Cartilha de Segurança para Internet
Parte IV: Fraudes na Internet

NIC BR Security Office
nbso@nic.br

Versão 2.0
11 de março de 2003

Resumo

Esta parte da cartilha aborda questões relacionadas à 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.

Como Obter este Documento

Este documento pode ser obtido em http://www.nbso.nic.br/docs/cartilha/. 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@nic.br.

Nota de *Copyright* e Distribuição

Sumário

1 Engenharia Social

Nos ataques de engenharia social normalmente o atacante frauda a sua identidade, se fazendo 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, como por exemplo executar um programa, acessar a página de *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) desta Cartilha. Exemplos específicos destes ataques, envolvendo fraudes em comércio eletrônico e *Internet Banking*, são abordados na seção 2.1.

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 em Comércio Eletrônico e *Internet Banking*

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.

Portanto, é muito importante que usuários de Internet tenham certos cuidados ao acessar *sites* de comércio eletrônico ou *Internet Banking*.

A seção 2.1 discute algumas situações envolvendo fraudes no acesso a estes *sites* e a seção 2.2 apresenta alguns cuidados a serem tomados pelos usuários de Internet.

2.1 Que situações podem ser citadas sobre fraudes envolvendo comércio eletrônico ou *Internet Banking*?

Existem diversas situações que vêm sendo utilizadas por atacantes em fraudes envolvendo o comércio eletrônico e *Internet Banking*. A maior parte das situações apresentadas abaixo, com exceção das situações 3 e 5, envolvem técnicas de engenharia social.

Situação 1 o usuário recebe um *e-mail* ou ligação telefônica, de um suposto funcionário da instituição que mantém o *site* de comércio eletrônico ou de um banco. Neste *e-mail* ou ligação telefônica o usuário é persuadido a fornecer informações sensíveis, como senhas de acesso ou número de cartões de crédito.

Situação 2 o usuário recebe um *e-mail*, cujo remetente pode ser um suposto funcionário, gerente, ou até mesmo uma pessoa conhecida, sendo que este *e-mail* contém um programa anexado. A mensagem, então, solicita que o usuário execute o programa para, por exemplo, obter acesso mais rápido a um *site* de comércio eletrônico ou ter acesso a informações mais detalhadas em sua conta bancária.

Estes programas normalmente são cavalos de tróia, especificamente projetados para monitorar as ações do usuário nos acessos a *sites* de comércio eletrônico ou *Internet Banking*, e têm como principal objetivo capturar e enviar senhas ou números de cartões de crétido para um atacante.

Para realizar o monitoramento, um programa deste tipo pode utilizar diversas formas. Dentre elas, podem-se citar:

Teclas digitadas: um programa pode capturar e armazenar todas as teclas digitadas pelo usuário, em particular, aquelas digitadas logo após a entrada em um *site* de comércio eletrônico ou de *Internet Banking*. Deste modo, o programa pode armazenar e enviar informações sensíveis (como senhas de acesso ao banco ou números de cartões de crétido) para um atacante;

Posição do cursor e tela: alguns *sites* de *Internet Banking* têm fornecido um teclado virtual, para evitar que seus usuários utilizem o teclado convencional e, assim, aumentar o nível de segurança na realização de transações bancárias via *Web*. O fato é que um programa pode armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* foi clicado. Estas informações permitem que um atacante, por exemplo, saiba qual foi a senha de acesso ao banco utilizada pelo usuário;

***Webcam*:** um programa pode controlar a *Webcam* do usuário, direcionando-a para o teclado, no momento em que o usuário estiver acessando um *site* de comércio eletrônico ou de *Internet Banking*. Deste modo, as imagens coletadas (incluindo aquelas que contém a digitação de senhas ou número de cartões de crédito) podem ser enviadas para um atacante.

Situação 3 um atacante compromete o servidor de nomes do provedor do usuário, de modo que todos os acessos a um *site* de comércio eletrônico ou *Internet Banking* são redirecionados para uma página *Web* falsificada, semelhante ao *site* verdadeiro. Neste caso, um atacante pode monitorar todas as ações do usuário, incluindo, por exemplo, a digitação de sua senha bancária ou do número de seu cartão de crédito. É importante ressaltar que nesta situação normalmente o usuário deve aceitar um novo certificado (que não corresponde ao *site* verdadeiro) e o endereço mostrado no *browser* do usuário poderá ser diferente do endereço correspodente ao *site* verdadeiro;

