FACULDADE DE TECNOLOGIA DE SÃO PAULO

**LEANDRO FARIAS DOS SANTOS ABREU**

# A Segurança da Informação nas Redes Sociais

**São Paulo**

**2011**

FACULDADE DE TECNOLOGIA DE SÃO PAULO

**LEANDRO FARIAS DOS SANTOS ABREU**

# A Segurança da Informação nas Redes Sociais

Monografia submetida como exigência
parcial para a obtenção do Grau de
Tecnólogo em Processamento de Dados
Orientador: Professor Mestre Gabriel Issa Jabra Shammas

**São Paulo**

**2011**

## Agradecimentos

Agradeço primeiramente ao Professor Gabriel pela confiança depositada em mim e pela orientação para o desenvolvimento desse trabalho. Também agradeço aos colegas e amigos por sempre me apoiarem e ao constante incentivo para dar continuidade ao trabalho. Diego, Erick, Felipe, Gustavo e Roberto, obrigado.

**Resumo**

As redes sociais na Internet, através dos sites de relacionamento, contém inúmeras informações compartilhadas entre seus usuários, os quais disponibilizam seus dados, alguns deles sensíveis, e estes ficam à disposição de outros membros da rede. É como se estes usuários, ou a maioria deles, nem se quer tem em mente do conteúdo que consciente e incoscientemente está sendo distribuíndo, e desse modo não levam em conta a importância de se manter um meio seguro para proteger seus dados sensíveis de pessoas e códigos mal intencionados na Web. Este trabalho visa mostrar como chegar ao nível de equilíbrio entre estar presente em redes sociais na Internet e ao mesmo tempo seguro, de um modo que se faça bom uso das mídias sociais sem se expor demasiadamente, protegendo as informações com a aplicação de técnicas e métodos práticos de segurança da informação, sabendo os tipos de ameças comuns que podem ser encontradas durante o uso da Internet, e assim evitadas.

**Palavras-chave**: Segurança da Informação. Internet. Redes Sociais. Ameaças. Privacidade. Geolocalização. Mídias Sociais. Cyberstalking.

**Abstract**

Internet social networking websites contains a wealth of shared information among its users, who provide their personal data, some of them sensitive, and it becomes available to all other social network members. It seems like these users, or most of them do not even have in mind that these information is being conscious and unconsciously distributed, and then they do not bear in mind the importance of maintaining a secure environment to protect their sensitive data from people and malicious code on the Web. This paperwork aims to show how to reach balance between being part of social networking websites while keep information secure, by making good use of social media without exposing yourself too much, protecting information by applying techniques and practical methods of information security, and keeping in mind common threats that can be found while using the Internet and therefore, can be avoided.

**Keywords**: Information Security. Internet. Social Networing. Threats. Privacy. Geolocation. Social Media. Cyberstalking.

**Lista de Ilustrações**

## Lista de Tabelas

**Sumário**

# 1 Introdução

Encontramo-nos na era da informação, com a Internet cada vez mais ao alcance de todos. Com a facilidade de acesso à rede[1], adicionada à mobilidade[2] da Internet (Tabelas 1 e 2) - cada vez mais independente do microcomputador, dada a evolução da tecnologia dos aparelhos de telefone móveis e outros dispositivos -, a informação está sendo dispersada segundo a segundo, de praticamente qualquer lugar pelos usuários conectados às redes sociais.

| Percentual (%) | | Sim | Não | NS/NR |
|---|---|---|---|---|
| **TOTAL BRASIL** | | **27** | **73** | **-** |
| **ÁREA** | **URBANA** | 31 | 69 | - |
| | **RURAL** | 6 | 94 | - |
| **REGIÕES DO PAÍS** | **SUDESTE** | 36 | 63 | - |
| | **NORDESTE** | 11 | 89 | - |
| | **SUL** | 30 | 70 | - |
| | **NORTE** | 14 | 86 | - |
| | **CENTRO-OESTE** | 33 | 67 | - |
| **RENDA FAMILIAR** | **Até 1 Salário Mínimo** | 3 | 97 | - |
| | **1 SM - 2 SM** | 13 | 87 | - |
| | **2 SM - 3 SM** | 30 | 69 | 1 |
| | **3 SM - 5 SM** | 48 | 51 | - |
| | **5 SM - 10 SM** | 70 | 30 | - |
| | **10 SM ou +** | 86 | 14 | - |
| **CLASSE SOCIAL** | **A** | 90 | 10 | - |
| | **B** | 65 | 34 | - |
| | **C** | 24 | 76 | - |
| | **DE** | 3 | 97 | - |

**Tabela 1 – Proporção de domicílios com acesso à Internet (Brasil)**

[1] NIC.br. Acesso às Tecnologias da Informação e da Comunicação (TIC). CETIC.br, Brasil, nov. 2010. Disponível em <http://www.cetic.br/usuarios/tic/2010-total-brasil/rel-geral-04.htm>. Acesso em: 01 out. 2011.

[2] NIC.br. Acesso sem Fio (Uso do Celular). CETIC.br, Brasil, nov. 2010. Disponível em <http://www.cetic.br/usuarios/tic/2010-total-brasil/rel-semfio-01.htm>. Acesso em: 01 out. 2011.

| Percentual (%) | | Sim | Não | NS/NR 2 |
|---|---|---|---|---|
| **TOTAL BRASIL** | | **79** | **21** | **-** |
| **ÁREA** | **URBANA** | 81 | 19 | - |
| | **RURAL** | 65 | 35 | - |
| **REGIÕES DO PAÍS** | **SUDESTE** | 78 | 22 | - |
| | **NORDESTE** | 76 | 24 | - |
| | **SUL** | 79 | 21 | - |
| | **NORTE** | 80 | 20 | - |
| | **CENTRO-OESTE** | 86 | 14 | - |
| **FAIXA ETÁRIA** | **De 10 a 15 anos** | 78 | 22 | - |
| | **De 16 a 24 anos** | 91 | 9 | - |
| | **De 25 a 34 anos** | 90 | 10 | - |
| | **De 35 a 44 anos** | 85 | 15 | - |
| | **De 45 a 59 anos** | 75 | 25 | - |
| | **De 60 anos ou mais** | 51 | 49 | - |
| **RENDA FAMILIAR** | **Até 1 Salário Mínimo** | 60 | 40 | - |
| | **1 SM - 2 SM** | 78 | 22 | - |
| | **2 SM - 3 SM** | 83 | 17 | - |
| | **3 SM - 5 SM** | 88 | 12 | - |
| | **5 SM - 10 SM** | 94 | 6 | - |
| | **10 SM ou +** | 91 | 9 | - |
| **CLASSE SOCIAL 3** | **A** | 96 | 4 | - |
| | **B** | 91 | 9 | - |
| | **C** | 82 | 18 | - |
| | **DE** | 61 | 39 | - |

**Tabela 2 – Proporção de indivíduos que usaram telefone celular (set-nov 2010)**

Isso vem gerando um volume imenso de compartilhamento de informações através da Internet - que hoje já deve passar dos 500 bilhões de gigabytes de conteúdo[3] - quantidade digital que se fosse impressa e armazenada em livros, formariam uma pilha que se estenderia dez vezes a distância da Terra à Plutão.

[3] WRAY, Richard. Internet data heads for 500bn gigabytes. The Guardian, Reino Unido, 18 mai. 2009. Disponível em <http://www.guardian.co.uk/business/2009/may/18/digital-content-expansion>. Acesso em: 01 out. 2011.

Quando surgiram e se popularizaram as redes sociais no Brasil – Figura1 (em meados de 2004 com a rede social Orkut)[4], houve alguma resistência da parte dos usuários, quanto a disponibilizarem seus dados pessoais para todos os participantes da rede.


**Figura 1 – Redes sociais no Brasil (jul 2004)**

Porém, a partir do momento em que os usuários se sentiram confiantes, incentivados por outros usuários e motivados pela sensação de estar em constante contato com colegas distantes, ou estabelecer grupos de interesse para troca de experiências, as redes começaram a crescer em conteúdo e número de usuários, e assim, surgiram preocupações quanto à segurança de cada um, a necessidade de se conhecer os riscos associados a esse novo ambiente, e a segurança da informação compartilhada.

## 2 A Segurança da Informação

Entende-se por informação qualquer conteúdo ou conjunto de dados com valor para determinada organização ou pessoa, sendo esta, um recurso de extremo valor na sociedade atual. Com a utilização de sistemas informatizados conectados e integrados através das redes, as informações armazenadas e trafegadas dentre estes estão, de uma forma ou de outra,

[4] Google Insights. Web Search Interest. Brasil, nov. 2010. Disponível em <http://www.google.com/insights/search/#q=facebook.com%2Corkut.com%2Ctwitter.com&geo=BR&cmpt=q>. Acesso em 20 nov. 2011.

vulneráveis e sujeitas a ameaças diversas que possam comprometer a integridade destes sistemas, também como a segurança das entidades e outras informações a elas concernentes.

A segurança da informação nesse contexto se mostra essencial, e até mesmo crítica em alguns casos, para que a consistência dos sistemas não seja afetada, garantindo a redução de riscos de fraudes, erros, vazamento, roubo e uso indevido e uso indevido de informações.

A segurança pode ser afetada por certos comportamentos de seus usuários, pelo ambiente ou estrutura que a cerca, ou por sujeitos mal intencionados com o objetivo de furtar, destruir ou alterar alguma informação.

Existem níveis de segurança que podem ser estabelecidos, tais como identificados em políticas de segurança para garantir que o nível de segurança que se deseja estabelecer seja mantido.

Para a construção de uma política de segurança existem alguns fatores que devem ser considerados, tais quais, riscos, benefícios, custos e esforços de implementação dos mecanismos.

## 2.1 Princípios básicos

Os princípios básicos da segurança da informação são representadas pela tríade conhecida por CIA: Confidencialidade, Integridade e Disponibilidade (*Confidentiality, Integrity and Availability*).


**Figura 2 – Segurança da Informação: Tríade CIA**

Estes principais atributos do conceito de segurança de informação orientam a análise, o planejamento e a implementação da segurança para um determinado conjunto de informações que se deseja protejer, e são definidos a seguir:

**Confidencialidade**

A confidencialidade dos dados significa que estes estão disponíveis apenas para as partes apropriadas, que podem ser partes que requerem acesso a dados ou partes que são confiáveis. Os dados que têm sido mantidos confidenciais são aqueles que não foram comprometidos por outras partes; dados confidenciais não são divulgados a pessoas que não necessitam ou que não deveriam ter acesso a eles.

Garantir a confidencialidade significa que a informação é organizada em termos de quem deveria ter acesso, bem como a sua sensibilidade. Entretanto, a quebra de sigilo pode ocorrer através de diferentes meios, como por exemplo, a engenharia social.

**Integridade**

A integridade dos dados refere-se à certeza de que os dados não são adulterados, destruídos ou corrompidos. É a certeza de que os dados não serão modificados por pessoas não autorizadas. Existem basicamente dois pontos durante o processo de transmissão no qual a integridade pode ser comprometida: durante o carregamento de dados e/ou durante o armazenamento ou coleta do banco de dados.

