Núcleo de Informação e Coordenação do Ponto BR
Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

Cartilha de Segurança para Internet

Versão 4.0

Comitê Gestor da Internet no Brasil

São Paulo
2012

Comitê Gestor da Internet no Brasil (CGI.br)
Núcleo de Informação e Coordenação do Ponto BR (NIC.br)
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)

Textos e Edição: Equipe do CERT.br
Ilustrações: Héctor Gómez e Osnei

Cartilha de Segurança para Internet, versão 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012.

Primeira edição: 2006
ISBN: 978-85-60062-05-8
ISBN: 85-60062-05-X

Segunda edição: 2012
ISBN: 978-85-60062-54-6

Prefácio

A Cartilha de Segurança para Internet é um documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças. O documento apresenta o significado de diversos termos e conceitos utilizados na Internet, aborda os riscos de uso desta tecnologia e fornece uma série de dicas e cuidados a serem tomados pelos usuários para se protegerem destas ameaças.

A produção desta Cartilha foi feita pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que é um dos serviços prestados para a comunidade Internet do Brasil pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), o braço executivo do Comitê Gestor da Internet no Brasil (CGI.br).

Nós esperamos que esta Cartilha possa auxiliá-lo não só a compreender as ameaças do ambiente Internet, mas também a usufruir dos benefícios de forma consciente e a manter a segurança de seus dados, computadores e dispositivos móveis. Gostaríamos ainda de ressaltar que é muito importante ficar sempre atento ao usar a Internet, pois somente aliando medidas técnicas a boas práticas é possível atingir um nível de segurança que permita o pleno uso deste ambiente.

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

Boa leitura!

Equipe do CERT.br
Junho de 2012

Estrutura da Cartilha

Este documento conta com quatorze capítulos, que dividem o conteúdo em diferentes áreas relacionadas com a segurança da Internet, além de um glossário e um índice remissivo.

De forma geral, o Capítulo 1 apresenta uma introdução sobre a importância de uso da Internet, os riscos a que os usuários estão sujeitos e os cuidados a serem tomados. Do Capítulo 2 ao 6 os riscos são apresentados de forma mais detalhada, enquanto que do Capítulo 7 ao 14 o foco principal são os cuidados a serem tomados e os mecanismos de segurança existentes.

1. **Segurança na Internet:** Trata dos benefícios que a Internet pode trazer na realização de atividades cotidianas e descreve, de forma geral, os riscos relacionados ao seu uso. Procura também esclarecer que a Internet não tem nada de "virtual" e que os cuidados a serem tomados ao usá-la são semelhantes aos que se deve ter no dia a dia.

2. Golpes na Internet: Apresenta os principais golpes aplicados na Internet, os riscos que estes golpes representam e os cuidados que devem ser tomados para se proteger deles.

3. Ataques na Internet: Aborda os ataques que costumam ser realizados por meio da Internet, as motivações que levam os atacantes a praticar atividades deste tipo e as técnicas que costumam ser utilizadas. Ressalta a importância de cada um fazer a sua parte para que a segurança geral da Internet possa ser melhorada.

4. Códigos maliciosos (*Malware*): Aborda os diferentes tipos de códigos maliciosos, as diversas formas de infecção e as principais ações danosas e atividades maliciosas por eles executadas. Apresenta também um resumo comparativo para facilitar a classificação dos diferentes tipos.

5. *Spam*: Discute os problemas acarretados pelo *spam*, principalmente aqueles que possam ter implicações de segurança, e métodos de prevenção.

6. Outros riscos: Aborda alguns dos serviços e recursos de navegação incorporados a grande maioria dos navegadores *Web* e leitores de *e-mails*, os riscos que eles podem representar e os cuidados que devem ser tomados ao utilizá-los. Trata também dos riscos apresentados e dos cuidados a serem tomados ao compartilhar recursos na Internet.

7. Mecanismos de segurança: Apresenta os principais mecanismos de segurança existentes e os cuidados que devem ser tomados ao utilizá-los. Ressalta a importância de utilização de ferramentas de segurança aliada a uma postura preventiva.

8. Contas e senhas: Aborda o principal mecanismo de autenticação usado na Internet que são as contas e as senhas. Inclui dicas de uso, elaboração, gerenciamento, alteração e recuperação, entre outras.

9. Criptografia: Apresenta alguns conceitos de criptografia, como funções de resumo, assinatura digital, certificado digital e as chaves simétricas e assimétricas. Trata também dos cuidados que devem ser tomados ao utilizá-la.

10. Uso seguro da Internet: Apresenta, de forma geral, os principais usos que são feitos da Internet e os cuidados que devem ser tomados ao utilizá-los. Aborda questões referentes a segurança nas conexões *Web* especialmente as envolvem o uso de certificados digitais.

11. Privacidade: Discute questões relacionadas à privacidade do usuário ao utilizar a Internet e aos cuidados que ele deve ter com seus dados pessoais. Apresenta detalhadamente dicas referentes a disponibilização de informações pessoais nas redes sociais.

12. Segurança de computadores: Apresenta os principais cuidados que devem ser tomados ao usar computadores, tanto pessoais como de terceiros. Ressalta a importância de manter os computadores atualizados e com mecanismos de proteção instalados.

13. Segurança de redes: Apresenta os riscos relacionados ao uso das principais tecnologias de acesso à Internet, como banda larga (fixa e móvel), Wi-Fi e *Bluetooth*.

14. Segurança em dispositivos móveis: Aborda os riscos relacionados ao uso de dispositivos móveis e procura demonstrar que eles são similares aos computadores e que, por isto, necessitam dos mesmos cuidados de segurança.

Licença de Uso da Cartilha

Histórico da Cartilha

No início de 2000, um grupo de estudos que, entre outros, envolveu a Abranet e o CERT.br (que à época chamava-se NBSO – NIC BR Security Office), identificou a necessidade de um guia com informações sobre segurança que pudesse ser usado como referência pelos diversos setores usuários de Internet. Como conseqüência, a pedido do Comitê Gestor da Internet no Brasil e sob supervisão do CERT.br, em julho do mesmo ano foi lançada a Cartilha de Segurança para Internet Versão 1.0.

