CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

Thaíne Alves da Silva

O IMPACTO DO *SPAM* NA EMPRESA DE PEQUENO PORTE

Americana, SP
2015

CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

Thaíne Alves da Silva

O IMPACTO DO *SPAM* NA EMPRESA DE PEQUENO PORTE

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação do Prof. Esp. José William Pinto Gomes.

Área de concentração: Segurança da Informação.

Americana, SP
2015

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

	Silva, Thaine Alves da
S584i	O impacto do spam na empresa de pequeno porte. / Thaíne Alves da Silva. – Americana: 2015.
	51f.
	Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
	Orientador: Prof. Esp. José William Pinto Gomes
	1.Rede de computadores I. Gomes, José William Pinto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.
	CDU: 681.519

Thaíne Alves da Silva

O IMPACTO DO *SPAM* NA EMPRESA DE PEQUENO PORTE

Trabalho de conclusão de curso apresentado à Faculdade de Tecnologia de Americana como parte dos requisitos para obtenção do título de Tecnólogo em Segurança da Informação.

Área de concentração: Segurança da Informação.

Americana, 24 de Junho de 2015.

Banca Examinadora:

José William Pinto Gomes
Especialista
Faculdade de Tecnologia de Americana

Juliane Borsato Beckedorff Pinto
Graduada
Faculdade de Tecnologia de Americana

Mariana Godoy Vazquez Miano
Doutora
Faculdade de Tecnologia de Americana

Solidários, seremos união.

Separados uns dos outros seremos pontos de vista.

Juntos, alcançaremos a realização de nossos propósitos.

Bezerra de Menezes

AGRADECIMENTOS

Primeiramente, agradeço à Deus por ter me concedido tamanha oportunidade em minha vida.

Ao professor e orientador José William Pinto Gomes, pelo apoio incondicional no desenvolvimento do trabalho.

Aos meus pais e irmãs, por estarem comigo sempre e em quaisquer momentos, por toda dedicação, compreensão e amor.

Ao meu marido, pela paciência, amor e pelo companheirismo.

DEDICATÓRIA

Aos meus pais Vera Lúcia e Roberto.

Às minhas irmãs Ana Estela e Raquel.

Ao meu marido Alan.

RESUMO

O progressivo uso de canais eletrônicos tem a finalidade de simplificar a comunicabilidade, com resultados ágeis e acessíveis dos dados em uma instituição. No entanto, a grande quantidade de tráfego de *e-mails* não solicitados (*spam*) circulando na *Web* desperdiçam recursos que poderiam ser usados para melhores finalidades, uma vez que ficam expostos a vulnerabilidades, perda de produtividade e a elevadas despesas, principalmente para as pequenas empresas. Assim, este trabalho visa analisar e conceituar os malefícios causados pelo *spam* em empresas de pequeno porte.

Palavras-chave: *Spam;* Empresas de Pequeno Porte.

ABSTRACT

The progressive use of electronic channels is intended to simplify the communicability, with agile and accessible data results in an institution. However, the large amount of e-mail traffic unsolicited (*spam*) circulating on the *Web* waste resources that could be used for better purposes, since they are exposed to vulnerabilities, productivity lost and high cost especially for small companies. This work aims to analyze and conceptualize the harm caused by *spam* in small businesses.

Keyworks: *Spam;* Small Businesses.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ARPA	*Advanced Research Projects Agency*
ARPANET	*Advanced Research Projects Agency Network*
ASCII	*American Standard Code for Information Interchange*
CERT.BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGI.BR	Comitê Gestor da Internet no Brasil
E-MAIL	*Eletronic Mail*
EPP	Empresa de Pequeno Porte
HTML	*HyperText Markup Language*
ME	MicroEmpresa
OSI	*Open System Interconnection*
PDF	*Portable Document Format*
SEBRAE	Serviço Brasileiro de Apoio às Micro e Pequenas Empresas
SMTP	*Simple Mail Transfer Protocol*
SNDMSG	*Send Message*
TCP	*Transmission Control Protocol*
TCP/IP	*Transmission Control Protocol/ Internet Protocol*
TI	Tecnologia da Informação
UCE	*Unsolicited Comercial E-mail*
US-ASCII	*United States-American Standard Code for Information Interchange*

SUMÁRIO

1 INTRODUÇÃO

Com o advento da Internet, diversas modificações no comportamento e na realidade da sociedade foram observadas. A facilidade no seu manuseio e a expectativa de ultrapassar barreiras físicas, diminuindo os distanciamentos geográficos e aumentando a velocidade na troca de conhecimentos, provocaram verdadeiras revoluções e resultados jamais vistos anteriormente.

Novos costumes, formas de relações interpessoais, econômicas e até mesmo trabalhistas, foram modificados com o fácil acesso à Internet. Esta vem se tornando elemento fundamental no cotidiano dos indivíduos, principalmente com o aumento do contato com computadores e a decrescente despesa de aquisição. Antigamente o mesmo era considerado artigo de luxo, nos dias de hoje é considerado extremamente necessário. O acesso através da rede mundial de computadores se tornou componente inevitável para as organizações que desejam e as que já se estabeleceram e têm a pretensão de seguir nos negócios e no mercado de trabalho.

O efeito da extensão da quantidade de acessos à rede é a utilização de *e-mail* como canal de comunicação predominante em uso na Internet. Os números de provedores de correios eletrônicos e a simplicidade na utilização de *softwares* clientes para o encaminhamento e a receptividade de mensagens contribuíram para a sua popularização. As instituições, de qualquer regime de apuração, pretendem fazer uso cada vez maior dessa prática para a transmissão de dados com seus clientes, mesmo para fins de envio e/ou recebimento de informações confidenciais.

Tal ferramenta, dada como uma verdadeira inovação trouxe consigo inúmeros benefícios nas mais diversas áreas do conhecimento, da saúde e da educação, entre outros; apesar disso, os malefícios também acompanharam a evolução dessa renovação praticamente indispensável no cotidiano da sociedade atual. Um exemplo efetivo desses malefícios é o *spam,* utilizado de forma negativa na Internet.

Tal como descrito pelo Comitê Gestor da Internet no Brasil (CGI, 2015) *spam* é definido como "*e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas". Enquanto a temática dessas mensagens for

exclusivamente comercial, as mesmas continuam sendo denominadas *Unsolicited Comercial E-mail* (UCE) pelo referido CGI.

No âmbito profissional o *spam* é considerado uma problemática que atinge principalmente as atividades comerciais, sociais e econômicas de uma instituição, uma vez que podem ser os responsáveis por possíveis distrações de colaboradores com *e-mails* indesejáveis, dentre outras eventualidades. Muito embora, fora desse ambiente, o *spam* seja avaliado como apenas um desprazer momentâneo.

No que diz respeito aos prejuízos econômicos procedentes da disseminação do *spam*, os impactos gerados por este mostram que a infraestrutura de rede da Internet está sendo utilizada para conter o tráfego proveniente do *spam*, podendo ser interpretado como dano financeiro, em consequência do consumo da largura de banda utilizada, além do aumento da carga em servidores e clientes de *e-mail*.

Nos dias de hoje, o *spam* está relacionado a ataques de clientes e à segurança da Internet, distribuindo vírus e golpes, pretendendo, dessa maneira, obter lucros de forma ilícita, com o acesso a informações confidenciais. No entanto, não é somente o aumento da quantidade de *spam* na rede que são alarmantes, o seu objetivo e seu contexto nem sempre possuem caráter publicitário, tópicos esses que são abordados ao longo do trabalho.

Assim, o presente trabalho possui como objetivo geral o relato dos diversos malefícios provocados pelo *spam* na empresa de pequeno porte, demonstrando o quanto o mesmo pode ser prejudicial para esta. Para fins de confirmação foram elaborados questionários enviados a três pequenas empresas no interior do estado de São Paulo, nas quais os resultados obtidos permitem a observação real dos danos causados pelo *spam* no dia a dia de uma empresa de pequeno porte.

Como objetivos específicos são apresentados:

- Tratar o *e-mail* e a sua origem, canal de comunicabilidade mais usado na *Web*. O protocolo padrão de transferência de *e-mail*, responsável pela facilitação da transmissão de mensagens eletrônicas e que está contido na camada de aplicação o Modelo OSI, *Simple Mail Transfer Protocol* (SMTP).

- Retratar a estrutura elementar do SMTP e os seus métodos funcionais.

- Definir *spam*, conceitos de empresa de pequeno porte.

- Apresentar e elaborar um estudo de caso, por meio da utilização de questionário como instrumento de pesquisa para verificação do impacto do *spam*em três empresas de pequeno porte.

- Realçar a vulnerabilidade no quesito segurança do protocolo SMTP, os principais tipos de spam, as mutações no decorrer da ampliação pela rede, os inconvenientes originados pela difusão deste e determinadas estatísticas que listam a sua quantidade considerável, como, também, a apresentação de mecanismos de filtragem de *spams* e algumas de suas ferramentas.

- Apresentar a insegurança contida no *phishing scam* e os reais motivos do seu funcionamento.

- Esclarecer a relação entre *spam*, *phishing scam* e *Internet banking*.

Em sua organização este trabalho foi estruturado da seguinte forma:

A Introdução (1) contextualiza o tema, apresenta os objetivos, tanto geral quanto específicos, do estudo, bem como a forma como este estudo foi elaborado.

A Revisão Bibliográfica (2) discorre sobre o *E-mail*, sua origem e suas funcionalidades; apresenta o *Simple Mail Transfer Protocol* (SMTP), como é alicerçado e seus métodos; explana sobre o *Spam* e o conceitua; finaliza com enfoque na Empresa de Pequeno Porte e como é classificada.

O Estudo de Caso (3) apresenta os procedimentos utilizados na pesquisa, que se deu por meio de questionário aplicado em três empresas do interior do estado de São Paulo, os resultados obtidos e a conclusão sobre os dados.

O Impacto do *Spam* na Empresa de Pequeno Porte (4) aborda as questões de segurança no SMTP, apresenta os tipos de spam com suas mutações, danos e alguns dados estatísticos; apresenta algumas técnicas *Anti-Spam*, bem como ferramentas *Anti-Spam*; explana, ainda, sobre o *Phishing Scam* e o *Internet Banking.*

As Considerações Finais (5) apresentam os resultados obtidos com o estudo, discorre sobre os objetivos objetivando a verificação se estes foram atingidos e apresenta sugestão para trabalhos futuros.

Ao final, são apresentadas as Referências (6) utilizadas para a composição do referencial teórico deste trabalho.

2 REVISÃO BIBLIOGRÁFICA

Nesta revisão bibliográfica são abordadas as temáticas que envolvem o *e-mail* e a sua origem, destacando a sua relevância para uma sociedade cada vez mais globalizada, bem como, as principais características do protocolo responsável pela sua transferência, conhecido como SMTP.

Igualmente, foram apresentadas definições acerca do *spam*, seu desenvolvimento e impacto nas empresas de pequeno porte. As empresas de pequeno porte também foram contempladas nesta revisão.

2.1 *E-Mail*

É essencial, em primeiro plano, entender o que é *e-mail*. Para Carneiro (2000), o *e-mail* é a atividade disponibilizada na *Web*, para efetuar transações de mensagens eletrônicas, compostas, a princípio, somente de textos simples.

