UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS QUIXADÁ

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

RAMON DOS SANTOS CAPISTRANO

REDES SOCIAIS VIRTUAIS COMO AMBIENTE DE EXPOSIÇÃO DE DADOS PESSOAIS PARA A ENGENHARIA SOCIAL

QUIXADÁ

2013

RAMON DOS SANTOS CAPISTRANO

REDES SOCIAIS VIRTUAIS COMO AMBIENTE DE EXPOSIÇÃO DE DADOS PESSOAIS PARA A ENGENHARIA SOCIAL

Monografia apresentada à Universidade Federal do Ceará (UFC), como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Sob a Orientação do Prof. Marcos Dantas Ortiz

QUIXADÁ

2013

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Campus de Quixadá

C242r Capistrano, Ramon dos Santos
Redes sociais virtuais como ambiente de exposição de dados pessoais para a engenharia social / Ramon dos Santos Capistrano. – 2013.
36 f. : il. color., enc. ; 30 cm.

Monografia (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Sistemas de Informação, Quixadá, 2013.
Orientação: Prof. MSc. Marcos Dantas Ortiz
Área de concentração: Computação

1. Redes socias on line 2. Facebook (Rede social on line) 3. Hackers I. Título.

CDD 006.754

Aos meus pais...

AGRADECIMENTOS

Ao corpo docente da UFC campus de Quixadá, especialmente aos professores Marcos Dantas Ortiz e Tânia Saraiva de Melo Pinheiro.

Às trinta pessoas que participaram desta pesquisa, a minha família e por último, mas não menos importante, a Deus.

“Apenas duas coisas são infinitas: o universo e a estupidez humana,
e eu não tenho certeza se isso é verdadeiro sobre o primeiro.”
(Albert Einstein)

RESUMO

As redes sociais virtuais vêm atraindo cada vez mais usuários da *Internet* e com a popularização deste seguimento cresce também o fluxo de informações pessoais expostas por parte de pessoas despreparadas para atuar nestes ambientes. O *Facebook* é a maior rede social virtual de todas e por isso foi escolhida para este trabalho relacionado à segurança da informação. Foi realizada uma pesquisa qualitativa com trinta pessoas de um universo específico através de questionário, entrevistas e análise das respectivas páginas sociais no *Facebook*. A atitude e o comportamento destas pessoas na rede social foram confrontados com técnicas da engenharia social de Kevin Mitnick. O resultado deste confronto é apresentado através de índices que mostram a quantidade de informações sensíveis que os usuários exibem na rede social, bem como seu nível de vulnerabilidade a possíveis ataques de um engenheiro social. O resultado da análise mostrou que a grande maioria das pessoas acaba colocando sua segurança em risco em virtude de um comportamento inadequado na rede social.

Palavras chave: Engenharia social; Redes sociais virtuais; Segurança da informação; *Facebook*.

ABSTRACT

Virtual social networks are attracting Internet users and their popularization also increases the flow of personal information exposed by people to untrained use these environments. Facebook is the largest virtual social network of all, and so it was chosen for this work related to information security. We performed a qualitative study of thirty people from a specific universe through questionnaires, interviews and the analysis of their social pages on Facebook. The attitude and behavior of these people in the social network were confronted with Kevin Mitnick´s social engineering techniques. The result of this comparison is presented using indices that show the amount of sensitive information that users present in the social network as well as their level of vulnerability to possible attacks from a social engineer. The result of the analysis showed that the vast majority of people end up putting their safety at risk because of inappropriate behavior in the social network.

Keywords: Social engineering; Virtual social networks; Information security; Facebook.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

As redes sociais virtuais estão presentes na vida da grande maioria das pessoas que acessam a *Internet.* De acordo com a (*E-Commerce News*, 2011 apud *comScore*, 2011) as redes sociais já conquistaram 81,4% de todos os internautas do mundo. As pessoas utilizam redes sociais com vários intuitos, seja por diversão, entretenimento, *hobby*, relacionamento, oportunidade, conhecimento ou interação. No entanto, em muitos casos as pessoas não percebem que estão expondo informações sensíveis e tornando-se alvos em potencial para pessoas mal intencionadas.

O crescimento nos últimos anos do uso das redes sociais virtuais tem como consequência dentre outras, a disponibilização de uma grande quantidade de dados e informações pessoais que podem muito bem ser utilizadas por *hackers* para os mais diversos fins. Essas informações podem servir de base para criminosos traçarem o perfil de pessoas que estão presentes nas redes sociais e, a partir daí, torná-las alvos de ataques baseados na engenharia social com objetivo de obter informações privilegiadas como senhas e números de cartão de crédito.

A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é. Como resultado, o engenheiro social pode aproveitar-se das vítimas para obter informações com ou sem o uso da tecnologia (MITNICK, 2003).

No mundo em que vivemos a informação é um bem precioso que deve ser protegido, no entanto é comum encontrar usuários que exibem algum tipo de informação pessoal sensível ou se relacionem facilmente com pessoas desconhecidas. Essas ações são vulnerabilidades que dão margem para que as informações desses usuários acabem sendo facilmente coletadas. Como o vazamento de informações sigilosas pode gerar sérias consequências de cunho moral e/ou financeiro, é fundamental saber atuar nas redes sociais sem cometer excessos que abram vulnerabilidades de fácil exploração.

Neste trabalho, foi realizado um estudo referente aos riscos de Segurança da Informação sobre os dados de usuários divulgados na rede social *Facebook*. A pesquisa foi organizada em várias etapas (leitura dos perfis, questionário, entrevista e análise dos dados), que se basearam tanto na abordagem quantitativa como na qualitativa, através de uma amostra de trinta pessoas que se enquadravam em um perfil previamente determinado (ver sessão 3.1).

