2. Golpes na Internet

Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial e, por este motivo, golpistas vêm concentrando esforços na exploração de fragilidades dos usuários. Utilizando técnicas de engenharia social e por diferentes meios e discursos, os golpistas procuram enganar e persuadir as potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas.

De posse dos dados das vítimas, os golpistas costumam efetuar transações financeiras, acessar *sites*, enviar mensagens eletrônicas, abrir empresas fantasmas e criar contas bancárias ilegítimas, entre outras atividades maliciosas.

Muitos dos golpes aplicados na Internet podem ser considerados crimes contra o patrimônio, tipificados como estelionato. Dessa forma, o golpista pode ser considerado um estelionatário.

Nas próximas seções são apresentados alguns dos principais golpes aplicados na Internet e alguns cuidados que você deve tomar para se proteger deles.

2.1 Furto de identidade (*Identity theft*)

O furto de identidade, ou *identity theft*, é o ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas. Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade.

No seu dia a dia, sua identidade pode ser furtada caso, por exemplo, alguém abra uma empresa ou uma conta bancária usando seu nome e seus documentos. Na Internet isto também pode ocorrer, caso alguém crie um perfil em seu nome em uma rede social, acesse sua conta de *e-mail* e envie mensagens se passando por você ou falsifique os campos de *e-mail*, fazendo parecer que ele foi enviado por você.

Quanto mais informações você disponibiliza sobre a sua vida e rotina, mais fácil se torna para um golpista furtar a sua identidade, pois mais dados ele tem disponíveis e mais convincente ele pode ser. Além disto, o golpista pode usar outros tipos de golpes e ataques para coletar informações sobre você, inclusive suas senhas, como códigos maliciosos (mais detalhes no Capítulo Códigos maliciosos (*Malware*)), ataques de força bruta e interceptação de tráfego (mais detalhes no Capítulo Ataques na Internet).

Caso a sua identidade seja furtada, você poderá arcar com consequências como perdas financeiras, perda de reputação e falta de crédito. Além disto, pode levar muito tempo e ser bastante desgastante até que você consiga reverter todos os problemas causados pelo impostor.

Prevenção:

A melhor forma de impedir que sua identidade seja furtada é evitar que o impostor tenha acesso aos seus dados e às suas contas de usuário (mais detalhes no Capítulo Privacidade). Além disto, para evitar que suas senhas sejam obtidas e indevidamente usadas, é muito importante que você seja cuidadoso, tanto ao usá-las quanto ao elaborá-las (mais detalhes no Capítulo Contas e senhas).

É necessário também que você fique atento a alguns indícios que podem demonstrar que sua identidade está sendo indevidamente usada por golpistas, tais como:

- você começa a ter problemas com órgãos de proteção de crédito;
- você recebe o retorno de *e-mails* que não foram enviados por você;
- você verifica nas notificações de acesso que a sua conta de *e-mail* ou seu perfil na rede social foi acessado em horários ou locais em que você próprio não estava acessando;
- ao analisar o extrato da sua conta bancária ou do seu cartão de crédito você percebe transações que não foram realizadas por você;
- você recebe ligações telefônicas, correspondências e *e-mails* se referindo a assuntos sobre os quais você não sabe nada a respeito, como uma conta bancária que não lhe pertence e uma compra não realizada por você.

2.2 Fraude de antecipação de recursos (*Advance fee fraud*)

A fraude de antecipação de recursos, ou *advance fee fraud*, é aquela na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.

Por meio do recebimento de mensagens eletrônicas ou do acesso a *sites* fraudulentos, a pessoa é envolvida em alguma situação ou história mirabolante, que justifique a necessidade de envio de informações pessoais ou a realização de algum pagamento adiantado, para a obtenção de um benefício futuro. Após fornecer os recursos solicitados a pessoa percebe que o tal benefício prometido não existe, constata que foi vítima de um golpe e que seus dados/dinheiro estão em posse de golpistas.

