

## **Mensagens Eletrônicas: Heroína ou Vilã**

ÁREA:

### **9. Sistemas de informação e comunicação industrial**

**Luiz Carlos de Oliveira**

Lco2001@gmail.com

Fundação CEFETMINAS

+55 31 992731998

Rua Zurick, 1205/301 CEP 30421-112 – Nova Suiça – Belo Horizonte MG

**Waldri dos Santos Oliveira**

CEFET-MG

[wladri.so@gmail.com](mailto:wladri.so@gmail.com)

(31)99745-3974

Rua das princesas, 320 D, Vila Oeste – Belo Horizonte – MG

**Resumo.** *O tempo dedicado às mensagens eletrônicas está se tornando cada vez maior e estas estão totalmente inseridas em nosso cotidiano. Os benefícios, abusos, complexidades e armadilhas inerentes a sua utilização, tornam as ferramentas usadas uma origem de constante monitoramento e estudo. Os desafios enfrentados por quem se utiliza de meios eletrônicos para se comunicar são grandes. O ambiente está em constante processo de mudanças e atualizações. Mensagens não solicitadas, boatos, propaganda, softwares maliciosos, pornografia e a preocupação com a segurança permeiam o ambiente dos usuários que necessitam fazer uso de ferramentas relacionadas às mensagens eletrônicas, tanto para o trabalho quanto para o lazer, influenciando diretamente a qualidade de suas vidas e atividades profissionais.*

**Palavras-chave:** *Mensagens eletrônicas, e-mail, Produtividade, vulnerabilidade.*

## 1. INTRODUÇÃO

O homem está cada vez mais conectado. O tempo que passamos na frente dos computadores, *tablets*, smartphones e assemelhados, fazendo uso de ferramentas de gerenciamento de mensagens e redes sociais é crescente. Estamos aqui falando de mensagens eletrônicas e o impacto delas em nossas vidas.

As horas dispendidas com usos excessivos e não regrados de softwares e hardwares sempre nos trazem prejuízo. São ferramentas necessárias em nosso cotidiano, mas podem nos trazer grandes transtornos.

O fato de nosso tempo ser limitado, e cada vez menos disponível devido à agitação e as obrigações da vida urbana, influencia de forma diferente as pessoas. Sabemos que o uso indiscriminado de mensagens pode levar ao vício, principalmente pela abundância de mídias e canais as quais são oferecidos, como computadores, tablets, celulares e outros eletrônicos (os chamados e-gadgets) e este vício torna-se preocupante não só pelas coisas que fazemos em excesso por ele, mas também, pelas coisas de deixamos de fazer por estarmos dedicados a ele.

Existe um abuso no uso de mensagens eletrônicas. Até uma grande operadora de telefonia, principal “beneficiada” pela troca de mensagens, lançou uma campanha de conscientização sobre a hora certa para se enviar mensagens (HERZOG, 2013), que com certeza não é quando estamos ao volante. A gigante de pesquisas Google criou um programa para seus funcionários que se chama “Search inside yourself”, com tradução literal, busque dentro de si mesmo, que conscientiza seus funcionários a ter momentos de desconexão e meditação (KELLY, 2012), com utilização de aparelhos de ginástica, ambientes relaxantes e de lazer.

O site de pesquisas Google está totalmente presente em nossas vidas. Fonte inesgotável de informação, muitas vezes errôneas e abundantemente excessivas. Tenho um filho de 9 anos e, certa vez, estava tentando dar independência a ele em questionamentos comuns do dia a dia, tipo “o que é e-mail?”, “como surgiram os dinossauros?”, etc. Tive infelizmente de dar uma parada ao propagandear para ele o Google, tal volume de informação errada, inconveniente, ampla, contraditória, enfim, era preciso mais discernimento para digerir estas informações, era preciso ter um ceticismo crítico e sadio.

## 2. DESENVOLVIMENTO

### 2.1 MENSAGENS ELETRÔNICAS EM REDES DE COMPUTADORES (E-MAIL)

E-mail ou “*electronic mail*” é um serviço disponível na internet que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação. Aceita a comunicação entre pessoas utilizando o meio eletrônico. Dos serviços que a internet oferece, o e-mail é um dos que são mais utilizados, por ser uma forma rápida e barata de comunicação e por meio dele é possível enviar arquivos de texto, músicas, imagens, vídeos e até programas.