Em 2003 foi verificada a necessidade de uma revisão geral do documento, que não só incluísse novos tópicos, mas que também facilitasse sua leitura e a localização de assuntos específicos. Neste processo de revisão a Cartilha foi completamente reescrita, dando origem à versão 2.0. Esta versão, a primeira totalmente sob responsabilidade do CERT.br, possuía estrutura dividida em partes, além de contar com o *checklist* e o glossário. Também nesta versão foram introduzidas as seções relativas a fraudes na Internet, banda larga, redes sem fio, *spam* e incidentes de segurança.

Na versão 3.0, de 2005, a Cartilha continuou com sua estrutura, mas, devido à evolução da tecnologia, novos assuntos foram incluídos. Foi criada uma parte específica sobre códigos maliciosos, expandida a parte sobre segurança de redes sem fio e incluídos tópicos específicos sobre segurança em dispositivos móveis. Esta versão também foi a primeira a disponibilizar um folheto com as dicas básicas para proteção contra as ameaças mais comuns.

A versão 3.1 não introduziu partes novas, mas incorporou diversas sugestões de melhoria recebidas, corrigiu alguns erros de digitação e atendeu a um pedido de muitos leitores: lançá-la em formato de livro, para facilitar a leitura e a impressão do conteúdo completo.

Em 2012 foi verificada novamente a necessidade de revisão geral do documento, o que deu origem à versão 4.0. Com o uso crescente da Internet e das redes sociais, impulsionado principalmente pela popularização dos dispositivos móveis e facilidades de conexão, constatou-se a necessidade de abordar novos conteúdos e agrupar os assuntos de maneira diferente. Esta versão conta com um livro com todo o conteúdo que, com o objetivo de facilitar a leitura e torná-la mais agradável, é totalmente ilustrado. Este livro, por sua vez, é complementado por fascículos com versões resumidas de alguns dos tópicos, de forma a facilitar a difusão de conteúdos específicos.

Agradecimentos

Agradecemos a todos leitores da Cartilha, que têm contribuído para a elaboração deste documento, enviando comentários, críticas, sugestões ou revisões.

Agradecemos as contribuições de Rafael Rodrigues Obelheiro, na versão 3.0, e de Nelson Murilo, na Parte V da versão 3.1 e no Capítulo 13 da atual versão.

Agradecemos a toda equipe do CERT.br, especialmente a Luiz E. R. Cordeiro, pelo texto da primeira versão; a Marcelo H. P. C. Chaves, pela produção das versões 2.0, 3.0 e 3.1 e pela criação das figuras da atual versão; a Lucimara Desiderá, pelas pesquisas realizadas, pela contribuição nos Capítulos 9 e 13 e também pela pela criação das figuras da atual versão; e a Miriam von Zuben, pela produção da versão 4.0 e por ser a principal mantenedora da Cartilha.

Sumário

Lista de Figuras

Lista de Tabelas

1. Segurança na Internet

A Internet já está presente no cotidiano de grande parte da população e, provavelmente para estas pessoas, seria muito difícil imaginar como seria a vida sem poder usufruir das diversas facilidades e oportunidades trazidas por esta tecnologia. Por meio da Internet você pode:

- encontrar antigos amigos, fazer novas amizades, encontrar pessoas que compartilham seus gostos e manter contato com amigos e familiares distantes;
- acessar *sites* de notícias e de esportes, participar de cursos à distância, pesquisar assuntos de interesse e tirar dúvidas em listas de discussão;
- efetuar serviços bancários, como transferências, pagamentos de contas e verificação de extratos;
- fazer compras em supermercados e em lojas de comércio eletrônico, pesquisar preços e verificar a opinião de outras pessoas sobre os produtos ou serviços ofertados por uma determinada loja;
- acessar *sites* dedicados a brincadeiras, passatempos e histórias em quadrinhos, além de grande variedade de jogos, para as mais diversas faixas etárias;
- enviar a sua declaração de Imposto de Renda, emitir boletim de ocorrência, consultar os pontos em sua carteira de habilitação e agendar a emissão de passaporte;

- consultar a programação das salas de cinema, verificar a agenda de espetáculos teatrais, exposições e *shows* e adquirir seus ingressos antecipadamente;

- consultar acervos de museus e *sites* dedicados à obra de grandes artistas, onde é possível conhecer a biografia e as técnicas empregadas por cada um.

Estes são apenas alguns exemplos de como você pode utilizar a Internet para facilitar e melhorar a sua vida. Aproveitar esses benefícios de forma segura, entretanto, requer que alguns cuidados sejam tomados e, para isto, é importante que você esteja informado dos riscos aos quais está exposto para que possa tomar as medidas preventivas necessárias. Alguns destes riscos são:

Acesso a conteúdos impróprios ou ofensivos: ao navegar você pode se deparar com páginas que contenham pornografia, que atentem contra a honra ou que incitem o ódio e o racismo.

Contato com pessoas mal-intencionadas: existem pessoas que se aproveitam da falsa sensação de anonimato da Internet para aplicar golpes, tentar se passar por outras pessoas e cometer crimes como, por exemplo, estelionato, pornografia infantil e sequestro.

Furto de identidade: assim como você pode ter contato direto com impostores, também pode ocorrer de alguém tentar se passar por você e executar ações em seu nome, levando outras pessoas a acreditarem que estão se relacionando com você, e colocando em risco a sua imagem ou reputação.

Furto e perda de dados: os dados presentes em seus equipamentos conectados à Internet podem ser furtados e apagados, pela ação de ladrões, atacantes e códigos maliciosos.

Invasão de privacidade: a divulgação de informações pessoais pode comprometer a sua privacidade, de seus amigos e familiares e, mesmo que você restrinja o acesso, não há como controlar que elas não serão repassadas. Além disto, os *sites* costumam ter políticas próprias de privacidade e podem alterá-las sem aviso prévio, tornando público aquilo que antes era privado.

