De modo geral, os boatos não são responsáveis por grandes problemas de segurança, a não ser ocupar espaço nas caixa de *e-mails* de usuários.

Mas podem existir casos com conseqüências mais sérias como, por exemplo, um boato que procura induzir usuários de Internet a fornecer informações importantes (como números de documentos, de contas-corrente em banco ou de cartões de crédito), ou um boato que indica uma série de ações a serem realizadas pelos usuários e que, se forem realmente efetivadas, podem resultar em danos mais sérios (como instruções para apagar um arquivo que supostamente contém um vírus, mas que na verdade é parte importante do sistema operacional instalado no computador).

Além disso, *e-mails* de boatos podem conter vírus, cavalos de tróia ou outros tipos de *malware* anexados. Maiores detalhes podem ser encontrados na parte VIII: Códigos Maliciosos (*Malware*).

É importante ressaltar que um boato também pode comprometer a credibilidade e a reputação tanto da pessoa ou entidade referenciada como suposta criadora do boato, quanto daqueles que o repassam.

3.2 Como evitar a distribuição dos boatos?

Normalmente, os boatos se propagam pela boa vontade e solidariedade de quem os recebe. Isto ocorre, muitas vezes, porque aqueles que o recebem:

- confiam no remetente da mensagem;
- não verificam a procedência da mensagem;
- não checam a veracidade do conteúdo da mensagem.

Para que você possa evitar a distribuição de boatos é muito importante checar a procedência dos *e-mails*, e mesmo que tenham como remetente alguém conhecido, é preciso certificar-se que a mensagem não é um boato (veja seção 3.3).

É importante ressaltar que você **nunca** deve repassar este tipo de mensagem, pois estará endossando ou concordando com o seu conteúdo.

3.3 Como posso saber se um *e-mail* é um boato?

Um boato normalmente apresenta pelo menos uma das características listadas abaixo. Observe que estas características devem ser usadas apenas como guia. Nem todo boato apresenta uma destas características e mensagens legítimas podem apresentar algumas delas.

Muitas vezes, um boato:

- sugere conseqüências trágicas se uma determinada tarefa não for realizada;
- promete ganhos financeiros ou prêmios mediante a realização de alguma ação;

- fornece instruções ou arquivos anexados para, supostamente, proteger seu computador de um vírus não detectado por programas antivírus;
- afirma não ser um boato;
- apresenta diversos erros gramaticais e de ortografia;
- apresenta uma mensagem contraditória;
- contém algum texto enfatizando que você deve repassar a mensagem para o maior número de pessoas possível;
- já foi repassado diversas vezes (no corpo da mensagem normalmente é possível observar cabeçalhos de *e-mails* repassados por outras pessoas).

Existem *sites* especializados na Internet onde podem ser encontradas listas contendo os boatos que estão circulando e seus respectivos conteúdos.

Alguns destes *sites* são:

- *Hoaxbusters* – http://hoaxbusters.ciac.org/
- QuatroCantos – http://www.quatrocantos.com/LENDAS/ (em português)
- *Urban Legends and Folklore* – http://urbanlegends.about.com/
- *Urban Legends Reference Pages* – http://www.snopes.com/
- *Stiller Research Virus Hoax News* – http://www.stiller.com/hoaxes.htm
- *TruthOrFiction.com* – http://www.truthorfiction.com/
- *Symantec Security Response Hoaxes* – http://www.symantec.com/avcenter/hoax.html
- *McAfee Security Virus Hoaxes* – http://vil.mcafee.com/hoax.asp

Além disso, os cadernos de informática dos jornais de grande circulação, normalmente, trazem matérias ou avisos sobre os boatos mais recentes.

Como Obter este Documento

Este documento pode ser obtido em http://cartilha.cert.br/. Como ele é periodicamente atualizado, certifique-se de ter sempre a versão mais recente.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, entre em contato através do endereço doc@cert.br.

Nota de *Copyright* e Distribuição

Agradecimentos

O CERT.br agradece a todos que contribuíram para a elaboração deste documento, enviando comentários, críticas, sugestões ou revisões.