Segurança em Redes

Aula 11 - Spams

Apresentação

Nesta aula, você vai estudar mais sobre um dos maiores problemas que afetam os usuários de vários meios de comunicação eletrônica (e-mail, SMS etc.) e que podem gerar vários problemas de segurança: o spam.

Vídeo 01 - Apresentação

Objetivos

Ao final desta aula, você será capaz de:

- Saber o que é spam.
- Caracterizar spams.
- Conhecer os tipos e formas de envio de spam.
- Saber como se prevenir contra spams.
- Aprender onde denunciar spams.

Conceito de Spam

O termo spam, também conhecido como mensagem eletrônica não solicitada, é um problema importante em comunicações eletrônicas nos dias atuais. A mensagem é chamada de spam, seus autores são conhecidos como *spammers*, e o processo é chamado de *spamming*.

Há controvérsias quanto à origem do termo spam. Uma das versões mais populares sobre a origem afirma que vem de uma marca de carne suína enlatada, chamada SPAM, conforme ilustra a Figura 1. Há versões que relacionam o termo a acrônimos: (i) spam (*Sending and Posting Adverstisement in Mass* – enviar e postar publicidade em massa); (ii) spam (*Single Post to All Messageboards* – mensagem única para todos os fóruns de discussão) [Fonte: Wikipédia].

Figura 01 - Marca de carne suína.

Fonte: Wikipédia.

O primeiro spam foi registrado em 1994 [Fonte: Cert.br] e vem evoluindo com o desenvolvimento da internet e de outras mídias, como a telefonia celular.

Estamos estudando spams neste curso porque eles estão muito relacionados a ataques à segurança da internet e do usuário, uma vez que são responsáveis pela propagação de vírus, códigos maliciosos, disseminação de golpes e venda ilegal de produtos.

Esta aula tem como objetivo discutir mais esse assunto, caracterizando os spams, mostrando os tipos, os meios de envio e as maneiras de se prevenir contra eles.

Características dos Spams

É importante se conhecer as principais características dos spams para saber como evitá-los. As principais características são:

1. **Cabeçalhos suspeitos:** desconfie se receber um e-mail com cabeçalho incompleto, sem remetente ou destinatário, ou com remetente com nomes genéricos como: suporte@, segurança@, etc.

2. Campo **Assunto (***Subject***) suspeito ou com nomes atraentes**: em geral, os filtros antispam barram e-mails com assuntos considerados suspeitos, no entanto, os *spammers* estão cada vez mais criativos para tentar enganar os filtros. Desconfie se você encontrar e-mails com textos atraentes como: "Você recebeu um prêmio", "Parabéns", "Ganhe um brinde", "Sua senha está inválida".

3. **Correntes e boatos**: e-mails contendo textos com histórias assustadoras, pedindo ajuda financeira, descrevendo uma corrente dizendo que você não pode quebrar senão acontecerá uma tragédia, mandando você repassar a "todos que você ama".

4. **Golpes e fraudes:** *spammers* gostam de enviar e-mails com promoções e passando-se por instituições financeiras ou governamentais, pedindo para você atualizar os seus dados bancários.

5. Com opção para **remover** seu e-mail de uma lista de divulgação: muitas vezes em um e-mail que é spam, colocam no seu conteúdo uma opção para o usuário clicar em um link para remover o seu e-mail da lista de divulgação. Isso é apenas um artifício para ter certeza que alguém está lendo o e-mail. Nunca clique em um link enviado por e-mail suspeito. Para

diferenciar se é spam ou não, o usuário deve certificar-se que fez o cadastro na lista em questão.

Vídeo 02 - O Que é Spam?

Curiosidade

Você sabia que o Comitê Gestor de Internet no Brasil (CGI.br) lançou recentemente, o site http://www.antispam.br/ com informações sobre os spams? A página criada por especialistas do CGI.br tem como objetivo educar os usuários e administradores de redes em relação ao assunto.

Atividade 01

1. O que você deve fazer se receber um e-mail com o cabeçalho: "Você ganhou 10 mil reais" e no conteúdo do e-mail vier um link para você clicar e enviar seus dados bancários?

2. Qual a relação entre spams e segurança?

Meios de Envio de Spams

Atualmente, os spams não são enviados apenas para os e-mails. Eles estão sendo disseminados via várias outras mídias que veremos nesta seção.

1. **E-mail** é o meio mais comum de propagação de spams que, tipicamente, são enviados para uma vasta lista de destinatários. Para coletar endereços de e-mail, os *spammers* recorrem a diversos artifícios como: (i) compra de banco de dados com lista de e-mails; (ii) coleta de endereços de e-mail através de varredura de páginas web, técnica que é chamada de

harvesting; (iii) códigos maliciosos que varrem computadores infectados buscando endereços de e-mail.