Divulgação de boatos: as informações na Internet podem se propagar rapidamente e atingir um grande número de pessoas em curto período de tempo. Enquanto isto pode ser desejável em certos casos, também pode ser usado para a divulgação de informações falsas, que podem gerar pânico e prejudicar pessoas e empresas.

Dificuldade de exclusão: aquilo que é divulgado na Internet nem sempre pode ser totalmente excluído ou ter o acesso controlado. Uma opinião dada em um momento de impulso pode ficar acessível por tempo indeterminado e pode, de alguma forma, ser usada contra você e acessada por diferentes pessoas, desde seus familiares até seus chefes.

Dificuldade de detectar e expressar sentimentos: quando você se comunica via Internet não há como observar as expressões faciais ou o tom da voz das outras pessoas, assim como elas não podem observar você (a não ser que vocês estejam utilizando *webcams* e microfones). Isto pode dificultar a percepção do risco, gerar mal-entendido e interpretação dúbia.

Dificuldade de manter sigilo: no seu dia a dia é possível ter uma conversa confidencial com alguém e tomar cuidados para que ninguém mais tenha acesso ao que está sendo dito. Na Internet, caso não sejam tomados os devidos cuidados, as informações podem trafegar ou ficar armazenadas de forma que outras pessoas tenham acesso ao conteúdo.

Uso excessivo: o uso desmedido da Internet, assim como de outras tecnologias, pode colocar em risco a sua saúde física, diminuir a sua produtividade e afetar a sua vida social ou profissional.

Plágio e violação de direitos autorais: a cópia, alteração ou distribuição não autorizada de conteúdos e materiais protegidos pode contrariar a lei de direitos autorais e resultar em problemas jurídicos e em perdas financeiras.

Outro grande risco relacionado ao uso da Internet é o de você achar que não corre riscos, pois supõe que ninguém tem interesse em utilizar o seu computador[1] ou que, entre os diversos computadores conectados à Internet, o seu dificilmente será localizado. É justamente este tipo de pensamento que é explorado pelos atacantes, pois, ao se sentir seguro, você pode achar que não precisa se prevenir.

Esta ilusão, infelizmente, costuma terminar quando os primeiros problemas começam a acontecer. Muitas vezes os atacantes estão interessados em conseguir acesso a grandes quantidades de computadores, independente de quais são, e para isto, podem efetuar varreduras na rede e localizar grande parte dos computadores conectados à Internet, inclusive o seu.

Um problema de segurança em seu computador pode torná-lo indisponível e colocar em risco a confidencialidade e a integridade dos dados nele armazenados. Além disto, ao ser comprometido, seu computador pode ser usado para a prática de atividades maliciosas como, por exemplo, servir de repositório para dados fraudulentos, lançar ataques contra outros computadores (e assim esconder a real identidade e localização do atacante), propagar códigos maliciosos e disseminar *spam*.

Os principais riscos relacionados ao uso da Internet são detalhados nos Capítulos: Golpes na Internet, Ataques na Internet, Códigos maliciosos (*Malware*), *Spam* e Outros riscos.

O primeiro passo para se prevenir dos riscos relacionados ao uso da Internet é estar ciente de que ela não tem nada de "virtual". Tudo o que ocorre ou é realizado por meio da Internet é real: os dados são reais e as empresas e pessoas com quem você interage são as mesmas que estão fora dela. Desta forma, os riscos aos quais você está exposto ao usá-la são os mesmos presentes no seu dia a dia e os golpes que são aplicados por meio dela são similares àqueles que ocorrem na rua ou por telefone.

É preciso, portanto, que você leve para a Internet os mesmos cuidados e as mesmas preocupações que você tem no seu dia a dia, como por exemplo: visitar apenas lojas confiáveis, não deixar públicos dados sensíveis, ficar atento quando "for ao banco" ou "fizer compras", não passar informações a estranhos, não deixar a porta da sua casa aberta, etc.

Para tentar reduzir os riscos e se proteger é importante que você adote uma postura preventiva e que a atenção com a segurança seja um hábito incorporado à sua rotina, independente de questões como local, tecnologia ou meio utilizado. Para ajudá-lo nisto, há diversos mecanismos de segurança que você pode usar e que são detalhados nos Capítulos: Mecanismos de segurança, Contas e senhas e Criptografia.

Outros cuidados, relativos ao uso da Internet, como aqueles que você deve tomar para manter a sua privacidade e ao utilizar redes e dispositivos móveis, são detalhados nos demais Capítulos: Uso seguro da Internet, Privacidade, Segurança de computadores, Segurança de redes e Segurança em dispositivos móveis.

[1] Nesta Cartilha a palavra "computador" será usada para se referir a todos os dispositivos computacionais passíveis de invasão e/ou de infecção por códigos maliciosos, como computadores e dispositivos móveis.

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)

3. Ataques na Internet

Ataques costumam ocorrer na Internet com diversos objetivos, visando diferentes alvos e usando variadas técnicas. Qualquer serviço, computador ou rede que seja acessível via Internet pode ser alvo de um ataque, assim como qualquer computador com acesso à Internet pode participar de um ataque.

Os motivos que levam os atacantes a desferir ataques na Internet são bastante diversos, variando da simples diversão até a realização de ações criminosas. Alguns exemplos são:

Demonstração de poder: mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente.

Prestígio: vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar *sites* considerados visados ou difíceis de serem atacados; disputar com outros atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo.

Motivações financeiras: coletar e utilizar informações confidenciais de usuários para aplicar golpes (mais detalhes no Capítulo Golpes na Internet).

Motivações ideológicas: tornar inacessível ou invadir *sites* que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia.

Motivações comerciais: tornar inacessível ou invadir *sites* e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas.

Para alcançar estes objetivos os atacantes costumam usar técnicas, como as descritas nas próximas seções.

3.1 Exploração de vulnerabilidades

Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.

Um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.

3.2 Varredura em redes (*Scan*)

Varredura em redes, ou *scan*[1], é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

A varredura em redes e a exploração de vulnerabilidades associadas podem ser usadas de forma:

Legítima: por pessoas devidamente autorizadas, para verificar a segurança de computadores e redes e, assim, tomar medidas corretivas e preventivas.

