POLÍTICA ANTI-SPAM

Web & Marketing Digital

O QUE É SPAM?

Spam é o termo usado para referir-se aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês*Unsolicited Commercial E-mail*).

O SPAM não pode ser considerado E-mail marketing ou Newsletter porque não faz uso correto e/ou ético da publicidade online. As mensagens SPAM, freqüentemente, apresentam as seguintes características:

- Não possuem Remetente identificável ou sua identidade é falsa;
- Sua base de dados não é composta por usuários opt-in (aceite do recebimento da mensagem por parte do usuário);
- Não apresentam opção para opt-out (remoção do endereço do usuário da lista);
- Apresentam uma abordagem enganosa do Assunto da mensagem.

O QUE SÃO SPAM ZOMBIES?

Spam *zombies* são computadores de usuários finais que foram comprometidos por códigos maliciosos em geral, como*worms*, *bots*, vírus e cavalos de tróia. Estes códigos maliciosos, uma vez instalados, permitem que *spammers* utilizem a máquina para o envio de spam, sem o conhecimento do usuário. Enquanto utilizam máquinas comprometidas para executar suas atividades, dificultam a identificação da origem do spam e dos autores também. Os spam *zombies* são muito explorados pelos *spammers*, por proporcionar o anonimato que tanto os protege.

PROBLEMAS CAUSADOS PELO SPAM

O spam pode afetar os usuários do serviço de correio eletrônico de diversas formas. Alguns exemplos a seguir mostram como a produtividade, a segurança, entre outros, podem ser ameaçadas.

NÃO RECEBIMENTO DE E-MAILS: Boa parte dos provedores de Internet limita o tamanho da caixa postal do usuário no seu servidor. Caso o número de spams recebidos seja grande, ele corre o risco de ter sua caixa postal lotada com mensagens não solicitadas. Se isto ocorrer, passará a não receber e-mails e, até que possa liberar espaço em sua caixa postal, todas as mensagens recebidas serão devolvidas ao remetente. Outro problema é quando o usuário deixa de receber e-mails nos casos em que regras anti-spam ineficientes são utilizadas, por exemplo, classificando como spam mensagens legítimas.

GASTO DESNECESSÁRIO DE TEMPO: Para cada spam recebido, o usuário necessita gastar um determinado tempo para ler, identificar o e-mail como spam e removê-lo da caixa postal.

AUMENTO DE CUSTOS: Independente do tipo de acesso à Internet utilizado, quem paga a conta pelo envio do spam é quem o recebe. Por exemplo, para um usuário que utiliza acesso discado à Internet, cada spam representa alguns segundos a mais de ligação que ele estará pagando.

PERDA DE PRODUTIVIDADE: Para quem usa o e-mail como ferramenta de trabalho, o recebimento de spams aumenta o tempo dedicado à tarefa de leitura de e-mails, além de existir a chance de mensagens importantes não serem lidas, serem apagadas por engano ou lidas com atraso.

CONTEÚDO IMPRÓPRIO OU OFENSIVO: Como a maior parte dos spams é enviada para conjuntos aleatórios de endereços de e-mail, é bem provável que o usuário receba mensagens com conteúdo que julgue impróprio ou ofensivo.

PREJUÍZOS FINANCEIROS CAUSADOS POR FRAUDE: O spam tem sido amplamente utilizado como veículo para disseminar esquemas fraudulentos, que tentam induzir o usuário a acessar páginas clonadas de instituições financeiras ou a instalar programas maliciosos, projetados para furtar dados pessoais e financeiros. Esse tipo de spam é conhecido como *phishing/scam*. O usuário pode sofrer grandes prejuízos financeiros, caso forneça as informações ou execute as instruções solicitadas nesse tipo de mensagem fraudulenta.

COMO IDENTIFICAR

É muito importante conhecer as principais características dos spams, freqüentemente encontrados na Internet. Dessa forma, o usuário não será pego de surpresa e facilitará a detecção dessa prática indesejável em sua caixa postal.