A análise dos dados tentou avaliar as vulnerabilidades, expostas pelos usuários, que podem ser alvo de ataques de um engenheiro social. Foi verificado o tipo de informações pessoais que estes usuários exibem na rede social e se eles têm um perfil (comportamento/ações) que os enquadra como vítimas em potencial para um engenheiro social. Além disso, também se analisou o nível de confiança que esses usuários têm em pessoas que não conhecem pessoalmente, mas que são seus amigos na rede social. Os resultados mostraram, por exemplo, o quão propensos estes usuários estão a clicar em *links* enviados por seus amigos na rede social e que tipo de conversa (informações) eles manteriam com pessoas que não conhecem pessoalmente.

As maneiras como estes trinta usuários se comportam e reagem diante de determinadas situações no *Facebook* (sob o ponto de vista da divulgação de informações pessoais) foram analisadas sob os olhos da engenharia social e apresentadas como resultados deste trabalho.

2. REVISÃO BIBLIOGRÁFICA

2.1. Conhecendo o Ambiente das Redes Sociais Virtuais

2.1.1. Surgimento e Conceitos

As primeiras redes sociais virtuais surgiram há mais de 15 anos, mais precisamente em 1997, com o lançamento do *Sixdegrees*. Este *site*, apesar de pioneiro e de ter conseguido inúmeros usuários, não conseguiu um retorno financeiro satisfatório, o que acabou resultando no seu fechamento três anos mais tarde (E-DIALOG, 2010).

Segundo Aguiar (2006), as redes sociais virtuais caracterizam-se pelas interações de indivíduos em suas relações cotidianas, familiares, comunitárias, círculos de amizades, trabalho, estudo, militância, dentre outros. Elas também podem ser fomentadas por indivíduos ou grupos com poder de liderança, que articulam pessoas em torno de interesses, necessidades e/ou objetivos comuns (AGUIAR, 2006).

Como visto acima, a estrutura de uma rede social virtual é composta basicamente por dois elementos: os atores (pessoas, instituições ou grupos; os nós da rede) e suas conexões (interações ou laços sociais). Os atores são elementos das redes sociais também conhecidos como nós, que representam as pessoas que compõem a rede, eles constroem estruturas sociais através da interação e da constituição de laços sociais (RECUERO, 2009). Os nós podem ser classificados como: ativos, focal, isolados, lideres de opinião, especialistas e ponte, conforme apresentado no Quadro 1 (AGUIAR, 2006).

• Ativos: aqueles que mais frequentemente tomam a iniciativa da comunicação, alimentando a rede com informações.
• Focal: recebe o maior fluxo de mensagens da rede.
• Isolados: mantêm um comportamento passivo na rede, observam o fluxo de informações e discussões, mas são pouco comunicativos.
• Líderes de opinião: pessoas com o poder de influenciar as atitudes de um indivíduo ou de um grupo de participantes de uma rede.
• Especialistas: pessoas que possuem certos conhecimentos e/ou experiências vitais para a dinâmica e os objetivos da rede.
• Ponte: exerce o papel de único elemento de ligação entre dois ou mais nós.

Quadro 1 – Classificação de nós de uma rede social. Fonte: Aguiar (2006).

As conexões em uma rede social virtual são formadas pelos caminhos que ligam os nós, ou seja, pelas interações sociais entre os atores. Essas interações também são conhecidas por laços sociais (RECUERO, 2009, p. 30).

Os laços sociais podem ser fortes e fracos. Os laços fortes são caracterizados pela intimidade, pela proximidade e se dão em vias mais amplas e concretas para as trocas sociais. Os laços fracos, por sua vez, caracterizam-se por relações esporádicas que não traduzem proximidade nem intimidade (WELLMAN, 1997 apud RECUERO, 2005).

2.1.2. Dinâmicas

De acordo com Recuero (2005), elementos das redes sociais assumem diferentes formas dependendo do contexto onde se inserem. Quanto maior a centralização da rede,

menor a interação entre seus integrantes, por outro lado, quando a comunicação entre os usuários é aberta e abrangente, mais participação acontece na rede.

> Enquanto a teoria dos grafos e a topologia mapeiam uma rede como um conjunto de nós e arestas (entidades individuais e as relações entre elas), esta abordagem distorce um viés de polarização em direção a uma visão espacial das redes. Uma topologia ou mapa de uma rede não é uma representação em tempo real, está parada no espaço, mostrando-nos todos os possíveis nós e conexões. Entretanto, um nível de nossas experiências diárias – em comunicação, transporte e socialidade – a rede cria efeitos que são eminentemente baseados no tempo, na dinâmica. Isto significa que as redes são inerentemente dinâmicas, com mudanças constantes e variáveis, ambas dentro da composição dos nós individuais e das relações entre os nós. (RECUERO, 2009, p. 79).

O fluxo de informações em uma rede social virtual está sempre se modificando. Essas modificações constituem-se em um padrão importante para a compreensão das dinâmicas dessa rede. Para Aguiar (2006), a dinâmica de uma rede social corresponde ao processo de desenvolvimento das relações espaço-temporais estabelecido pelos integrantes da rede, podendo ser observada por quatro aspectos principais apresentados no Quadro 2.

• O padrão do fluxo de informação entre os nós.
• O ritmo das interconexões e do fluxo de informação, que pode ser contínuo ou descontínuo, regular (periódico), sazonal ou eventual.
• A frequência de participação (comunicação) dos usuários da rede.
• Os efeitos dessa participação nos demais membros e no desenvolvimento da rede.

Quadro 2 – Dinânica de uma rede social. Fonte: Aguiar (2006).