Maliciosa: por atacantes, para explorar as vulnerabilidades encontradas nos serviços disponibilizados e nos programas instalados para a execução de atividades maliciosas. Os atacantes também podem utilizar os computadores ativos detectados como potenciais alvos no processo de propagação automática de códigos maliciosos e em ataques de força bruta (mais detalhes no Capítulo Códigos maliciosos (*Malware*) e na Seção 3.5, respectivamente).

3.3 Falsificação de *e-mail* (*E-mail spoofing*)

Falsificação de *e-mail*, ou *e-mail spoofing*, é uma técnica que consiste em alterar campos do cabeçalho de um *e-mail*, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

[1] Não confunda *scan* com *scam*. *Scams*, com "m", são esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras (mais detalhes no Capítulo Golpes na Internet).

Esta técnica é possível devido a características do protocolo SMTP (***S**imple **M**ail **T**ransfer **P**roto-col*) que permitem que campos do cabeçalho, como "`From:`" (endereço de quem enviou a mensagem), "`Reply-To`" (endereço de resposta da mensagem) e "`Return-Path`" (endereço para onde possíveis erros no envio da mensagem são reportados), sejam falsificados.

Ataques deste tipo são bastante usados para propagação de códigos maliciosos, envio de *spam* e em golpes de *phishing*. Atacantes utilizam-se de endereços de *e-mail* coletados de computadores infectados para enviar mensagens e tentar fazer com que os seus destinatários acreditem que elas partiram de pessoas conhecidas.

Exemplos de *e-mails* com campos falsificados são aqueles recebidos como sendo:

- de alguém conhecido, solicitando que você clique em um *link* ou execute um arquivo anexo;
- do seu banco, solicitando que você siga um *link* fornecido na própria mensagem e informe dados da sua conta bancária;
- do administrador do serviço de *e-mail* que você utiliza, solicitando informações pessoais e ameaçando bloquear a sua conta caso você não as envie.

Você também pode já ter observado situações onde o seu próprio endereço de *e-mail* foi indevidamente utilizado. Alguns indícios disto são:

- você recebe respostas de *e-mails* que você nunca enviou;
- você recebe *e-mails* aparentemente enviados por você mesmo, sem que você tenha feito isto;
- você recebe mensagens de devolução de *e-mails* que você nunca enviou, reportando erros como usuário desconhecido e caixa de entrada lotada (cota excedida).

3.4 Interceptação de tráfego (*Sniffing*)

Interceptação de tráfego, ou *sniffing*, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*. Esta técnica pode ser utilizada de forma:

Legítima: por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados.

Maliciosa: por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

Note que as informações capturadas por esta técnica são armazenadas na forma como trafegam, ou seja, informações que trafegam criptografadas apenas serão úteis ao atacante se ele conseguir decodificá-las (mais detalhes no Capítulo Criptografia).

3.5 Força bruta (*Brute force*)

Um ataque de força bruta, ou *brute force*, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar *sites*, computadores e serviços em nome e com os mesmos privilégios deste usuário.

Qualquer computador, equipamento de rede ou serviço que seja acessível via Internet, com um nome de usuário e uma senha, pode ser alvo de um ataque de força bruta. Dispositivos móveis, que estejam protegidos por senha, além de poderem ser atacados pela rede, também podem ser alvo deste tipo de ataque caso o atacante tenha acesso físico a eles.

Se um atacante tiver conhecimento do seu nome de usuário e da sua senha ele pode efetuar ações maliciosas em seu nome como, por exemplo:

- trocar a sua senha, dificultando que você acesse novamente o *site* ou computador invadido;
- invadir o serviço de *e-mail* que você utiliza e ter acesso ao conteúdo das suas mensagens e à sua lista de contatos, além de poder enviar mensagens em seu nome;
- acessar a sua rede social e enviar mensagens aos seus seguidores contendo códigos maliciosos ou alterar as suas opções de privacidade;
- invadir o seu computador e, de acordo com as permissões do seu usuário, executar ações, como apagar arquivos, obter informações confidenciais e instalar códigos maliciosos.

Mesmo que o atacante não consiga descobrir a sua senha, você pode ter problemas ao acessar a sua conta caso ela tenha sofrido um ataque de força bruta, pois muitos sistemas bloqueiam as contas quando várias tentativas de acesso sem sucesso são realizadas.

Apesar dos ataques de força bruta poderem ser realizados manualmente, na grande maioria dos casos, eles são realizados com o uso de ferramentas automatizadas facilmente obtidas na Internet e que permitem tornar o ataque bem mais efetivo.

As tentativas de adivinhação costumam ser baseadas em:

- dicionários de diferentes idiomas e que podem ser facilmente obtidos na Internet;
- listas de palavras comumente usadas, como personagens de filmes e nomes de times de futebol;
- substituições óbvias de caracteres, como trocar "`a`" por "`@`" e "`o`" por "`0`"";
- sequências numéricas e de teclado, como "`123456`", "`qwert`" e "`1qaz2wsx`";
- informações pessoais, de conhecimento prévio do atacante ou coletadas na Internet em redes sociais e *blogs*, como nome, sobrenome, datas e números de documentos.

Um ataque de força bruta, dependendo de como é realizado, pode resultar em um ataque de negação de serviço, devido à sobrecarga produzida pela grande quantidade de tentativas realizadas em um pequeno período de tempo (mais detalhes no Capítulo Contas e senhas).

3.6 Desfiguração de página (*Defacement*)

Desfiguração de página, *defacement* ou pichação, é uma técnica que consiste em alterar o conteúdo da página *Web* de um *site*.

As principais formas que um atacante, neste caso também chamado de *defacer*, pode utilizar para desfigurar uma página *Web* são:

- explorar erros da aplicação *Web*;
- explorar vulnerabilidades do servidor de aplicação *Web*;
- explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação *Web*;
- invadir o servidor onde a aplicação *Web* está hospedada e alterar diretamente os arquivos que compõem o *site*;
- furtar senhas de acesso à interface *Web* usada para administração remota.