**Disponibilidade**

A disponibilidade dos dados e da informação significa que esta está disponível quando for necessária. Para que um sistema demonstre disponibilidade, deve dispor um sistema computacional, de controles de segurança e canais de comunicação de

> bom funcionamento. A maioria dos sistemas disponíveis são acessíveis em todos os momentos e tem garantias contra falhas de energia, desastres naturais, falhas de hardware e atualizações de sistemas.
>
> A disponibilidade é um grande desafio em ambientes colaborativos como tais ambientes devem ser estáveis e continuamente mantido. Tais sistemas também deve permitir que os usuários acessem as informações necessárias com o tempo de espera pequeno. Sistemas redundantes pode ser posto em prática para oferecer um alto nível de fail-over. O conceito de disponibilidade pode também referir-se a usabilidade de um sistema.
>
> Segurança da informação refere-se à preservação da integridade e do sigilo, quando a informação é armazenada ou transmitida. Violações de segurança da informação ocorrem quando as informações são acessadas por pessoas não autorizadas ou festas. Violações podem ser o resultado de ações de hackers, as agências de inteligência, os criminosos, concorrentes, funcionários ou outros. Além disso, pessoas que valorizam e desejam preservar a sua privacidade está interessado em segurança da informação.
> (BROOK, 2010)

Além dos três principais atributos, se aplicam também a irretrabilidade, ou o não-repúdio, a autenticidade, e a privacidade – este último mais recentemente, surgiu da preocupação da proteção dos dados, com a evolução da sociedade da informação.

A irretrabilidade pode ser vista como a combinação da autenticidade com a integridade da informação, ou seja, a garantia origem da informação com a garantia de que ela não foi alterada durante qualquer processo.

Segundo sugere Stoneburner (2001), a segurança é obtida somente através da relação e correta implementação desses quatro princípios da segurança, três já mencionados: confidencialidade, integridade, disponibilidade e auditoria, conforme relação ilustrada a seguir – Figura 3.
De acordo com Guimarães (2008), a auditoria consiste em analisar de que forma os recursos computacionais estão sendo utilizados, por quem, quando e as alterações realizadas.

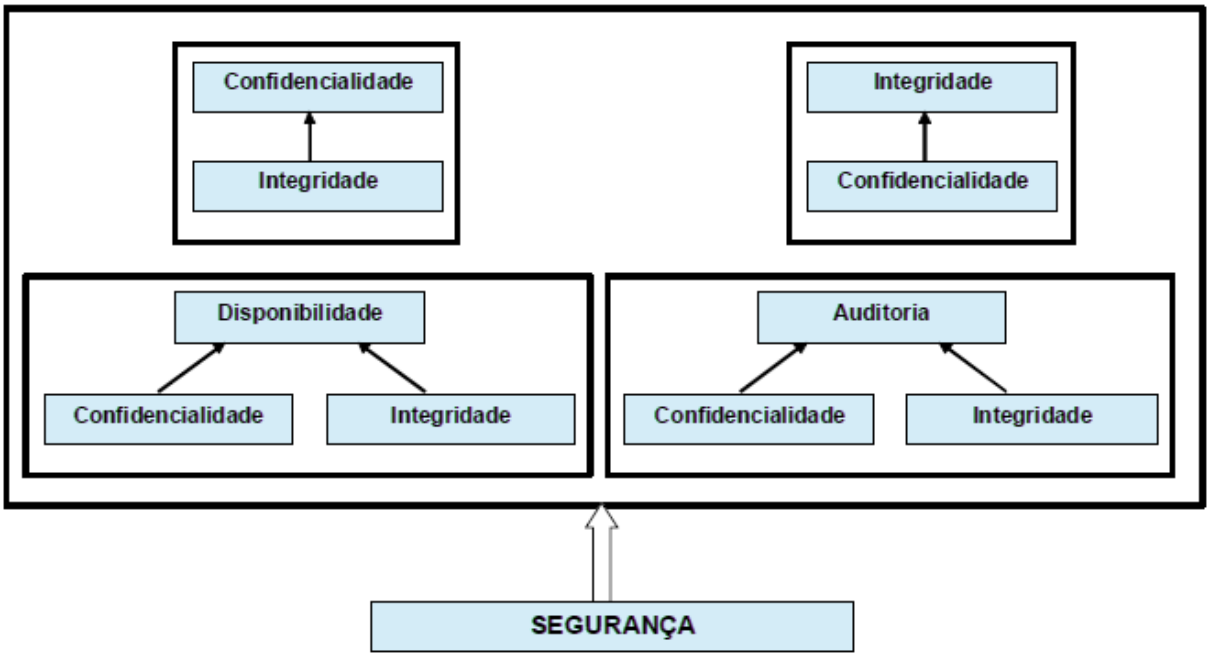


**Figura 3 – Segurança da Informação**

Onde, a confidencialidade depende da integridade - que uma vez perdida, faz com que os mecanismos controladores da da confidencialidade deixem de ser confiáveis; a integridade depende da confidencialidade, pois se alguma informação confidencial é perdida, os mecanismos de integridade podem ser desativados (por exemplo, a senha para administração dos sistema); e a auditoria e disponibilidade dependem da integridade e da confidencialidade, uma vez que estes mecanismos garantem a auditoria (registros históricos) e disponibilidade do sistema.

Para que sejam aplicados os três princípios básicos da segurança da informação, são utilizados mecanismos de segurança, ou seja, recursos disponíveis para que estes possam ser oferecidos.

## 2.2 Mecanismos de segurança

Um meio de se aplicar e suportar os princípios básicos de segurança da informação é a utilização de mecanismos e controles (físicos e lógicos), que podem ser encontrados em:

**Controles físicos**

Controles físicos podem ser definidos como barreiras que limitam o contato ou acesso direto à informação ou infra-estrutura a qual garante a sua existência.

Exemplos de mecanismos de controles físicos: portas, trancas, paredes, blindagens.

**Controles lógicos**

Controles lógicos podem ser definidos como barreiras que impedem ou limitam acesso à informação em meio eletrônico.
Exemplos de mecanismos de controles lógicos: criptografia, assinatura digital, autenticação.

Controladores lógicos são apoiados por mecanismos de segurança tais como a criptografia e a assinatura digital, porém é mais comum encontrar na Internet, limitadores e controladores de acesso para autenticação de usuários, por meio de um sistema de senhas.

Da Silva e Stein (2007) discutem, contudo, que os requistos para a elaboração de uma senha segura esbarram na capacidade cognitiva de seus usuários, dando origem a inúmeros problemas.

### 2.2.1. Senhas

Uma senha é um mecanismo de autenticação, utilizada no processo de verificação de identidade do usuário, assegurando que este é quem realmente diz ser.

Uma senha mal elaborada, fácil de ser decifrada, pode ser obitda por sujeitos mal intencionados, e uma vez que autenticado como outra pessoa, obter informações privilegiadas e desferir ataques sem ser identificada.

Em um levantamento realizado por uma companhia privada que vende serviços e produtos (*softwares*) para senhas, foram divulgadas as piores senhas do ano de 2011[5], mostradas na tabela a seguir – Tabela 3.

[5] NANCE-NASH, S. Internet Insecurity: The 25 Worst Passwords of 2011. DailyFinance, EUA, nov. 2011. Disponível em < http://www.dailyfinance.com/2011/11/15/Internet-insecurity-the-25-worst-passwords-of-2011>. Acesso em 20 nov. 2011.

| Posição | Senha |
|---|---|
| 1 | password |
| 2 | 123456 |
| 3 | 12345678 |
| 4 | qwerty |
| 5 | abc123 |
| 6 | monkey |
| 7 | 1234567 |
| 8 | letmein |
| 9 | trustno1 |
| 10 | dragon |
| 11 | baseball |
| 12 | 111111 |
| 13 | iloveyou |
| 14 | master |
| 15 | sunshine |
| 16 | ashley |
| 17 | bailey |
| 18 | passwOrd |
| 19 | shadow |
| 20 | 123123 |
| 21 | 654321 |
| 22 | superman |
| 23 | qazwsx |
| 24 | michael |
| 25 | football |

**Tabela 3 – Piores senhas de 2011**

Estas senhas refletem a preocupação citada anteriormente, mostrando que os usuários preferem a criação de senhas fracas, o que os deixam mais vulneráveis a ataques, à criação de senhas mais complexas e portanto mais difíceis de serem decifradas, o que as tornam mais seguras. A segurança da informação neste caso, esbarram no componente humano.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br, com o apoio do Comitê Gestor da Internet no Brasil – CGI.br (2006), aconselha que nomes, sobrenomes, números de documentos, placas de carros e números de telefones estejam fora das senhas, além de apontar regras para a elaboração de senhas seguras.

"Uma regra muito importante é **jamais** utilizar palavras que façam parte de dicionários." (CERT.br, 2006, p.3, grifo do autor)

Quanto mais elaborada for a senha, mais segura, e portanto mais difícil de ser descoberta. Assim, ao elaborar uma senha, é recomendável misturar letras maiúsculas, minúsculas, números e sinais de pontuacção. Uma regra realmente prática e que gera boas senhas é selecionar uma frase randomicamente e utilizar dela, a primeira, segunda ou última letra de cada palavra. Por exemplo, no uso da frase "batatinha quando nasce se esparrama pelo chão" podemos gerar a senha "!BqnsepC" (o sinal de exclamação foi acrescentado no início para se obter um símbolo na senha). Senhas geradas desta maneira são facilmente lembradas e normalmente difíceis de serem descobertas. Vale ressaltar que é preferível anotar a senha e guardá-la em local seguro, do que optar pelo uso de senhas fracas apenas para memorização mais conveniente. (CERT.br, 2006, p.3, grifo do autor).

É importante ressaltar que não basta apenas manter uma única senha bem elaborada, e fazer desta uma chave única para diversos fins. O número de sistemas e locais ou serviços que necessitam o uso de uma senha, deve ser proporcional ao número de senhas distintas que se deve manter.

Algumas recomendações gerais[6] para o gerenciamento de senhas na Internet, são dadas pelo Centro de Atendimento a Incidentes de Segurança (CAIS/RNP)

> Use pelo menos 8 caracteres na sua senha. Utilize números, letras maiúsculas e minúsculas, alguns caracteres especiais ( "_" e "-" são os mais indicados). Os sites normalmente indicam se a senha que você escolheu é "Forte" ou não. Escolha senhas que indiquem "Strong" (Forte) ou "Very Strong" (Muito forte). Não use a mesma senha de outros serviços!
>
> Use um software para gerenciar suas senhas. (...) Troque sua senha com frequência, especialmente quando utilizar o serviço de redes sociais em locais públicos como redes Wi-Fi de aeroportos, eventos, lan houses ou no computador de outra pessoa.
>
> (CAIS/RNP, 2011, p.2)

Sistemas de senhas ainda constituem a abordagem mais utilizada para autenticação, apesar de causar problemas de memorabilidade para os usuários. As vantagens, porém, decorrem do fato de que estes não requerem equipamento especial, como leitores de impressões digitais. Ainda assim, se comprometidos por uma invasão, por exemplo, os objetos de

[6] RNP. Segurança em Redes Sociais: recomendações gerais. CAIS/RNP, Rio de Janeiro, set. 2011. Disponível em <http://www.rnp.br/_arquivo/cais/Seguranca_em_Redes_Sociais.pdf>. Acesso em: 01 out. 2011.