> O espaço em que as redes sociais se constituem e se proliferam são inerentes à informação e ao conhecimento, uma vez que são eles que movimentam as redes **(TOMAÉL; ALCARÁ; DI CHIARA, 2005).**

2.2. *Facebook*

O *Facebook* é a rede social mais popular e com mais usuários no mundo. É uma rede na qual o indivíduo pode criar o seu perfil e interagir com outras pessoas através de mensagens, vídeos, chats, games e outros aplicativos. Ela foi criada por Mark Zuckerberg e lançada em 2004 com o objetivo de ajudar alunos de escolas e faculdades dos EUA a trocar informações e manter contato com amigos (G1, 2008).

Em seu início, o *Facebook* era limitado com relação a quem poderia utilizá-lo, estando disponível apenas para alunos da Universidade de *Harvard*, onde estudava seu fundador. Em seguida, foi progredindo e permitindo a inscrição de estudantes de outras universidades até que em 2006 estava disponível para todo o mundo. Uma das particularidades do *Facebook* está no seu lado híbrido, em que, por um lado ela é uma rede social de estudantes com a interação proveniente dos jovens, enquanto, por outro, uma rede social para uso profissional onde as empresas não criam perfis, mas páginas personalizadas que podem ser divididas em abas com conteúdos diferenciados e com diferentes grupos de utilizadores (KIOSKEA.NET, 2010).

O sucesso das redes sociais virtuais é tão grande que apenas o *Facebook*, a maior delas, afirma ter mais de um bilhão de usuários, G1 (2013). Esse número é superior ao de pessoas que tinham acesso à *Internet* em 2004, ano em questão a população da *Internet* era de 757 milhões de pessoas. A empresa divulgou que a rede social possui mais usuários ativos (pessoas que não passam mais de um mês sem acessarem o site) do que as populações da Europa e da Rússia juntas, que chegam a totalizar 727 milhões de pessoas (G1, 2011).

Como é comum nas redes sociais, depois de criar uma conta o usuário pode adicionar ao seu perfil informações pessoais, como: data de nascimento, onde estuda, onde trabalha, onde mora, onde nasceu e preferências sobre uma série de temas. As informações vão desde seus filmes favoritos até sua orientação sexual e política, sendo o usuário quem decide quais informações deseja publicar, e consequentemente o grau de exposição que pretende assumir.

2.3. Segurança da Informação no Componente Humano

Garantir a segurança de suas informações é uma necessidade que o homem tem desde os primórdios da humanidade. Segredos, enigmas e códigos secretos existem há milhares de anos, consequentemente, as tentativas de decifrar tais códigos existem desde então. Partindo desse princípio não é errado afirmar que a segurança da informação existe há milhares de anos, porém, seu uso tem se destacado apenas nas últimas décadas com o advento da *Internet*.

Atualmente, a Segurança da Informação é de fundamental importância e indispensável na vida das empresas e de indivíduos comuns, afinal, em um mundo capitalista informação é dinheiro, e dinheiro é algo que todos querem manter em segurança. Dessa forma, as pessoas precisam manter seus dados confidenciais em sigilo, íntegros e acessíveis. De acordo com Silva e Stein (2007), a Segurança da Informação (SI) não está confinada a sistemas de computação, nem à informação em formato eletrônico, a SI se aplica a todos os aspectos de proteção da informação ou dados, em qualquer formato.

> A informação nos dias de hoje tem um valor altamente significativo e pode representar grande poder para quem a possui, seja pessoa, seja instituição. Ela possui seu valor, pois está presente em todas as atividades que envolvem pessoas, processos, sistemas, recursos financeiros, tecnologias etc. (REZENDE; ABREU, 2000 p.97).

Quando queremos ter acesso às informações que estão guardadas em algum sistema, usamos mecanismos de controle como a autenticação que ajuda a manter a confidencialidade e a integridade dos nossos dados, e um dos mecanismos mais usados pelas pessoas no exercício da Segurança da Informação são as senhas. Para Silva e Stein (2007), o uso de senhas como forma mais comum de controlar o acesso a informações secretas envolve dois mundos muito diferentes, o tecnológico e o humano; ambos têm características diferentes e por vezes conflitantes, o que torna mais complicada a tarefa da Segurança da Informação.

Pessoas podem elaborar senhas das mais variadas formas, sendo elas fortes ou fracas. Aparentemente, guardar uma senha que você mesmo idealizou não seria um problema, mas o que ocorre quando a quantidade de senhas que se precisa guardar é muito grande? Para resolver essa questão Silva e Stein (2007) explicam que muitas pessoas criam algum tipo de registro físico dos códigos secretos, seja eletronicamente ou em papel. Esse registro físico é disfarçado ou escondido, o que por sua vez pode gerar outros problemas como: lembrar qual o disfarce usado ou onde o registro físico foi armazenado. Pessoas escondem coisas das mais diversas formas, mas em geral existe uma lógica ou padrão envolvido nessas escolhas.

Conforme pode-se observar, a Segurança da Informação envolve dois mundos, o tecnológico e o humano. No que diz respeito à tecnologia existem ferramentas e sistemas que podem garantir um alto nível de proteção das informações, mas não se pode dizer o mesmo do

ser humano. Por mais treinada que uma pessoa seja, ela sempre costuma ser o elo mais fraco da Segurança da Informação e consequentemente o mais visado.

2.4. Engenharia Social

A engenharia social é a arte de manipular pessoas a fim de obter informações sigilosas sem que percebam que estão sendo vítimas de um engenheiro social. De acordo com Mitnick (2003, p.4) a engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na realidade ele não é. As maneiras de atuar são variadas e ele pode agir com ou sem o uso da tecnologia.

Muito da vulnerabilidade encontrada nas organizações não está em seus sistemas informatizados ou em suas normas de segurança, e sim, no elo mais fraco da segurança que é o ser humano. Uma organização pode ter adquirido as melhores tecnologias de segurança existentes no mercado, pode ter orientado e treinado muito bem seu pessoal de maneira que eles sigam as melhores práticas de segurança recomendadas pelos melhores especialistas, pode ter contratado os melhores guardas para o prédio, mesmo assim essa organização ainda estará vulnerável (MITNICK, 2003, p.4).