Para ganhar mais visibilidade, chamar mais atenção e atingir maior número de visitantes, geralmente, os atacantes alteram a página principal do *site*, porém páginas internas também podem ser alteradas.

3.7 Negação de serviço (DoS e DDoS)

Negação de serviço, ou DoS (***D**enial **o**f **S**ervice*), é uma técnica pela qual um atacante utiliza **um computador** para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando utilizada de forma coordenada e distribuída, ou seja, quando **um conjunto de computadores** é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (***D**istributed **D**enial of **S**ervice*).

O objetivo destes ataques não é invadir e nem coletar informações, mas sim exaurir recursos e causar indisponibilidades ao alvo. Quando isto ocorre, todas as pessoas que dependem dos recursos afetados são prejudicadas, pois ficam impossibilitadas de acessar ou realizar as operações desejadas.

Nos casos já registrados de ataques, os alvos ficaram impedidos de oferecer serviços durante o período em que eles ocorreram, mas, ao final, voltaram a operar normalmente, sem que tivesse havido vazamento de informações ou comprometimento de sistemas ou computadores.

Uma pessoa pode voluntariamente usar ferramentas e fazer com que seu computador seja utilizado em ataques. A grande maioria dos computadores, porém, participa dos ataques sem o conhecimento de seu dono, por estar infectado e fazendo parte de *botnets* (mais detalhes na Seção 4.3 do Capítulo Códigos maliciosos (*Malware*)).

Ataques de negação de serviço podem ser realizados por diversos meios, como:

- pelo envio de grande quantidade de requisições para um serviço, consumindo os recursos necessários ao seu funcionamento (processamento, número de conexões simultâneas, memória e espaço em disco, por exemplo) e impedindo que as requisições dos demais usuários sejam atendidas;

- pela geração de grande tráfego de dados para uma rede, ocupando toda a banda disponível e tornando indisponível qualquer acesso a computadores ou serviços desta rede;
- pela exploração de vulnerabilidades existentes em programas, que podem fazer com que um determinado serviço fique inacessível.

Nas situações onde há saturação de recursos, caso um serviço não tenha sido bem dimensionado, ele pode ficar inoperante ao tentar atender as próprias solicitações legítimas. Por exemplo, um *site* de transmissão dos jogos da Copa de Mundo pode não suportar uma grande quantidade de usuários que queiram assistir aos jogos finais e parar de funcionar.

3.8 Prevenção

O que define as chances de um ataque na Internet ser ou não bem sucedido é o conjunto de medidas preventivas tomadas pelos usuários, desenvolvedores de aplicações e administradores dos computadores, serviços e equipamentos envolvidos.

Se cada um fizer a sua parte, muitos dos ataques realizados via Internet podem ser evitados ou, ao menos, minimizados.

A parte que cabe a você, como usuário da Internet, é proteger os seus dados, fazer uso dos mecanismos de proteção disponíveis e manter o seu computador atualizado e livre de códigos maliciosos. Ao fazer isto, você estará contribuindo para a segurança geral da Internet, pois:

- quanto menor a quantidade de computadores vulneráveis e infectados, menor será a potência das *botnets* e menos eficazes serão os ataques de negação de serviço (mais detalhes na Seção 4.3, do Capítulo Códigos maliciosos (*Malware*));
- quanto mais consciente dos mecanismos de segurança você estiver, menores serão as chances de sucesso dos atacantes (mais detalhes no Capítulo Mecanismos de segurança);
- quanto melhores forem as suas senhas, menores serão as chances de sucesso de ataques de força bruta e, consequentemente, de suas contas serem invadidas (mais detalhes no Capítulo Contas e senhas);
- quanto mais os usuários usarem criptografia para proteger os dados armazenados nos computadores ou aqueles transmitidos pela Internet, menores serão as chances de tráfego em texto claro ser interceptado por atacantes (mais detalhes no Capítulo Criptografia);
- quanto menor a quantidade de vulnerabilidades existentes em seu computador, menores serão as chances de ele ser invadido ou infectado (mais detalhes no Capítulo Segurança de computadores).

Faça sua parte e contribua para a segurança da Internet, incluindo a sua própria!

4. Códigos maliciosos (*Malware*)

Códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:

- pela exploração de vulnerabilidades existentes nos programas instalados;
- pela auto-execução de mídias removíveis infectadas, como *pen-drives*;
- pelo acesso a páginas *Web* maliciosas, utilizando navegadores vulneráveis;
- pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas *Web* ou diretamente de outros computadores (através do compartilhamento de recursos).

Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.

Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de *spam* (mais detalhes nos Capítulos Golpes na Internet, Ataques na Internet e *Spam*, respectivamente).

Os principais tipos de códigos maliciosos existentes são apresentados nas próximas seções.

4.1 Vírus

Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado.

O principal meio de propagação de vírus costumava ser os disquetes. Com o tempo, porém, estas mídias caíram em desuso e começaram a surgir novas maneiras, como o envio de *e-mail*. Atualmente, as mídias removíveis tornaram-se novamente o principal meio de propagação, não mais por disquetes, mas, principalmente, pelo uso de *pen-drives*.

Há diferentes tipos de vírus. Alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas. Alguns dos tipos de vírus mais comuns são:

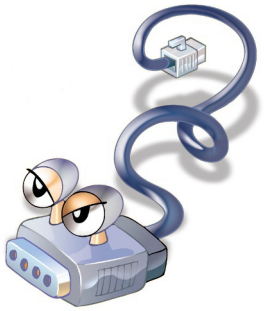
Vírus propagado por *e-mail*: recebido como um arquivo anexo a um *e-mail* cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os *e-mails* encontrados nas listas de contatos gravadas no computador.

Vírus de *script*: escrito em linguagem de *script*, como *VBScript* e *JavaScript*, e recebido ao acessar uma página *Web* ou por *e-mail*, como um arquivo anexo ou como parte do próprio *e-mail* escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador *Web* e do programa leitor de *e-mails* do usuário.

Vírus de macro: tipo específico de vírus de *script*, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros).

Vírus de telefone celular: vírus que se propaga de celular para celular por meio da tecnologia *bluetooth* ou de mensagens MMS (***M**ultimedia **M**essage **S**ervice*). A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria, além de tentar se propagar para outros celulares.