> identificação, isto é, nome de usuário e senha, podem ser alterados facilmente, e a um custo muito baixo. (DA SILVA; STEIN, 2007, p.48)
>
> Por isso é importante que um serviço que envolva fornecimento de senha disponibilize serviços criptografados para melhor segurança durante o tráfego dos dados dentro de um sistema ou rede.

## 2.3 Riscos no uso da Internet

Existem diversos riscos envolvidos no uso da Internet. Nesta seção, iremos abordar alguns deles: serão discutidos os programas leitores de e-mails, navegadores (*browsers*), programas de troca de mensagens, de distribuição de arquivos e recursos de compartilhamento de arquivos. (CERT.br, 2006, p.13)

### 2.3.1. Navegadores

A principal ferramenta de acesso à Internet é ainda o navegador, ou *browser*. Um programa navegador é aquele que possibilita usuários acessarem e interagirm com páginas da Internet. Existem diversos programas navegadores disponíveis hoje, entretanto nenhum deles é capaz de ser totalmente seguro. Existem alguns riscos relacionados ao uso de navegadores de Internet:

• Execução de JavaScript ou de programas Java hostis;

• Execução de programas ou controles ActiveX hostis;

• Obtenção e execução de programas hostis em sites não confiáveis ou falsos;

• Acesso a sites falsos, se fazendo passar por instituições bancárias ou de comércio eletrônico;

• Realização de transações comerciais ou bancárias via Web, sem qualquer mecanismo de segurança.

Nos dois primeiros casos o *browser* executa os programas automaticamente, ou seja, sem a interferência e consentimento do usuário.

Normalmente os *browsers* contem módulos específicos para processar programas Java. Apesar destes módulos fornecerem mecanismos de segurança, podem conter falhas de implementação e, neste caso, permitir que um programa Java hostil cause alguma violação de segurança em um computador.

JavaScripts, entre outros scripts Web disponíveis, são muito utilizados atualmente para incorporar maior funcionalidade e melhorar a aparência de páginas Web. Apesar de nem sempre apresentarem riscos, vem sendo utilizados por atacantes para causar violações de segurança em computadores. Um tipo de ataque envolvendo JavaScript consiste em redirecionar usuários de um site legíitimo para um site falso, para que o usuário instale programas maliciosos ou forneça informações pessoais. (CERT.br, 2006, p.15)

### 2.3.2. Programas leitores de e-mail

Grande parte dos problemas de segurança envolvendo e-mails estão relacionados aos conteúdos das mensagens, que normalmente abusam das técnicas de engenharia social ou de características de determinados programas leitores de e-mails, que permitem abrir arquivos ou executar programas anexados às mensagens automaticamente.

É possível configurar um programa leitor de e-mails para que ele se comporte de uma maneira mais segura, seguindo algumas dicas de configuração:

- Desligar as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens;
- Desligar as opções de execução de JavaScript e de programas Java;
- Desligar, se possível, o modo de visualização de e-mails no formato HTML.

Estas configurações podem evitar que o programa leitor de e-mails propague automaticamente vírus e cavalos de tróia, entre outras ameaças. Existem programas leitores de e-mails que não implementam tais funções e, portanto, não possuem estas opções.

É importante ressaltar que se o usuário seguir as recomendações, mas ainda assim abrir os arquivos ou executar manualmente os programas que vêm anexados aos e-mails, poderá ter algum problema que resulte na violação da segurança de seu computador.

Algumas medidas preventivas que minimizam os problemas trazidos com os e-mails são:

• Manter sempre a versão mais atualizada do programa leitor de e-mails;

• Não clicar em links que, por ventura, possam aparecer no conteúdo do e-mail. Caso seja realmente necessário acessar a página do link, digitar o endereço diretamente no navegador;

• Evitar abrir arquivos ou executar programas anexados aos e-mails, sem antes verificá-los com um programa antivírus;

• Desconfiar sempre dos arquivos anexados à mensagem, mesmo que tenham sido enviados por pessoas ou instituições conhecidas. O endereço do remetente pode ter sido forjado e o arquivo anexo pode ser, por exemplo, um víirus ou um cavalo de tróia;

• Fazer o download de programas diretamente do site do fabricante;

• Evitar utilizar o programa leitor de e-mails como um browser, desligando o modo de visualização de e-mails no formato HTML.

Atualmente, usuários da Internet têm sido bombardeados com e-mails indesejáveis e, principalmente, com mensagens fraudulentas cuja finalidade é a obtenção de vantagens financeiras. Alguns exemplos são:

• Mensagens oferecendo grandes quantias em dinheiro, mediante uma transferência eletrônica de fundos;

• Mensagens com ofertas de produtos com preços muito abaixo dos preços praticados pelo mercado;

• Mensagens que procuram induzir o usuário a acessar uma determinada página na Internet ou a instalar um programa, abrir um álbum de fotos, visualizar cartões virtuais etc., mas cujo verdadeiro intuito é fazer com que o usuário forneça dados pessoais e sensíveis, como contas bancárias, senhas e números de cartões de crédito. (CERT.br, 2006, p.13-14)

### 2.3.3. Vulnerabilidades

Vulnerabilidade é definida como uma falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Existem casos onde um software ou sistema operacional instalado em um computador pode conter uma vulnerabilidade que permite sua exploração remota, ou seja, através da rede. Portanto, um atacante conectado à Internet, ao explorar tal vulnerabilidade, pode obter acesso não autorizado ao computador vulnerável. (CERT.br, 2006, p.7)

Existem sites na Internet que mantem listas atualizadas de vulnerabilidades em softwares e sistemas operacionais.[7] Além disso, fabricantes também costumam manter páginas na Internet com considerações a respeito de possíveis vulnerabilidades em seus softwares.

Portanto, a idéia é estar sempre atento aos sites especializados em acompanhar estas vulnerabilidades, aos sites dos fabricantes, às revistas especializadas e aos cadernos de informática dos jornais, para verificar a existência de vulnerabilidades no sistema operacional e nos softwares instalados em seu computador.

A melhor forma de evitar que o sistema operacional e os softwares instalados em um computador possuam vulnerabilidades é mantê-los sempre atualizados.

Entretanto, fabricantes em muitos casos não disponibilizam novas versões de seus softwares quando é descoberta alguma vulnerabilidade, mas sim correções específicas (*patches*). Estes *patches*, em alguns casos também chamados de *hot fixes* ou *service packs*, tem por finalidade corrigir os problemas de segurança referentes às vulnerabilidades descobertas.

Portanto, é extremamente importante, além de manter o sistema operacional e os softwares sempre atualizados, instalar *patches* sempre que forem disponibilizados. (CERT.br, 2006, p.20)

[7] Exemplos: http://www.cert.org/, http://cve.mitre.org/ e http://www.us-cert.gov/cas/alerts/.

### 2.3.4. Programas de troca de mensagens

Os maiores riscos associados ao uso destes programas estão no conteúdo dos próprios diálogos. Alguém pode utilizar técnicas de engenharia social para obter informações (muitas vezes sensíveis) dos usuários destes programas.

O atacante pode ser persuadir a vítima a fornecer em uma conversa “amigável”, alguns dados como endereço de e-mail, telefone, endereço, senhas (como a de acesso ao provedor), número de cartões de crédito etc. As consequências podem ser desde o recebimento de mensagens com conteúdo falso/alarmante ou mensagens não solicitadas contendo propagandas, até a utilização da conta do provedor de acesso para realizar atividades ilícitas ou a utilização de números de cartões de crédito para fazer compras em nome das vítimas.

Além disso, estes programas podem fornecer o endereço IP do usuário. Um atacante pode usar esta informação para, por exemplo, tentar explorar uma possível vulnerabilidade no computador da vítima.

Programas tais como o ICQ, AOL Instant Messenger, Yahoo! Messenger e Windows Live Messenger (antigamente MSN Messenger), por se comunicarem constantemente com um servidor (de outra forma não teriam como saber quem está conectado), ficam mais expostos e sujeitos a ataques, caso possuam alguma vulnerabilidade.

Algumas medidas preventivas para o uso de programas de troca de mensagens são:

• Manter o programa de troca de mensagens sempre atualizado, para evitar que possua alguma vulnerabilidade;

• Não aceitar arquivos de pessoas desconhecidas, principalmente programas de computadores;

• Utilizar um bom programa antivíirus, sempre atualizado, para verificar todo e qualquer arquivo ou software obtido através do programa de troca de mensagens, mesmo que venha de pessoas conhecidas;

• Evitar fornecer muita informação, principalmente a pessoas recém conhecidas;

• Não fornecer, em hipótese alguma, informações sensíveis, tais como senhas ou números de cartões de crédito;

• Configurar o programa para ocultar o endereço IP.

### 2.3.5. Programas de distribuição de arquivos

Existem diversos riscos envolvidos na utilização de programas de distribuiçãao de arquivos, tais como o Kazaa, Morpheus, Edonkey, Gnutella e BitTorrent. Dentre estes riscos, podem-se citar:

Acesso não autorizado: o programa de distribuição de arquivos pode permitir o acesso não autorizado ao computador do usuário, caso esteja mal configurado ou possua alguma vulnerabilidade;

Softwares ou arquivos maliciosos: os softwares ou arquivos distribuídos podem ter finalidades maliciosas.

Podem, por exemplo, conter vírus, ser um *bot* ou cavalo de tróia, ou instalar *backdoors* em um computador;

Violação de direitos autorais (*Copyright*): a distribuiçãao não autorizada de arquivos de música, filmes, textos ou programas protegidos pela lei de direitos autorais constitui a violação desta lei.

Algumas medidas preventivas para o uso de programas de distribuição de arquivos são:

• Manter o programa de distribuição de arquivos sempre atualizado e bem configurado;

• Manter um bom programa antivírus instalado e atualizado, e utilizá-lo para verificar qualquer arquivo obtido, pois eles podem conter vírus, cavalos de tróia, entre outros tipos de *malware*;

• Certificar-se que os arquivos obtidos ou distribuídos são livres, ou seja, não violam as leis de direitos autorais. (CERT.br, 2006, p.22)

### 2.3.6. Compartilhamento de recursos

Alguns dos riscos envolvidos na utilização de recursos compartilhados por terceiros são:

• Abrir arquivos ou executar programas que contenham vírus;

• Executar programas que sejam cavalos de trróia ou outros tipos de *malware*.

Já alguns dos riscos envolvidos em compartilhar recursos do computador são:

• Permitir o acesso não autorizado a recursos ou informações sensíveis;

• Permitir que um atacante possa utilizar tais recursos, sem quaisquer restrições, para fins maliciosos.

Isto pode ocorrer se não forem definidas senhas para os compartilhamentos.