O Golpe da Nigéria (*Nigerian 4-1-9 Scam*[1]) é um dos tipos de fraude de antecipação de recursos mais conhecidos e é aplicado, geralmente, da seguinte forma:

a. Você recebe uma mensagem eletrônica em nome de alguém ou de alguma instituição dizendo-se ser da Nigéria, na qual é solicitado que você atue como intermediário em uma transferência internacional de fundos;

b. o valor citado na mensagem é absurdamente alto e, caso você aceite intermediar a transação, recebe a promessa de futuramente ser recompensado com uma porcentagem deste valor;

c. o motivo, descrito na mensagem, pelo qual você foi selecionado para participar da transação geralmente é a indicação de algum funcionário ou amigo que o apontou como sendo uma pessoa honesta, confiável e merecedora do tal benefício;

d. a mensagem deixa claro que se trata de uma transferência ilegal e, por isto, solicita sigilo absoluto e urgência na resposta, caso contrário, a pessoa procurará por outro parceiro e você perderá a oportunidade;

e. após responder a mensagem e aceitar a proposta, os golpistas solicitam que você pague antecipadamente uma quantia bem elevada (porém bem inferior ao total que lhe foi prometido) para arcar com custos, como advogados e taxas de transferência de fundos;

f. após informar os dados e efetivar o pagamento solicitado, você é informado que necessita realizar novos pagamentos ou perde o contato com os golpistas;

g. finalmente, você percebe que, além de perder todo o dinheiro investido, nunca verá a quantia prometida como recompensa e que seus dados podem estar sendo indevidamente usados.

Apesar deste golpe ter ficado conhecido como sendo da Nigéria, já foram registrados diversos casos semelhantes, originados ou que mencionavam outros países, geralmente de regiões pobres ou que estejam passando por conflitos políticos, econômicos ou raciais.

A fraude de antecipação de recursos possui diversas variações que, apesar de apresentarem diferentes discursos, assemelham-se pela forma como são aplicadas e pelos danos causados. Algumas destas variações são:

[1] O número 419 refere-se à seção do Código Penal da Nigéria equivalente ao artigo 171 do Código Penal Brasileiro, ou seja, estelionato.

Loteria internacional: você recebe um *e-mail* informando que foi sorteado em uma loteria internacional, mas que para receber o prêmio a que tem direito, precisa fornecer seus dados pessoais e informações sobre a sua conta bancária.

Crédito fácil: você recebe um *e-mail* contendo uma oferta de empréstimo ou financiamento com taxas de juros muito inferiores às praticadas no mercado. Após o seu crédito ser supostamente aprovado você é informado que necessita efetuar um depósito bancário para o ressarcimento das despesas.

Doação de animais: você deseja adquirir um animal de uma raça bastante cara e, ao pesquisar por possíveis vendedores, descobre que há *sites* oferecendo estes animais para doação. Após entrar em contato, é solicitado que você envie dinheiro para despesas de transporte.

Oferta de emprego: você recebe uma mensagem em seu celular contendo uma proposta tentadora de emprego. Para efetivar a contratação, no entanto, é necessário que você informe detalhes de sua conta bancária.

Noiva russa: alguém deixa um recado em sua rede social contendo insinuações sobre um possível relacionamento amoroso entre vocês. Esta pessoa mora em outro país, geralmente a Rússia, e após alguns contatos iniciais sugere que vocês se encontrem pessoalmente, mas, para que ela possa vir até o seu país, necessita ajuda financeira para as despesas de viagem.

Prevenção:

A melhor forma de se prevenir é identificar as mensagens contendo tentativas de golpes. Uma mensagem deste tipo, geralmente, possui características como:

- oferece quantias astronômicas de dinheiro;
- solicita sigilo nas transações;
- solicita que você a responda rapidamente;
- apresenta palavras como "urgente" e "confidencial" no campo de assunto;
- apresenta erros gramaticais e de ortografia (muitas mensagens são escritas por meio do uso de programas tradutores e podem apresentar erros de tradução e de concordância).