O termo “e-mail” é aplicado tanto aos sistemas que utilizam a Internet e que são baseados nos protocolos POP3, IMAP e SMTP, como aqueles sistemas conhecidos como intranets, que permitem a troca de mensagens dentro de uma empresa ou organização e que são, normalmente, baseados em protocolos proprietários.

Os endereços de e-mail são compostos por: Nome de usuário: ex: Luiz, o @: chama-se arroba, vêm do inglês, lê-se “at” e significa em algum lugar, o Servidor de e-mail, é o nome do servidor de e-mail que torna acessível este serviço de correio eletrônico ao usuário, geralmente o nome do site que você está acessando, tipo @gmail ou @hotmail, a extensão referente à categoria do servidor, “.com” para comerciais e “.org” para organizações, e a extensão referente a origem do servidor, como “.br” para sites brasileiros ou “.jp” para sites japoneses, assim, um exemplo de nomes de e-mails seria luiz@gmail.com, luiz@jovempan.com.br, etc.

Assim como ao enviar uma carta, para enviar um e-mail é necessário ter um emissor e um destinatário. Ao enviar o e-mail para uma pessoa, a mensagem irá viajar, em forma de pacotes por várias

redes, onde no final será remontada pelo protocolo TCP. Existem softwares que são utilizados por pessoas mal intencionadas com a finalidade de interceptar esses pacotes e serem lidas por eles. Por isso, é importante tomar medidas preventivas para que as informações não sejam lidas por terceiros.

Um fato interessante além do número de contas de e-mail em todo o mundo continua a crescer a um ritmo ligeiramente mais rápido a cada ano, é também o número de contas por usuário cresce em média saltando de 1,6 contas por usuário em 2014 para 1,7 em 2015 e a previsão que continue crescendo. (THE RADICATI GROUP). Com isso surge a necessidade de tratar de várias contas simultaneamente.

Existem softwares que são clientes de e-mail e dão opções de tratamento mais personalizadas que os atuais navegadores de internet. Com eles é possível colocar uma assinatura personalizada, tratar imagens e formatar o texto de maneira simples. Alguns deles também possuem recursos mais avançados que possibilitam filtrar lixo eletrônico, utilizar antivírus para verificar e-mails recebidos e bloquear e-mails, de acordo com o desejo do dono da conta.

Em 2014, segundo a Radicati Group, tínhamos tráfego de 196.3 bilhões de mensagens de e-mail por dia até, hoje passamos para 205.6 de mensagens enviadas e recebidas diariamente. Grandes empresas fazem campanha para redução do tráfego de e-mail, que além de gerar custos extras como consumo de energia, prejudica a velocidade das tomadas de decisões, pois boa parte do que é tratado via e-mail poderia ser tratado pessoalmente, logo serem resolvidas mais rapidamente. (THE RADICATI GROUP)

## 2.2 MENSAGENS ELETRÔNICAS SEM REDES DE COMPUTADORES

As mensagens de texto ou "Short Messages Services" (SMS), bem como as MMS "Multimedia Messaging Service" ou serviço de mensagens multimídia se popularizaram no Brasil com o nome de torpedo. São mensagens muito úteis e sua utilização tem sofrido forte concorrência de aplicativos específicos de mensagens, que fazem uso da internet, tais como o Whatsapp, Viber, etc, que oferecem vantagens adicionais. Entre essas vantagens, podemos citar o compartilhamento de arquivos, o menor custo e integração com outras ferramentas e aplicativos disponíveis no celular.

## 2.3 MENSAGENS ELETRÔNICAS TROCADAS PELAS REDES SOCIAIS E MÍDIAS SOCIAIS

No ano de 2003, vários embriões de redes sociais surgiram. O LinkedIn, que funciona até hoje com foco em profissionais, o Tribe.net, que permitia aos membros criar uma "tribo" em torno de um interesse específico, o Friendster, criado no ano anterior crescia rapidamente mas enfrentava problemas técnicos desde a sua criação. O MySpace, também criada em 2003, fornecia uma rede interativa de fotos, blogs e perfis de usuário, com um sistema interno de e-mail, fóruns e grupos. A rede social Sixdegrees ficará obsoleta, dando espaço para o surgimento de um concorrente de peso.