Em seu significado mais amplo, pode ser definido como correio eletrônico. *E-mail* (abreviação *de eletronic mail*) é um instrumento que permite a construção, o envio e o recebimento de mensagens eletrônicas, contendo matérias, ilustrações, entre outros documentos por meio da *Web* e não depende da presença do remetente ou do receptor da mensagem. Apresenta diversas facilidades de utilização, e se tornou uma ferramenta essencial para a comunicação no sentido de ultrapassar barreiras físicas, ou seja, quando a informação e a comunicabilidade precisam ser efetuadas entre indivíduos que estejam geograficamente distantes.

2.1.1 Origem do *E-mail*

O desenvolvimento da Internet se deu em ritmo tão frenético e acelerado que transformou a distância em uma simples particularidade e promoveu uma revolução na comunicação. Com essa facilidade, os correios eletrônicos se tornaram endereços virtuais para as mais diversas funcionalidades e, atualmente, passaram de um simples colaborador para o canal de comunicabilidade mais difundido e

utilizado na *Web*. Segundo Levine (1997), o *e-mail* é um instrumento de trabalho e, fundamentalmente, um canal de comunicação.

O progresso do primeiro sistema, que autorizava a transmissão de mensagens eletrônicas através de computadores distintos, ocorreu em 1965, possibilitando, dessa forma, a comunicação entre os diversos usuários de um computador de modelo *mainframe*. Para Levine (1997), esse mesmo sistema se transformou rapidamente em um correio eletrônico na *Web*, proporcionando assim, que os clientes localizados em divergentes computadores enviassem mensagens entre si.

Ray Tomlinson, um engenheiro programador de *softwares* dos Estados Unidos, criou o aplicativo SNDMSG (*send message*), um *software* simples, com apenas 200 linhas de código fonte, mas que permitia a transmissão de mensagens por meio de usuários interligados em um mesmo computador. Para conseguir adaptar o SNDMSG, Tomlinson utilizou um protocolo de transação de arquivos, conhecido como CYPNET. Consequentemente, era possível que usuários que estivessem conectados à ARPANET (rede de computadores que permitiu e deu origem à Internet) efetuassem a troca de mensagens, mesmo que não utilizassem a mesma máquina. Igualmente, decidiu adotar e assumir a "@" (arroba) para fins de identificação da origem das mensagens, logo após o nome definido pelo usuário. Existiram protótipos similares à proposta de Ray Tomlinson, no entanto, foi a sua obra que deu início *ao e-mail* conhecido atualmente. (LEVINE, 1997).

A princípio, a função do correio eletrônico era única e exclusiva de trocar mensagens de texto simples entre usuários da ARPANET. Na proporção que o modelo foi crescendo, a possibilidade de enviar mensagens maiores foi aumentando respectiva e gradativamente. Posteriormente, o correio eletrônico foi visto também como uma oportunidade comercial. Em 1978, Gary Thuerk, um gerente de marketing, enviou para cerca de 600 pessoas da ARPANET uma mensagem tentando vender o Decsystem-20, um computador novo para a época. Foi a partir desse período que o *spam* iniciou seu progresso e sua expansão. Contudo, a maior oportunidade que o *e-mail* visava era a possibilidade de poder se comunicar com outros usuários de qualquer outro lugar do mundo. Ultrapassar barreiras físicas era um dos principais propósitos para o sistema que ainda estava em fase de desenvolvimento. Grande parte da população não teve a chance de ter o seu próprio

e-mail em 1970. Todavia, em meados de 1990 começaram a surgir os primeiros serviços de hospedagem. Assim, já era possível, e relativamente normal, receber *e-mails* quando assinasse e tivesse vínculos com algum provedor. (KARASINSKI, 2009).

Segundo a *Reader's Digest* Seleções (2001), a criação do primeiro *e-mail* sem custo, ou seja, gratuito, só foi possível graças a Sabeer Bhatia, um empresário de nacionalidade indiana. O mesmo foi o responsável pela criação do serviço eletrônico mundialmente conhecido como Hotmail. O objetivo era desenvolver o correio eletrônico com base na *Web*. Consequentemente, o cliente poderia acessar o seu *e-mail* em diversos computadores. Posteriormente, Bhatia vendeu o Hotmail para a Microsoft em 1997, pela grandiosa somatória de 400 milhões de dólares. Nos dias de hoje, conhecido como *Windows Live Hotmail*, incorpora várias atividades.

Desse modo, se deu origem ao *e-mail* eletrônico.

2.2 *Simple Mail Transfer Protocol*

O SMTP (*Simple Mail Transfer Protocol*) é um protocolo padrão de envio de *e-mail* com base em textos simples, em que um ou diversos receptores de mensagens eletrônicas são estabelecidos. A utilização em massa deste protocolo teve início em 1980. Na especificação inicial o protocolo era contemplado somente de texto ASCII (*American Standard Code for Information Interchange*), o que impossibilitava a transmissão de arquivos, no qual foram definidos, posteriormente, alguns formatos para este tipo de transmissão.

Uma importante característica desse protocolo é a possibilidade de transmissão de *e-mail* para computadores destinos em uma mesma rede ou em redes diferentes. O mesmo integra o conjunto de protocolos da camada de aplicação da arquitetura de redes TCP/IP (*Transmission Control Protocol/Internet Protocol*). O objetivo do SMTP é a envio de mensagens eletrônicas. Conforme Klensin (2001), o SMTP é independente de subsistemas de transmissão particulares e requer apenas um canal de transmissão de dados confiável e ordenado.

2.2.1 A Estrutura Básica do SMTP

O recurso de transferência do SMTP fundamenta-se no padrão cliente/servidor. À medida que um usuário pretende enviar um *e-mail*, o mesmo desenvolve uma conexão bidirecional com o servidor SMTP que, por referência, usa o protocolo de transporte TCP (*Transmission Control Protocol*) e o servidor recebe conexões na porta 25. Com a conexão já definida, o usuário transfere a mensagem para o servidor ou atribui para o usuário determinados erros de emissão.

O protocolo SMTP não tem a função de definir se a mensagem a ser encaminhada é reservada ao servidor local ou ao servidor remoto de SMTP. Segundo Klensin (2001), o mesmo pode ser tanto o último destinatário ou, ainda, um *relay* intermediário (ou seja, pode atribuir à função de um cliente SMTP depois do recebimento da mensagem) ou *gateway* (isto é, o mesmo pode transmitir a mensagem seguidamente usando um protocolo divergente do SMTP), ou seja, a conexão SMTP pode ser estabelecida entre o usuário original SMTP e o servidor SMTP final ou entre uma sequência de servidores intermediários.

Após a abertura da conexão da camada de transporte, com o servidor o cliente SMTP inicializa a composição de transmissão. Essa transação baseia-se em um seguimento de comandos emitidos pelo cliente que classifica o início e o destino final da mensagem. Com o seguimento organizado nesta ordem de comandos, o conteúdo é então emitido.

Cada instrução encaminhada através do cliente SMTP é respondida pelo servidor por meio de um código. Cada um desses códigos pode informar e apontar que os comandos recebidos foram aprovados, ou que comandos complementares são precisos, ou ainda que falhas momentâneas ou mesmo efetivas aconteceram. Posterior à emissão da mensagem, o cliente SMTP pode solicitar o encerramento da conexão ou promover o encaminhamento de uma nova mensagem.

2.2.2 Os Métodos do SMTP

O protocolo SMTP é responsável pelo transporte de objetos *mail*. Os mesmos são compostos de um conteúdo e um envelope. O conteúdo apresenta uma separação em duas partes: cabeçalho e corpo.

Segundo Resnick (2001), os campos do cabeçalho são constituídos por linhas formadas por meio de uma terminologia de campo, continuado através do sinal gráfico de pontuação, dois pontos (":") que, por sua vez, é seguido pelo corpo do campo e concluído com caracteres de retorno e alimentação de linha. O corpo é de caráter textual, formado de caracteres *US-ASCII* (*United States-American Standard Code for Information Interchange*). Já o envelope é uma série de instruções SMTP encaminhadas através do cliente que englobam dados tais como destinatário, remetente e determinadas amplificações do protocolo.

Uma sessão SMTP é estabelecida após a abertura de uma conexão da camada de transporte. Depois da estabilidade dessa mesma conexão, o servidor corresponde com um código de abertura. Uma implementação SMTP pode compreender, posteriormente, a mensagem de código de abertura, dados de identificação do *software* SMTP. Entre outras, geralmente são inseridas referências sobre a versão e o fabricante do *software*. É atividade habitual de determinados administradores de rede, excluir as informações de versão e fabricante do *software* SMTP para impossibilitar que esses dados ofereçam contribuições para invasores investigarem fragilidades atribuídas ao *software* servidor.

2.3 *SPAM*

Spam pode ser definido como mensagens eletrônicas enviadas a inúmeros usuários/consumidores sem que os mesmos façam essa solicitação ou mesmo considerem a alternativa de recebê-los. Basicamente, esta atividade tem como principal objetivo a publicidade e a comercialização virtual. No entanto, da mesma forma, pode ser um canal para a dissipação de golpes, difamação, entre outros. Portanto, é viável que instituições de todos e quaisquer segmentos estejam vulneráveis a ataque de *spam*.

O *spam* se caracteriza por ser um tipo de mensagem, que tem como comportamento padrão o disparo de *e-mails* para inúmeros usuários simultaneamente, sendo esta, uma das causas da sua origem e utilização. Pode atingir uma quantidade notavelmente extensa de indivíduos em um espaço reduzido de tempo e sem a exigência de grandes esforços.

Isso acontece devido ao *spammer* (autor pela transferência do s*pam*) ter consciência que a mensagem enviada só causará repercussão em uma pequena parcela da sociedade e, desta maneira, precisa de ferramentas para que a conquista de seus propósitos seja a maior e mais concreta possível. Outro fator que tem grande influência na utilização de *spam* é o custo. O *spammer* faz uso de ferramentas criadas exclusivamente para esta finalidade, uma vez que o resultado alcançado é maior que as despesas para usá-las.

Segundo Levitt (2004), *spam* pode ser definido como "uma grande quantidade de *e-mail* não solicitado" encaminhado através de instituições pouco reconhecidas, por profissionais de *marketing* disponibilizando serviços e produtos, ou ainda com a finalidade de utilizar o *e-mail* para a distribuição de vírus, além de cidadãos com ofertas de produtos de origem duvidosa ou mesmo inexistentes.

Para Teixeira (2004), *spam* é considerado uma arbitrariedade e faz referência à emissão de uma quantidade considerável de mensagens não requisitadas, isto é, o encaminhamento de mensagens eletrônicas a diversos usuários, sem que os mesmos tenham solicitado tais dados. O contexto do *spam* pode ser publicidade e propaganda de serviços e/ou produtos, assistência para ações de caridade, correntes, propostas enganosas, boatos, entre outros.

Já Graham (2002), entende que *spam* não se trata de *e-mail* não requisitado. Para o mesmo, o aspecto que define o *spam* é o fato deste ser totalmente automatizado.