De acordo com Mitnick (2003, p.4), a segurança da informação avança a cada dia. Especialistas desenvolvem novas tecnologias de segurança, o que torna cada vez mais difícil a exploração de vulnerabilidades em um sistema. À medida que esse quadro evolui, os atacantes se voltaram cada vez mais para a exploração do elemento humano, porque quebrar a trava de segurança humana quase sempre é mais fácil e corresponde a um risco mínimo.

Diante do cenário apresentado acima, conseguimos compreender o porquê da engenharia social estar relacionada ao ser humano, mas o que levaria o homem a ser considerado o elo mais fraco da segurança? Mitnick (2003, p.4) explica que as pessoas são passíveis de sentimentos e ainda fica pior quando entra em jogo a credulidade, a inocência ou a ignorância.

2.4.1. Ataques

Existem muitos tipos de ataques que vão desde enviar um *link* passando-se por um amigo da vítima, até ataques mais complicados que envolvem diversas etapas de planejamento. Para Mitnick (2003, p.25) é incrível como um engenheiro social habilidoso pode alcançar seu objetivo com um ataque simples e direto. Um dos fatores principais para o sucesso de um engenheiro social é conhecer o campo onde se vai atuar. No caso de uma empresa, é necessário conhecer a linguagem (jargões e procedimentos), a sua estrutura corporativa, como seus escritórios e departamentos funcionam e as informações que utilizam. Dessa forma, pode-se fazer o reconhecimento do alvo para agir com naturalidade.

> Nunca ache que os ataques da engenharia social precisem ter mentiras elaboradas tão complexas que provavelmente serão reconhecidas antes de serem concluídas. Alguns são ataques diretos, rápidos e muito simples, os quais nada mais são do que... bem, simplesmente pedir as informações (MITNICK, 2003, p.30).

A citação acima pode nos dar a entender que a maioria das pessoas que possuem informações valiosas são completamente idiotas e que entregariam seus segredos facilmente, mas Mitnick (2003, p.33) nos mostra que o engenheiro social sabe que isso não é verdade. Um bom atacante prevê a suspeita e a resistência e sempre estará preparado para transformar a desconfiança em confiança, tudo faz parte de um jogo estratégico. Uma das técnicas para ganhar a confiança do alvo é prever as perguntas que ele pode fazer e com isso se preparar para dar as respostas corretas.

Como pôde ser observado até aqui, a confiança é o segredo para o sucesso de um ataque. Quando as pessoas não têm motivo para suspeitar, o trabalho do engenheiro social é facilitado e as chances desse ataque ter êxito são muito grandes. Assim, o atacante pode manipular e induzir a vítima a revelar informações sigilosas ou fazer com que ela execute ações de acordo com o que ele deseja. De acordo com Mitnick (2003, p.266), os sinais de um ataque são: recusa em dar um número de retorno, solicitação fora do comum, alegação de autoridade, ênfase na urgência, ameaça de consequências negativas em caso de não atendimento, mostra desconforto quando questionado, nome falso, cumprimentos ou lisonja e flerte.

Para ilustrar quão perigosos são os ataques de um engenheiro social, segue um exemplo simples: umas das práticas mais utilizadas na Segurança da Informação é a segurança física (através de controles de acesso e dispositivos eletrônicos) e Mitnick (2003, p.67) explica que essa prática de segurança não tem efeito para bloquear os ataques da engenharia social, pois todo e qualquer sistema de computadores do mundo que guardam informações sigilosas tem pelo menos um ser humano que o opera. Logo, se o engenheiro social puder manipular as pessoas que utilizam os sistemas, a segurança física do sistema é irrelevante.

> É da natureza humana achar que é improvável que você seja enganado em determinada transação, pelo menos até que tenha algum motivo para acreditar no contrário, Nós ponderamos o risco e, em seguida, na maior parte das vezes, damos às pessoas o benefício da dúvida. Esse é o comportamento natural das pessoas civilizadas... pelo menos as pessoas civilizadas que nunca foram enganadas, manipuladas ou trapaceadas em uma soma grande em dinheiro. Quando éramos crianças, nossos pais nos ensinavam a não confiar em estranhos. Talvez todos devêssemos adotar esse antigo princípio no ambiente de trabalho de hoje (MITNICK, 2003, p.37).

2.4.2. O ciclo da Engenharia Social

De acordo com Mitnick (2003, p.264), a engenharia social tem um ciclo baseado em quatro ações: pesquisa, desenvolvimento da credibilidade e da confiança, exploração da confiança e utilização das informações.

A primeira ação do ciclo, a pesquisa, consiste em aprender o máximo sobre o seu alvo e colher todas as informações possíveis sobre a vítima sem manter um contato direto com ela. De posse dessas informações é possível manter um primeiro contato com a vítima sem levantar qualquer suspeita, pois para ela aquilo parecerá um encontro casual.

A segunda ação consiste no desenvolvimento da credibilidade e da confiança, para isso serão usadas as informações obtidas com a pesquisa. O engenheiro age, fingindo ser outra pessoa, cita pessoas conhecidas da vítima, busca ajuda ou explora as afinidades.

A terceira ação é a exploração da confiança: o atacante solicita informações ou ações por parte da vítima. Inversamente, manipula a vítima para que ela peça ajuda ao atacante.

Por fim, a quarta ação do ciclo é a utilização das informações para a consumação do ato. Se as informações obtidas são apenas uma etapa para o objetivo final, o atacante retorna às etapas anteriores do ciclo até que o objetivo seja atingido.