Em 2004, seriam lançadas as redes Orkut e o Facebook. Neste ambiente competitivo, várias destas redes funcionam até hoje, mas sem dúvida o Facebook é a principal, envolvendo todo o mundo, com mais de um bilhão de usuários.

O que todas estas redes possuíam e possuem em comum a capacidade de troca de mensagens, criação de grupos de interesse comum, etc.

Na rede de livrarias Leitura a utilização do aplicativo Whatsapp para troca de mensagens corporativas surgiu naturalmente a alguns anos. O software, de fácil configuração e utilização, facilitou o seu surgimento e consolidação. Hoje a rede possui dezenas de grupos colaborativos, como:

- Supervisores de Papelaria, para troca de mensagens sobre compra de produtos, negociações e mensagens diversas.
- Supervisores de Papelaria, para troca de mensagens sobre compra de livros, negociações e mensagens diversas.
- Gerentes, para mensagens de eventos, compartilhar experiências e dúvidas gerenciais.
- grupo de vitrines, com fotos e temas relevantes abordados na decoração e exposição, etc.

Contudo, ainda existe uma troca excessiva de mensagens, por vezes desnecessária, o que atrapalha o andamento dos grupos. Mensagens desnecessárias são perda de tempo e dinheiro, por vezes resultando em abandono do grupo por usuários de relevante importância para o bom andamento dos trabalhos. Uma boa discussão seria quando e como melhor poderemos fazer uso destas mensagens e como nos prevenir de seu uso como distração, bem como quais procedimentos adotar para banir o uso inapropriado e lidar com pessoas que o fazem.

## 2.4 Seguranças da informação relacionada com as mensagens eletrônicas

### 2.4.1 Spam

O termo *SPAM* possui várias origens. Deste “*Sending and Posting Advertisement in Mass*”, que significa enviar e postar mensagens em massa, até a sua associação a uma marca de carne suína americana SPAM. O termo pode ser melhor explicado não como uma mensagem comercial não solicitada, mais sim uma mensagem automatizada não autorizada (GRAHAN, p.65). As razões para isso são bem simples. Se um vizinho seu fica sabendo que você está interessado em comprar uma bicicleta usada em boas condições e lhe manda uma oferta por e-mail, você ficaria feliz. Mesmo assim a mensagem seria comercial e não solicitada. Outra questão seria receber um e-mail apoiando um político ou uma causa contra o racismo. Este conteúdo seria spam assim como a promessa de acesso gratuito a um site pornográfico. Estes e-mails não desejados e automatizados que acabam enchendo a caixa de e-mail seriam, portanto, spam.



**Figura 1- Origem Spam (lata)**  
Fonte: <http://www.ribasmith.com/>

Antes da popularização do e-mail, os comerciantes investiam tempo e dinheiro para anunciar seus produtos em jornais, revistas ou de cliente em cliente, mas descobriram que é possível fazer a mesma coisa, em um período menor de tempo com um alcance maior. Então passaram a utilizar o e-mail como meio de anunciar suas ofertas.

Apesar de parecer uma atividade inofensiva, existem alguns problemas que os spams podem causar:

**Perda de produtividade:** um funcionário geralmente usa o e-mail para negócios da empresa. Os softwares clientes de e-mail fazem download de todos os e-mails recentes.

Um usuário doméstico também acessa os e-mails para ver assuntos de seu interesse. Porém, quanto maior o número de spams recebidos, maior é o tempo de download dos e-mails e o tempo para o usuário descobrir quais são os e-mails reais, o que resulta na perda de produtividade.

Existem alguns filtros *anti-Spam* disponíveis, alguns pagos, outros gratuitos que ajudam a amenizar a quantidade de spams recebidos pelos usuários. Porém, algumas vezes, erros acontecem e esses filtros acabam por excluir e-mails autênticos, confundindo-os com spams. O usuário, outra vez precisará dispor de tempo para tentar recuperar esses e-mails excluídos por engano.