Vale ressaltar que nem todas essas características estarão presentes ao mesmo tempo, em um mesmo spam. Da mesma forma, poderão existir spams que não atendam às propriedades citadas, podendo, eventualmente, ser um novo tipo.

PRINCIPAIS CARACTERÍSTICAS DOS SPAMS:

CABEÇALHOS SUSPEITOS
O cabeçalho do e-mail aparece incompleto, sem o remetente ou o destinatário. Ambos podem aparecer como apelidos ou nomes genéricos, tais como: amigo@, suporte@ etc. A omissão do destinatário é um dos casos mais comuns, pois, os spammers colocam listas enormes de e-mails no campo reservado para Cópias Carbono Ocultas ou Blind carbon copies (Cco: ou Bcc:), já que tais campos não são mostrados ao usuário que recebe a mensagem.
Campo Assunto (Subject) suspeito
O campo reservado para o assunto do e-mail (subject) é uma armadilha para os usuários e um artifício poderoso para os spammers. A maioria dos filtros anti-spam está preparada para barrar e-mails com diversos assuntos considerados suspeitos. No entanto, os spammers adaptam-se e tentam enganar os filtros colocando no campo assunto conteúdos enganosos, tais como: vi@gra (em vez de viagra) etc. Como os spammers utilizam esses subterfúgios, alguns e-mails suspeitos podem não ser identificados e, nesse momento, os usuários devem estar atentos para não abrir e-mails de spam, executar arquivos em anexo e ter sua máquina contaminada por um código malicioso.

Ainda em relação ao campo assunto, os spammers costumam colocar textos atraentes e/ou vagos demais, confundindo os filtros e os usuários, que abrem os e-mails acreditando ser informação importante. São exemplos desse fato: "Sua senha está inválida", "A informação que você pediu" e "Parabéns". Vale observar que alguns conteúdos suspeitos no campo assunto também são decorrentes de propagação de vírus ou worms e, portanto, devem ser removidos.

As referências "ADV" (ADVertisement, do inglês, propaganda), "MEEPS" (Mensagem Eletrônica de Publicidade de Produtos e Serviços) ou "NS" (Não Solicitado) não são aceitas como justificativas para o envio de e-mails não solicitados. Dessa forma, os e-mails com essa notificação no campo assunto são considerados spam.

OPÇÕES PARA SAIR DA LISTA DE DIVULGAÇÃO

Existem spams que tentam justificar o abuso, alegando que é possível sair da lista de divulgação, "clicando" no endereço anexo ao e-mail. O usuário deve verificar se fez realmente o cadastro na lista em questão. Se não tiver certeza, melhor ignorar o e-mail, afinal, um dos artifícios usados pelos spammers para validar a existência dos endereços de e-mail é justamente solicitar a confirmação. Também é importante jamais clicar em um link enviado por e-mail. Sempre digite a URL no navegador.

E-MAILS ENVIADOS "UMA ÚNICA VEZ"

Embora seja um dos recursos mais antigos, entre aqueles utilizados pelos spammers, ainda são encontrados e-mails de spam alegando que serão enviados "uma única vez". Essa é uma característica de e-mail de spam.

SUGESTÃO PARA APENAS REMOVER

Uma das mais freqüentes, e piores, desculpas usadas pelos spammers é alegar que se o usuário não tem interesse no e-mail não solicitado, basta "removê-lo". Essa é uma característica de e-mail de spam.

LEIS E REGULAMENTAÇÕES

Não existem regulamentações brasileiras referentes à prática de spam. Portanto, citações que envolvam leis e regulamentações são características de e-mail de spam.

CORRENTES, BOATOS E LENDAS URBANAS

São características de spam os e-mails contendo: textos pedindo ajuda financeira, contando histórias assustadoras, pedindo para que sejam enviados "a todos que você ama" ou, ainda, ameaçando que algo acontecerá caso não seja repassado a um determinado número de pessoas.