2.5. Trabalho Relacionado

As vulnerabilidades do ser humano em relação à segurança da informação têm sido frequentemente pesquisadas nos últimos anos. Oliveira et al. (2011) em seu trabalho *Quantificação de vulnerabilidades em segurança da informação avaliando maturidade de pessoas (2011)* apresentam um instrumento que também quantifica às vulnerabilidades e ao mesmo tempo avaliam a maturidade das pessoas no que diz respeito a ameaças como *phishing* por e-mail, o uso de códigos maliciosos para a criação de vírus, *worms, backdoors* e *exploits.* A autora classifica a maturidade das pessoas com base em pontos (GR - grau de risco) atribuídos a cada opção de resposta das perguntas do seu questionário. Utilizando técnicas de Segurança da Informação e Engenharia Social, o trabalho apresenta resultados que afirmam ser possível quantificar o risco de quebra de segurança no que tange a maturidade das pessoas.

O trabalho de Oliveira et al. (2011) apresenta várias similaridades com a pesquisa apresentada neste trabalho. Dentre elas, é possível destacar o número de participantes (quarenta x trinta), a exposição das vulnerabilidades do fator humano, a engenharia social e a utilização de um questionário como parte da metodologia. Porém, existem diferenças importantes: o trabalho relacionado teve sua pesquisa voltada para as organizações empresariais, enquanto o presente trabalho investigou como o uso inadequado de uma rede social (*Facebook*) pode tornar-se um mecanismo facilitador para a engenharia social. Outra diferença entre os trabalhos são os resultados, enquanto o trabalho relacionado utiliza níveis (0 a 3 - grau de risco) para classificar a maturidade das pessoas e apontar as vulnerabilidades dos setores da organização pesquisada, o presente trabalho exibe os resultados apresentando as vulnerabilidades proporcionadas por pessoas ao se fazerem presentes no *Facebook* e o modo como elas poderiam ser exploradas por um engenheiro social.

3. PROCEDIMENTOS METODOLÓGICOS

3.1. Perfil dos Participantes

O trabalho foi realizado com trinta usuários da rede social *Facebook* naturais do estado do Ceará. Eles têm entre dezoito e quarenta anos e no momento da pesquisa faziam parte do quadro de funcionários de alguma empresa. São dez mulheres e vinte homens que usam o *Facebook* há pelo menos um ano e que possuem um nível de escolaridade igual ou superior ao ensino médio completo. A escolha do perfil foi baseada em três requisitos: (i) grau de escolaridade mínimo, para evitar pessoas que tivessem problemas sérios de interpretação de textos (ii) tempo mínimo de experiência com a rede social *Facebook*, evitar usuários novatos que não conhecem os recursos de segurança/privacidade além de não terem experiência em relacionar-se no ambiente social virtual e (iii) fazer parte do quadro funcional de alguma empresa pois vulnerabilidades nos recursos humanos de uma organização são um atrativo para a prática da engenharia social. Esse ambiente, teoricamente, deveria exigir dos usuários atenção com a privacidade das informações, relacionadas à organização, que são trocadas/expostas na rede social.

Os participantes da pesquisa (atores/nós da rede social) são todos do tipo isolados. Segundo Aguiar (2006), nós isolados mantêm um comportamento passivo na rede, observam o fluxo de informações e discussões, mas são pouco comunicativos. Como nós isolados são predominantes nas redes sociais, esta pesquisa buscou esse perfil na composição da amostra (pesquisar a classe mais populosa).

Todos os participantes da pesquisa foram escolhidos aleatoriamente desde que fizessem parte do universo dos perfis retratados nos dois parágrafos acima, neste trabalho não foram realizados ataques de engenharia social.

3.2. Coleta de Dados

Os dados da pesquisa foram obtidos em três etapas, são elas: análise das páginas dos usuários no *Facebook*, aplicação de questionários e entrevistas *online*. Essas etapas foram executadas na ordem apresentada acima e cada um dos trinta participantes da pesquisa foi

submetido a elas individualmente. Os questionários e as entrevistas foram elaborados e aplicados pelo autor.

Na primeira fase do trabalho é realizada uma pesquisa quantitativa, os usuários do *Facebook* tiveram suas páginas (mural, informações) exploradas pelo pesquisador a procura de dados e informações que pudessem ajudar a traçar o perfil dessas pessoas em relação à quantidade de informações que elas expõem e para quem elas expõem na rede social.

Na segunda fase segue a pesquisa quantitativa, porém, com abertura para comentários subjetivos. Foi solicitado aos participantes da pesquisa que respondessem a um questionário contendo treze perguntas objetivas e subjetivas. A aplicação do questionário se deu via *e-mail*.

De posse das respostas do questionário, iniciou-se a etapa qualitativa da coleta dos dados. Foram realizadas entrevistas através do *chat* do *Facebook* para ajudar a elucidar possíveis dúvidas nas respostas do questionário e obter um melhor aproveitamento da pesquisa com o cuidado necessário para não influenciar nas respostas.

Os dados coletados durante todas as etapas da pesquisa foram analisados e confrontados com as técnicas da engenharia social para que o objetivo geral do trabalho pudesse ser alcançado. O método de análise dos dados através da engenharia social foi desenvolvido com base no livro: *The art of deception: controlling the human element of security,* Mitnick (2003). As falhas de segurança encontradas no comportamento dos participantes foram exploradas de acordo com técnicas, relatos e experiências de Kevin Mitinick encontradas no livro citado acima. É importante ressaltar que todos os indivíduos que participaram dessa pesquisa consentiram no uso das informações obtidas neste trabalho.

4. RESULTADOS DA PESQUISA

4.1 Análises das Páginas dos Usuários no Facebook

O *Facebook* possui uma vasta lista de seções que possibilitam ao usuário adicionar suas informações e preferências sobre os mais variados temas. Se preenchidas, estas seções (músicas, status de relacionamento, grupos, cidade natal, etc.) exibem informações que podem parecer sem importância e inofensivas à segurança de quem as postou, mas para um

engenheiro social elas são uma verdadeira fonte de conhecimentos que facilita amplamente seu trabalho.