2. **Programas de mensagens instantâneas:** apesar de não ser tão comum como via e-mail, os programas de mensagens instantâneas, como MSN, Google talk etc., têm sido vítimas dos spams. Como não são bloqueados por filtros, há uma maior facilidade de atingir o alvo. Para evitar isso, a dica é permitir que se receba mensagens apenas de pessoas que estão na lista de contatos.

3. **Celulares:** tem acontecido muito o envio de spams através de torpedos, ou seja, de troca de mensagens SMS.

4. **Páginas de compartilhamento de vídeos:** os spams também estão atingindo páginas de compartilhamento de vídeos, como o YouTube. Em geral, aparecem links nessas páginas para outras páginas com conteúdo pornográfico ou com propagandas de algum produto.

Tipos de Spams

1. **Vírus,** ***worms*** **e cavalos de troia**, que já estudamos anteriormente neste curso, comumente se propagam via spams.

2. **Boatos (***hoaxes***):** e-mails contando histórias inverídicas ou algum apelo dramático, por exemplo, e-mails relatando que foi encontrada uma barata em um refrigerante.

3. **Propagandas:** são o tipo mais comum de spam. Seu conteúdo contém a oferta de produtos como medicamentos, relógios rolex, viagra, etc.

4. **Correntes:** são tipos de spams que incentivam o leitor a enviá-los para seus amigos, por exemplo, citando histórias de crianças doentes.

5. **Golpes:** consiste no envio de e-mails em nome de instituições conhecidas, bancos etc., solicitando algum recadastramento ou oferecendo algum benefício falso. Em geral, o e-mail vem com a solicitação de preenchimento de um formulário ou então com um link de uma página web parecida com a página original da instituição. Cuidado, em geral o golpe é bem feito, preste atenção nas imagens e nos textos para tentar identificar se é spam ou não. Bancos nunca enviam e-mail pedindo dados pessoas nem senhas de usuários. Nunca forneça sua senha via internet! Um tipo de golpe muito conhecido são mensagens cujo remetente se diz um nigeriano que deseja

transferir um dinheiro para o destinatário, caso este pague uma quantia como garantia. Esse spam é conhecido como "419" devido ao número do código criminal nigeriano ao qual o caso se aplica, descrito em http://home.rica.net/alphae/419coal/.

6. **Programas maliciosos:** são e-mails que induzem o usuário a executar um arquivo em anexo que, na verdade, é um programa executável malicioso. Por exemplo, desconfie se você recebe um e-mail de um desconhecido dizendo: "segue uma foto sua muito comprometedora" e indica um arquivo .jpg, que na verdade é um programa malicioso que vai ser executado em seu computador e pode realizar ações catastróficas, como apagar todos os seus arquivos. Portanto, nunca clique em anexos que vem de alguém que você não conhece.

Vídeo 03 - Tipos de Spam e Meios de Envio

Atividade 02

1. Por que há uma maior facilidade dos spams afetarem programas de mensagens instantâneas?
2. Quando você recebe um e-mail de uma instituição pedindo os dados da sua conta bancária, o que você deve fazer?

Problemas Causados por Spams

Empresas e provedores têm tido vários problemas causados pela proliferação de spams. O tráfego de rede gerado por essas mensagens é muito alto e em geral as empresas precisam aumentar a capacidade dos seus links de conexão com a internet para sua rede não ficar muito lenta.

Além disso, as empresas comumente precisam investir em potentes equipamentos para hospedar o servidor de e-mail, uma vez que parte do processamento e espaço em disco do servidor de e-mails é dedicado ao tratamento de spams.

Curiosidade!

Você sabia que se um provedor tem usuários que são *spammers*, ele pode ser incluído em listas de bloqueios e os demais usuários não conseguem enviar e-mails para vários destinos?

Cuidados para Diminuir a Quantidade de Spams

Evitar spams tem sido bastante difícil, mas é comum os sistemas de e-mails terem mecanismos de filtragem que ajudam bastante a diminuir a quantidade de spams na caixa de entrada do e-mail do usuário. O próprio usuário tem de tomar alguns cuidados para diminuir o recebimento de spams, tais como:

1. Cuidado ao fornecer seu e-mail, selecione as pessoas e empresas para os quais você informa seu e-mail. Atualmente, vários formulários de lojas solicitam cadastro do usuário e pedem e-mail. Pense antes se você realmente quer receber e-mail da empresa.
2. Não clique em links recebidos em e-mails e não responda mensagens que você desconfia serem spams.
3. Ao usar redes sociais, como Facebook, Orkut etc., use as opções de privacidade, restringindo as pessoas que terão acesso ao seu perfil, incluindo seu e-mail.
4. Desabilite a abertura de imagens em e-mails HTML (o fato de uma imagem ser acessada pode servir para confirmar que a mensagem foi lida).
5. Não exponha outras pessoas em e-mails que você envia, para evitar que elas sejam vítimas de spams. Se for encaminhar uma mensagem a várias pessoas, use a opção "Bcc".