GOLPES E FRAUDES

Com certa freqüência, os e-mails de spam são portadores de fraudes e golpes disseminados na rede. Alguns exemplos são: e-mails de promoções e e-mails de instituições financeiras ou governamentais. Nesses casos, a melhor defesa é a informação. Conhecer os tipos de golpes e como eles podem chegar até a sua caixa postal é a melhor estratégia de defesa.

COMO REDUZIR O VOLUME DE SPAM

A resposta simples é navegar consciente na rede. Este conselho é o mesmo que recebemos para zelar pela nossa segurança no trânsito ou ao entrar e sair de nossas casas. As dicas para reduzir o volume de spam estão diretamente relacionadas aos cuidados recomendados aos usuários da Internet, para que desfrutem de todos os recursos e benefícios da rede, com segurança.

PRINCIPAIS DICAS:

- Preservar as informações pessoais como endereços de e-mail, dados pessoais e, principalmente, cadastrais de bancos, cartões de crédito e senhas. Um bom exercício é pensar que ninguém forneceria dados pessoais a um estranho na rua, certo? Então, por que o faria na Internet?

- Ter, sempre que possível, e-mails separados para assuntos pessoais, profissionais, para as compras e cadastros on-line. Certos usuários mantêm um e-mail somente para assinatura de listas de discussão.

- Não ser um "clicador compulsivo", ou seja, o usuário deve procurar controlar a curiosidade de verificar sempre a indicação de um site em um e-mail suspeito de spam. Pensar, analisar as características do e-mail e verificar se não é mesmo um golpe ou código malicioso.

- Não ser um "caça-brindes", "papa-liquidações" ou "destruidor-de-promoções". Ao receber e-mails sobre brindes, promoções ou descontos, reserve um tempo para analisar o e-mail, sua procedência e verificar no site da empresa as informações sobre a promoção em questão. Vale lembrar que os sites das empresas e instituições financeiras têm mantido alertas em destaque sobre os golpes envolvendo seus serviços. Assim, a visita ao *site* da empresa pode confirmar a promoção ou alertá-lo sobre o golpe que acabou de receber por e-mail! No caso de promoções, na maioria das vezes, será necessário preencher formulários. Ter um e-mail para cadastros on-line é uma boa prática para os usuários com o perfil descrito. Ao preencher o cadastro, desabilite as opções de recebimento de material de divulgação do *site* e de seus parceiros. É justamente nesse item que muitos usuários atraem spam, inadvertidamente.

- Ter um filtro anti-spam instalado, ou ainda, usar os recursos anti-spam oferecidos pelo seu provedor de acesso.

- Além do anti-spam, existem outras ferramentas bastante importantes para o usuário da rede: *anti-spyware*, firewall pessoal e antivírus.

COMO PRESERVAR OS ENDEREÇOS DE E-MAIL

DICAS PARA PRESERVAR O SEU ENDEREÇO DE E-MAIL:

Cuide de seu(s) e-mail(s) como cuida do endereço de sua casa. Ninguém passa o endereço a qualquer estranho, nem mesmo fornece esses dados sem perguntar sua utilidade. Logo, o seu e-mail deve ser tratado da mesma forma, para que não seja vítima de uma enxurrada cada vez maior de e-mails não solicitados.

Utilize e-mails separados para uso pessoal, trabalho, compras on-line e cadastros em sites em geral. Assim, é possível mantê-los com caráter de "público", enquanto outros são mantidos "restritos" ao trabalho e à família.

Leia com atenção os formulários e cadastros on-line, evitando preencher ou concordar, inadvertidamente, com as opções para recebimento de e-mails de divulgação do site e de seus parceiros.

Verifique a existência da política de privacidade dos sites, espaço para preenchimento de cadastros e formulários. A empresa que mantém o site, ao possuir uma política de privacidade, pode garantir que seus e-mails não serão repassados ou vendidos a terceiros.

Evite utilizar e-mails simples e comuns (João, Maria, compras), pois podem ser facilmente descobertos por ferramentas automáticas ou por ataques de dicionário. O spammer forma endereços de e-mail a partir de listas de nomes de pessoas, de palavras presentes em dicionários e/ou da combinação de caracteres alfanuméricos.