Sejam quais for os motivos que levam as pessoas a preencher tão detalhadamente seus perfis na rede social, o fato é que pela configuração atual do *Facebook* essas informações adicionadas à rede social em um primeiro momento aparecem como públicas. Se o usuário não tiver o cuidado de configurar a privacidade das seções do seu perfil, toda e qualquer pessoa que tenha uma conta no *Facebook* poderá visualizá-las.

O Quadro 3 abaixo apresenta o resultado da análise das páginas dos trinta participantes desta pesquisa. Nele, observa-se a variedade de informações exibidas pelos usuários, bem como o nível de privacidade adotado por eles.

	Linha do tempo	Lista de amigos	Músicas	Filmes	Jogos	Livros	Programas de TV	Opções 'Curtir'	Grupos	Atividades recentes	Onde estuda/estudou	Onde mora/morou	Onde trabalha/trabalhou	Cidade natal	Dia do aniversário	Status de relacionamento	Telefone	Endereço	Quem são seus parentes	Fotos pessoais	Fotos da família	Fotos do ambiente de trabalho	Fotos da residência/interior
User 1	A	F	F	F	F	F	F	F	F	A	F	F	F	F	F				F	A			
User 2	A	F	F	F		A	F	A	A	A	A	A	A	A	F					A	F		
User 3	A	A	A	A	A		A	A	A	A	A	A	A	A	A	A	F		A	A	A		
User 4	F	A	A					A		A	A	A	A	A	F	A			A	A	A		
User 5	F	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A			A	A	A		
User 6	A	A	A	F	A	F	F	A	A	A	A	A	A	A	F				A	A	A		
User 7	A	A	A	A	A	A	A	A	A	A	A	A		A	A	A			A	A	A	A	A
User 8	A	A	A	A	A	A	A	A	A	A	A	A			F			F	A	A	F		
User 9	A	A	A	A	A	A	A	A	A	A	A	A		A	F	F			A	A			
User 10	A	A	A	A	A	A	A	A	A	A	A	A	A	A	F	F			A	A			
User 11	F	F								F	F		F		F	F				F			
User 12	A	F	F	F	F	F	F	F	A	A	F	F		F	F	F			F	F	F		
User 13	A	A	A	F		F	F	A	A	A	A	F	A	A	F					A			
User 14	A	A	A	A	A	A	A	A	A	A	A	A	A	A	F	F			A	A	A		A
User 15	A	F	A	A	A	A	F	A	A	A	A	A	A	A	F					A	A		
User 16	A	A			A			A	A	A	A	A		A	F	F			A	A	A		
User 17	A	F	A					A	A	A	A	F	F	F	A	F			A	A	A	F	
User 18	A	A	A	A		A	A	A	A	A		F		F	A	A			A	A	A		
User 19	A	A	A		A		A	A	A	A	A	A	A	A	F	A			A	A			
User 20	A	A	A	A	A	A	A	A	A	A	A	F	A	A	F	F			A	A			

User 21	A	A	F	F	A	F	F	A	A	A	A	F	A	F	F	F			F	A	A		A
User 22	A	A						A		A	A				F	A				A			
User 23	A	A	A	A	A	A	A	A	A	A	A	A	F	A	F					A	A		
User 24	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A				A	A	A		
User 25	A	A	A	A	A	A	A	A	A	A	A	A	A	A	F	A			A	A	A		A
User 26	A	A	A					A	A	A	A	A	A	A	F	A			A	A	A		
User 27	A	A	F	F	F		F	F	A	A	F	A	F	A	A	A			F	A	A		
User 28	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A				A	A			
User 29	A	A	A					A	A	A	A	A		A	A					A			
User 30	A	A	A		A	A		A	A	A	A	A	A	A	F	A	F		A	A	A		
A – Informações abertas ao público																							
F – Informações fechadas ao público e aberta aos amigos																							

Quadro 3 – Conteúdo das páginas dos usuários do *Facebook* e seus níveis de privacidade.

É possível constatar no quadro acima que todos os usuários da pesquisa adicionaram informações pessoais em pelo menos quatro seções das suas páginas/perfis na rede social Deste total, 90% deixaram a maioria das suas informações em modo público, enquanto os outros 10% restringiram a maioria de suas informações ao público deixando-as visíveis apenas aos amigos.

Um resultado importante é a presença de números de telefones e endereços nas páginas de alguns usuários. A pesquisa nos mostra que 10% dos participantes exibem estas informações para os seus amigos no *Facebook* apesar desse tipo de informação abrir diversas possibilidades de ataques por parte de um engenheiro social. Além disso, através dessas informações é possível conseguir outras ainda mais sensíveis. Existem mecanismos para descobrir o endereço através do número do telefone e vice-versa. Alguns ataques podem ser realizados apenas com o intuido de conseguir um número de telefone ou o endereço da vítima, o que implica dizer que em 10% dos casos o engenheiro social teria seu trabalho amplamente facilitado, bastaria se tornar amigo da vítima na rede social.

> Quebrar a "*firewall* humana" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo. (MITNICK, 2003, p. 4).

4.1.1 Primeira Ação da Engenharia Social

Os resultados apresentados no Quadro 3 mostram a variedade e a quantidade de informações que podem ser colhidas através de uma simples visita à página de um usuário do *Facebook.* Para Mitnick (2003, p.264), o primeiro passo de um engenheiro social ao elaborar

um ataque é estudar bem a vítima, procurar colher o máximo de informações sobre ela para que o ataque seja rico em detalhes e consequentemente tenha mais chances de sucesso. Com as informações conseguidas, o engenheiro social será capaz de traçar o perfil da vítima e iniciar os trabalhos com um primeiro contato que parecerá completamente casual. Esse é um passo importantíssimo, pois além de se aproximar da vítima sem levantar suspeitas, também serve como alicerce para que em um segundo momento o engenheiro possa iniciar a fase de ganhar a confiança da vítima.