Conteúdo ofensivo: Alguns spams podem trazer conteúdos ofensivos, como fotos ou anúncios pornográficos que ao serem abertos podem trazer constrangimentos e até mesmo demissões.

Os tipos de spams mais comuns são:

1. Correntes: são e-mails enviados contando uma história, muitas vezes supersticiosa, que finaliza pedindo para que o usuário repasse a mensagem a vários amigos com a finalidade de não quebrar a corrente. No conteúdo de algumas mensagens é dito que se o usuário não repassar o e-mail para uma quantidade X de pessoas, algo de ruim poderá acontecer. Em outras, é dito que se a mensagem for repassada a uma quantidade Y de amigos, algo bom irá acontecer. Então, por medo ou com a pretensão de receber algum benefício, as pessoas compartilham esse tipo de corrente, cooperando com o aumento do número de mensagens indesejadas.

2. Propagandas: são e-mails geralmente enviados por algumas empresas, podem conter propaganda de algum evento, ou de produtos e serviços que ela oferece. São conhecidos pela sigla UCE (Unsolicited Commercial E-mail).

3. Pornografia: são e-mails com conteúdo adulto apelativo que na maioria das vezes causam constrangimentos aqueles que o recebem. Alguns dos problemas é o recebimento desse tipo de e-mail por crianças e o de propagação de pedofilia. No primeiro caso, os pais ou responsáveis devem supervisionar as atividades das crianças e conscientizá-las dos perigos da internet. No segundo caso, ao receber mensagens com pedofilia, deve-se denunciar a órgãos responsáveis pelo combate a esse crime, como a Polícia Federal.

4. *Phishing Scan*: Principais perigos existentes na internet acarretam grandes transtornos até mesmo prejuízos financeiros. Geralmente chega via e-mail e utiliza-se de “iscas” para atrair a atenção de uma pessoa e fazê-la realizar alguma ação. Normalmente, mensagens deste tipo são criadas para parecerem ter sido emitidas por instituições sérias, como bancos, operadoras de telefonia ou órgãos de governo, embora também possa se passar por pessoas. As ações executadas pelos usuários ao receberem uma mensagem do tipo phishing scan determinarão o próximo passo a ser tomado pelo hacker. Por exemplo, se o usuário apenas responder esta mensagem já indicará ao emissor que o e-mail é ativo e poderá coloca-lo em listas para receber propaganda. Se o usuário além de confirmar que o e-mail é ativo e atualizar dados bancários ou enviar senhas os prejuízos serão maiores.

Ninguém está livre de spams, mas existem medidas que podem ser tomadas para evitar que eles sejam propagados e distribuídos em larga escala.

Usar um filtro *AntiSpam* é uma alternativa válida para ajudar a diminuir o número de e-mails indesejados recebidos. A forma que ele age é bem simples. Primeiramente ele filtra as mensagens, as que detecta como sendo spam, envia para uma pasta específica de lixo eletrônico. Embora seja um programa bem útil e venha sendo aprimorado no decorrer dos anos, não está livre de erros. Em alguns casos, pode acontecer do filtro enviar uma mensagem legítima para a caixa de lixo eletrônico. Por conta disso, o usuário deve ficar atento para não perder e-mails importantes. Ao verificar os e-mails recebidos, constatando que foi recebido um spam, deve-se configurar o software cliente de e-mail para não receber mais e-mails daquele remetente. Se for possível, marca mensagem como sendo spam.

Em cadastros de certos sites, existe uma opção relacionada a receber e-mails com atualizações de notícias e inovações do site. Porém, esses e-mails são enviados com muita frequência e acabam tendo o mesmo efeito que os spams. Para cancelar esse tipo de e-mail é necessário saber se foi feito algum tipo de cadastro no site. Caso seja confirmado, é possível enviar um e-mail para os responsáveis pelo e-mail marketing solicitando que não desejam mais receber esse tipo de e-mail. Alguns desses e-mails podem vir com um link para que o usuário clique nele caso não queira mais receber os e-mails. Nesse caso, é necessário ter cuidado, pois alguns “spammers” – pessoas que enviam spam- enviam essa opção de cancelar emails somente para saber se o e-mail que eles enviaram é de um usuário ativo. Então, ao clicar na opção de cancelamento, o usuário na verdade estará indicando ao “spammer” que o e-mail está ativo. Em último caso, é possível em alguns softwares clientes de e-mail indicar que o remetente é um spam e acionar a opção de bloquear mensagens desse remetente.