Algumas medidas preventivas para o uso do compartilhamento de recursos do Windows s˜ao:

• Ter um bom programa antivírus instalado, mantê-lo atualizado e utilizá-lo para verificar qualquer arquivo ou programa compartilhado, pois eles podem conter víırus ou cavalos de tróia, entre outros tipos de *malware*;

• Estabelecer senhas para os compartilhamentos, caso seja estritamente necessário compartilhar recursos do computador. As senhas devem ser idealmente fáceis de lembrar e difíceis de serem descobertas.

É importante ressaltar que devem sempre ser utilizadas senhas para os recursos que se deseja compartilhar, principalmente os que estão habilitados para leitura e escrita. E, quando possível, não compartilhar recursos ou não mantê-los compartilhados por muito tempo. (CERT.br, 2006, p.22-23)

## 2.4 Segurança na Internet

Serão discutidos programas e métodos que possibilitam aumentar a segurança de um computador, como antivírus, *firewalls*, *proxies*, e a importância da realização de cópias de segurança (*backups*). (CERT.br, 2006, p.13)

### 2.4.1. Antivírus

Os antivírus são programas que procuram detectar e, então, anular ou remover os vírus de computador.

Atualmente, novas funcionalidades têm sido adicionadas aos programas antivírus, de modo que alguns procuram detectar e remover cavalos de tróia e outros tipos de código malicioso, barrar programas hostis e verificar e-mails.

Um bom antivírus deve:

• Identificar e eliminar a maior quantidade possível de vírus e outros tipos de malware;

• Analisar os arquivos que estão sendo obtidos pela Internet;

• Verificar continuamente os discos ríigidos (HDs), flexíveis (disquetes) e unidades removíveis, como CDs, DVDs e *pen drives*, de forma transparente ao usuário;

• Procurar vírus, cavalos de tróia e outros tipos de *malware* em arquivos anexados aos e-mails;

• Criar, sempre que possível, uma mídia de verificação (disquete ou CD de *boot*) que possa ser utilizado caso um vírus desative o antivírus que está instalado no computador;

• Atualizar as assinaturas de vírus e *malwares* conhecidos, pela rede, de preferência diariamente.

Alguns antivírus, além das funcionalidades acima, permitem verificar e-mails enviados, podendo detectar e barrar a propagação por e-mail de vírus, *worms*, e outros tipos de *malware*.

As dicas para o bom uso do antivírus são simples:

• Mantenha o programa antivírus e suas assinaturas sempre atualizados;

• Configure-o para verificar automaticamente arquivos anexados aos e-mails e arquivos obtidos pela Internet;

• Configure-o para verificar automaticamente mídias removíveis (CDs, DVDs, *pen drives*, disquetes, discos para Zip, etc);

• Configure-o para verificar todo e qualquer formato de arquivo (qualquer tipo de extensão de arquivo);

• Se possível, crie o disquete de verificação e utilize-o esporadicamente, ou quando o computador estiver apresentando um comportamento anormal (mais lento, gravando ou lendo o disco rígido fora de hora, etc);

Algumas versões de antivírus são gratuitas para uso pessoal e podem ser obtidas pela Internet. Mas antes de obter um antivírus pela Internet, verifique sua procedência e certifique-se que o fabricante é confiável.

Um antivírus não é capaz de impedir que um atacante tente explorar alguma vulnerabilidade existente em um computador. Também não é capaz de evitar o acesso não autorizado a um *backdoor* instalado em um computador.

Existem também outros mecanismos de defesa, conhecidos como *firewalls*, que podem prevenir contra tais ameaças. (CERT.br, 2006, p.17-19)

### 2.4.2. *Firewalls*

Se alguém ou algum programa suspeito tentar se conectar a outro computador, um *firewall* bem configurado entra em ação para bloquear tentativas de invasão, podendo barrar também o acesso a *backdoors*, mesmo se estes já estiverem instalados no computador alvo.

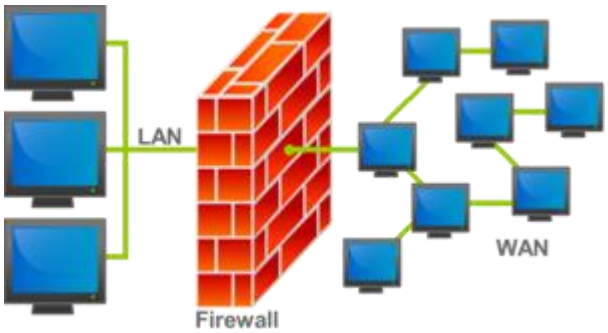


**Figura 4 – Esquema genérico de um *Firewall***

Alguns programas de *firewall* permitem analisar continuamente o conteúdo das conexões, filtrando vírus de e-mail, cavalos de tróia e outros tipos de *malware*, antes mesmo que os antivírus entrem em ação.

Também existem pacotes de *firewall* que funcionam em conjunto com os antivírus, provendo um maior nível de segurança para os computadores onde são utilizados.

É comum observar relatos de usuários que acreditam ter computadores seguros por utilizarem apenas programas antivírus. O fato é que a segurança de um computador não pode basear-se apenas em um mecanismo de defesa.

Um antivírus não é capaz de impedir o acesso a um *backdoor* instalado em um computador. Já um *firewall* bem configurado pode bloquear o acesso a ele.

Além disso, um *firewall* poderá bloquear as tentativas de invasão ao computador e possibilitar a identificação das origens destas tentativas.

Alguns fabricantes de *firewalls* oferecem versões gratuitas de seus produtos para uso pessoal. Mas antes de obter um *firewall*, é recomendado verificar sua procedência e certificar-se que o fabricante é confiável.

Normalmente os *firewalls* criam arquivos denominados arquivos de registro de eventos (*logs*). Nestes arquivos são armazenadas as tentativas de acesso não autorizado ao computador, para serviços que podem ou não estar habilitados. (CERT.br, 2006, p.19-20)

### 2.4.3. *Proxies*

*Proxy* nada mais é do que um servidor que atua como intermediador entre um cliente e outro servidor. (CERT.br, 2006, p.83)

*Proxies* são comumente usados por vários motivos: segurança, balanceamento de carga, *caching* de dados, a fim de reduzir as exigências de largura de banda, e censura ou filtragem. *Proxies* de filtragem isolam-no a partir de elementos censuráveis de páginas Web, tais como *cookies*, *banners*, conteúdo dinâmico, como Javascript, Applets Java e controles ActiveX. Alguns *proxies* anônimos criptografam suas comunicações Web, protegendo-o de

monitoramento de rotina ou até mesmo de vigilância dedicados. Porém, nem todos os *proxies* são anônimos.

*Proxies* mal configurados podem ser abusados por atacantes e utilizados como uma forma detornar anônimas algumas ações na Internet, como atacar outras redes ou enviar spam.

### 2.4.4. *Backups*

Cópias de segurança dos dados armazenados em um computador são importantes, não só para se recuperar de eventuais falhas, mas também das consequências de uma possível infecção por vírus, ou de uma invasão.

Cópias de segurança podem ser simples como o armazenamento de arquivos em CDs ou DVDs, ou mais complexas como o espelhamento de um disco rígido inteiro em um outro disco de um computador.

Atualmente, uma unidade gravadora de CDs/DVDs e um *software* que possibilite copiar dados para um CD/DVD são suficientes para que a maior parte dos usuários de computadores realizem suas cópias de segurança. Existem também serviços disponíveis *online* que permitem guardar arquivos em discos virtuais, sem o risco de se perder em caso de falha ou danos físicos ao disco rígido.

A frequência com que é realizada uma cópia de segurança e a quantidade de dados armazenados neste processo depende da periodicidade com que o usuário cria ou modifica arquivos. Cada usuário deve criar sua própria política para a realização de cópias de segurança.

Os cuidados com cópias de segurança também dependem das necessidades do usuário. O usuário deve procurar responder algumas perguntas antes de adotar um ou mais cuidados com suas cópias de segurança, como por exemplo:

• Que informações realmente importantes precisam estar armazenadas em minhas cópias de segurança?

• Quais seriam as consequências/prejuízos, caso minhas cópias de segurança fossem destruídas ou danificadas?

• O que aconteceria se minhas cópias de segurança fossem furtadas?

Baseado nas respostas para as perguntas anteriores, o usuário deve atribuir maior ou menor importância a cada um dos cuidados discutidos abaixo.

**Escolha dos dados**

Cópias de segurança devem conter apenas arquivos confiáveis do usuário, ou seja, que não contenham vírus e nem sejam algum outro tipo de *malware*. Arquivos do sistema operacional e que façam parte da instalação dos softwares de um computador não devem fazer parte das cópias. Eles podem ter sido modificados ou substituídos por versões maliciosas, que quando restauradas podem trazer uma série de problemas de segurança para um computador. O sistema operacional e os softwares de um computador podem ser reinstalados de mídias confiáveis, fornecidas por fabricantes.

**Mídia utilizada**

A escolha da mídia para a realização das cópias de segurança é extremamente importante e depende do grau da importância e da vida útil que a cópia deve ter. A utilização de alguns disquetes para armazenar um pequeno volume de dados que estão sendo modificados constantemente é perfeitamente viável, porém para um grande volume de dados, de maior importância e que deve perdurar por longos períodos, é preferível que seja armazenado em outros tipos de mídia mais confiáveis, como por exemplo DVDs ou discos rígidos removíveis.

**Local de armazenamento**

Cópias de segurança devem ser guardadas em um local condicionado (longe de muito frio ou muito calor) e restrito, de modo que apenas pessoas autorizadas tenham acesso a este local (segurança física). Cópias de segurança podem ser guardadas em locais diferentes. Um exemplo seria manter uma cópia em casa e outra no escritório. Também existem empresas especializadas em manter áreas de armazenamento com cópias de segurança de seus clientes.

**Criptografia dos dados**

Os dados armazenados em uma cópia de segurança podem conter informações sigilosas. Neste caso, os dados que contenham informações sigilosas devem ser armazenados em algum formato criptografado. (CERT.br, 2006, p.23-24)

# 3 Redes Sociais

O conceito de Redes Sociais está relacionado com a gama de *websites* e portais de relacionamento existentes e disponíveis hoje na Internet. Porém, por definição, uma rede social é baiscamente uma estrutura composta por pessoas conectadas por um ou mais tipos de relações que partilham valores e objetivos em comum.

Redes sociais nos permitem encontrar emprego e fazer amizades, através das relações entre as pessoas conhecidas. Por exemplo, um determinado indivíduo que busca por um emprego tem um amigo, que por sua vez é amigo de outra pessoa, que procura um candidato para uma vaga que está disponível em sua empresa. Através das relações entre estes indivíduos, o primeiro da rede consegue o emprego daquela determinada vaga que estava em aberto.

Um problema que existe nas redes sociais é que muitas vezes, as conexões são desconhecidas. Este problema está sendo resolvido com as Redes Sociais na Internet (sites de relacionamento), as quais permitem visualizar estas conexões até então desconhecidas, revelando todo o valor potencial da rede de relacionamentos de um determinado indivíduo[8].

De acordo com De Ugarte (2007), com a Era das Redes Distribuídas (Figura 5), nascida da conexão de milhões de pontos hierarquicamente iguais através da Internet, qualquer indivíduo pode potencialmente, econtrar, reconhecer e comunicar-se com qualquer um.