Evite colocar em sites os e-mails no formato comumente utilizado (fulano@dominio.com.br), pois facilita a atuação bem-sucedida de ferramentas automáticas de harvesting (colheita) de e-mails. É recomendado, se necessário, implementar o contato via formulário que não exiba o e-mail ou por meio de imagens.

COMO ESCOLHER UM FILTRO DE ANTI-SPAM ADEQUADO

Existem diversos pontos a serem discutidos na escolha de um filtro anti-spam, adequado às necessidades de um usuário ou ambiente corporativo. A seguir, alguns conselhos importantes que podem auxiliar a tomar uma decisão acertada:

- Liste as funcionalidades esperadas do software de filtragem, como a quarentena, por exemplo.
- Verifique se o seu provedor de acesso possui algum tipo de serviço de filtragem de spams.
- Identifique a política de suporte ao software de filtragem, incluindo os horários de atendimento.
- Se utilizar acessos discados, é importante que o filtro possua mecanismos para filtrar mensagens somente pelo cabeçalho, permitindo a identificação de alguns spams e possibilitando apagá-los antes mesmo de serem transferidos para a máquina pessoal.
- Avalie a interface de configuração e administração do software e verifique se é fácil de utilizar.

COMO GERENCIAR FILTROS ANTI-SPAM

Os filtros anti-spam, de maneira geral, trabalham com conceitos semelhantes, embora possam receber denominações distintas. São eles:

- Listas negras (*blacklists*): e-mails, domínios e/ou IPs daqueles que você considera *spammers*;
- Listas brancas (*whitelists*): e-mails, domínios e/ou IPs de quem você deseja receber e-mails;
- Quarentena: local onde são armazenados os e-mails suspeitos de serem spams.

Um dos desafios do usuário é exatamente gerenciar esses recursos, necessários para a configuração adequada do aplicativo anti-spam. Resumidamente, as listas negras deverão conter os e-mails, domínios e/ou IPs daqueles que o usuário considera *spammers* ou, ainda, que são reconhecidamente *spammers*, conforme dados disponíveis na Internet. As mensagens vindas de endereços que estiverem na lista negra do usuário não serão mais recebidas.

Por outro lado, as listas brancas existem para definir, especificamente, os e-mails, domínios e/ou IPs, considerados confiáveis, ou seja, que terão passagem livre pelo filtro anti-spam.

O que deve constar na lista branca:

- Os e-mails e domínios de familiares, amigos, colegas de trabalho, parceiros e fornecedores.
- Os endereços das listas de discussão que o usuário assina regularmente com o e-mail em questão.

Em relação à quarentena, o método de gerenciamento depende do tratamento e da configuração do aplicativo anti-spam. Geralmente, vão para a quarentena e-mails que são identificados como spams, porém também podem ir os e-mails legítimos, mas que foram considerados spam por engano. Estes são os chamados falsos positivos. Dependendo do índice de falsos positivos apresentado pelo filtro, é recomendado configurá-lo para manter os e-mails suspeitos de spam na quarentena por um determinado tempo. Dessa forma, o usuário poderá recuperá-los.

Caso o índice de falsos positivos seja pequeno e o risco de perder um e-mail importante seja mínimo, pode-se configurar o aplicativo para descartar os e-mails, em vez de armazená-los na quarentena. De modo geral, o importante é utilizar o recurso de quarentena e verificar as mensagens lá armazenadas com freqüência.

COMO EVITAR QUE SEU COMPUTADOR SE TORNE UM SPAM ZOMBIE

Os computadores infectados por códigos maliciosos, capazes de transformar o sistema do usuário em um servidor de e-mail para envio de spam, são chamados de spam *zombies*. Em muitos casos, o usuário do computador infectado demora a perceber tal comportamento anômalo, exceto por lentidão na máquina ou na conexão com a rede.