O quadro abaixo apresenta alguns resultados que mostram o quanto esse levantamento de informações da vítima é facilitado através do *Facebook*.

- 16,6% das pessoas exibem fotos do interior da sua residência ou do seu ambiente de trabalho.
- A linha do tempo do *Facebook* é a área que mostra todas as publicações do usuário e está aberta ao público em 90% dos casos.
- 80% das pessoas mantém sua lista de amigos na rede social em modo público.
- 66,6% dos usuários exibem para todos do *Facebook* quem são seus parentes.

Quadro 4 – Resultados percentuais da análise das páginas no *Facebook*.

Pode-se notar não só a relevância das informações exibidas, como também o alto percentual de usuários que as exibem em modo público. As informações são de vários tipos e fornecem um amplo material ao engenheiro social: informações visuais (as fotos do interior da casa ou do trabalho), informações sobre o que o usuário anda fazendo (publicações na linha do tempo) ou informações sobre as pessoas que os rodeiam. Todas essas vertentes podem ser seguidas por um atacante inescrupuloso na busca por uma aproximação casual, na busca por este primeiro contato que é à base de sustentação para todo o restante do ataque.

Onde mora/morou, onde estuda/estudou, onde trabalha/trabalhou, 90% das pessoas deixam abertas ao público pelo menos uma dessas três informações, que descrevem uma trajetória de vida e estão disponíveis para todos no *Facebook*. Com acesso a tais informações, um engenheiro social não só enriqueceria sua pesquisa como também abriria uma nova possibilidade de ataque. Sabendo onde essas pessoas trabalham, ele poderia aplicar golpes nas respectivas empresas usando informações privilegiadas que estas mesmas pessoas venham a fornecer.

4.1.2 Segunda Ação da Engenharia Social

O ganho da confiança da vítima pode ser conseguido de várias formas, seja demonstrando conhecimento ou afinidades, no entanto o engenheiro social nunca pode titubear e demonstrar desconhecimento sobre aquilo que está falando. Segundo Mitnick (2003, p.33), o engenheiro social, que prevê a suspeita e a resistência, está sempre preparado para transformar a desconfiança em confiança. Um bom engenheiro social planeja o seu ataque como um jogo de xadrez e prevê as perguntas que o seu alvo pode fazer para estar pronto para dar as respostas corretas.

Informações relacionadas às afinidades dos usuários como livros, filmes e músicas favoritas são fáceis de inserir no *Facebook* e chegam até a serem estimuladas com anúncios na rede social. O resultado é que 50% das pessoas preenchem pelo menos dois desses três quesitos e os deixam em modo público. Estas são preferências comuns a muita gente e aparentemente um engenheiro social não tiraria grande proveito dessas informações. No entanto, o engenheiro social poderia, por exemplo, usar os dados da seção de filmes para ajudar no processo de ganhar confiança. Neste caso, ele não iria explorar um filme ganhador de vários prêmios e que todo mundo conhece, mas sim procurar na lista de filmes favoritos da vítima o filme mais desconhecido, o mais incomum, justamente aquele que vai fazer com que a vítima se surpreenda ao saber que este alguém também gosta do mesmo filme que ela. Mas é preciso saber usar esta informação, um bom engenheiro social não iria simplesmente citar o nome filme e tentar mostrar que ele é uma boa pessoa só porque gosta do mesmo filme que a vítima. Ele iria usar de sutileza e buscar uma frase marcante do filme para usá-la num momento oportuno. Isso traria um impacto mais positivo e faria a vítima se sentir mais confortável, e ao se sentir confortável ela inconscientemente iria baixando suas defesas e progressivamente o atacante ganharia terreno.

4.1.3 Terceira Ação da Engenharia Social

Após consolidar o ganho de credibilidade e de confiança por parte da vítima, o engenheiro social começa a explorar esta confiança adquirida para extrair as informações desejadas. Ele pode fazer isso de várias formas que vão desde simplesmente pedir a informação em uma conversa informal, até o uso de processos mais elaborados com o uso da tecnologia. Um exemplo são os ataques onde o engenheiro ajuda a vítima com sugestões ou

mesmo soluções de problemas no seu computador, só que estes problemas que o atacante solucionou para a vítima foram criados por ele mesmo. No transcorrer do golpe, ele pede informações que, segundo ele, são necessárias para a resolução dos tais problemas na máquina. A vítima, na ânsia de ter seus problemas resolvidos, acaba cedendo o que o engenheiro social quer. O engenheiro também pode agir solucionado questões mais simples de uma forma bem solícita, para que depois a vítima se sinta agradecida e finalmente ele joga com sua gratidão para extrair informações através de um ou outro favor.

Um dos resultados obtidos através do questionário aplicado neste trabalho mostra que 73,2% dos participantes pesquisados pediriam ajuda a um amigo do *Facebook* que eles não conhecem pessoalmente. Este resultado mostra um alto índice de pessoas que estão propensas a agir de acordo com as práticas da engenharia social descritas no parágrafo anterior.

4.2 O Questionário e seus Resultados

Durante aplicação do questionário, os participantes não tiveram acesso às justificativas de criação de cada questão e a nenhum outro tipo de informação que pudesse influenciá-los nas respostas. O questionário foi apresentado contendo somente as seguintes treze perguntas.