2.4 EMPRESA DE PEQUENO PORTE

A empresa de pequeno porte tem sido considerada a responsável por parte da economia, principalmente ao se analisar o setor informal. Nos últimos anos, estudiosos e especialistas vêm destacando a atribuição expressiva que tem sido desempenhada pelas empresas de pequeno porte na geração de novos empregos, criação de serviços e/ou produtos, sendo tida, também, como um meio para a saída da crise econômica mundial. A mesma representa diversas áreas e tem obtido resultado em vários deles, suprindo, muitas vezes, a demanda exigida pelo atual mercado de trabalho. Porém, da mesma forma, encontra fatalidades tais como, problemas de ordem financeira, econômica, mercadológica, técnica, comportamental ou ainda administrativa. Através da complexidade de superação, as mesmas finalizam suas tarefas de forma automática.

Segundo o Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE, 2015) e a Lei Complementar 123/06, conhecida como "Lei Geral da Micro e Pequena Empresa", é Empresa de Pequeno Porte, ou EPP, a pessoa jurídica que obtém o faturamento bruto anual superior a R$ 360.000,00 (trezentos e sessenta mil reais) e igual ou inferior a R$ 3.600.000,00 (três milhões e seiscentos mil reais). Assim, se a empresa ME (Microempresa) conseguir faturar mais de R$ 360.000,00 de receita bruta passa automaticamente para a classificação de EPP. Da mesma maneira, se a empresa EPP não faturar o total bruto anual superior a R$ 360.000,00 passa para a condição de ME.

A classificação pode ser feita também através do número total de colaboradores. Uma indústria é considerada de pequeno porte quando o número é igual a 20 ou até 99 funcionários. Todavia, no Comércio e Serviços, a quantidade de empregados deve ser igual a 10 ou até 49 empregados para ser classificada como EPP.

Conforme Matias e Lopes (2002) podem ser empregadas outras diferentes formas de classificação, tais como capital registrado, investimento em ativo permanente e quantidade produzida.

Portanto, é importante definir que os termos e atribuições práticas do presente estudo são baseados em empresas regulamentadas e classificadas no regime EPP.

3 ESTUDO DE CASO

Independentemente da elevada quantidade de técnicas *anti-spam* disponibilizadas nos dias de hoje (SCHRYEN, 2007), concentradas na redução do número de *spams* nas caixas postais dos usuários, o mesmo continua responsável por grande parte do tráfego na *Web*.

O atual estudo tem o objetivo de demonstrar como o *spam* interfere e prejudica o rendimento diário de uma pequena organização.

3.1. Procedimentos de Pesquisa

O cenário atual é composto pelo acompanhamento de três empresas de pequeno porte, localizadas nas cidades de Santa Bárbara d'Oeste e Americana, interior do estado de São Paulo, durante o período de elaboração do trabalho acadêmico. As mesmas, sem exceção, não permitiram a divulgação de nomes, dados cadastrais e internos, considerando tais informações de procedência sigilosa, buscando, dessa forma, total preservação e integridade profissional.

O primeiro desafio foi elaborado através da coleta de informações, por meio do questionário, como instrumento de pesquisa, enviado para as referidas empresas, a fim de revelar uma amostra representativa do tráfego de *spam* na Internet dentro dessas mesmas empresas. Tal amostra, efetuada de forma quantitativa, tem a finalidade de apresentar as relativas perdas de forma generalizada que, seguidamente servem de dados, apurados pela própria pesquisa e são posicionados para efeito de demonstração de produtividade, participação efetiva de *spam* nas pequenas corporações e o quanto a ação negativa dos mesmos resultam em prejuízos para estas.

O segundo desafio foi, após a sistematização dos dados, promover a elaboração dos resultados obtidos na pesquisa e a identificação das principais consequências que uma instituição, ainda que de pequeno porte, pode sofrer ao ser vítima do *spam* e ao se deparar com essa realidade, que só tende a aumentar.

Foram enviados 82 questionários contendo três perguntas (conforme Figura 01) para 03 empresas de pequeno porte. Para preservar o sigilo acordado entre as partes (pesquisados e pesquisadora), não foram citados os nomes das mesmas.

Figura 1: Modelo de Questionário enviado aos pesquisados.

Nome:_____

Empresa: _____

	Tempo gasto para ler os e-mails	Total de e-mails Recebidos	Total de e-mails Válidos
Segunda-Feira			
Terça-Feira			
Quarta-Feira			
Quinta-Feira			
Sexta-Feira			

Fonte: Própria autora.

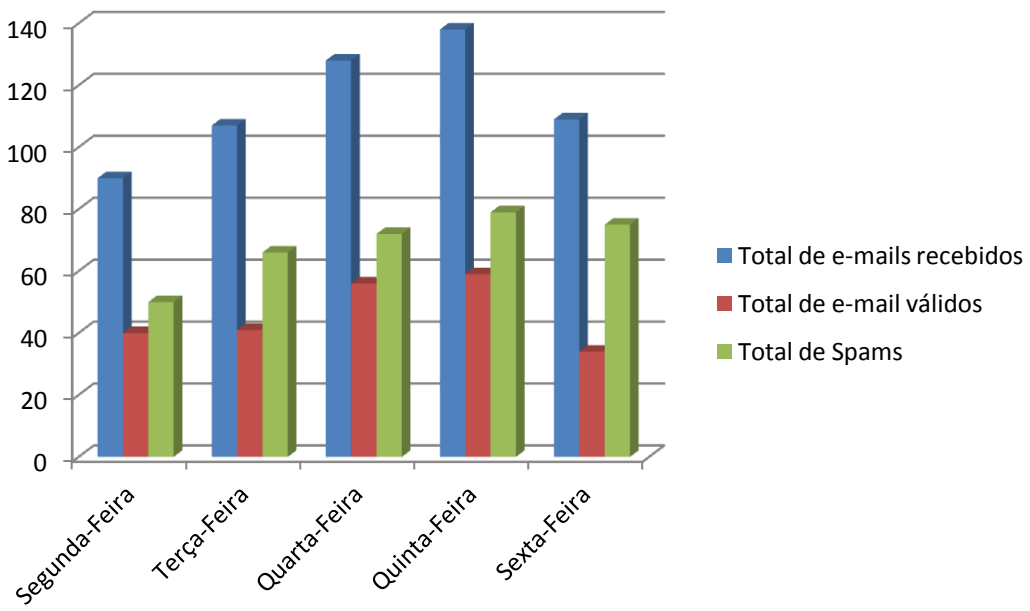
3.2 Resultados e Conclusões

Do total de 82 questionários enviados foram obtidos 47 questionários respondidos, sendo 26 provenientes de respondentes homens e 21 de mulheres. Todos foram informados previamente quanto ao objetivo da pesquisa.

Empresa 01: A Empresa 01 é constituída por 52 colaboradores efetivos, sendo que 31 deles responderam o questionário, entre eles 13 homens e 18 mulheres. A empresa não possui nenhuma ferramenta declarada de *anti-spam* e não tem a pretensão de investir em tais mecanismos, apenas faz frequentes recomendações, através de feedbacks com os funcionários, referente a boas práticas de utilização da Tecnologia da Informação (TI), tais como, políticas de uso, devidas e corretas utilizações de equipamentos de informática e infraestrutura, entre outros, porém, utiliza ferramentas gratuitas para assegurar a segurança dos dados, comprometendo a estabilidade da mesma. Através das Figuras 2 e 3 é possível observar que os funcionários desperdiçam um tempo considerável com a análise e leitura de *e-mails*

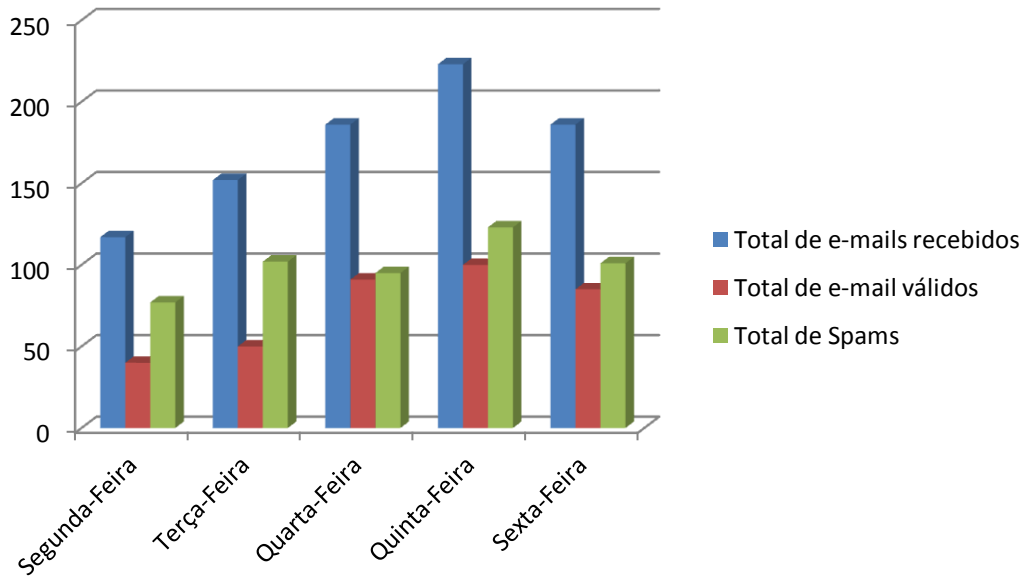
ao longo de uma semana, tempo esse que poderia ser revertido em produtividade e lucro para a empresa.

Figura 2: Gráfico com o Resultado do Questionário - Empresa 01 (Homens).



Fonte: Própria autora.

Figura 3: Gráfico com o Resultado do Questionário - Empresa 01 (Mulheres).

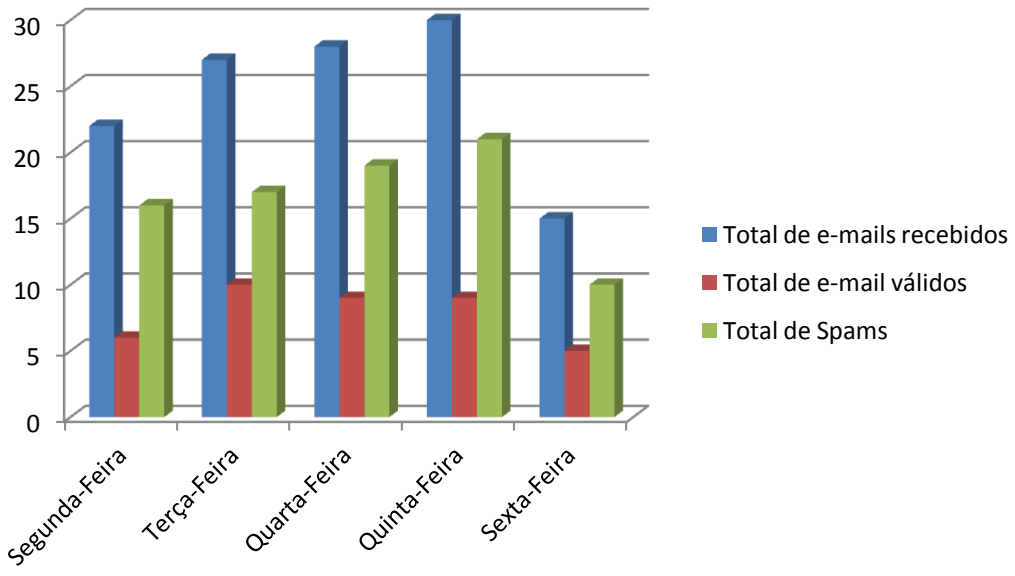


Fonte: Própria autora.