Ao enviar e-mail para uma lista de contatos, determinadas pessoas tem o costume de deixar a lista visível permitindo que todos que receberem o e-mail vejam para quais pessoas ele foi enviado. Um “*spammer*” pode ter acesso a essa lista de e-mails e passar a incomodar os usuários com e-mails indesejados.

Por conta disso, deve-se ao enviar e-mails a vários contatos, usar a opção “cópia oculta”, para evitar que pessoas não autorizadas tenham acesso a lista de e-mails.

Ao receber mensagens contendo promoções, brindes, vantagens ou informando um prêmio é sempre bom ter cautela. Caso seja algo de interesse, deve-se procurar saber se a fonte é confiável. Caso haja dúvida se é um e-mail confiável, pode-se fazer uma pesquisa em sites de busca para tentar descobrir se as “ofertas” são reais. No caso de ser spam, possivelmente será visto alguma notícia relacionada esclarecendo.

Existem vários aliados na luta contra spams. Podemos citar o TMDA (Tagged Message Delivery Agent) que funciona tentando diminuir ou até mesmo eliminar o recebimento de spams em sua caixa postal. Sua principal desvantagem é que sua tecnologia em baseada em servidores, portanto não funciona em desktops. Alguns servidores de e-mail utilizam esta tecnologia, como o UOL. O TMDA baseia-se basicamente em lista negras, e-mails de origem indesejadas, listas brancas, e-mails confiáveis, confirmação, permitindo que remetentes desconhecidos possam lhe enviar mensagens, desde que você posse por um processo de confirmação e endereços previamente conhecidos (tagged), com propósitos especiais, ex. uma campanha eleitoral, por exemplo.

#### 2.4.2 HOAX

Dá-se o nome de hoax (“embuste” numa tradução literal, ou farsa) a histórias falsas recebidas por e-mail, onde há uma tentativa de fazer com que os destinatários repassem o e-mail recebido para todos os contatos. Alguns consideram como sendo um vírus social, pois ele se utiliza da boa fé das pessoas para se reproduzir. Existem dois tipos de hoax mais comuns: Os difamatórios e os filantrópicos.

O hoax difamatório é um tipo de mensagem que traz fatos inverídicos sobre uma empresa, instituições, produtos ou necessidades com o objetivo de sensibilizar pessoas com relação a um determinado. É também utilizado por algumas empresas para manchar a imagem das empresas concorrentes.

O hoax filantrópico relata histórias de pessoas com problemas de saúde, passando dificuldades financeiras ou usam catástrofes naturais para sensibilizar as pessoas a contribuírem financeiramente para certas instituições, quando na verdade, o dinheiro é entregue a outra pessoa. É comum nesse tipo de e-mail informar que a cada pessoa que for enviado o e-mail, uma instituição irá doar um valor em dinheiro pela causa. O conteúdo é apelativo e mexe com o emocional de quem recebe a mensagem. A grande maioria das pessoas fica emocionada e na tentativa de querer ajudar, repassam esse conteúdo para outras pessoas e assim, várias pessoas acabam contribuindo com a disseminação de spams pelo mundo.

Os “Hoaxes” são criados basicamente para “chamarem atenção” e seu alvo são os usuários básicos e na maioria das vezes distraído, ingênuo ou desavisado.

#### 2.4.3 PROGRAMAS MALICIOSOS (MALWARES)

As mensagens eletrônicas podem vir acompanhadas de softwares maliciosos, os chamados “*Malwares*”. Podem ser recebidos por e-mail, redes sociais ou mensagens instantâneas. A lista destes programas é vasta, mas especificamente relacionadas a mensagens, podemos destacar:

Vírus – “Software” ou parte de um programa malicioso, que se propaga, inserindo cópias de si mesmo e se tornando parte de outros programas ou arquivos.