Além disto, adotar uma postura preventiva pode, muitas vezes, evitar que você seja vítima de golpes. Por isto, é muito importante que você:

- questione-se por que justamente você, entre os inúmeros usuários da Internet, foi escolhido para receber o benefício proposto na mensagem e como chegaram até você;
- desconfie de situações onde é necessário efetuar algum pagamento com a promessa de futuramente receber um valor maior (pense que, em muitos casos, as despesas poderiam ser descontadas do valor total).

Aplicar a sabedoria popular de ditados como "Quando a esmola é demais, o santo desconfia" ou "Tudo que vem fácil, vai fácil", também pode ajudá-lo nesses casos.

Vale alertar que mensagens deste tipo nunca devem ser respondidas, pois isto pode servir para confirmar que o seu endereço de *e-mail* é válido. Esta informação pode ser usada, por exemplo, para incluí-lo em listas de *spam* ou de possíveis vítimas em outros tipos de golpes.

2.3 *Phishing*

Phishing[2], *phishing-scam* ou *phishing/scam*, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

O *phishing* ocorre por meio do envio de mensagens eletrônicas que:

- tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um *site* popular;
- procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;
- informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;
- tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas *Web*.

Para atrair a atenção do usuário as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento, como exemplificado na Tabela 2.1[3]. Exemplos de situações envolvendo *phishing* são:

Páginas falsas de comércio eletrônico ou *Internet Banking*: você recebe um *e-mail*, em nome de um *site* de comércio eletrônico ou de uma instituição financeira, que tenta induzi-lo a clicar em um *link*. Ao fazer isto, você é direcionado para uma página *Web* falsa, semelhante ao *site* que você realmente deseja acessar, onde são solicitados os seus dados pessoais e financeiros.

Páginas falsas de redes sociais ou de companhias aéreas: você recebe uma mensagem contendo um *link* para o *site* da rede social ou da companhia aérea que você utiliza. Ao clicar, você é direcionado para uma página *Web* falsa onde é solicitado o seu nome de usuário e a sua senha que, ao serem fornecidos, serão enviados aos golpistas que passarão a ter acesso ao *site* e poderão efetuar ações em seu nome, como enviar mensagens ou emitir passagens aéreas.

Mensagens contendo formulários: você recebe uma mensagem eletrônica contendo um formulário com campos para a digitação de dados pessoais e financeiros. A mensagem solicita que você preencha o formulário e apresenta um botão para confirmar o envio das informações. Ao preencher os campos e confirmar o envio, seus dados são transmitidos para os golpistas.

Mensagens contendo *links* para códigos maliciosos: você recebe um *e-mail* que tenta induzi-lo a clicar em um *link*, para baixar e abrir/executar um arquivo. Ao clicar, é apresentada uma mensagem de erro ou uma janela pedindo que você salve o arquivo. Após salvo, quando você abri-lo/executá-lo, será instalado um código malicioso em seu computador.

[2] A palavra *phishing*, do inglês "*fishing*", vem de uma analogia criada pelos fraudadores, onde "iscas" (mensagens eletrônicas) são usadas para "pescar" senhas e dados financeiros de usuários da Internet.

[3] Esta lista não é exaustiva e nem se aplica a todos os casos, pois ela pode variar conforme o destaque do momento.

Solicitação de recadastramento: você recebe uma mensagem, supostamente enviada pelo grupo de suporte da instituição de ensino que frequenta ou da empresa em que trabalha, informando que o serviço de *e-mail* está passando por manutenção e que é necessário o recadastramento. Para isto, é preciso que você forneça seus dados pessoais, como nome de usuário e senha.