Empresa 02: A Empresa 02 é constituída por 10 colaboradores efetivos, dos quais 08 responderam o questionário, sendo 05 homens e 03 mulheres. Apesar de ser física e estruturalmente menor e com uma quantidade também menor de colaboradores, a empresa solicita, da mesma forma, boas práticas do uso da Tecnologia da Informação, porém, assim como a Empresa 01, não possui ferramentas *anti-spam* específicas ao combate do "lixo eletrônico" e utilizam soluções de baixo custo para garantir a segurança da organização.

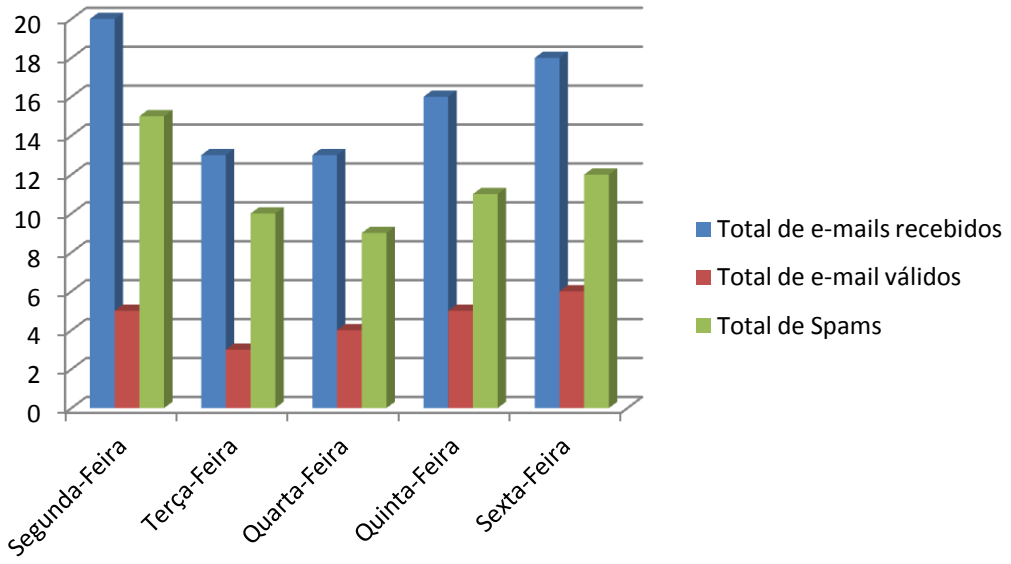
Por meio das Figuras 4 e 5 é possível identificar que os funcionários perdem um tempo considerável com a leitura e análise de *e-mails*, tempo esse que poderia ser revertido em produtividade. É possível observar ainda o baixo número de *e-mails* legítimos, levando em consideração a quantidade recebida.

Figura 4: Gráfico com o Resultado do Questionário - Empresa 02 (Homens).



Fonte: Própria autora.

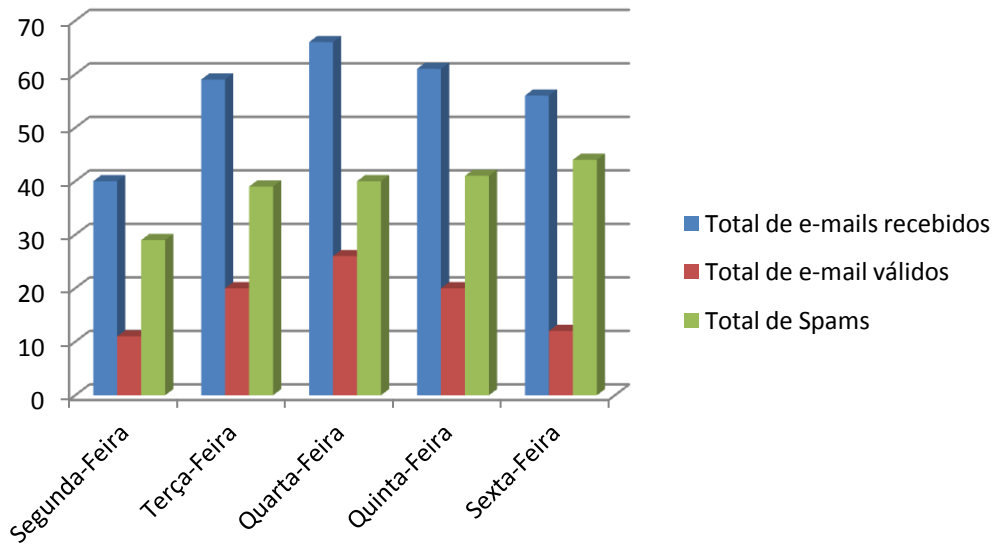
Figura 5: Gráfico com o Resultado do Questionário - Empresa 02 (Mulheres).



Fonte: Própria autora.

Empresa 03: A Empresa 03 é constituída por 20 colaboradores efetivos, dos quais 08 responderam o questionário, sendo os mesmos unicamente respondidos por homens. A mesma não possui ferramentas *anti-spam* adequadas e também não realiza reuniões para fins de instrução aos funcionários e raramente faz uso de instrumentos, ainda que gratuitos, para prover a segurança dos dados na empresa. Pela Figura 6 é clara a percepção do desperdício de tempo com leitura de *e-mails* não requisitados e que não fazem parte da atividade diária da organização.

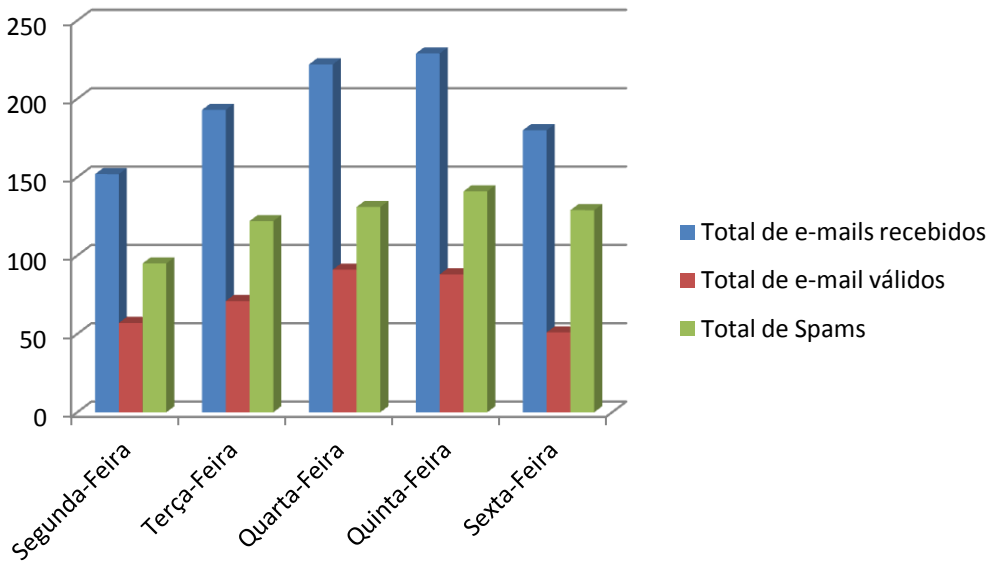
Figura 6: Gráfico com o Resultado do Questionário - Empresa 03 (Homens).



Fonte: Própria autora.

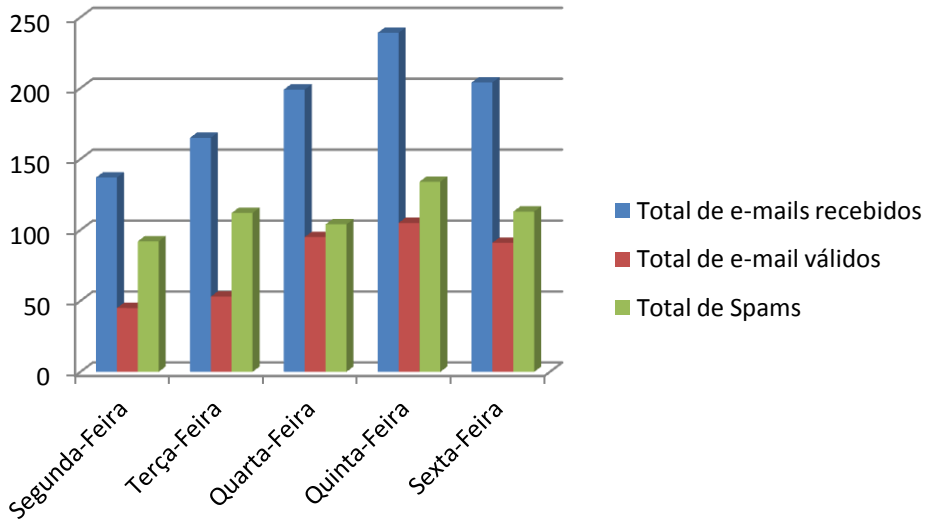
Total de todas as Empresas: Foi elaborada a análise da quantidade de *spams* recebidos em todas as empresas objetos deste estudo de caso. O resultado revela que a quantidade dos mesmos é bastante elevada, conforme demonstrado nas Figuras 7 e 8.

Figura 7: Gráfico com o Resultado do Questionário - Total de todas as Empresas (Homens).



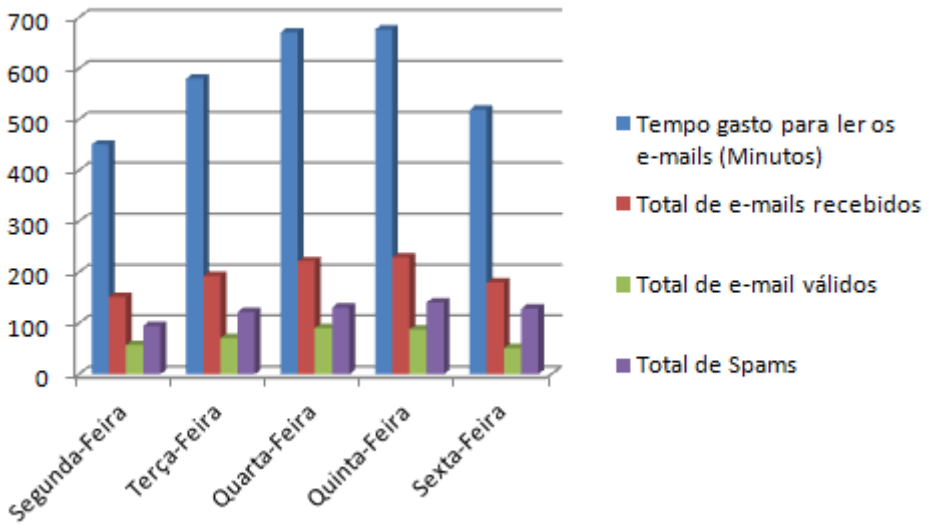
Fonte: Própria autora.

Figura 8: Gráfico com o Resultado do Questionário - Total de todas as Empresas (Mulheres).