[8] LEFEVER, Lee. Social Networking in Plain English: A short introduction to the concepts behind social networking websites. Commoncraft. Disponível em <http://www.commoncraft.com/video/social-networking>. Acesso em: 25 nov. 2011.

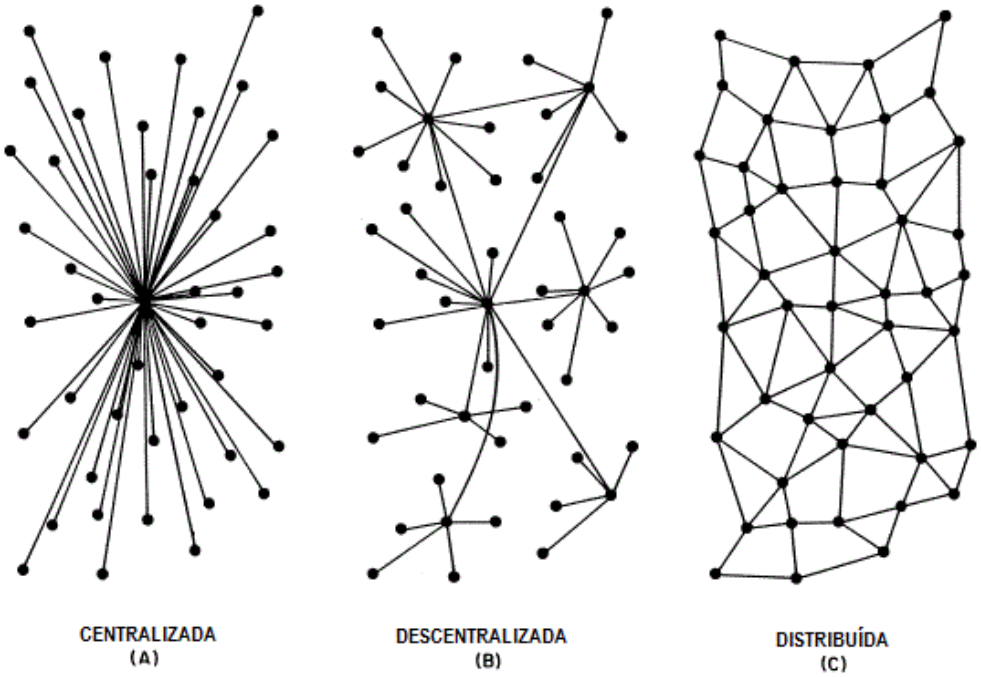


**Figura 5 – Rede distribuída (C)**

Na figura acima, são descritas três diferentes maneiras de se unir os mesmos pontos. Conforme De Ugarte (2007, p. 20) essa ilustração foi criada por Paul Baran, nos anos 1960, para o dossiê em que descrevia a estrutura de um projeto que mais tarde se converteria na Internet. [9]

"Este mundo distribuído está dando à luz um meio de comunicação à sua imagem e semelhança: a blogosfera, o conjunto de ferramentas *on-line* de publicação e comunicação pessoal." (DE UGARTE, 2007, p. 110)

## 3.1 Mídias sociais vs. Redes sociais

O conjunto de ferramentas *on-line* citado por De Ugarte (2007) e definido por blogosfera, nada mais é do que o que hoje conhecemos por mídias sociais.

[9] RAND. Paul Baran and the Origins of the Internet. Disponível em <http://www.rand.org/about/history/baran.html>. Acesso em: 26 nov. 2011.

As mídias sociais podem ser entendidas como os meios em que os indivíduos de uma rede exercem relacionamentos entre elas. E um meio existente na Internet, são os chamaods sites de relacionamento, comumente conhecidos hoje por Redes Sociais[10] [11].

Esses meios não passam de ferramentas de diálogo, mecanismos virtuais de emissão e troca de mensagens, que possibilitam a interação das pessoas, e assim, formam dentro destas plataformas, as chamadas redes sociais.

As redes sociais, por sua vez, existem desde que existam pessoas se relacionando e interagindo entre elas. As ferramentas de redes sociais na Internet apenas permitem que as pessoas se conectem com mais facilidade, acelerando o processo, permitindo em tempo real a interação de pessoas não importam onde ela estejam – removendo o fator distância.

## 3.2 Os tipos de mídias sociais

Existem diversas plataformas de mídia social disponíveis na Internet. Elas abrangem diversas atividades que integram tecnologia, interação social e a compartilhamento multimídia, como fotos, vídeos e formatos de áudio.

Algumas das mais utilizadas são relacionadas abaixo:

- Facebook (facebook.com)

[10] DEGÁSPERI, Israel S. Redes Sociais e Mídias Sociais, quais as diferenças? **Blog Mídias Sociais**, Brasil, mar. 2010. Disponível em <http://midiassociais.blog.br/2010/03/30/redes-sociais-e-midias-sociais-quais-as-diferencas/>. Acesso em: 26 nov. 2011.

[11] DEGÁSPERI, Israel S. Entendendo Redes Sociais e Mídias Sociais assim como suas ferramentas. **Blog Mídias Sociais**, Brasil, fev. 2010. Disponível em <http://midiassociais.blog.br/2010/02/23/redessociais-vs-midiassociais/>. Acesso em: 26 nov. 2011.


**Figura 6 – Página do Facebook**

Facebook é a mais popular das mídias de relacionamento pessoal. Milhões de pessoas usam o Facebook todos os dias para manter o contato com os amigos, compartilhar fotos, links e vídeos, e aprender mais sobre as pessoas que encontram[12].

- Twitter (twitter.com)


**Figura 7 – Página do Twitter**

Twitter é a mais popular das mídias de *microblogging*. É uma rede de informação em tempo real, que conecta as pessoas com as últimas informações sobre o que cada uma achar interessante. Basta encontrar os perfis e seguir as conversas.

- Orkut (orkut.com)

[12] Sobre o Facebook. Disponível em <http://www.facebook.com/facebook?sk=info>. Acesso em: 26 nov. 2011.

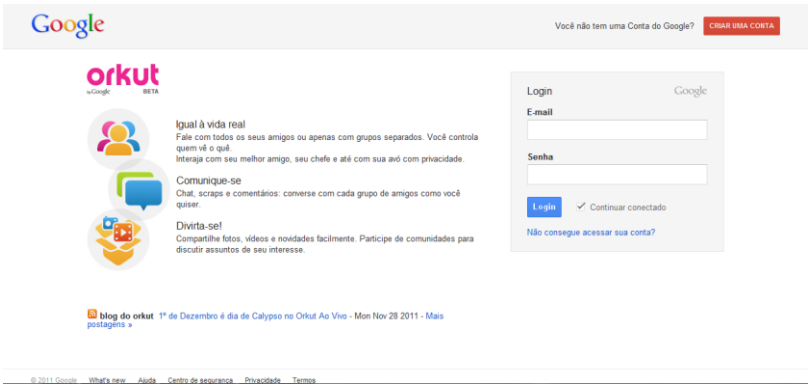


**Figura 8 – Página do Orkut**

Orkut foi a primeira mídia de relacionamento pessoal a ser popular no Brasil. Similar ao Facebook, permite entrar em contato com amigos e compartilhar conteúdo multimídia.

- Formspring (formspring.me)

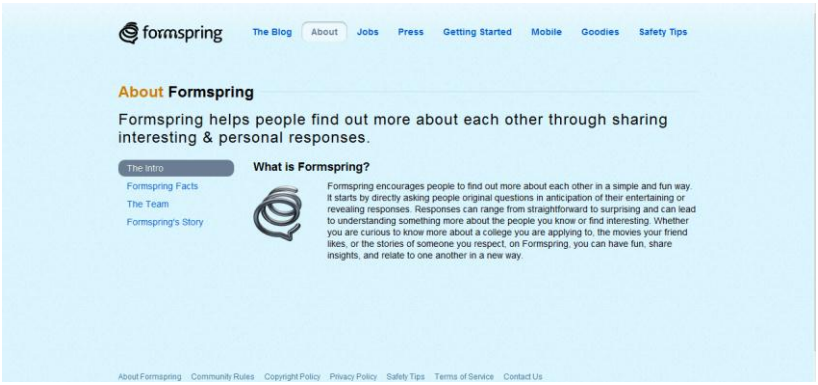


**Figura 9 – Página do Formspring**

Formspring é um tipo de mídia social baseada em perguntas e respostas: incentiva as pessoas a saber mais uns sobre os outros de uma forma simples e divertida, enviando perguntas diretamente aos usuários da rede social[13].

- Foursquare (foursquare.com)

[13] Sobre o Formspring. Disponível em <http://about.formspring.me/#intro>. Acesso em: 26 nov. 2011.

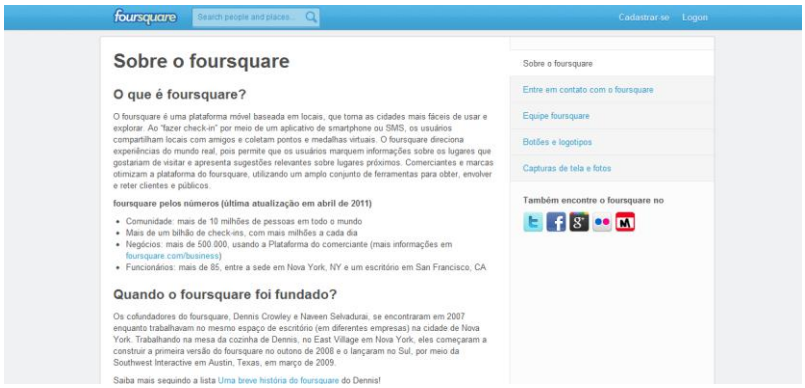


**Figura 10 – Página do Foursquare**

> Foursquare é uma plataforma móvel baseada em locais, que torna as cidades mais fáceis de usar e explorar. Os usuários compartilham locais com amigos e coletam pontos e medalhas virtuais. O foursquare direciona experiências do mundo real, pois permite que os usuários marquem informações sobre os lugares que gostariam de visitar e apresenta sugestões relevantes sobre lugares próximos. Comerciantes e marcas otimizam a plataforma do foursquare, utilizando um amplo conjunto de ferramentas para obter, envolver e reter clientes e públicos[14].

Além dos citados acima, existem tantos outros tipos de mídias sociais, cada um para um devido fim ou com uma característica única.

A lista a seguir mostra algumas ferramentas para Redes sociais[15].

- **Birghtkite** (http://brightkite.com/)
  Rede social por posição geográfica
- **Blip.fm** (http://blip.fm/)
  Rede social que compartilha em mensagens curtas o que você está ouvindo
- **Blip.tv** (http://blip.tv/)
  Rede social para postar e compartilhar vídeos

[14] Sobre o Foursquare. Disponível em <http://pt.foursquare.com/about/>. Acesso em: 26 nov. 2011.

[15] DEGÁSPERI, Israel S. Mídias Sociais. **Blog Mídias Sociais**, Brasil, mar. 2010. Disponível em <http://midiassociais.blog.br/redes-sociais/>. Acesso em: 26 nov. 2011.