Vídeo 04 - Consultando a Blacklist

Curiosidade!

Você sabia que alguns sites publicam **Listas Negras** que contêm a lista de endereços IP que são conhecidos como servidores *spammers*?

Suporte de Webmails para Evitar Spam

Webmails em geral adotam políticas e mecanismos para proteger os seus usuários contra spams. Alguns usam filtros que associam uma lista de remetentes autorizados pelo usuário para lhe enviar e-mail. Toda vez que o usuário recebe um e-mail de alguém desconhecido o sistema pergunta se o remetente é autorizado ou não e inclui tal remetente na lista, se o usuário autorizar.

Vários webmails também adotam filtros que colocam mensagens suspeitas em uma pastam chamada *spams*. O usuário deve verificar essa pasta constantemente para ver se mensagens normais foram classificadas equivocadamente como spams. Ao mesmo tempo, o usuário deve observar se recebe spam que não cai nessa pasta, e deve classificá-lo para que o filtro conheçam os novos spams.

Denuncie um Spam

Não deixe de denunciar spam! Isso pode ser feito no site Antispam (http://antispam.br/) do Comitê Gestor da Internet no Brasil (CGI.br). Para isso, encaminhe o e-mail para: mailto:mail-abuse@cert.br.

Curiosidade

Segundo o site http://www.antispam.br, circulam pela Internet mensagens em nome do antispam.br apontando para um link de um falso sistema removedor de vírus e spam. O antispam.br não envia mensagens e não possui nenhum sistema antispam para download.

Dica!

Não escreva o seu endereço abertamente em páginas web para evitar que eles sejam encontrados por programas de garimpo de endereços de e-mails feito por *spammers*. É usual colocar *at* ao invés de @ no endereço de e-mail, pois como o *at* é usado em diferentes contextos além desse do e-mail, os programas de garimpo de endereços de e-mails não usam o *at* na busca

Resumo

Nesta aula, você estudou sobre spam. Aprendeu que spams podem gerar vários problemas de segurança, pois podem conter vírus e outros programas maliciosos. Também aprendeu que deve se prevenir, selecionando onde expor seu e-mail, evitando colocá-lo em questionários quaisquer. Também aprendeu que os webmails mantêm filtros para evitar que os spams sejam colocados na caixa de entrada do usuário e que spams estão sendo enviados não somente através de e-mails, mas também de outros meios de comunicação eletrônica. Você viu também que nunca se deve informar sua senha por e-mail e nunca preencher formulários enviados através de e-mails cujo remetente você não tenha total certeza de que é alguém ou alguma instituição confiável. Bancos nunca enviam e-mails pedindo seus dados! Você ficou sabendo que no Brasil há uma entidade, o Comitê Gestor da Internet no Brasil (CGI.br), que está sempre alerta aos spams que são veiculados pela internet.

Autoavaliação

1. Quais os principais tipos de spams?

2. O que é *harvesting*?

3. Nas alternativas a seguir, assinale V para verdadeiro e F para falso.

   ( ) Webmails não adotam políticas contra spam, isso é responsabilidade exclusiva do usuário.
   ( ) Spams podem ser denunciados no site Antispam do CGI.br.
   ( ) Uma das formas de evitar spam é usar as opções de privacidade das redes sociais.
   ( ) O único meio de envio de spams é o e-mail.

Referências

COLLAVIZA, Alberto; MENEGAT, Wagner; ENNES, Michel. **Spam.** Disponível em: <http://www.gta.ufrj.br/grad/09_1/versao-final/spam/index.html>. Acesso em: 03 set. 2012.

JACKSON, Todd. **How our spam filter works** - Gmail Blog. Disponível em: <http://gmailblog.blogspot.com/2007/10/how-our-spam-filter-works.html>. Acesso em: 03 set. 2012.

WIKIPEDIA. **Anti-spam Techniques.** Disponível em: <http://en.wikipedia.org/wiki/Anti-spam_techniques_(e-mail)>. 03 set. 2012.