Tópico	Tema da mensagem
Álbuns de fotos e vídeos	pessoa supostamente conhecida, celebridades algum fato noticiado em jornais, revistas ou televisão traição, nudez ou pornografia, serviço de acompanhantes
Antivírus	atualização de vacinas, eliminação de vírus lançamento de nova versão ou de novas funcionalidades
Associações assistenciais	AACD Teleton, Click Fome, Criança Esperança
Avisos judiciais	intimação para participação em audiência comunicado de protesto, ordem de despejo
Cartões de crédito	programa de fidelidade, promoção
Cartões virtuais	UOL, *Voxcards*, Yahoo! Cartões, O Carteiro, *Emotioncard*
Comércio eletrônico	cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em *site* de compras coletivas
Companhias aéreas	promoção, programa de milhagem
Eleições	título eleitoral cancelado, convocação para mesário
Empregos	cadastro e atualização de currículos, processo seletivo em aberto
Imposto de renda	nova versão ou correção de programa consulta de restituição, problema nos dados da declaração
Internet Banking	unificação de bancos e contas, suspensão de acesso atualização de cadastro e de cartão de senhas lançamento ou atualização de módulo de segurança comprovante de transferência e depósito, cadastramento de computador
Multas e infrações de trânsito	aviso de recebimento, recurso, transferência de pontos
Músicas	canção dedicada por amigos
Notícias e boatos	fato amplamente noticiado, ataque terrorista, tragédia natural
Prêmios	loteria, instituição financeira
Programas em geral	lançamento de nova versão ou de novas funcionalidades
Promoções	vale-compra, assinatura de jornal e revista desconto elevado, preço muito reduzido, distribuição gratuita
Propagandas	produto, curso, treinamento, concurso
Reality shows	Big Brother Brasil, A Fazenda, Ídolos
Redes sociais	notificação pendente, convite para participação aviso sobre foto marcada, permissão para divulgação de foto
Serviços de Correios	recebimento de telegrama *online*
Serviços de *e-mail*	recadastramento, caixa postal lotada, atualização de banco de dados
Serviços de proteção de crédito	regularização de débitos, restrição ou pendência financeira
Serviços de telefonia	recebimento de mensagem, pendência de débito bloqueio de serviços, detalhamento de fatura, créditos gratuitos
Sites com dicas de segurança	aviso de conta de *e-mail* sendo usada para envio de *spam* (Antispam.br) cartilha de segurança (CERT.br, FEBRABAN, Abranet, etc.)
Solicitações	orçamento, documento, relatório, cotação de preços, lista de produtos

Tabela 2.1: Exemplos de tópicos e temas de mensagens de *phishing*.

Prevenção:

- fique atento a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em *links*;
- questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há porque recadastrar dados ou atualizar módulos de segurança);
- fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos;
- não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada (mais detalhes na Seção 3.3 do Capítulo Ataques na Internet);
- seja cuidadoso ao acessar *links*. Procure digitar o endereço diretamente no navegador *Web*;
- verifique o *link* apresentado na mensagem. Golpistas costumam usar técnicas para ofuscar o *link* real para o *phishing*. Ao posicionar o *mouse* sobre o *link*, muitas vezes é possível ver o endereço real da página falsa ou código malicioso;
- utilize mecanismos de segurança, como programas *antimalware*, *firewall* pessoal e filtros *antiphishing* (mais detalhes no Capítulo Mecanismos de segurança);
- verifique se a página utiliza conexão segura. *Sites* de comércio eletrônico ou *Internet Banking* confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados (mais detalhes na Seção 10.1.1 do Capítulo Uso seguro da Internet);
- verifique as informações mostradas no certificado. Caso a página falsa utilize conexão segura, um novo certificado será apresentado e, possivelmente, o endereço mostrado no navegador *Web* será diferente do endereço correspondente ao *site* verdadeiro (mais detalhes na Seção 10.1.2 do Capítulo Uso seguro da Internet);
- acesse a página da instituição que supostamente enviou a mensagem e procure por informações (você vai observar que não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, para os seus usuários).