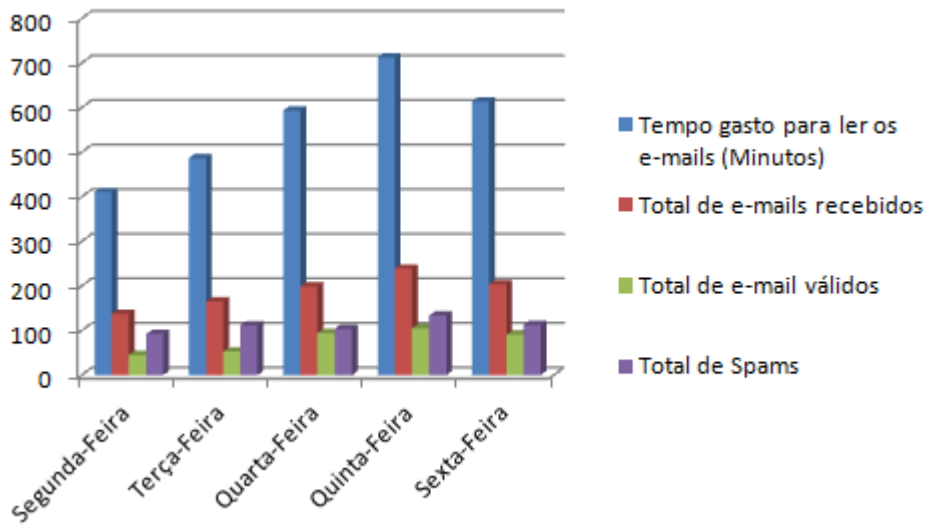
Fonte: Própria autora.

Figura 9: Gráfico com o Tempo Gasto para Ler os E-mails - Todas as Empresas (Homens).



Fonte: Própria autora.

Figura 10: Gráfico com o Tempo Gasto para Ler os E-mails - Todas as Empresas (Mulheres).



Fonte: Própria autora.

A partir dos resultados coletados na pesquisa, pode-se constatar que a perda de produtividade causada pelo uso da Internet já é uma realidade, que tende a ser cada vez mais presente, considerando-se o aumento da participação efetiva do *spam* na sociedade globalizada, como é possível constatar nas comparações mostradas nas figuras 9 e 10.

4 O IMPACTO DO *SPAM* NA EMPRESA DE PEQUENO PORTE

A sociedade moderna ainda está se contemporizando e, assim como a vida nas grandes capitais foi alterada por inúmeros problemas tendo a sua origem em uma centralização de indivíduos de culturas, doutrinas e incentivos divergentes, a Internet igualmente sofre com isso, porquanto, o que ocorre na mesma é, fundamentalmente, um retrato de vida fora dela.

Resumidamente, *spam* ou "lixo eletrônico", é qualquer mensagem eletrônica encaminhada por algum indivíduo sem aprovação evidente e declarada de quem a recebe. Todos os dias surgem novos modelos da chamada "praga digital". Em outra época o *spam* era proveniente, apenas de mensagens com propósito comercial, características que foram alteradas com a modernização de golpes eletrônicos. Hoje, o recebimento de mensagens é substancialmente maior e muitas vezes mascarado de entidades respeitáveis e conhecidas, para que, dessa forma, seja possível a obtenção de dados pessoais, através de programas de captura, do que propagandas propriamente ditas.

Os prejuízos e problemas causados pelo *spam* no cotidiano não são explícitos para a maior parte da população, entretanto, é fato, que devido ao tráfego excessivo dessas mensagens, a Internet fica congestionada. As instituições da atualidade estão continuamente envolvidas na precaução dessa praga, tentando reprimi-las com o desenvolvimento e a implantação de filtros em suas ferramentas de *e-mail.* O *spam* atinge mais os negócios, levando em consideração que mensagens não requisitadas elevaram-se excessivamente nos últimos anos e ainda causam grande impacto negativo às instituições, especialmente as de pequeno porte, que encontram grandes dificuldades na sua preservação. O mesmo, independentemente de recentes regulamentações e avanços tecnológicos que objetivam o seu combate, prossegue atingindo amplamente o mercado de trabalho, custando às instituições valores elevados a cada ano, e para o colaborador no quesito de redução de produtividade.

O *spam* pode causar problemas para um usuário de Internet, bem como para os usuários de serviço de correio eletrônico que, por sua vez, podem ser afetados de modos distintos. Alguns dos problemas sentidos pelos provedores e empresas são:

- Impacto na estrutura interna: Para as instituições e provedores a capacidade de tráfego gerada por conta dos *spams* os forçam a aumentar a capacidade de seus links de conexão com a rede de Internet. Como o consumo dos links é elevado, isto minimiza os lucros do provedor e, em alguns casos, pode refletir no aumento dos custos também para o usuário.

- Utilização incorreta dos servidores: Os servidores de *e-mail* dispensam grande parcela de seu tempo de processamento para tratar de mensagens não solicitadas. Além disso, a capacidade em disco atingida e ocupada por mensagens não solicitadas encaminhadas para um considerável número de usuários é relevante.

- Inclusão em listas de bloqueio: O provedor que tenha usuários envolvidos em casos de *spam* pode ter sua rede incluída em listas de bloqueio. Esta inclusão pode prejudicar o recebimento de *e-mails* por parte de seus usuários e resultar em perda de clientes.

- Investimento em equipe, dispositivos e equipamentos: Para enfrentar, resistir e desafiar os problemas originados pelo *spam*, os provedores precisam reclamar a contratação de mais técnicos qualificados, aquisição de instrumentos e o acréscimo de sistemas de filtragem de *spam*. Como efeito, os custos do provedor aumentam.

A recuperação de um ataque pode ser trabalhosa ou até mesmo inviável para uma empresa de pequeno porte. A insegurança dos usuários após a violação de informações acaba denegrindo o prestígio da empresa de forma definitiva. Além do que, o impacto econômico pode arruinar a pequena empresa, simultaneamente com as finanças pessoais dos empresários e colaboradores, que perdem seus recursos de sobrevivência. Em consequência disso, somente metade das novas empresas de pequeno porte conservam-se por mais de cinco anos viva no mercado, e cerca de um terço permanece por mais de 10 anos, ou seja, uma invasão de informações tem um impacto ruinoso em uma área já debilitada. Segundo a *National Cyber Security Alliance*, todos os anos, uma em cinco pequenas empresas são vítimas do crime

cibernético. Dentre as mesmas, cerca de 60% deixam o mercado de trabalho seis meses após o ataque. (SOLO NETWORK, 2015a).

As empresas de pequeno porte estão frequentemente ameaçadas por vulnerabilidades comuns. Diferentemente das instituições de grande porte que possuem setores de Tecnologia da Informação organizados, repetidamente os pequenos empresários lidam com a segurança da informação por conta própria, sem tomarem as devidas precauções. Comumente, não possuem noção alguma sobre o assunto, ou adquirem apenas conhecimentos básicos, insuficientes para administração de uma empresa, ainda que de pequeno porte. Os mesmos assumem o compromisso pela segurança virtual com determinados *softwares* de segurança adquiridos anteriormente, sem verificar se estes continuam atendendo às exigências da instituição.

Determinados administradores que obtém melhores conhecimentos sobre a tecnologia da informação praticam a incorreta instalação de *softwares* de segurança desenvolvido para corporações superiores, em lugar de implantar soluções criadas exclusivamente para pequenas empresas. O orçamento é outro motivo de ameaça e que eleva a possibilidade de uma pequena empresa se transformar em alvo de criminosos cibernéticos. Com a limitação do orçamento atribuído à segurança da informação, os proprietários de empresas de pequeno porte, quase sempre, efetuam suas escolhas baseados no custo e despesas e não na execução e capacidade de preservação e segurança. Uma solução de custo baixo, ou ainda gratuita, desenvolvida para dispositivos individuais, não está apta para assegurar a proteção adequada de uma empresa de pequeno porte e seus respectivos dados.

Segundo informações da Solo NetWork (2015a), para manter uma maior segurança na pequena empresa, algumas medidas básicas de segurança podem ser tomadas como, por exemplo, os privilégios e direitos consentidos apenas se necessário, assim como privilégios e direitos (de acesso) consentidos aos usuários que devem ser adequadamente gerenciados.

Outro quesito são as verificações regulares sobre as vulnerabilidades da rede e também a análise e detecção de serviços e aplicativos, além de frequentes atualizações de componentes suscetíveis. Caso não seja possível proceder com as

devidas atualizações, as vulnerabilidades dos *softwares* necessitam ser bloqueadas. É importante também a implantação de resoluções de segurança eficazes para a realização de boas práticas de TI, envolvendo serviços de tecnologia da informação, segurança, gerenciamento da infraestrutura, gestão de ativos, entre outros.

A instrução aos funcionários também é de extrema importância para a conservação da segurança da informação em uma pequena empresa. Assim, é possível ressaltar que é relevante a implementação de requisitos básicos de segurança na empresa de pequeno porte para que a mesma tenha a possibilidade de maiores desenvolvimentos frente a uma sociedade cada vez mais exigente e um mercado de trabalho excessivamente concorrido. (SOLO NETWORK, 2015b).

4.1 Considerações de Segurança no SMTP

Independentemente de consistir em um dos protocolos mais usados na Internet, o SMTP, no momento em que foi elaborado, em 1980, e reavaliado na década de 2000, não possuía como condição básica a segurança da informação na emissão de mensagens.

O protocolo foi estabelecido para alcançar maior capacidade e desenvoltura possíveis na transmissão de mensagens eletrônicas. No entanto, no quesito segurança, uma realidade é que, quanto mais completa a agilidade e o funcionalismo, a segurança se torna notadamente inferior.

De acordo com Klensin (2001), o e-mail SMTP é incerto, pois é permitido até mesmo para usuários comuns a negociação com servidores SMTP e a elaboração de mensagens que, possivelmente, enganarão destinatários inocentes que acreditarão que as mesmas tiveram sua procedência por meio de outro indivíduo.

O efeito é que quanto maior a sabedoria dos cidadãos sobre temáticas que envolvam Internet e seus derivados, maior o conhecimento sobre as vulnerabilidades do protocolo SMTP, que não fornece, em seus princípios, comprovação de integridade. A segurança rogada de autenticação e plenitude é direcionada para outros protocolos de aplicação, tais como: HTTP (*Hyper Text Transfer Protocol*), DNS (*Domain Name System*), entre outros.

4.2 Tipos de *Spam*

Apesar de ter conquistado destaque devido à extensa dimensão de mensagens eletrônicas, nos dias de hoje existem diversas classificações para o *spam*. Normalmente os mecanismos *anti-spam* tem seus próprios catálogos de divisões, permitindo maior facilidade para identificar os *spams*, determinando assim, a qual possível classificação os mesmos são pertencentes. Para categorizá-los é possível tomar como referência a especificação elaborada pelo Comitê Gestor da Internet no Brasil – CGI.BR por meio do site: Antispam.br.

Segundo os mesmos, os *spams* são identificados como:

- Correntes: Mensagens que apresentam conteúdos conclusivos tendo como aspecto principal a solicitação para que o destinatário final reenvie a mensagem para outras pessoas da lista de seus contatos. Habitualmente, as correntes buscam que as mensagens sejam encaminhadas para "todos os indivíduos da relação de convívio" ou "todos os indivíduos próximos e amados". A mensagem geralmente é composta de histórias obsoletas, com um "final feliz" ou que envolvam algum tipo de fanatismo. Comumente abrange sugestões como, por exemplo: "se o indivíduo desfizer a corrente, o remetente terá azar", entre outros.