Situação 4 o usuário pode ser persuadido a acessar um *site* de comércio eletrônico ou de *Internet Banking*, através de um *link* recebido por *e-mail* ou em uma página de terceiros. Este *link* pode direcionar o usuário para uma página *Web* falsificada, semelhante ao *site* que o usuário realmente deseja acessar. A partir daí, um atacante pode monitorar todas as ações do usuário,

incluindo, por exemplo, a digitação de sua senha bancária ou do número de seu cartão de crédito. Também é importante ressaltar que nesta situação normalmente o usuário deve aceitar um novo certificado (que não corresponde ao *site* verdadeiro) e o endereço mostrado no *browser* do usuário será diferente do endereço correspodente ao *site* verdadeiro;

Situação 5 o usuário, ao utilizar computadores de terceiros para acessar *sites* de comércio eletrônico ou de *Internet Banking*, 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 situação 2).

Apesar de existirem todas estas situações de risco, também existem alguns cuidados, relativamente simples, que podem e devem ser seguidos pelos usuários ao acessarem *sites* de comércio eletrônico e *Internet Banking*, de modo a evitar que fraudadores utilizem seus dados (principalmente dados sensíveis).

2.2 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:

- estar atento e prevenir-se dos ataques de engenharia social (como visto na seção 1.1);
- realizar transações somente em *sites* de instituições que você considere confiáveis;
- certificar-se de que o endereço apresentado em seu *browser* corresponde ao *site* que você realmente quer acessar, antes de realizar qualquer ação;
- antes de aceitar um novo certificado, verificar junto à instituição que mantém o *site* sobre sua emissão e quais são os dados nele contidos;
- procurar sempre digitar em seu *browser* o endereço desejado. Não utilize *links* em páginas de terceiros ou recebidos por *e-mail*;
- 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 2.3);
- verificar o certificado do *site*, para assegurar-se que ele foi emitido para a instituição que se deseja acessar e está dentro do prazo de validade (vide seção 2.5);
- não acessar *sites* de comércio eletrônico ou *Internet Banking* através de computadores de terceiros;
- desligar sua *Webcam* (caso vecê 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 programa de *e-mail* 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) sejam instalados em seu computador para, dentre outras finalidades, fraudar seus acessos a *sites* de comércio eletrônico ou *Internet Banking*. Maiores detalhes sobre estes cuidados podem ser obtidos na parte II (Riscos Envolvidos no Uso da Internet e Métodos de Prevenção) desta Cartilha.

2.3 Como verificar se a conexão é criptografada?

Existem dois ítens 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 com conexão segura, observado nos *browsers Netscape* e *Internet Explorer*, respectivamente.

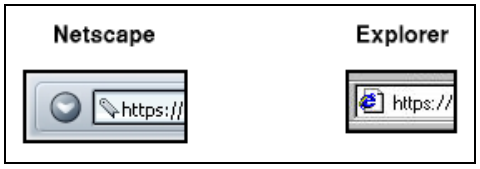

Figura 1: **https** - identificando site com conexão segura.

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**" (se o cadeado estiver aberto, a conexão não é segura).

A figura 2 apresenta desenhos dos cadeados fechados, indicando conexões seguras, observados nos *browsers Netscape* 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 2.5), 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 III desta Cartilha: Privacidade.

2.4 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 2.1, 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 2.5).

2.5 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 Thu Sep 05, 2002 to Sat
```

```
Sep 06, 2003
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 em um *site* seguro pela primeira vez, seu *browser* irá apresentar 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[1].

Se ao entrar em um *site* seguro, que você utilize com frequência, 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 além das informações contidas no certificado normalmente não corresponderem à instituição que você realmente deseja acessar, seu *browser* possivelmente irá informar 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.

3 Boatos

Boatos (*Hoaxes*) são *e-mails* que possuem conteúdos alarmantes ou falsos, e que geralmente têm como remetente ou apontam com autor 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 contéudo 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:

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

- correntes ou pirâmides;
- pessoas ou crianças que estão prestes a morrer de câncer;
- a República Federativa de algum país oferencendo elevadas quantias em dinheiro e pedindo a confirmação do usuário ou, até mesmo, solicitando algum dinheiro para efetuar a transferência.

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 consequências 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 ou cavalos de tróia anexados. Maiores detalhes sobre vírus e cavalos de tróia podem ser encontrados nas partes I (Conceitos de Segurança) e II (Riscos Envolvidos no Uso da Internet e Métodos de Prevenção) desta Cartilha.

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 rementente 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 rementente 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?

Existem *sites*, como o http://HoaxBusters.ciac.org/, onde podem-se encontrar listas contendo os boatos que estão circulando pela Internet e seus respectivos conteúdos.

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