Além de propagar-se por e-mail, a maior parte dos códigos maliciosos se tem disseminado automaticamente pela rede. Esses programas maliciosos, em geral *worms* ou *bots,* buscam por máquinas com programas que possuem alguma vulnerabilidade e as comprometem. Após conseguirem acesso a uma máquina, esses programas passam a ser controlados pelos invasores e podem, entre outros fins, ser utilizados para o envio de spam.

DICAS PARA PROTEÇÃO

- Utilize softwares de proteção (antivírus, antispam, *anti-spyware* e *firewall* pessoal) nos computadores de uso doméstico e corporativo.
- Mantenha atualizadas as versões dos softwares de proteção.
- Mantenha atualizadas as assinaturas do antivírus e do *anti-spyware*.
- Não clique em URLs (*links*) incluídas em e-mails, principalmente, se forem e-mails suspeitos de spam ou de origem desconhecida.
- Não execute arquivos anexados aos e-mails sem examiná-los previamente com um antivírus.
- Esteja atento à navegação em *sites* na Internet, e evite clicar em *links* que aparecem em janelas do tipo *pop-up*.
- Caso note comportamento anômalo em seu computador (reinicializações sem motivo aparente, lentidão e erros diversos, por exemplo), faça um rastreamento com o antivírus e, se o problema persistir, reinstale totalmente o sistema operacional e os aplicativos.
- Em casos de contaminação por vírus ou outro código malicioso, reinstale totalmente o sistema operacional e os aplicativos, evitando restaurar *backups* antigos.

FIQUE DE OLHO!

Saiba mais detalhadamente sobre como identificar spams.

BOATOS (*HOAXES*)

São parecidos com as correntes. Utilizam a engenharia social e apelam para que o usuário (destinatário) os envie "para todos os seus conhecidos" ou "para todas as pessoas especiais de sua vida".

A diferença entre correntes e boatos está no conteúdo, pois, os boatos geralmente contam histórias alarmantes e falsas, sensibilizando o usuário (destinatário) a continuar a propagação. Os boatos mais comuns são:

- **Difamatórios:** denigrem empresas ou produtos, prometendo brindes ou falam dos riscos que determinado componente da fórmula do produto causa à saúde.
- **Filantrópicos:** contam histórias de crianças doentes, usando as tragédias e as catástrofes naturais como argumentos para pedir ajuda em dinheiro, que não será repassada às reais vítimas.

Um fato curioso é a recorrência de alguns boatos famosos, divulgados de tempos em tempos na rede. Acredita-se que isto ocorra devido à grande quantidade de novos usuários na Internet que, por falta de informação ou de experiência, repassam os boatos antigos, iniciando um novo ciclo de propagação. Um exemplo é o boato sobre o Roubo da Amazônia (**http://www.quatrocantos.com/LENDAS/27_amazonia.htm**). Outros exemplos de boatos que circularam e circulam na Internet podem ser consultados em **http://www.quatrocantos.com/LENDAS/index_crono.htm**.

LENDAS URBANAS

São as histórias disseminadas na Internet, sejam elas tristes, alegres, assustadoras ou misteriosas. Podem ser confundidas com os boatos, mas, diferem, principalmente, pelas justificativas utilizadas para atrair a atenção do usuário, conferindo veracidade aos relatos. Alguns exemplos são: "Aconteceu com o primo do amigo do meu pai...", "O avô do marido da minha prima disse que foi mesmo verdade..." e "Quem está no hospital é o sobrinho do primo da esposa do meu amigo".

Existem muitas lendas urbanas propagadas pela Internet e algumas delas podem ser vistas em **http://www.quatrocantos.com/LENDAS/index_crono.htm**. Outro exemplo bastante ilustrativo e recente de lenda urbana é o caso da cobra encontrada na piscina de bolinhas de uma famosa lanchonete de uma cidade do interior de São Paulo (**http://www.quatrocantos.com/lendas/192a_cobra_na_piscina.htm**).