- Boatos: Mensagens similares as correntes. Quase sempre é suplicado que as mensagens eletrônicas sejam emitidas para "todos os indivíduos da relação de convívio" ou algo desta natureza. A diferença entre correntes e boatos é a mensagem em si, o conteúdo. Os boatos citam histórias assustadoras e fictícias. Estas costumam ser pejorativas, denigrem a reputação de instituições, prometem recompensas inegáveis ou, ainda, são filantropos altruístas, entre outros.

- Propagandas: São *e-mails* comerciais compreendendo serviços e produtos. É o tipo de mensagem que mais causa discussão, uma vez que se responsabiliza pela ação de se implementar comercialização via Internet usando como ferramenta principal o *e-mail,* sem que o mesmo seja qualificado como *spam*. Independentemente de existir alterações de entendimento por parte das instituições, muitas delas instituem propagandas publicitárias em massa fazendo uso de *e-mails* não solicitados, o que compromete a própria reputação da corporação.

- Ameaças, brincadeiras e calúnias: Mensagens que podem envolver ameaças, brincadeiras e calúnias de indivíduos, englobando antigos relacionamentos amorosos, entre outros.

- Pornografia: Trata-se de um dos tipos de *spam* mais populares. No entanto, apesar de já ter tido um público considerável, o volume de mensagens eletrônicas pornográficas vem diminuindo no decorrer do tempo.

- Códigos maliciosos: Mensagens que têm como finalidade a disseminação de códigos maliciosos (*malwares*). É crescente o volume de *e-mails* reproduzindo e multiplicando códigos de procedência duvidosa.

- Fraudes: Mensagens que vêm aumentando consideravelmente na Internet. Esse tipo de *spam* faz uso de mecanismos de engenharia social, buscando induzir o usuário a prover seus dados pessoais e financeiros.

- *Spam* via redes sociais: Com o uso de sites de relacionamentos, atualmente tem aparecido esse novo modelo de *spam*. Os mesmos são encaminhados para as páginas de visitas dos usuários, ou por meio de correios eletrônicos emitidos através de um *spammer* pelo sistema de e-*mail* do site de relacionamento.

4.2.1 Mutações do *Spam*

Há um permanente combate entre os *spammers* e os criadores de filtros *anti-spam*. A partir das primeiras mensagens classificadas como *spam* até poucos anos antes, o progresso do mesmo era retraído. Os filtros que usavam somente as chamadas listas negras, ou *black-lists*, de palavras eram bastante aceitáveis para impossibilitar as mensagens escritas apenas em caracteres ASCII por um período de tempo. Correspondendo à rápida alteração de mensagens e conteúdos, foram desenvolvidos mecanismos que usavam como filtros, algoritmos adequados que se delineavam rapidamente às modificações das palavras-chave.

Com exceção de capturar *spams* redigidos unicamente em ASCII e com a gramática correta, os algoritmos adequados podiam descobrir e localizar novas

diversidades do *spam*, o mesmo que sobrepunha as letras por determinados números ou caracteres especiais, no entanto, ainda os tornavam entendíveis pelos destinatários finais.

Em meados de 2005, uma arriscada mutação de *spam* surgiu, o então denominado ASCII-*spam,* que usou a inovadora concepção de produzir imagens manipulando unicamente caracteres ASCII. Assim, palavras e mensagens que seriam naturamente identificadas por qualquer filtro *anti-spam* eram apresentadas em formato de ilustrações ASCII.

Nos primeiros anos da década de 2000, os *spammers* deram início a um novo avanço no que diz respeito ao desenvolvimento de *spam*. As mensagens não mais faziam uso de caracteres em ASCII ou mesmo HTML (*HyperText Markup Language)*, agora os *spams* surgiam exclusivamente como imagens anexas. Como a maior parte dos correios eletrônicos tem funcionalidade de apresentar mensagens anexas no corpo do *e-mail*, o *spam* era visualizado pelo usuário final e excessivamente trabalhoso de ser identificado pelos mecanismos *anti-spam* que não se encontravam suficientemente capacitados para esta nova variação.

Após a progressiva adaptação dos filtros *anti-spam* aos *spams* como figuras, este tipo de mensagem eletrônica começou a fracassar. Porém, posteriormente, os *spammers* modernizaram mais uma vez e iniciaram a emissão de uma recente mutação, os que abrangiam somente documentos e arquivos com a extensão PDF (*Portable Document Format*) como anexos. Novamente, as aplicações *anti-spam* não estavam preparadas para essa novidade e, com isso, a caixa postal dos usuários comuns ficou ocupada com tais mensagens.

4.2.2 Danos Causados pelo *Spam*

Os usuários do serviço de *e-mail* podem ser abordados de inúmeras formas. De baixo custo e com capacidade para atingir uma elevada quantidade de pessoas rápida e simultaneamente, o *spam* causa transtornos de todas as ordens, para usuários e organizações. Seguem, alguns dos fundamentais impasses promovidos pela atividade e ação de *spam*, listados pelo CGI.BR:

- Não visualização de *e-mails*: Uma quantidade extensa de provedores de Internet delimita a dimensão da caixa postal do usuário em seu servidor. Se eventualmente a quantia de *spams* recebidos for maior que o recomendado, o mesmo pode deixar a caixa postal cheia de mensagens não solicitadas. Caso, isso de fato ocorra, a hipótese de não receber *e-mails* até a liberação de espaço é grande e as mensagens já recebidas serão restituídas ao remetente. Esse fato pode acarretar em acúmulo de problemas que, provavelmente, serão ampliados com a ação do tempo.

- Desperdício de tempo: Para cada *spam* recebido, o usuário precisa de um determinado tempo para lê-lo, identificá-lo como *spam* e então removê-lo de sua caixa postal.

- Redução de produtividade: O recebimento de *spams* aumenta o tempo aplicado à função de leitura e análise de *e-mails*, além de existir a possibilidade da não leitura de mensagens importantes, removidas por equívoco, ou ainda lidas com margens de atraso. Todas essas características resultam em perda de produtividade.

- Conteúdo ofensivo ou impróprio: Como a grande parcela de *spams* é encaminhada para endereços de *e-mails* aleatórios, é viável que o internauta encontre e receba mensagens com conteúdos que acredite ser impróprios ou até mesmo ofensivos.

- Danos financeiros causados por fraude: O *spam* tem sido extensamente usado como meio propagador para projetos fraudatórios, que procuram induzir o usuário a acessar páginas clonadas de organizações financeiras ou para instalar programas maliciosos, com a finalidade de coletar informações pessoais e financeiras. Esse tipo de atividade é conhecida como *phishing scam,* que segue convenientemente relatada no decorrer do trabalho. O usuário pode sofrer prejuízos financeiros, caso ceda às informações ou proceda com as instruções solicitadas em mensagens dessa natureza.

- Impropriedade: O *spam* é inapropriado, "degrada" a caixa postal do internauta, fazendo o mesmo desperdiçar tempo hábil removendo as mensagens; preenche a capacidade de armazenamento do *e-mail*; exibe questões inapropriadas;

entre outras características, além do que, essa atividade pode se tornar incômoda em diversas ocasiões.

- Despesas adicionais para a instituição: O *spam* provoca agravos para as corporações, particularmente aos provedores de Internet e serviços de correios eletrônicos. O motivo de tais fatos é a estimativa que de que grande parte das mensagens em tráfego na Internet seja identificada como *spam*, exigindo que instituições custeiem com a circulação de informações, armazenamento de dados, aplicativos e instrumentos de segurança e ainda estruturas e suporte adequados ao cliente.

- Ameaças à segurança e danos financeiros: O *spam* pode englobar links ou anexos que redirecionam para *malwares* ou sites falsos (*phishing scam*), do mesmo modo que pode levar o indivíduo a comprar produtos de origem suspeita. No caso de contaminação, o computador pode ainda enviar *spams* para outros usuários sem a pessoa observar, condição essa que compromete a performance do computador.

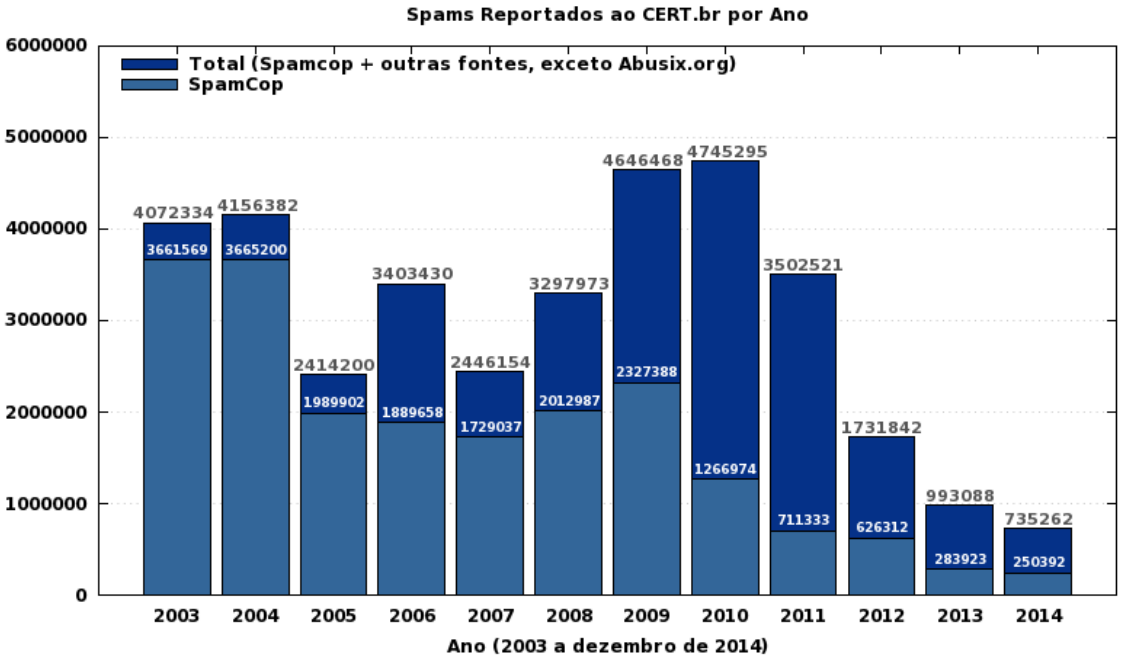
- Não recebimento de mensagens autênticas: Para combater o *spam*, as corporações investem em filtros e outros instrumentos apropriados para impossibilitar este tipo de mensagens. Estes mecanismos costumeiramente são eficazes, porém, estão vulneráveis a falhas. Uma das problemáticas é a possibilidade de o filtro categorizar como *spam* uma mensagem verdadeira. Conhecedor desse fato, o usuário é forçado a visualizar a caixa de *spams* frequentemente para "recuperar" mensagens legítimas. Um filtro *anti-spam* também pode fazer com que uma mensagem seja incapaz de encaminhar links através de redes sociais a amigos, ou reenviar *e-mails* devido ao fato dos mesmos terem conteúdo aparentemente duvidoso, por exemplo, dentre outras características.

4.2.3 Estatísticas sobre o *Spam*

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), preserva estatísticas sobre insatisfações de *spams* recebidas. As mesmas, são desenvolvidas por meio de dados fornecidos pelas reclamações de *spams*, originárias do Brasil, efetuadas pelo *SpamCop* e pelo *Abusix.org*.