4.2 *Worm*



Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o *worm* não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.

O processo de propagação e infecção dos *worms* ocorre da seguinte maneira:

a. **Identificação dos computadores alvos:** após infectar um computador, o *worm* tenta se propagar e continuar o processo de infecção. Para isto, necessita identificar os computadores alvos para os quais tentará se copiar, o que pode ser feito de uma ou mais das seguintes maneiras:

   - efetuar varredura na rede e identificar computadores ativos;
   - aguardar que outros computadores contatem o computador infectado;
   - utilizar listas, predefinidas ou obtidas na Internet, contendo a identificação dos alvos;
   - utilizar informações contidas no computador infectado, como arquivos de configuração e listas de endereços de *e-mail*.

b. **Envio das cópias:** após identificar os alvos, o *worm* efetua cópias de si mesmo e tenta enviá-las para estes computadores, por uma ou mais das seguintes formas:

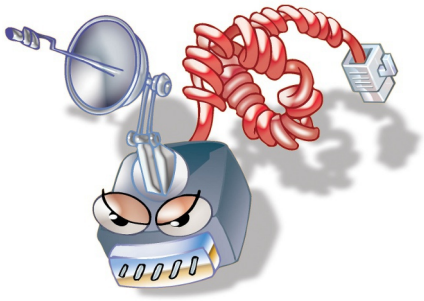
   - como parte da exploração de vulnerabilidades existentes em programas instalados no computador alvo;
   - anexadas a *e-mails*;
   - via canais de IRC (***I**nternet **R**elay **C**hat*);
   - via programas de troca de mensagens instantâneas;
   - incluídas em pastas compartilhadas em redes locais ou do tipo P2P (*Peer to Peer*).

c. **Ativação das cópias:** após realizado o envio da cópia, o *worm* necessita ser executado para que a infecção ocorra, o que pode acontecer de uma ou mais das seguintes maneiras:

   - imediatamente após ter sido transmitido, pela exploração de vulnerabilidades em programas sendo executados no computador alvo no momento do recebimento da cópia;
   - diretamente pelo usuário, pela execução de uma das cópias enviadas ao seu computador;
   - pela realização de uma ação específica do usuário, a qual o *worm* está condicionado como, por exemplo, a inserção de uma mídia removível.

d. **Reinício do processo:** após o alvo ser infectado, o processo de propagação e infecção recomeça, sendo que, a partir de agora, o computador que antes era o alvo passa a ser também o computador originador dos ataques.

4.3 *Bot* e *botnet*

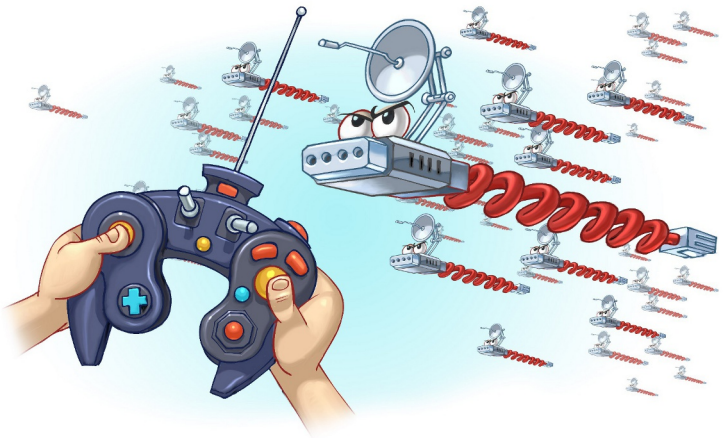


Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do *worm*, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

A comunicação entre o invasor e o computador infectado pelo *bot* pode ocorrer via canais de IRC, servidores *Web* e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar *spam*.

Um computador infectado por um *bot* costuma ser chamado de zumbi (*zombie computer*), pois pode ser controlado remotamente, sem o conhecimento do seu dono. Também pode ser chamado de *spam zombie* quando o *bot* instalado o transforma em um servidor de *e-mails* e o utiliza para o envio de *spam*.

Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos *bots*.



Quanto mais zumbis participarem da *botnet* mais potente ela será. O atacante que a controlar, além de usá-la para seus próprios ataques, também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada.

Algumas das ações maliciosas que costumam ser executadas por intermédio de *botnets* são: ataques de negação de serviço, propagação de códigos maliciosos (inclusive do próprio *bot*), coleta de informações de um grande número de computadores, envio de *spam* e camuflagem da identidade do atacante (com o uso de *proxies* instalados nos zumbis).

O esquema simplificado apresentado a seguir exemplifica o funcionamento básico de uma *botnet*:

a. Um atacante propaga um tipo específico de *bot* na esperança de infectar e conseguir a maior quantidade possível de zumbis;

b. os zumbis ficam então à disposição do atacante, agora seu controlador, à espera dos comandos a serem executados;

c. quando o controlador deseja que uma ação seja realizada, ele envia aos zumbis os comandos a serem executados, usando, por exemplo, redes do tipo P2P ou servidores centralizados;

d. os zumbis executam então os comandos recebidos, durante o período predeterminado pelo controlador;

e. quando a ação se encerra, os zumbis voltam a ficar à espera dos próximos comandos a serem executados.

4.4 *Spyware*

Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

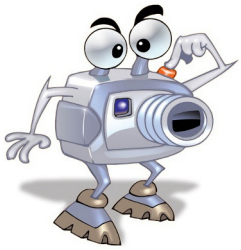
Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas. Pode ser considerado de uso:

Legítimo: quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.

Malicioso: quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Alguns tipos específicos de programas *spyware* são:

***Keylogger*:** capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um *site* específico de comércio eletrônico ou de *Internet Banking*.



***Screenlogger*:** similar ao *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou a região que circunda a posição onde o *mouse* é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em *sites* de *Internet Banking*.