FRAUDES

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

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

GOLPES (*SCAMS*)

Um dos fatos marcantes na história do spam tem sido sua utilização para disseminação de golpes. Os antigos, já praticados por meio de cartas ou ligações telefônicas, migraram para a Internet, propagados via spam. Um exemplo é o Golpe da Nigéria, também conhecido como golpe do 419 ou do 171, os famosos "contos do vigário".

Os golpes nigerianos são classificados como AFF (*advance fee fraud*), ou seja, fraude da antecipação de pagamentos. Utilizando engenharia social, são elaboradas mensagens longas, contando histórias mirabolantes e pedindo que o usuário envie determinada quantidade de dinheiro, prometendo altas recompensas no futuro, quando o objetivo colocado na história for concretizado. Esses objetivos são tão diversos quanto a quantidade de golpes nigerianos. Entre eles, o financiamento para a construção de aeroportos na Nigéria, o resgate da fortuna de um parente ex-ditador da Nigéria ou outro país africano, e o resgate de um astronauta perdido numa base espacial.

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

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

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

PHISHING: SITUAÇÕES EM QUE PODE OCORRER ESTE TIPO DE FRAUDE

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

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

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

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

Novas formas de *phishing* podem surgir, portanto é muito importante que você se mantenha informado sobre os tipos de *phishing* que vêm sendo utilizados pelos fraudadores, através dos veículos de comunicação, como jornais, revistas e *sites* especializados.

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

MENSAGENS QUE CONTÊM *LINKS* PARA PROGRAMAS MALICIOSOS

Você recebe uma mensagem por *e-mail* ou via serviço de troca instantânea de mensagens, onde o texto procura atrair sua atenção, seja por curiosidade, por caridade, pela possibilidade de obter alguma vantagem (normalmente financeira), entre outras. O texto da mensagem também pode indicar que a não execução dos procedimentos descritos acarretarão conseqüências mais sérias, como, por exemplo, a inclusão do seu nome no SPC/SERASA, o cancelamento de um cadastro, da sua conta bancária ou do seu cartão de crédito, etc. A mensagem, então, procura induzí-lo a clicar em um *link*, para baixar e abrir/executar um arquivo.

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

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

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

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

COMO O FRAUDADOR CONSEGUE ACESSO AO SEU COMPUTADOR

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

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

Esse tipo de programa malicioso pode utilizar diversas formas para furtar dados de um usuário, dentre elas: capturar teclas digitadas no teclado; capturar a posição do cursor e a tela ou regiões da tela, no momento em que o *mouse* é clicado; sobrepor a janela do *browser* do usuário com uma janela falsa, onde os dados serão inseridos; ou espionar o teclado do usuário através da *Webcam* (caso o usuário a possua e ela esteja apontada para o teclado). Mais detalhes sobre algumas destas técnicas podem ser obtidos na **Cartilha de Segurança para Internet – Capítulo 4: Códigos Maliciosos (*Malware*)**, **seção 4.4. *Spyware***.

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

COMO IDENTIFICAR

Seguem algumas dicas para identificar este tipo de mensagem fraudulenta:

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

RECOMENDAÇÕES

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

DÚVIDAS?

Tendo dúvidas, fique a vontade em contatar o suporte Loja de Internet, empresa responsável pela administração e manutenção do site e sistemas.

Contate-nos por telefone e exponha suas dúvidas, o atendimento da Loja de Internet irá lhe encaminhar ao suporte adequado e, dependendo de como for, será agendado um atendimento personalizado para você.

Lembramos que o suporte será efetuado exclusivamente via telefone fixo e dentro dos horários de funcionamento da empresa, que são:

- Segunda a Sexta das 9:00hs às 12:00hs |15:00hs às 17:00hs.

Dados de contato da Loja de Internet:

Site: www.lojadoscatalogos.com.br
Email: suporte@lojadoscatalogos.com.br
Telefones (fixos**)**: (27) 3074-9500 / 3062-3752
Celular (para emergências**)**: (27) 7811-7130
ID Nextel: 118*65861

Obrigado por usar nossos serviços!
Estamos sempre à sua disposição!