- **Carbonmade** (http://carbonmade.com/)
  Rede social de portfólio online

- **CouchSurfing** (http://www.couchsurfing.org/)
  Rede social para mochileiros

- **Delicious** (http://delicious.com/)
  Rede social de favoritos (*bookmarks*) online

- **DeviantArt** (http://www.deviantart.com/)
  Rede social para compartilhar ou vender artes gráficas

- **Digg** (http://digg.com/)
  Rede social para compartilhamento de conteúdo na Internet

- **Drimio** (http://www.drimio.com/)
  Rede social que avalia seu relacionamento com as marcas

- **Ebah!** (http://www.ebah.com.br/)
  Rede social acadêmica

- **Elgg** (http://elgg.org/)
  Ferramenta para criação de redes sociais

- **Fashion.me** (http://fashion.me/)
  Rede social do mundo da moda

- **Filmow** (http://filmow.com/)
  Rede social para cinéfilos

- **Flickr** (http://www.flickr.com/)
  Rede social para compartilhar fotografias, ilustrações e até *screenshots*

- **FriendFeed** (http://friendfeed.com/)
  Rede social que agrega em feeds, as atualizações de várias redes sociais

- **Gengibre** (http://www.gengibre.com.br/)
  Rede social para postar mensagens curtas de voz

- **GetGlue** (http://getglue.com/)
  Rede social de entretenimento onde usuários compartilham o que estão assistindo, ouvindo e lendo

- **Hi5** (http://www.hi5.com/)
  Rede social de relacionamento

- **Hulu** (http://www.hulu.com/)
  Rede social para compartilhar vídeos e assistir filmes e seriados de TV

- **Ikwa** (http://www.ikwa.com.br/)
  Rede social para conhecer profissões e o mercado de trabalho

- **ImgFave** (http://imgfave.com/)
  Rede social para compartilhar fotos e imagens

- **Italki** (http://www.italki.com/)
  Rede social para aprendizado de língua estrangeira

- **Joost** (http://www.joost.com/)
  Rede social para compartilhar e assitir canais de vídeo

- **Justin.tv** (http://www.justin.tv/)
  Rede social para transmitir vídeos online , com chat integrado

- **Last.fm** (http://www.last.fm/)
  Rede social para ouvir e descobrir músicas *online*

- **LinkedIn** (http://www.linkedin.com/)
  Rede social para contatos profissionais e curriculum *online*

- **Livemocha** (http://www.livemocha.com/)
  Rede social para aprender idiomas

- **Meme** (http://meme.yahoo.com/)
  Rede social do tipo *microblogging*

- **Mumsnet** (http://www.mumsnet.com/)
  Rede social para unir mães e compartilhar dicas sobre gravidez

- **MySpace** (http://www.myspace.com/)
  Rede social para compartilhar músicas, vídeos e textos

- **Ning** (http://www.ning.com/)
  Ferramenta para criação de redes sociais

- **Noosfero** (http://noosfero.org/)
  Plataforma para criação de redes sociais

- **Plurk** (http://www.plurk.com/)
  Rede social do tipo *microblogging* (compartilhamento de pensamentos e *links*)

- **PureVolume** (http://www.purevolume.com/)
  Rede social para compartilhar músicas, vídeos e eventos

- **Skoob** (http://www.skoob.com.br/)
  Rede social para usuários compartilharem e recomendarem o que estão lendo

- **SoundCloud** (http://soundcloud.com/)
  Rede social para postar músicas e disponibilizá-las para *download*
- **Tumblr** (http://www.tumblr.com/)
  Rede social do tipo *microblogging*, para conteúdo multimídia
- **Ustream** (http://www.ustream.tv/)
  Rede social para transmissão de vídeos *online*
- **Vimeo** (http://vimeo.com/)
  Rede social de criação e compartilhamento de vídeos

## 3.3 Privacidade e segurança

Nas Redes Sociais na Internet, é preciso ter cautela e evitar fornecer dados pessoais (como nome, e-mail, endereço e números de documentos) para terceiros. Também nunca devem ser fornecidas informações sensíveis, como senhas e números de cartão de crédito), a menos que esteja sendo realizada uma transação (comercial ou financeira) e se tenha certeza da idoneidade da instituição que mantém o site.

Estas informações geralmente são armazenadas em servidores das instituições que mantem os sites. Com isso, corre-se o risco destas informações serem repassadas sem sua autorização para outras instituições ou de um atacante comprometer este servidor e obter acesso a todas as informações.

Ao ter acesso a seus dados pessoais, um atacante poderia, por exemplo, utilizar o e-mail da vítima em alguma lista de distribuição de *spams* ou se fazer passar por ela na Internet (através do uso de uma de suas senhas).

Sites de redes de relacionamentos, como o Orkut, tiveram uma ampla aceitação e inserção de usuários da Internet, por proporcionarem o encontro de pessoas (amigos) e permitirem a criação e participação em comunidades com interesses em comum.

Um site de redes de relacionamento normalmente permite que o usuário cadastre informações pessoais (como nome, endereços residencial e comercial, telefones, endereços de e-mail, data de nascimento etc.), além de outros dados que irão compor o seu perfil. Se o usuário não limitar o acesso aos seus dados para apenas aqueles de interesse, todas as suas informações poderão ser visualizadas por qualquer um que utilize este site. Além disso, é recomendável

que o usuário evite fornecer muita informação a seu respeito, pois nenhum site está isento do risco de ser invadido e de ter suas informações furtadas por um invasor.

A participação de um usuário em determinados tipos de comunidades também pode fornecer muita informação para terceiros. Por exemplo, a comunidade de donos de um determinado veículo, ou dos frequentadores de um estabelecimento específico, pode dizer qual é a classe social de um usuário, que locais ele gosta de frequentar etc. Informações dos locais os quais determinada pessoa frequenta, assim como caminhos rotineiros são facilmente obtidos em redes sociais baseadas em localização, como o Foursquare.

Desta forma, é extremamente importante que usuário esteja atento, e avalie com cuidado que informações estarão disponíveis nos sites de redes de relacionamentos - principalmente aquelas que poderão ser vistas por todos - e quais comunidades participar. Estas informações podem não apenas ser utilizadas por alguém mal-intencionado, mas também para atentar contra a segurança física do próprio usuário. (CERT.br, 2006, p.30)

## 4 Ataques e incidentes em redes sociais

Apesar de todo o potencial apresentado, as redes sociais são igualmente uma séria ameaça. Em particular aquelas de maior dimensão e que apresentam maior representatividade, são alvo de ataques visando explorar a principal vulnerabilidade destas mesmas redes: os seus usuários.

Uma das principais ameaças à segurança e privacidade dos usuários é proveniente do tipo de conteúdos e de informação que estes partilham nas redes sociais. Um pequeno exemplo: uma foto divertida hoje compartilhada no Facebook, pode se tornar uma foto comprometedora no futuro. Existe alguma falta de percepção por parte dos usuários sobre o impacto que o compartilhamento destes conteúdos e outros pode provocar. Os conteúdos compartilhados hoje numa rede social, serão distribuídos e compartilhados por inúmeras pessoas e vão persistir na rede social, mesmo que a conta do usuário seja removida da rede. Não há retorno.

Da mesma forma. numa perspectiva empresarial e profissional, estas redes sociais podem ser uma ameaça, uma vez que hoje em dia, as empresas recorrem frequentemente às redes sociais como uma forma complementar de verificar o perfil dos candidatos. Adicionalmente, existe o

sério perigo de quebra de confidencialidade pelo facto dos colaboradores de uma organização ao divulgarem informação interna das suas organizações.

Num estudo recente realizado pela Sophos, no qual estiveram envolvidas cerca de 500 empresas em que responderam a um inquérito, cerca de 60% consideraram que o Facebook apresenta-se como um dos principais ameaças à segurança e privacidade da informação das suas organizações (Facebook 60%, Myspace 18%, Twitter 17% e Linkedin 4%).

O Facebook cresceu exponencialmente nos últimos tempos passando a ser a maior das redes sociais (com cerca de 400 milhões de utilizadores em 6 anos de existência). A sua dimensão torna-a o alvo preferencial para ameaças de diversos tipos.

Do ponto de vista da privacidade, o Facebook é extremamente agressivo na violação "consentida" dessa mesma privacidade. A mudança da politica de privacidade do Facebook mudou no ano passado, passando a apresentar valores de partilha com o toda a rede social, de informação pessoal. Ou seja, por defeito, se nada for feito por parte do utilizador, todos os seus dados e conteúdos são partilhados com toda a rede, para sempre.

A isto alia-se o facto de que os usuários das redes sociais (extrapolando para a própria utilização da Internet e da WWW) terem pouca consciência das implicações da divulgação da sua informação pessoal e privada em redes pessoais. O mesmo estudo realizado pela Sophos, chegou a conclusões assustadoras sobre o comportamento dos utilizadores no Facebook, em relação aos dados que revelam. Assim, conclui-se que:

46% dos utilizadores do Facebook aceitam pedidos de amizade de estranhos;

89% dos utilizadores da faixa etária dos 20 divulgam a sua data de aniversário;

Quase 100% dos utilizadores divulgam o seu endereço de email;

Entre 30-40% dos utilizadores listam dados sobre a sua família e amigos.

O fato dos usuários estarem tão disponíveis para compartilhar tanta da sua própria informação pessoal no Facebook, faz com que o risco de ocorrência de ataques de roubo de identidade ou de engenharia social aumentem consideravelmente. Um exemplo muito curioso e recentemente relatado na comunicação social diz respeito a uma história que contava como a esposa do director do MI6 do Reino Unido, tinha colocado no seu perfil no Facebook detalhes

sobre a sua residência e sobre os seus amigos, colocando a própria segurança nacional em risco.

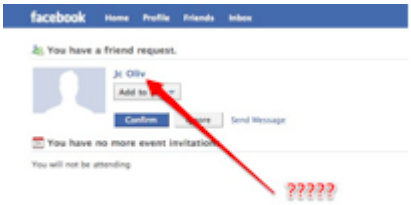


**Figura 11 – Solicitação de amizade de um estranho**

Recomenda-se a utilização das redes sociais de uma forma racional, e acima de tudo a percepção de quais dados compartilhar e que tipos de conteúdo disponibilizar - e para quem. Um conjunto simples de indicações pode melhorar em muito a privacidade dos usuários e reduzir o risco de exposição às possíveis ameaças. Estas indicações podem ser resumidas no seguinte:

- Usar corretamente as listas de amigos;
- Remover-se dos resultados de pesquisa do Facebook;
- Evitar o *tagging* (marcação) em fotos e vídeos;
- Proteger ou restringir os álbuns de fotografias;
- Evitar que as histórias apareçam no *feed* de notícias dos seus amigos;
- Proteger-se contra histórias publicadas por outras aplicações;
- Tornar a sua informação de contato privada;
- Evitar postagens que possam ser embaraçosas;
- Tornar as suas relações privadas.

No entanto, as ameaças não estão resumidas à privacidade dos usuários. As ameaças que populam as redes sociais, em particular as de maior dimensão, são cada vez mais perigosas. Uma das ameaças recentes no Facebook é uma aplicação misteriosa que afeta os usuários.