2.3.1 *Pharming*

Pharming é um tipo específico de *phishing* que envolve a redireção da navegação do usuário para *sites* falsos, por meio de alterações no serviço de DNS (***D**omain **N**ame **S**ystem*). Neste caso, quando você tenta acessar um *site* legítimo, o seu navegador *Web* é redirecionado, de forma transparente, para uma página falsa. Esta redireção pode ocorrer:

- por meio do comprometimento do servidor de DNS do provedor que você utiliza;
- pela ação de códigos maliciosos projetados para alterar o comportamento do serviço de DNS do seu computador;

- pela ação direta de um invasor, que venha a ter acesso às configurações do serviço de DNS do seu computador ou *modem* de banda larga.

Prevenção:

- desconfie se, ao digitar uma URL, for redirecionado para outro *site*, o qual tenta realizar alguma ação suspeita, como abrir um arquivo ou tentar instalar um programa;
- desconfie imediatamente caso o *site* de comércio eletrônico ou *Internet Banking* que você está acessando não utilize conexão segura. *Sites* confiáveis de comércio eletrônico e *Internet Banking* sempre usam conexões seguras quando dados pessoais e financeiros são solicitados (mais detalhes na Seção 10.1.1 do Capítulo Uso seguro da Internet);
- observe se o certificado apresentado corresponde ao do *site* verdadeiro (mais detalhes na Seção 10.1.2 do Capítulo Uso seguro da Internet).

2.4 Golpes de comércio eletrônico

Golpes de comércio eletrônico são aqueles nos quais golpistas, com o objetivo de obter vantagens financeiras, exploram a relação de confiança existente entre as partes envolvidas em uma transação comercial. Alguns destes golpes são apresentados nas próximas seções.

2.4.1 Golpe do *site* de comércio eletrônico fraudulento

Neste golpe, o golpista cria um *site* fraudulento, com o objetivo específico de enganar os possíveis clientes que, após efetuarem os pagamentos, não recebem as mercadorias.

Para aumentar as chances de sucesso, o golpista costuma utilizar artifícios como: enviar *spam*, fazer propaganda via *links* patrocinados, anunciar descontos em *sites* de compras coletivas e ofertar produtos muito procurados e com preços abaixo dos praticados pelo mercado.

Além do comprador, que paga mas não recebe a mercadoria, este tipo de golpe pode ter outras vítimas, como:

- uma empresa séria, cujo nome tenha sido vinculado ao golpe;
- um *site* de compras coletivas, caso ele tenha intermediado a compra;
- uma pessoa, cuja identidade tenha sido usada para a criação do *site* ou para abertura de empresas fantasmas.

Prevenção:

- faça uma pesquisa de mercado, comparando o preço do produto exposto no *site* com os valores obtidos na pesquisa e desconfie caso ele seja muito abaixo dos praticados pelo mercado;

- pesquise na Internet sobre o *site*, antes de efetuar a compra, para ver a opinião de outros clientes;
- acesse *sites* especializados em tratar reclamações de consumidores insatisfeitos, para verificar se há reclamações referentes a esta empresa;
- fique atento a propagandas recebidas através de *spam* (mais detalhes no Capítulo *Spam*);
- seja cuidadoso ao acessar *links* patrocinados (mais detalhes na Seção 6.5 do Capítulo Outros riscos);
- procure validar os dados de cadastro da empresa no *site* da Receita Federal[4];
- não informe dados de pagamento caso o *site* não ofereça conexão segura ou não apresente um certificado confiável (mais detalhes na Seção 10.1 do Capítulo Uso seguro da Internet).

2.4.2 Golpe envolvendo *sites* de compras coletivas

Sites de compras coletivas têm sido muito usados em golpes de *sites* de comércio eletrônico fraudulentos, como descrito na Seção 2.4.1. Além dos riscos inerentes às relações comerciais cotidianas, os *sites* de compras coletivas também apresentam riscos próprios, gerados principalmente pela pressão imposta ao consumidor em tomar decisões rápidas pois, caso contrário, podem perder a oportunidade de compra.

Golpistas criam *sites* fraudulentos e os utilizam para anunciar produtos nos *sites* de compras coletivas e, assim, conseguir grande quantidade de vítimas em um curto intervalo de tempo.