Posteriormente ao processamento, estas insatisfações são enviadas ao CERT.BR que cria estatísticas e outras ações publicamente disponíveis. A Figura 9 apresenta uma das mais atuais estatísticas elaboradas:

Figura 11: Gráfico com as Estatísticas de Notificações de *Spam*



Fonte: CERT.BR (2015)

4.3 Técnicas *Anti-Spam*

As orientações para a efetiva redução da quantidade de *spam* estão ligadas à precaução indicada aos usuários da *Web*, para que usufruam das vantagens oferecidas pela Internet, com confiança, tais como: proteger os dados particulares, correios eletrônicos, informações pessoais, dados bancários, etc. É necessário conferir a procedência de determinados sites, assim como a verificação de *e-mails* de origem suspeita de *spam* e averiguar a possível existência de códigos maliciosos ou golpes. Utilizar mecanismos ou possuir filtros *anti-spam* são, atualmente, algumas das opções mais viáveis e recomendadas para evitar a propagação dos chamados "lixos eletrônicos".

4.3.1 Falsos Positivos

Falsos positivos são as mensagens identificadas como s*pam* pela extensão de palavras duvidosas ou metodologias de observações usadas. Eventualmente, se um correio eletrônico englobar conteúdo duvidoso, não obrigatoriamente se trata de s*pam*, no entanto, através da pontuação total pode ser inserido e indicado como tal. A pontuação é elaborada de acordo com a quantia de palavras duvidosas, anexos estranhos, tais como arquivos executáveis, origem do remetente, entre outros.

4.3.2 Pontuação

Segundo Padron (2013), quando uma mensagem eletrônica é enviada, o servidor de *e-mail* que esse destinatário utiliza obriga esta a efetuar um teste *anti-spam* para conferir se a mesma é legítima ou trata-se de mensagens não requisitadas.

Comumente, os servidores de *e-mail* têm mecanismos *anti-spam* hospedados para a realização de testes nas mensagens. Diversas características da mesma são avaliadas, tais como o *e-mail* e o nome do remetente. Essa verificação ocorre através de análises de determinadas regras, configuradas anteriormente e, de acordo com as possíveis "violações" a estas, a mensagem adquire pontos de *spam*. Conforme a quantidade de pontos, mais aspectos de *spam* a mensagem adquire. Geralmente, a limitação exigida pelos servidores de *e-mail* vai de 5 a 10 pontos. Se a mensagem alcançar essa limitação, a mesma é enviada na caixa de *spam* dos usuários finais. Se a mensagem não atingir o limite, ficando abaixo deste, a mensagem eletrônica é encaminhada para a caixa postal dos usuários. E se a mensagem passar dessa limitação de pontos, o servidor de *e-mail* poderá ignorá-la e não enviar aos usuários.

Em cada mensagem, a pontuação é elaborada conforme um antecipado reservatório de palavras excessivamente usadas como, por exemplo, *password*, *money* e outras também identificadas como duvidosas. Esse banco de dados de palavras pode ser adaptado de acordo com a necessidade. Os *logs* devem ser frequentemente supervisionados para que mensagens autênticas não entrem na

lista de bloqueio de forma desnecessária. Então, para que a mensagem seja enviada aos usuários, é necessário criá-la de acordo com as boas práticas de tecnologia da informação que evitem a classificação de pontos como *spam*.

4.3.3 Ferramentas *Anti-Spam*

Para Lima (2010), a implantação de ferramentas *anti-spam*, seja via *software* ou via *hardware*, além de boas práticas de gestão e configuração de servidores de *e-mail*, é fundamental.

Uma ferramenta *anti-spam* tem seu objetivo centrado no combate ao recebimento não requisitado de correios eletrônicos, por meio de verificação dos conteúdos de todas as mensagens. Seguindo a filtragem adotada, o mesmo pode efetuar a pontuação de cada expressão ou palavra duvidosa identificada, classificando ou restringindo-a de acordo com os princípios adotados e elaborados pelo administrador. Essa pontuação esclarece o conteúdo da mensagem, que é categorizada como *spam* ou mensagem legítima.

Na sequência são apresentadas algumas das principais ferramentas *anti-spam* existentes na realidade:

4.3.3.1 *Anti-Spam* SMTP *proxy*

Segundo a SourceForge (2013), *Anti-Spam* SMTP *proxy* (ASSP) é um servidor, de código aberto (*Open Source*), plataforma transparente e independente. Faz uso de diversas tecnologias e métodos para fins de reconhecimento de *spam* por meio de análises do contexto de cada mensagem.

4.3.3.2 *SpamAssassin*

De acordo com a Apache SpamAssassin (2015), o SpamAssassin trata-se de uma ferramenta *anti-spam* administrada por meio da licença Apache (Apache 2013), de código aberto (*Open Source*), em que faz uso de diversos testes como instrumento de pesquisa em cada mensagem recebida. Conforme a análise, ele

aumenta os cabeçalhos nas mensagens, por intermédio de pontuações, alegando a categoria do *spam*, dentre outras ferramentas existentes.

4.4 *Phishing Scam*

E-mails não requisitados encaminhados para uma grande quantidade de destinatários estão sucessivamente ligados a atividades ilegais e podem ser identificados como *spam*. Independentemente de grande parte das mensagens de *spam* enviar publicidade de serviços e/ou produtos, *spam* também é usado para induzir usuários a reproduções enganosas de sites de serviços reais, conhecido como *phishing scam* (ORMAN, 2013).

Para Newman et al. (2002), *spam* é um dos maiores inconvenientes na rede. Além da natureza indesejada, os mesmos são diversas vezes associados à emissão de *phishing scam* e ao aumento de *malwares*, deixando-os mais prejudiciais e perigosos para usuários da *Web*. Devido a isso, estatísticas revelam que o excesso gerado pelo *spam* promove bilhões de dólares de danos às instituições e a população de forma generalizada (SIPIOR, 2004). O *spam* gera despesas não somente para usuários finais, vítimas de *phishing*, mas, também, para operadores de rede, que custeiam pela transferência do tráfego.

Phishing scam é o termo utilizado para caracterizar o desenvolvimento de sites e endereços falsos, para tentar induzir os usuários a revelarem informações como dados bancários ou *logins* e senhas de contas na internet. Estes estão no âmbito das principais ameaças efetivas e existentes na rede. As decorrências desta natureza de falsificação podem desencadear numerosos danos financeiros. A expressão "*phishing*" faz menção ao termo inglês "*fishing*", que pode ser traduzido como "pescaria". O vínculo com essa operação não é aleatoriedade: o *phishing* é um ensaio de golpe pela Internet que usa e beneficia-se de "iscas", ou seja, métodos para cativar a concentração de um usuário e fazê-lo cometer determinada ação.

O *phishing scam* frequentemente atinge os indivíduos através de *e-mail*. Apesar de testar outros meios, entre eles sites de redes sociais, o correio eletrônico é ainda o meio predileto, por ser o canal de informação mais acessível e popular da

Internet. Geralmente, mensagens desse gênero são criadas para representar a emissão por organizações sérias e respeitadas, tais como instituições bancárias ou órgãos governamentais, ainda que, igualmente, se passem por cidadãos simulando ser quem na realidade não são.

O crime cibernético direcionado a empresas de pequeno porte está crescendo, e as despesas das infrações de dados para as vítimas mais suscetíveis podem atingir um custo exageradamente elevado. O *phishing scam* segue sendo a principal metodologia de ataque através da engenharia social, particularmente, quando se trata de colaboradores de empresas de pequeno porte; devido a sua fragilidade de segurança estes ficam mais expostos e consequentemente mais vulneráveis. O acerto desta situação depende de reavaliações de políticas de segurança efetivas, assim como possíveis medidas de segurança necessárias, bem como, instruções de funcionários, sendo esta caracterizada por uma fase importante na intervenção contra esses tipos de riscos, especialmente, os que investem em erros que têm a sua origem nas atividades humanas.

4.4.1 Por que o *Spam* e o *Phishing Scam* funcionam?

O *spam* e o *phishing scam* se desenvolvem de variadas maneiras. Apesar disso, a forma de utilização mais eficaz acontece pela divulgação por intermédio do *e-mail*, baseada em relações (falsas) de confiabilidade e segurança. O *spam* e o *phishing scam* funcionam devido ao comportamento dos usuários, somado à inexperiência e desconhecimento técnico a respeito do assunto, ou seja, em virtude de tais características, juntamente com a ampliação da tecnologia mundial, que permite aos atacantes maiores alternativas de execução, os mesmos obtém sucesso em suas tentativas de propagação de *e-mails* não solicitados e/ou golpes virtuais. As vítimas do *spam* e do *phishing scam* são manipuladas mediante o recebimento de *e-mails* supostamente provenientes de órgãos de Estado e instituições de renome como, por exemplo, Tribunal Superior Eleitoral, Receita Federal, Banco do Brasil, entre outros.

4.4.2 *Internet Banking*

Fraudar informações em um servidor de uma organização comercial ou bancária não é uma atividade fácil. Assim, a fragilidade dos usuários está nos principais propósitos dos atacantes, uma vez que é mais simples investir em usuários comuns. A fim de obter vantagens, os atacantes utilizam o correio eletrônico, com linguagens que envolvem engenharia social e cuja finalidade é convencer o usuário a fornecer seus dados financeiros e pessoais. Em diversas situações, o usuário é estimulado a acessar uma página fraudatória ou a efetuar a instalação de códigos maliciosos, objetivando o furto de seus dados. Logo, é fundamental que usuários da *Web* se atentem aos *e-mails* recebidos e com a utilização de serviços de comércio eletrônico ou *Internet Banking*.

Internet Banking é uma forma de acesso ao serviço das instituições financeiras, em especial dos bancos. Por intermédio desse sistema, os usuários podem consultar saldos, pagar contas e realizar transferências bancárias. Dentre as várias formas de interação entre cliente e instituição o *Internet Banking* se mostra uma das mais ágeis, baratas e cômodas. O custo de uma transação bancária efetuada em agência é de aproximadamente 107% mais caro do que a mesma transação via *Internet Banking*. Daí o investimento das empresas nesse setor em constante ascensão. No entanto, é preciso utilizar esse recurso com segurança, para evitar fraudes. Segundo a cartilha.cert.br (2012), sites confiáveis de *Internet Banking* estabelecem conexões seguras quando informações bancárias ou pessoais são solicitadas, sendo o contrário, um forte indicio de golpes virtuais.

O uso do *Internet Banking* está se elevando consideravelmente, bem como os golpes aplicados no mesmo, tudo devido à larga utilização de tecnologias, que também promovem círculos favoráveis para atuações de atacantes pela *Web*. Assim, é possível observar que os usuários são os maiores afetados e que se faz necessário e urgente tomar medidas de informações, a fim de evitar crimes virtuais.

5 CONSIDERAÇÕES FINAIS

A comunicação pode ser atribuída como uma das maiores necessidades do ser humano. A mesma, atualmente, é classificada como indispensável no cotidiano, seja nas estruturas internas e funcionais de uma organização, seja em setores educacionais, científicos e governamentais, dentre outras características. Comunicar-se com outros indivíduos, por meio de contatos verbais, escritos, digitais ou mesmo ilustrados, desenvolve amplamente a sabedoria de todos os envolvidos nesse encadeamento. O aparecimento da Internet deu origem a um novo ambiente para o processamento da comunicação, ambiente este que diminuiu o distanciamento social e, hoje em dia, possibilita que os pontos mais extremos da globalização se comuniquem de forma eficiente.