Eles estão a sendo solicitados por outros usuários a instalarem uma aplicação chamada “Unnamed App”. A Sophos já identificou esta ameaça como sendo Mal/FakeVirPk-A.

**Figura 12 – Usuários do Facebook podem ser confrontados com aplicações estranhas**

Essas aplicações do Facebook são em sua maioria provindas de fabricantes terceiros, que se utilizam de dados do usuário. Muitas vezes elas podem ter comportamentos diferentes do que o esperado, inclusive enviar *links* indesejados – que podem conter códigos maliciosos – através de solicitações via *chat*. (Figura 13)

**Figura 13 – Solicitação de *chat***

Notificações dessas mesmas aplicações não são mais do que pedidos disfarçados para levar o usuário para outros sites na Internet.


**Figura 14 – Notificações de aplicativos**

Alguns desses pedidos servem para bombardear os utilizadores com publicidade não solicitada.


**Figura 15 – Publicidade indesejada**

Em 2009 foram duas as principais ameaças que afetaram as principais redes sociais e que estiveram na origem de inúmeros problemas. Uma destas ameaças deu pelo nome de Koobface (um anagrama da palavra Facebook), e que é um *worm* que ataca directamente os usuários de redes sociais como o Facebook, MySpace, e Twitter. O Koobface tenta, após infectar o sistema da vítima, obter informações diversas do usuário, tal como números de cartões de crédito.

O Koobface espalha-se através do envio de mensagens do Facebook a pessoas que são "amigas" de um usuário previamente infectado. Depois de recebida, a mensagem direciona o receptor a um site de Web, onde as vítimas são levadas a pensar na existência de uma atualização de uma versão recente do *software* Flash. Ao instalarem o arquivo, passam a ser igualmente infectados com o Koobface, passando a estar sob o controle do mesmo e passando a infectar mais usuários.

O Koobface é um *worm* tão sofisticado que é capaz de, entre outras coisas:

Registar uma conta no Facebook;

Ativar essa mesma conta através da confirmação do email enviado para uma conta do Gmail;

Fazer-se amigo de várias pessoas na rede social; inteligente ao ponto de não adicionar muitos amigos por dia, para não chamar as atenções para si próprio;

E colocar posts no mural de "amigos" com mensagens com links para sites ou para vídeos que são fontes de distribuição de *malware*.

A segunda grande ameaça identificada nas redes sociais foi o worm "stalkdaily" criado por um jovem de 17 anos chamado Mikeyy Mooney. Este *worm* lançou o pânico no Twitter, enviando mensagens aos utilizadores para visitarem site stalkdaily.com que infectava o perfil do visitante que tivesse uma conta de Twitter associada.

As redes sociais (principalmente o Facebook e o Twitter) tornaram-se assim meios preferenciais para lançar diversos tipo de ataques: *phishing*, *malware*, roubo de dados e de identidade, *stalking*, entre outros. Estes atacam não apenas a ingenuidade dos utilizadores, mas igualmente a própria infra-estrutura onde assentam estas redes sociais, em que as mesmas não são completamente imunes a problemas de segurança.

Uma recomendação importante que pode-se dizer que passa sem a menor preocupação por parte dos usuários, é rever politicas de privacidade das mídias sociais, para estar consciente do âmbito do compartilhamento de informações pelas mesmas, e além disso, desconfiar sempre dos links que são compartilhados por "amigos", conhecidos e desconhecidos  e não instalar discriminadamente aplicações por terceiros no (principalmente no Facebook e Twitter), sem antes saber do que esta se trata. (SERRAO, 2010)

## 4.1 *Social-phishing*

*Phishing* é uma forma de engenharia social na qual um invasor tenta adquirir, de forma fraudulenta, informações confidenciais de uma vítima através da personificação de uma terceira parte confiável.

Ataques de *phishing* tipicamente empregam "iscas" generalizadas, por exemplo, um invasor se passando por uma grande corporação bancária pode ter um razoável rendimento em seu ataque, apesar de não conhecer nada sobre sua vítima, uma vez que esta conheça e confie na corporação bancária a qual o atacante está se passando. (JAGATIC et. al., 2005)

## 4.2 Os perigos das redes baseadas em localização

Redes sociais baseadas em localização como o Foursquare incentivam o usuário a compartilhar sua localização atual com o resto do mundo ou com seus amigos. Ao fazer isso, o usuário também está dizendo para as pessoas que não está em casa.

Inclusive existe um site na Internet, o PleaseRobMe (Roube-me por favor), que mostra atualizações em tempo real dos usuários do Foursquare que difundem seus *check-ins* no Twitter. Uma maneira controversa de exibir estes dados compartilhados publicamente.

De acordo com os desenvolvedores responsáveis pelo site (Barry Borsboom, Frank Groeneveld e Boy van Amstel), "O objetivo do site é criar uma consciência do problema e fazer as pessoas pensarem em como eles utilizam estes serviços como o Foursquare, Brightkite, Google Buzz etc." [16]

O PleaseRobMe não mostra nada de tão novo que algum motor de busca comum do Twitter já não tenha feito, mas é a primeira vez que um serviço tenha destacado tão claramente essa informação. Não achamos que muitos ladrões estão realmente entrando na web para obter

[16] Please Rob Me. Disponível em <http://pleaserobme.com/why>. Acesso em: 27 nov. 2011.

informações de quando as pessoas não estão em casa, mas já aconteceram alguns roubos que estas atualizações de localização podem ter tido participação.

No entanto, isso não se limita apenas aos aplicativos baseados em localização. Atualizações do Twitter sobre férias também podem revelar que o usuário deixou sua casa.

Quando se trata de serviços baseados em localização e redes geo-sociais, é preferível utlizar serviços que permitam que o usuário envie essas localizações de forma privada para grupos específicos de amigos e contatos confiáveis. O Brightkite, um dos mais antigos serviços desse gênero, por exemplo, permite um certo controle de privacidade por *post*.

Serviços como estes (Foursquare, Brightkite etc.) fazem uma ligação entre o mundo virtual das redes sociais e o mundo real de uma maneira mais visível. Serviços como o PleaseRobMe deixa claro que podem haver consequências com as informações que divulgamos nas redes sociais, e que estas podem influenciar as nossas vidas fora delas.

Além dessa visão trazida pelo site PleaseRobMe, de que a vítima deixou a casa, há o outro lado da moeda: alguns usuários do Foursquare estão começando a dar *check-ins* em lugares como “Casa”, “*Home*”, “Casa do Fulano”, ou seja, lugares não públicos, e assim expondo publicamente suas residências e mostrando aos usuários exatamente o lugar onde moram, um prato cheio para os , um prato cheio para os *cyberstalkers*.


**Figura 16 – Geolocalização (Charge)**

## 4.3 *Cyberstalking*

*Cyberstalking* se refere ao assédio ou à comunicação indesejada, provinda de alguma forma de tecnologia, incluindo computadores, sistemas de posicionamento global (GPS), telefones móveis, entre outros. *Cyberstalking* é definido pelo The National Center for Victims of Crime como "Comportamento ameaçador ou avanços indesejados direcionados a outro usando a Internet e outras formas de comunicação on-line."

Os *Cyberstalkers*, ou seja, aqueles que praticam esse tipo de assédio, utilizam email, salas de bate papo, fóruns de discussão, câmeras escondidas, entre outros, para atingirem suas vítimas.

### *Cyberstalking* & Redes Sociais

O ato de perseguição (*stalking*) no Facebook, por exemplo, inclui, mas não se limita a verificar continuamente página de alguém de perfil, adicionando estranhos como amigos para obter informações sobre o seu interesse amoroso, fazer logon em suas contas de amigos 'para obter informações e ler murais de pessoas que você não conhece.

Houve vários casos documentados de *cyberstalking* via Facebook desde o início do site de rede social. Junto com o Facebook, outros sites populares como o Twitter permitiram *cyberstalkers* para ver atualizações sobre suas presas o tempo todo, e em alguns casos, permitindo-lhes ver o paradeiro da vítima. Aplicações recentes que utilizam software de tecnologia de posicionamento global (GPS), como Foursquare, tornar o ato de encontrar as vítimas ainda mais fácil.

> Algumas precauções irão manter os usuários do site a salvo de *cyberstalkers*:
>
> - Considerar a idade da pessoa: aplicativos e sites baseados em GPS realmente não são apropriados para crianças. Um pouco de maturidade é um longo caminho a frente de manter um membro do site seguro. Treze é uma idade razoável para conceder a utilização destes serviços, mas vários sites nem permitem usuários menores de 18 anos. Considerar tanto o serviço e da idade e maturidade da criança que irá usá-lo.
>
> - Postar avatares ou fotos de animais de estimação como identificadores para os jovens que fazem uso destes sites: eles absolutamente não devem postar fotos

> reais de si mesmos como identificadores, uma vez que estas podem representar riscos de segurança.
>
> - *Check-ins* frequentes com aplicativos “baixados” para o telefone de um jovem: cergunte o que são os aplicativos, e se um aplicativo envolve compartilhamento de localização da criança, verifique sua lista de amigos. Se o celular da criança estiver em um plano familiar, esses aplicativos podem ser bloqueados para *download* por um pai . Caso contrário, frequentes verificações com o celular da criança em mãos é a melhor abordagem.
>
> - Certifique-se que os amigos que recebem atualizações de GPS são amigos da vida real e não membros de uma rede estendida que pode incluir inúmeros desconhecidos: confirmar que as configurações de segurança do site / aplicativo permita somente seguidores desejados.
>
> - Considerar realizar "*check-in*" em um local quando se estiver deixando-o, ao invés de no momento da chegada, para minimizar a possibilidade de um encontro indesejado com alguém desconhecido.
>
> (GOODMAN, 2010)

## 4.4 O papel das mídias sociais em crimes *online*

A web e as mídias sociais têm tido grande papel nos crimes. No caso das redes sociais, existem algumas ocasiões em que esses crimes não passam de mal-entendidos ou confusões causadas por alguns usuários desavisados. Em outras, são casos sérios, nos quais a rede foi usada como evidência ou flagrante. Alguns casos em que o Facebook foi utilizado como meio para a prática de crimes são listados a seguir.

### A mulher que foi presa por “cutucar” um usuário

> Shannon Jackson, do estado Tennessee, nos Estados Unidos da América, infringiu a lei por cutucar outro usuário via Facebook. O que aconteceu foi que Shannon fez isso com seu requerente, violando uma medida cautelar.
>
> A ordem proibia a mulher especificamente de usar telefone, entrar em contato ou fazer qualquer tipo de comunicação com o requerente, incluindo o Facebook. A

> violação de uma medida cautelar no Tennessee é punível com até 11 meses e 29 dias de prisão, assim como multa de US$2.500.
>
> (PORPHÍRIO, 2011)

**Traficante vendia ecstasy via Facebook**

Daniel Izaías dos Santos, foi preso após chegar ao Rio de Janeiro com comprimidos de ecstasy, onde foi abordado por policiais e acabou preso em flagrante.