Além disto, *sites* de compras coletivas também podem ser usados como tema de mensagens de *phishing*. Golpistas costumam mandar mensagens como se tivessem sido enviadas pelo *site* verdadeiro e, desta forma, tentam induzir o usuário a acessar uma página falsa e a fornecer dados pessoais, como número de cartão de crédito e senhas.

Prevenção:

- procure não comprar por impulso apenas para garantir o produto ofertado;
- seja cauteloso e faça pesquisas prévias, pois há casos de produtos anunciados com desconto, mas que na verdade, apresentam valores superiores aos de mercado;
- pesquise na Internet sobre o *site* de compras coletivas, antes de efetuar a compra, para ver a opinião de outros clientes e observar se foi satisfatória a forma como os possíveis problemas foram resolvidos;
- siga as dicas apresentadas na Seção 2.3 para se prevenir de golpes envolvendo *phishing*;
- siga as dicas apresentadas na Seção 2.4.1 para se prevenir de golpes envolvendo *sites* de comércio eletrônico fraudulento.

[4] http://www.receita.fazenda.gov.br/.

2.4.3 Golpe do *site* de leilão e venda de produtos

O golpe do *site* de leilão e venda de produtos é aquele, por meio do qual, um comprador ou vendedor age de má-fé e não cumpre com as obrigações acordadas ou utiliza os dados pessoais e financeiros envolvidos na transação comercial para outros fins. Por exemplo:

- o comprador tenta receber a mercadoria sem realizar o pagamento ou o realiza por meio de transferência efetuada de uma conta bancária ilegítima ou furtada;
- o vendedor tenta receber o pagamento sem efetuar a entrega da mercadoria ou a entrega danificada, falsificada, com características diferentes do anunciado ou adquirida de forma ilícita e criminosa (por exemplo, proveniente de contrabando ou de roubo de carga);
- o comprador ou o vendedor envia *e-mails* falsos, em nome do sistema de gerenciamento de pagamentos, como forma de comprovar a realização do pagamento ou o envio da mercadoria que, na realidade, não foi feito.

Prevenção:

- faça uma pesquisa de mercado, comparando o preço do produto com os valores obtidos na pesquisa e desconfie caso ele seja muito abaixo dos praticados pelo mercado;
- marque encontros em locais públicos caso a entrega dos produtos seja feita pessoalmente;
- acesse *sites* especializados em tratar reclamações de consumidores insatisfeitos e que os coloca em contato com os responsáveis pela venda (você pode avaliar se a forma como o problema foi resolvido foi satisfatória ou não);
- utilize sistemas de gerenciamento de pagamentos pois, além de dificultarem a aplicação dos golpes, impedem que seus dados pessoais e financeiros sejam enviados aos golpistas;
- procure confirmar a realização de um pagamento diretamente em sua conta bancária ou pelo *site* do sistema de gerenciamento de pagamentos (não confie apenas em *e-mails* recebidos, pois eles podem ser falsos);
- verifique a reputação do usuário[5] (muitos *sites* possuem sistemas que medem a reputação de compradores e vendedores, por meio da opinião de pessoas que já negociaram com este usuário);
- acesse os *sites*, tanto do sistema de gerenciamento de pagamentos como o responsável pelas vendas, diretamente do navegador, sem clicar em *links* recebidos em mensagens;
- mesmo que o vendedor lhe envie o código de rastreamento fornecido pelos Correios, não utilize esta informação para comprovar o envio e liberar o pagamento (até que você tenha a mercadoria em mãos não há nenhuma garantia de que o que foi enviado é realmente o que foi solicitado).

[5] As informações dos sistemas de reputação, apesar de auxiliarem na seleção de usuários, não devem ser usadas como única medida de prevenção, pois contas com reputação alta são bastante visadas para golpes de *phishing*.

2.5 Boato (*Hoax*)

Um boato, ou *hoax*, é uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental. Por meio de uma leitura minuciosa de seu conteúdo, normalmente, é possível identificar informações sem sentido e tentativas de golpes, como correntes e pirâmides.