***Adware*:** projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.

4.5 *Backdoor*

Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

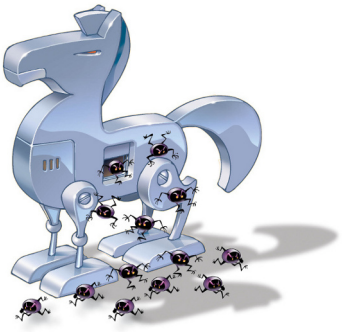
Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo.

Após incluído, o *backdoor* é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.

A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou na substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto. Programas de administração remota, como BackOrifice, NetBus, SubSeven, VNC e Radmin, se mal configurados ou utilizados sem o consentimento do usuário, também podem ser classificados como *backdoors*.

Há casos de *backdoors* incluídos propositalmente por fabricantes de programas, sob alegação de necessidades administrativas. Esses casos constituem uma séria ameaça à segurança de um computador que contenha um destes programas instalados pois, além de comprometerem a privacidade do usuário, também podem ser usados por invasores para acessarem remotamente o computador.

4.6 Cavalo de troia (*Trojan*)



Cavalo de troia[1], *trojan* ou *trojan-horse*, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Exemplos de *trojans* são programas que você recebe ou obtém de *sites* na Internet e que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

Trojans também podem ser instalados por atacantes que, após invadirem um computador, alteram programas já existentes para que, além de continuarem a desempenhar as funções originais, também executem ações maliciosas.

Há diferentes tipos de *trojans*, classificados[2] de acordo com as ações maliciosas que costumam executar ao infectar um computador. Alguns destes tipos são:

[1] O "Cavalo de Troia", segundo a mitologia grega, foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso à cidade de Troia. A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Troia.

[2] Esta classificação baseia-se em coletânea feita sobre os nomes mais comumente usados pelos programas *antimalware*.

***Trojan Downloader*:** instala outros códigos maliciosos, obtidos de *sites* na Internet.

***Trojan Dropper*:** instala outros códigos maliciosos, embutidos no próprio código do *trojan*.

***Trojan Backdoor*:** inclui *backdoors*, possibilitando o acesso remoto do atacante ao computador.

***Trojan DoS*:** instala ferramentas de negação de serviço e as utiliza para desferir ataques.

***Trojan* Destrutivo:** altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.

***Trojan Clicker*:** redireciona a navegação do usuário para *sites* específicos, com o objetivo de aumentar a quantidade de acessos a estes *sites* ou apresentar propagandas.

***Trojan Proxy*:** instala um servidor de *proxy*, possibilitando que o computador seja utilizado para navegação anônima e para envio de *spam*.

***Trojan Spy*:** instala programas *spyware* e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.

***Trojan Banker* ou Bancos:** coleta dados bancários do usuário, através da instalação de programas *spyware* que são ativados quando *sites* de *Internet Banking* são acessados. É similar ao *Trojan Spy* porém com objetivos mais específicos.

4.7 *Rootkit*

Rootkit[3] é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

O conjunto de programas e técnicas fornecido pelos *rootkits* pode ser usado para:

- remover evidências em arquivos de *logs* (mais detalhes na Seção 7.6 do Capítulo Mecanismos de segurança);
- instalar outros códigos maliciosos, como *backdoors*, para assegurar o acesso futuro ao computador infectado;
- esconder atividades e informações, como arquivos, diretórios, processos, chaves de registro, conexões de rede, etc;
- mapear potenciais vulnerabilidades em outros computadores, por meio de varreduras na rede;
- capturar informações da rede onde o computador comprometido está localizado, pela interceptação de tráfego.

[3] O termo *rootkit* origina-se da junção das palavras "*root*" (que corresponde à conta de superusuário ou administrador do computador em sistemas Unix) e "*kit*" (que corresponde ao conjunto de programas usados para manter os privilégios de acesso desta conta).

É muito importante ressaltar que o nome *rootkit* não indica que os programas e as técnicas que o compõe são usadas para obter acesso privilegiado a um computador, mas sim para mantê-lo.

Rootkits inicialmente eram usados por atacantes que, após invadirem um computador, os instalavam para manter o acesso privilegiado, sem precisar recorrer novamente aos métodos utilizados na invasão, e para esconder suas atividades do responsável e/ou dos usuários do computador. Apesar de ainda serem bastante usados por atacantes, os *rootkits* atualmente têm sido também utilizados e incorporados por outros códigos maliciosos para ficarem ocultos e não serem detectados pelo usuário e nem por mecanismos de proteção.

Há casos de *rootkits* instalados propositalmente por empresas distribuidoras de CDs de música, sob a alegação de necessidade de proteção aos direitos autorais de suas obras. A instalação nestes casos costumava ocorrer de forma automática, no momento em que um dos CDs distribuídos contendo o código malicioso era inserido e executado. É importante ressaltar que estes casos constituem uma séria ameaça à segurança do computador, pois os *rootkits* instalados, além de comprometerem a privacidade do usuário, também podem ser reconfigurados e utilizados para esconder a presença e os arquivos inseridos por atacantes ou por outros códigos maliciosos.

4.8 Prevenção

Para manter o seu computador livre da ação dos códigos maliciosos existe um conjunto de medidas preventivas que você precisa adotar. Essas medidas incluem manter os programas instalados com as versões mais recentes e com todas as atualizações disponíveis aplicadas e usar mecanismos de segurança, como *antimalware* e *firewall* pessoal.

Além disso, há alguns cuidados que você e todos que usam o seu computador devem tomar sempre que forem manipular arquivos. Novos códigos maliciosos podem surgir, a velocidades nem sempre acompanhadas pela capacidade de atualização dos mecanismos de segurança.

Informações sobre os principais mecanismos de segurança que você deve utilizar são apresentados no Capítulo Mecanismos de segurança. Outros cuidados que você deve tomar para manter seu computador seguro são apresentados no Capítulo Segurança de computadores.

4.9 Resumo comparativo

Cada tipo de código malicioso possui características próprias que o define e o diferencia dos demais tipos, como forma de obtenção, forma de instalação, meios usados para propagação e ações maliciosas mais comuns executadas nos computadores infectados. Para facilitar a classificação e a conceituação, a Tabela 4.1 apresenta um resumo comparativo das características de cada tipo.