> A polícia chegou até Izaías a partir de uma investigação da delegacia de Copacabana que monitorava os registros do rapaz, identificado como atacadista de uma quadrilha de traficantes, na Internet.
>
> Em alguns posts, Izaías e seus amigos usam codinomes e códigos. Referem-se aos comprimidos de ecstasy como "laranjinhas do Canadá", por exemplo.
>
> (AGÊNCIA ESTADO, 2011)

**Duas pré-adolescentes acusadas de cyberstalking por invadir a conta do Facebook da colega de sala**

> Duas pré-adolescentes foram acusadas de *cyberstalking* (ou perseguição online) e invasão de computador por entrar sem permissão na conta do Facebook da colega de sala e postar fotos e mensagens de conteúdo erótico.
>
> As meninas, de 11 e 12 anos, foram acusadas pelo Juizado da Infância e Juventude de King County, no estado de Washington, em 18 de março desse ano.
>
> As jovens postaram mensagens no mural da colega Leslie Cole onde marcavam encontros sexuais. Inclusive, enviaram mensagens privadas a vários amigos, onde propunham diversos tipos de jogos eróticos. Leslie, de 12 anos, fez questão de pedir que a mídia usasse seu nome para chamar atenção ao bullying que algumas crianças têm cometido.
>
> Embora ainda façam algumas aulas juntas, as três meninas se veem com menos frequência. Leslie conseguiu uma medida cautelar que impede as duas invasoras de entrarem no mesmo ônibus escolar que ela ou de fazerem contato por qualquer meio de comunicação.

(PORPHÍRIO, 2011)

### O adolescente que foi preso por admitir ter contratado um assassino profissional pelo Facebook

> Corey Christian Adams, de 19 anos, foi preso depois de aceitar um acordo judicial no qual foi acusado de ter contratado um assassino profissional, pelo Facebook, para matar uma mulher que o acusara de estupro. Corey também foi condenado por tentativa de assassinato e outras infrações.
>
> Depois que a mulher, de 20 anos, alegou ter sido estuprada, Adams postou em seu mural uma oferta de US$500 por quem "trouxesse sua cabeça". A publicação também dizia que o jovem "queria a cabeça da mulher o quanto antes".
>
> (PORPHÍRIO, 2011)

### O homem que foi preso por fazer uma solicitação de amizade no Facebook

> Dylan Osborn, um inglês de 37 anos, foi preso por um erro muito comum. Assim que entrou no Facebook, mandou solicitação de amizade para todos seus contatos de email, sem saber. Uma ação padrão no site.
>
> O problema é que entre eles estava a ex-mulher, Claire Tarbox, que já tinha conseguido uma medida cautelar contra o marido.
>
> Dylan já havia sido acusado de abuso por mandar diversas mensagens e fazer telefonemas sem permissão. O inglês foi mantido na cadeia por dez dias, mas ficou apenas sete, sob a alegação de que haveria se confundido com os métodos do Facebook.
>
> (PORPHÍRIO, 2011)

## 5 Conclusão

Analisando os assuntos propostos e as atividades desenvolvidas, vemos que as redes sociais existem a partir do momento em que se formam grupos de pessoas compartilhando

informações com um objetivo em comum, e não apenas é aquilo que conhecemos por mídias sociais, sites de relacionamento, ou até mesmo as chamadas redes sociais na Internet. Funcionam como ferramentas de compartilhamento de informações entre comunidades, e estão cada vez mais presentes na rotina das pessoas, podendo ser acompanhadas 24 horas por dia, 7 dias por semana, possível pela mobilidade da Internet,  e acesso às mídias por telefone celular, ou outros dispositivos móveis. Porém, no que se diz respeito à segurança dos usuários, vemos que por se tratar de mídias relacionadas a maior rede de computadores, existem considerações quanto aos riscos envolvidos ao uso da Internet, e da segurança da Informação. Como exemplos de métodos práticos para manter os dados de cada usuário mais protegidos, podemos citar a manutenção adequada do computador, ou dispositivo que se conecte e troque informações com servidores de Internet, mantendo um bom programa antivírus atualizado, e sistemas de *firewall*, que assegurem a integridade, a disponibilidade e a confidencialidade dos dados de cada um, ou seja, que eles não sejam alterados por nenhum código malicioso, ou até mesmo um idivíduo mal intencionado, e estejam sempre disponíveis para quem realmente deve ter acesso, na busca de determinadas informações.

Em uma geração onde a troca de informação é dinâmica, é realmente difícil pensar que entre milhões de usuários, algum deles seria capaz de, dentre tantas opções, acabar por optar em caçar vítimas ou se aproveitar do compartilhamento de algumas informações inicialmente inocentes por parte dos usuários das mídias sociais, como o Twitter, porém vimos que existem ferramentas que levantam a questão da privacidade e do perigo de se compartilhar publicamente informações tais como a localização exata de cada um da rede social.

Adicionalmente, é levantado o alerta quanto aos dados considerados sensíveis de cada usuário, que são capazes de identificá-lo na rede, e que um terceiro em posse de tais dados podem acabar comprometendo inclusive a segurança física de pessoas desprevinidas.

Por fim, chegamos à conclusão de que a existem vantagens no uso da Internet como meio de se interagir socialmente utilizando mídias sociais, com inúmeras opções para entretenimento, busca de informações e *networking*. O desafio está em manter a consciência e mensurar não só a quantidade de informações e dados a se disponibilizar na Web, como também a qualidade, tendo em mente as consequências do que aquele conteúdo compartilhado pode causar para os envolvidos.

Espera-se que este trabalho sirva também de apoio para que os usuários consigam chegar ao nível de consciência para o melhor uso das informações que são dispersas pela utilização das

mídias sociais, com a utilização de cada tipo de mídia para seu propósito, e que assim aproveitem a Internet de maneira mais segura, sabendo de onde obter o melhor de cada tipo de informação, dos meios para se chegar até ela, e com os fins e resultados esperados alcançados.

## Referências

[1] WRAY, Richard. Internet data heads for 500bn gigabytes. **The Guardian**, Reino Unido, 18 mai. 2009. Disponível em <http://www.guardian.co.uk/business/2009/may/18/digital-content-expansion>. Acesso em: 01 out. 2011.

[2] NIC.br. Acesso às Tecnologias da Informação e da Comunicação (TIC). **CETIC.br**, Brasil, nov. 2010. Disponível em <http://www.cetic.br/usuarios/tic/2010-total-brasil/rel-geral-04.htm>. Acesso em: 01 out. 2011.

[3] NIC.br. Acesso sem Fio (Uso do Celular). **CETIC.br**, Brasil, nov. 2010. Disponível em <http://www.cetic.br/usuarios/tic/2010-total-brasil/rel-semfio-01.htm>. Acesso em: 01 out. 2011.

[4] Google Insights. Web Search Interest. **Google**, Brasil, nov. 2010. Disponível em <http://www.google.com/insights/search/#q=facebook.com%2Corkut.com%2Ctwitter.com&geo=BR&cmpt=q>. Acesso em 20 nov. 2011.

[5] ARAUJO, Nonata S. Segurança da Informação (TI). **Administradores**, Fortaleza, jul. 2008. Disponível em < http://www.administradores.com.br/informe-se/artigos/seguranca-da-informacao-ti/23933>. Acesso em: 01 out. 2011.

[6] BROOK, Jon-Michael C. CIA Triad. **CIPP Guide**, Estados Unidos da América, ago. 2010. Disponível em <http://www.cippguide.org/2010/08/03/cia-triad>. Acesso em: 01 out. 2011.

[7] STONEBURNER, Gary. **Underlying Technical Models for Information Technology Security**. NIST Special Publication 800-33, 2001.

[8] GUIMARÃES, Matuzalém. Segurança da Informação na Internet. **Viva o Linux**, Brasil, mai. 2008. Disponível em < http://www.vivaolinux.com.br/artigo/Seguranca-da-Informacao-na-Internet?pagina=1>. Acesso em: 20 nov. 2011.

[9] CERT.br. Cartilha de Segurança para Internet. **Comitê Gestor da Internet no Brasil**, São Paulo, 2006. Disponível em <http://cartilha.cert.br>. Acesso em: 01 nov. 2011.

[10] DA SILVA, Denise R. P.; STEIN, Lilian M. Segurança da informação: uma reflexão sobre o componente humano. **Ciências & Cognição**, Porto Alegre, RS, v. 10, p. 46-53, mar. 2007. Disponível em < http://www.sumarios.org/sites/default/files/pdfs/52416_6138.PDF>. Acesso em: 20 out. 2011.

[11] LEFEVER, Lee. Social Networking in Plain English: A short introduction to the concepts behind social networking websites. Common Craft. Disponível em <http://www.commoncraft.com/video/social-networking>. Acesso em: 25 nov. 2011.

[12] RAND. Paul Baran and the Origins of the Internet. Disponível em <http://www.rand.org/about/history/baran.html>. Acesso em: 26 nov. 2011.

[13] DEGÁSPERI, Israel S. Redes Sociais e Mídias Sociais, quais as diferenças? **Blog Mídias Sociais**, Brasil, mar. 2010. Disponível em <http://midiassociais.blog.br/2010/03/30/redes-sociais-e-midias-sociais-quais-as-diferencas/>. Acesso em: 26 nov. 2011.

[14] DEGÁSPERI, Israel S. Entendendo Redes Sociais e Mídias Sociais assim como suas ferramentas. **Blog Mídias Sociais**, Brasil, fev. 2010. Disponível em <http://midiassociais.blog.br/2010/02/23/redessociais-vs-midiassociais/>. Acesso em: 26 nov. 2011.

[15] JAGATIC, Tom. et al. Social Phishing. **Indiana Universitiy**, Bloomington, IN, dec. 2005. Disponível em < http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf>. Acesso em: 26 nov. 2011.

[16] SERRAO, Carlos. A Privacidade e a Segurança nas Redes Sociais. **Segurança de Aplicações Web**, Portugal, fev. 2010. Disponível em <http://webappsec.netmust.eu/2010/02/06/a-privacidade-e-a-seguranca-nas-redes-sociais/>. Acesso em: 27 nov. 2011.

[18] PORPHÍRIO, Rebecca. Os nove crimes mais improváveis cometidos via Facebook. **Techtudo**, Brasil, ago. 2011. Disponível em <http://www.techtudo.com.br/curiosidades/noticia/2011/08/os-nove-crimes-mais-improvaveis-cometidos-facebook.html>. Acesso em: 26 nov. 2011.

[19] AGÊNCIA ESTADO. Traficante vendia ecstasy via Facebook. **Info Online**, Brasil, ago. 2011. Disponível em <http://info.abril.com.br/noticias/internet/traficante-vendia-ecstasy-via-facebook-01082011-19.shl>. Acesso em: 27 nov. 2011.

[17] GOODMAN, Tammy B. Privacy: Popular GPS–based Sites Pose Security Risks. **SafetyWeb**, Estados Unidos da América, jun 2010. Disponível em <http://blog.safetyweb.com/privacy-popular-gps%E2%80%93based-sites-pose-security-risks/>. Acesso em 27 nov. 2011.