Worm – É um vírus mais poderoso, capaz de se auto propagar, enviando cópias de si mesmo.

Bot - Diminutivo de “robot”, também conhecido como Internet “bot” ou “web robot”, é uma aplicação concebida para simular ações humanas repetidas vezes de maneira padrão. O computador se transforma em escravo do invasor, executando ações previamente determinadas

Spyware – Programa espião, utilizado para monitorar as atividades do dispositivo invadido.

Adware – Exibe anúncios “ad”, sem a permissão do usuário

Trojan – Ou Cavalo de Tróia, é um programa que além de executar as funções para as quais foi projetado, também executa outras funções maliciosas, sem a permissão do usuário.



### 3. CONCLUSÃO

A importância crescente e a penetração de novas ferramentas de trocas de mensagens eletrônicas no cotidiano das pessoas influencia diretamente o comportamento destas mesmas pessoas em casa e no trabalho, acarretando em perda de produtividade e riscos de segurança digital ou até mesmo distrações em ambientes de trabalho como indústrias ampliando os riscos de acidentes.

O tempo gasto e o uso concomitante de diversos tipos de plataformas de “softwares” e “hardwares” para a troca de mensagens eletrônicas é culpa da instantaneidade, característica principal da geração atual, com que as trocas acontecem, implicando em superficialidade do conteúdo da informação ou sua má interpretação. O ser humano sempre teve necessidade de se comunicar e isto nunca esteve tão fácil como agora, a ponto de se comunicar não mais o essencial, o crescimento da quantidade de informação veiculada interfere negativamente na qualidade da mesma.

É preciso que os usuários e os gestores destes recursos fiquem em constante monitoramento de suas atividades, com o intuito de não prejudicar sua vida profissional e pessoal, aproveitando seu tempo e os recursos as tecnologias de comunicação e informação de maneira favorável à sua produtividade e qualidade de vida, não deixando que o seu uso se transforme em vício ou comportamento inadequado ou vítimas do uso inadequado desses recursos.

### 4. REFERÊNCIAS

GRAHAN, Paul. **Hackers & Painters**. O’Reilly Media. Sebastopol, CA. 2010. 271p.;

HERZOG, Werner, **Watch Werner Herzog's harrowing documentary on texting and driving**. Disponível em <<http://www.theverge.com/2013/8/9/4604962/werner-herzog-from-one-second-to-the-next-texting-and-driving-documentary>>. Acesso em 11/04/2014.;

KELLY, Caitlin. O.K., Google, **Take a Deep Breath**. Disponível em:<[http://www.nytimes.com/2012/04/29/technology/google-course-asks-employees-to-take-a-deep-breath.html?pagewanted=all&\\_r=0](http://www.nytimes.com/2012/04/29/technology/google-course-asks-employees-to-take-a-deep-breath.html?pagewanted=all&_r=0)>. Acesso em 15/08/2015.;

THE RADICATI GROUP, INC. **Email Statistics Report, 2015-2019**, March 2015. A TECHNOLOGY MARKET RESEARCH FIRM PALO ALTO, CA, USA. Disponível em: <<http://www.radicati.com/>>. Acessado em 14/11/2015.;

### 5. DIREITOS AUTORAIS

Os autores são os únicos (e inteiramente) responsáveis pelo conteúdo deste trabalho.

Electronic messages: Heroin or Villain.

*Seminário Nacional de Sistemas Industriais e Automação*  
*Belo Horizonte, MG*



**Abstract.** *The time devoted to electronic messages is becoming increasing and they are fully inserted into our everyday lives. The benefits, abuses, and complexities inherent in its use traps, make the tools you use a source of constant monitoring and study. The challenges faced by those who use electronic means to communicate are great. The environment is in constant process of changes and updates. Unsolicited messages, rumors, propaganda, malicious software, pornography and concern for the safety permeate the environment of the users who need to make use of tools related to electronic messages, both for work and for leisure, directly influencing the quality of their lives and professional activities.*

**Keywords:** Electronic messages, e-mail, productivity, vulnerability.