Boatos podem trazer diversos problemas, tanto para aqueles que os recebem e os distribuem, como para aqueles que são citados em seus conteúdos. Entre estes diversos problemas, um boato pode:

- conter códigos maliciosos;
- espalhar desinformação pela Internet;
- ocupar, desnecessariamente, espaço nas caixas de *e-mails* dos usuários;
- comprometer a credibilidade e a reputação de pessoas ou entidades referenciadas na mensagem;
- comprometer a credibilidade e a reputação da pessoa que o repassa pois, ao fazer isto, esta pessoa estará supostamente endossando ou concordando com o conteúdo da mensagem;
- aumentar excessivamente a carga de servidores de *e-mail* e o consumo de banda de rede, necessários para a transmissão e o processamento das mensagens;
- indicar, no conteúdo da mensagem, ações a serem realizadas e que, se forem efetivadas, podem resultar em sérios danos, como apagar um arquivo que supostamente contém um código malicioso, mas que na verdade é parte importante do sistema operacional instalado no computador.

Prevenção:

Normalmente, os boatos se propagam pela boa vontade e solidariedade de quem os recebe, pois há uma grande tendência das pessoas em confiar no remetente, não verificar a procedência e não conferir a veracidade do conteúdo da mensagem. Para que você possa evitar a distribuição de boatos é muito importante conferir a procedência dos *e-mails* e, mesmo que tenham como remetente alguém conhecido, é preciso certificar-se de que a mensagem não é um boato.

Um boato, geralmente, apresenta pelo menos uma das seguintes características[6]:

- afirma não ser um boato;
- sugere consequências trágicas caso uma determinada tarefa não seja realizada;
- promete ganhos financeiros ou prêmios mediante a realização de alguma ação;
- apresenta erros gramaticais e de ortografia;
- apresenta informações contraditórias;

[6]Estas características devem ser usadas apenas como guia, pois podem existir boatos que não apresentem nenhuma delas, assim como podem haver mensagens legítimas que apresentem algumas.

- enfatiza que ele deve ser repassado rapidamente para o maior número de pessoas;
- já foi repassado diversas vezes (no corpo da mensagem, normalmente, é possível observar cabeçalhos de *e-mails* repassados por outras pessoas).

Além disto, muitas vezes, uma pesquisa na Internet pelo assunto da mensagem pode ser suficiente para localizar relatos e denúncias já feitas. É importante ressaltar que você **nunca** deve repassar boatos pois, ao fazer isto, estará endossando ou concordando com o seu conteúdo.

2.6 Prevenção

Outras dicas gerais para se proteger de golpes aplicados na Internet são:

Notifique: caso identifique uma tentativa de golpe, é importante notificar a instituição envolvida, para que ela possa tomar as providências que julgar cabíveis (mais detalhes na Seção 7.2 do Capítulo Mecanismos de segurança).

Mantenha-se informado: novas formas de golpes podem surgir, portanto é muito importante que você se mantenha informado. Algumas fontes de informação que você pode consultar são:

- seções de informática de jornais de grande circulação e de *sites* de notícias que, normalmente, trazem matérias ou avisos sobre os golpes mais recentes;
- *sites* de empresas mencionadas nas mensagens (algumas empresas colocam avisos em suas páginas quando percebem que o nome da instituição está sendo indevidamente usado);
- *sites* especializados que divulgam listas contendo os golpes que estão sendo aplicados e seus respectivos conteúdos. Alguns destes *sites* são:
  - Monitor das Fraudes
    http://www.fraudes.org/ (em português)
  - Quatro Cantos
    http://www.quatrocantos.com/LENDAS/ (em português)
  - *Snopes.com - Urban Legends Reference Pages*
    http://www.snopes.com/ (em inglês)
  - *Symantec Security Response Hoaxes*
    http://www.symantec.com/avcenter/hoax.html (em inglês)
  - *TruthOrFiction.com*
    http://www.truthorfiction.com/ (em inglês)
  - *Urban Legends and Folklore*
    http://urbanlegends.about.com/ (em inglês)