É importante ressaltar, entretanto, que definir e identificar essas características têm se tornado tarefas cada vez mais difíceis, devido às diferentes classificações existentes e ao surgimento de variantes que mesclam características dos demais códigos. Desta forma, o resumo apresentado na tabela não é definitivo e baseia-se nas definições apresentadas nesta Cartilha.

Códigos Maliciosos							
	Vírus	***Worm***	***Bot***	***Trojan***	***Spyware***	***Backdoor***	***Rootkit***
Como é obtido:							
Recebido automaticamente pela rede		✔	✔				
Recebido por *e-mail*	✔	✔	✔	✔	✔		
Baixado de *sites* na Internet	✔	✔	✔	✔	✔		
Compartilhamento de arquivos	✔	✔	✔	✔	✔		
Uso de mídias removíveis infectadas	✔	✔	✔	✔	✔		
Redes sociais	✔	✔	✔	✔	✔		
Mensagens instantâneas	✔	✔	✔	✔	✔		
Inserido por um invasor		✔	✔	✔	✔	✔	✔
Ação de outro código malicioso		✔	✔	✔	✔	✔	✔
Como ocorre a instalação:							
Execução de um arquivo infectado	✔						
Execução explícita do código malicioso		✔	✔	✔	✔		
Via execução de outro código malicioso						✔	✔
Exploração de vulnerabilidades		✔	✔			✔	✔
Como se propaga:							
Insere cópia de si próprio em arquivos	✔						
Envia cópia de si próprio automaticamente pela rede		✔	✔				
Envia cópia de si próprio automaticamente por *e-mail*		✔	✔				
Não se propaga				✔	✔	✔	✔
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✔			✔			✔
Consome grande quantidade de recursos		✔	✔				
Furta informações sensíveis			✔	✔	✔		
Instala outros códigos maliciosos		✔	✔	✔			✔
Possibilita o retorno do invasor						✔	✔
Envia *spam* e *phishing*			✔				
Desfere ataques na Internet		✔	✔				
Procura se manter escondido	✔				✔	✔	✔

Tabela 4.1: Resumo comparativo entre os códigos maliciosos.

5. *Spam*

Spam[1] é o termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é referenciado como UCE (***U**nsolicited **C**ommercial **E**-mail*).

O *spam* em alguns pontos se assemelha a outras formas de propaganda, como a carta colocada na caixa de correio, o panfleto recebido na esquina e a ligação telefônica ofertando produtos. Porém, o que o difere é justamente o que o torna tão atraente e motivante para quem o envia (*spammer*): ao passo que nas demais formas o remetente precisa fazer algum tipo de investimento, o *spammer* necessita investir muito pouco, ou até mesmo nada, para alcançar os mesmos objetivos e em uma escala muito maior.

Desde o primeiro *spam* registrado e batizado como tal, em 1994, essa prática tem evoluído, acompanhando o desenvolvimento da Internet e de novas aplicações e tecnologias. Atualmente, o envio de *spam* é uma prática que causa preocupação, tanto pelo aumento desenfreado do volume de mensagens na rede, como pela natureza e pelos objetivos destas mensagens.

[1] Para mais detalhes acesse o *site* Antispam.br, http://www.antispam.br/, mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), que constitui uma fonte de referência sobre o *spam* e tem o compromisso de informar usuários e administradores de redes sobre as implicações destas mensagens e as formas de proteção e de combate existentes.

Spams estão diretamente associados a ataques à segurança da Internet e do usuário, sendo um dos grandes responsáveis pela propagação de códigos maliciosos, disseminação de golpes e venda ilegal de produtos.

Algumas das formas como você pode ser afetado pelos problemas causados pelos *spams* são:

Perda de mensagens importantes: devido ao grande volume de *spam* recebido, você corre o risco de não ler mensagens importantes, lê-las com atraso ou apagá-las por engano.

Conteúdo impróprio ou ofensivo: como grande parte dos *spams* são enviados para conjuntos aleatórios de endereços de *e-mail*, é bastante provável que você receba mensagens cujo conteúdo considere impróprio ou ofensivo.

Gasto desnecessário de tempo: para cada *spam* recebido, é necessário que você gaste um tempo para lê-lo, identificá-lo e removê-lo da sua caixa postal, o que pode resultar em gasto desnecessário de tempo e em perda de produtividade.

Não recebimento de *e-mails*: caso o número de *spams* recebidos seja grande e você utilize um serviço de *e-mail* que limite o tamanho de caixa postal, você corre o risco de lotar a sua área de *e-mail* e, até que consiga liberar espaço, ficará impedido de receber novas mensagens.

Classificação errada de mensagens: caso utilize sistemas de filtragem com regras *antispam* ineficientes, você corre o risco de ter mensagens legítimas classificadas como *spam* e que, de acordo com as suas configurações, podem ser apagadas, movidas para quarentena ou redirecionadas para outras pastas de *e-mail*.

Independente do tipo de acesso à Internet usado, é o destinatário do *spam* quem paga pelo envio da mensagem. Os provedores, para tentar minimizar os problemas, provisionam mais recursos computacionais e os custos derivados acabam sendo transferidos e incorporados ao valor mensal que os usuários pagam.

Alguns dos problemas relacionados a *spam* que provedores e empresas costumam enfrentar são:

Impacto na banda: o volume de tráfego gerado pelos *spams* faz com que seja necessário aumentar a capacidade dos *links* de conexão com a Internet.

Má utilização dos servidores: boa parte dos recursos dos servidores de *e-mail*, como tempo de processamento e espaço em disco, são consumidos no tratamento de mensagens não solicitadas.

Inclusão em listas de bloqueio: um provedor que tenha usuários envolvidos em casos de envio de *spam* pode ter a rede incluída em listas de bloqueio, o que pode prejudicar o envio de *e-mails* por parte dos demais usuários e resultar em perda de clientes.

Investimento extra em recursos: os problemas gerados pelos *spams* fazem com que seja necessário aumentar os investimentos, para a aquisição de equipamentos e sistemas de filtragem e para a contratação de mais técnicos especializados na sua operação.