A transformação da Internet é uma evolução gradativa e contínua. No decorrer do seu ciclo, do seu princípio até o momento, determinadas tecnologias se distinguiram e se sobressaíram, entre elas as mensagens eletrônicas*, e-mails* ou ainda correios eletrônicos. Os mesmos representam um dos canais de comunicação mais abrangentes e usados de forma universal por quem faz uso constante da Internet.

O protocolo de transferência de correios eletrônicos, conhecido como SMTP, foi fundamental propagador dessa tecnologia, em virtude da clareza de manuseio. No entanto, essa mesma facilidade, simultaneamente, se tornou o seu maior oponente. A ausência de ferramentas e instrumentos específicos de segurança da informação no protocolo possibilitou que o *e-mail* fosse usado para finalidades negativas e prejudiciais, tais como o *spam*. Embora o *spam* tenha surgido somente como mero aborrecimento, atualmente o mesmo acarreta inúmeras apreensões, por ser um dos predominantes canais eletrônicos para a realização de golpes vinculados à criminalidade.

Acompanhando o progresso da Internet, o *spam* tem conservado um desenvolvimento em sua quantidade estatística que impressiona. Nos dias de hoje, vasta parcela da circulação de mensagens eletrônicas na rede é identificada como *spam*. Os prejuízos financeiros das instituições que utilizam a Internet no dia a dia, derivados do *spam*, são admiráveis, sobretudo, nas empresas de pequeno porte,

uma vez que nestas empresas a estrutura organizacional é sempre mais deficitária e carente de recursos que garantam a segurança da informação.

Um bom exemplo é o estudo de caso realizado nas três empresas que mostra a dificuldade das pequenas organizações para conservar-se e sustentar-se mediante as constantes atualizações e concorrência do mundo moderno, uma vez que, de acordo com os resultados obtidos, é facilmente perceptível a elevada quantidade de *spams* recebidos no dia a dia, bem como a fragilidade da infraestrutura das mesmas, que as expõem e as deixam sujeitas às vulnerabilidades e aos ataques virtuais de todas as ordens.

Atualmente tenta-se prevenir o spam com o uso de equipamentos *anti-spam* que impossibilitem o aparecimento de mensagens desse gênero nas caixas postais eletrônicas de usuários finais e são encontradas diversas técnicas, todas reunidas em torno de um único propósito: evitar a disseminação de *spam*. No entanto, as pequenas empresas dificilmente investem em tais tecnologias, o que compromete ainda mais seu desenvolvimento, frente a concorrência e ao acirrado mercado de trabalho.

Nas empresas estudadas pode-se perceber que existe falta de investimento na área de Tecnologia da Informação, sobretudo, no que diz respeito à segurança dos dados. A fim de minimizar as possíveis despesas com mecanismos e ferramentas adequadas que garantam maior confiabilidade de circulação de informações, essas mesmas empresas buscaram soluções alternativas para tentar diminuir o impacto causado pelo *spam* em seus negócios. Buscaram, ainda, recursos com capacidade e preços inferiores ou ainda gratuitos, mas que, no entanto, não estão aptas para atender as demandas e necessidades das mesmas, oferecendo abertura aos ataques cibernéticos e ao acúmulo de *spams* nas caixas de entrada de seus funcionários, entre outras várias desvantagens e prejuízos.

Assim, com a atualização e o aperfeiçoamento constantes das técnicas *anti-spam,* o investimento de empresas de pequeno porte em tais ferramentas e recursos mínimos de segurança, e ainda o aumento do conhecimento aos usuários da quantidade de malefícios ocasionados pelo *spam* e seus derivados, seria sim viável uma diminuição e, até mesmo, erradicação dessa praga que insiste em permanecer

e prejudicar as relações sociais e profissionais entre os cidadãos. Foram elaborados também diversos objetivos, geral e específicos, todos eles demonstrados ao longo do trabalho, contribuindo dessa forma na otimização do assunto proposto.

No desfecho destas Considerações intenciona-se, como sugestão para futuros trabalhos que seja explanado e bem explorado o tema sobre o desenvolvimento e a implementação de um *software* livre, tendo como finalidade a contribuição com a diminuição de problemas originados do *spam,* maior possibilidade de segurança dos dados e o bloqueio de endereços indesejáveis, voltados exclusivamente para empresas de pequeno porte, visando diminuir o seu impacto.

6 REFERÊNCIAS

ABUSIX.ORG. **Luta contra as ameaças da rede**. Disponível em: < https://abusix.com/company.html> Acesso em: 20 mar. 2015.

ANTISPAM.BR. **O que é Spam?**. Disponível em: <http://antispam.br/conceito/> Acesso em: 20 mar. 2015.

APACHE SPAMASSASSIN. ***The Apache SpamAssassin Project***. (2015). Disponível em: <http://spamassassin.apache.org/>. Acesso em: 30 mar. 2015.

BRASIL. **Lei Complementar nº 123**, de 14 de dezembro de 2006. Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte; altera dispositivos das Leis nº 8.212 e 8.213, ambas de 24 de julho de 1991, da Consolidação das Leis do Trabalho - CLT, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, da Lei nº 10.189, de 14 de fevereiro de 2001, da Lei Complementar nº 63, de 11 de janeiro de 1990; e revoga as Leis nº 9.317, de 5 de dezembro de 1996, e 9.841, de 5 de outubro de 1999. Brasília: Senado Federal, 2006.

CARMONA, Lisandro. **TextSecure e o falso positivo do avast!**. Disponível em: < https://blog.avast.com/pt-br/tag/falso-positivo-pt-br/>. 2014. Acesso em: 30 mar. 2015.

CARNEIRO, Marcio R. de F. **Treinamento de UNIX (Linux/Solaris) para usuários do IME.** 2000. 76 p. Monografia – Instituto de Matemática e Estatística da Universidade de São Paulo, São Paulo: USP, 2000.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. CERT.BR. **Estatísticas de Notificações de Spam**. Disponível em: <http://www.cgi.br/pagina/comissoes-de-trabalho-antispam/ 121>. Acesso em: 20 mar. 2015.

_____. Cartilha de Segurança para Internet. **10. Uso seguro da Internet**. 2012. Disponível em: < http://cartilha.cert.br/uso-seguro/>. Acesso em: 20 abr. 2015.

COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.BR. **Comissões de Trabalho - Antispam**. Disponível em: < http://www.cgi.br/pagina/comissoes-de-trabalho-antispam/121>. Acesso em: 20 mar. 2015.

GRAHAM, Paul. ***A Plan for Spam***. Disponível em <http://www.paulgraham.com/spam. html>. 2002. Acesso em: 05 abr. 2015.

KARASINSKI, Eduardo. **A história do email**. Disponível em < http://www.tecmundo.com.br/web/2763-a-historia-do-email.htm>. 2009. Acesso em: 05 abr. 2015.

KLENSIN, John C. ***Simple Mail Transfer Protocol***. Disponível em: <http://www.ietf.org/rfc/rfc2821.txt>. 2001. Acesso em: 21 maio 2015.

LEVINE, John R. **E-mail para leigos**. 1. ed. São Paulo: Berkeley, 1997.

LEVITT, Mark. ***What You Can and Should Do About the Rising Cost of Spam.*** Disponível em <http://www.surfcontrol.com/general/assets/whitepapers/rising_cost_of_spam.pdf>. 2004. Acesso em: 15 abr. 2015.

LIMA, Gustavo. **Soluções de Anti-spam: qual é a melhor?** Disponível em: <http://blog.corujadeti.com.br/solucoes-de-anti-spam-qual-e-a-melhor/>. 2010. Acesso em: 30 mai. 2015.

MATIAS, Alberto B., LOPES, Fábio J. **Administração financeira nas empresas de pequeno porte**. 1. ed. São Paulo: Manole, 2002.

NATIONAL CYBER SECURITY ALLIANCE (2015). In. SOLO NETWORK. **Kaspersky publica estudo sobre crimes virtuais e as pequenas empresas.** Disponível em: <http://solonetwork.com.br/news/15-01-28/kaspersky_publica_estudo_ sobre_crimes_virtuais_e_as_pequenas_empresas.aspx>. 2015. Acesso em: 5 mar. 2015.

NEWMAN, M. E. J.; FORREST, Stephanie; BALTHROP, Justin. *Email Networks and the Spread of Computer Viruses.* ***Physical Review*** E 66. 2002 Disponível em: < https://www.cs.unm.edu/~forrest/publications/email-viruses-02.pdf>. 2002. Acesso em: 20 abr. 2015.

ORMAN, Hilarie. ***The Compleat Story of Phish*****.** Internet Computing. 2013. Disponível em: <http://www.computer.org/csdl/mags/ic/2013/01/mic2013010087-abs.html> Acesso em: 16 maio 2015.

PADRON, Juliana. **Por que seu email marketing não deve ter apenas imagens.** Disponível em: < https://templateria.com/blog/templates/por-seu-email-marketing-nao-deve-ter-apenas-imagens/>. 2013. Acesso em: 16 abr. 2015.

READER'S DIGEST SELEÇÕES. **A história do inventor do Hotmail**. Disponível em <http://www.agr.feis.unesp.br/hotmail.htm>. 2001. Acesso em: 05 abr. 2015.

RESNICK, Philip. ***Internet Message Format***. Disponível em <http://www.ietf.org/rfc/rfc2822.txt>. 2001. Acesso em: 21 maio 2015.

SCHRYEN, G. **Anti-Spam Measures:** Analysis and Design. 1. ed. São Paulo: Springer, 2007.

SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS – SEBRAE. **Classificação das micro e pequenas empresas**. Disponível em < http://www.biblioteca.sebrae.com.br>. 2015. Acesso em: 21 maio 2015.

SIPIOR, J.C. *Should spam be on the menu?* ***Communications of the ACM***, June 2004, Vol. 47, N.6., 59.

SPAMCOP.NET. **Estatísticas de Spam**. Disponível em: < https://www.spamcop.net/spamstats.shtml> Acesso em: 20 mar. 2015.

SOLO NETWORK. **Kaspersky publica estudo sobre crimes virtuais e as pequenas empresas**. Disponível em: < http://solonetwork.com.br/news/15-01-28/kaspersky_publica_estudo_sobre_crimes_virtuais_e_as_pequenas_empresas.aspx> . 2015. Acesso em: 5 abr. 2015a.

_____. **O crime virtual atinge uma grande parcela das pequenas empresas**. Disponível em: < http://solonetwork.com.br/downloads/o-crime-virtual-atinge-uma-grande-parcela-das-pequenas-empresa-kaspersky-solo-network.pdf>. 2015. Acesso em: 5 mar. 2015b.

SOURCEFORGE. ***Anti-Spam SMTP Proxy Server***. 2013. Disponível em: <http://sourceforge.net/p/assp/wiki/Main_Page/>. 2015. Acesso em: 30 mar. 2015.

TEIXEIRA, Renata C. **Combatendo o Spam:** Aprenda a Evitar e Bloquear E-mail Não Solicitados. 1. ed. São Paulo: Novatec, 2004.

_____. **O Pesadelo do Spam**. Disponível em <http://www.rnp.br/newsgen/0101/spam.html>. 2001. Acesso em: 16 abr. 2015.