1. Com que frequência você usa o *Facebook* (horas por dia / dias por semana)?

Esta pergunta ajuda a traçar o perfil dos usuários mostrando o quão presentes eles estão na rede social. Como resultado, 10% dos pesquisados acessam o *Facebook* por no máximo três dias por semana. Estes usuários não permanecem mais que duas horas diárias conectados na rede social. Já os outros 90% acessam o *Facebook* todos os sete dias da semana. Estes usuários chegam a ficar conectados cerca de 03h40min (três horas e quarenta minutos) em média por dia, chegando a totalizar 25h40min (vinte e cinco horas e quarenta minutos) por semana.

Obviamente as facilidades de acesso oferecidas pelos dispositivos móveis contribuem para que as pessoas estejam sempre conectadas e façam esta média ser tão alta. Este resultado demonstra a intensidade da presença das pessoas nas redes sociais (mais especificamente no *Facebook*) e daí a importância de saberem atuar nesses ambientes.

2. Conhece pessoalmente todos os seus amigos do *Facebook*?

Caso a resposta seja não, já se abre a possibilidade para um engenheiro social estar entre eles.

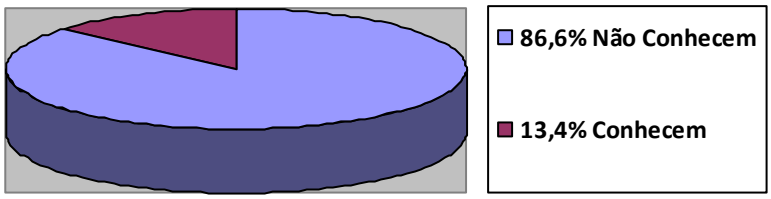

Gráfico 1 – Conhecer pessoalmente todos os amigos no *Facebook.*

Conforme ilustrado no Gráfico 1, 86,6% dos usuários não conhecem pessoalmente todos os seus amigos no *Facebook*. Diante da facilidade de interagir e encontrar pessoas nas redes sociais, este percentual não chega a ser surpreendente, pois a maioria das pessoas não leva a sério essa questão de aceitar como amigo alguém até então desconhecido. Este é mais um dos fatores que tornam as redes sociais lugares favoráveis à engenharia social.

3. Qual seu grau de dependência do *Facebook*?

A) Não consigo viver sem.

B) Se ele deixasse de existir eu estaria usando outra rede social tranquilamente.

C) Se ele deixasse de existir eu ficaria um período sem usar redes sociais.

Caso sinta necessidade de complementar sua resposta, faça abaixo.

Esta pergunta mostra não só a dependência que o usuário tem de *Facebook*, como também a dependência de redes sociais como um todo.

Com 97,7% dos usuários respondendo a alternativa B, pode-se concluir que o *Facebook* não é indispensável para essas pessoas, pois se ele deixasse de existir, os usuários estariam usando outra rede social numa boa. Por outro lado, fica claro como as redes sociais são imprescindíveis para elas, já que nem a extinção da maior das redes sociais afetaria esses usuários no sentido de continuarem presentes neste seguimento.

4. Você faz parte de algum grupo no *Facebook* onde as pessoas postam o que desejam comprar, vender ou trocar, como por exemplo, o mercado livre?

Expor os seus planos com relação ao que pretende comprar ou vender é mais uma informação que um engenheiro social poderia usar para promover um contato que pareça casual.

O *Facebook* está repleto de comunidades deste tipo, 70% dos participantes responderam que fazem parte de pelo menos um grupo de compra e venda de produtos de pessoa para pessoa. Foi constatado ainda que os grupos preferidos são aqueles compostos por pessoas geograficamente próximas (mesma cidade). Essa é uma oportunidade para um engenheiro social se aproximar da vítima sem levantar qualquer suspeita. O atacante ainda poderia explorar um pouco mais esta oportunidade para dar sequência ao seu ataque. Ele iniciaria a segunda etapa do clico da engenharia social ao demonstrar que tem confiança na vítima lhe vendendo algo parcelado. Isso geraria uma justificativa para contatos futuros que possibilitariam continuar o processo de conquista da confiança.

5. Você já utilizou algum daqueles aplicativos do *Facebook* que dizem com qual celebridade você se parece, ou qual personagem você é, ou ainda aqueles que listam quem são os amigos que mais visitam seu perfil, ou algum do tipo?

Pessoas que fazem isso, usam aplicativos que para poderem ser instalados necessitam ter acesso a uma série de permissões de acesso à conta do usuário no *Facebook*. Nada impede que um engenheiro social crie um aplicativo desses.

O resultado aponta que 82,5% dos pesquisados nunca utilizou nenhum aplicativo deste tipo. Aplicativos como os citados acima existem aos montes no *Facebook* e qualquer desenvolvedor pode criar um. Os demais participantes (17,5%) disseram que já utilizaram esses aplicativos em algum momento. Para citar um exemplo, uma das permissões que os usuários concedem aos administradores destes aplicativos é a de ‘publicar em meu nome’. Um engenheiro social poderia fazer grandes estragos com uma permissão dessas, como enviar *links* e convites para os amigos de uma determinada pessoa como se fosse ela. Após o engenheiro iniciar os ataques a diversas vítimas, ele teria seu aplicativo denunciado ou bloqueado pelo *Facebook*, porém o estrago já estaria feito.

6. Você costuma fazer *check-in* em locais aonde vai, (eventos, festas, viagens) e com que frequência?

Neste caso, o usuário está fornecendo informações em tempo real de onde se encontra. Essa é mais uma forma de um engenheiro social conseguir um primeiro contato com a vítima de modo que pareça casual. Consequentemente, o usuário também está fornecendo informações de onde não se encontra, nesse caso sua casa estaria sozinha e sua caixa de correio poderia ser visitada por alguém a procura de informações como um número de CPF.

Esta questão apontou que 63,4% dos participantes costumam fazer *check-in* quando saem de casa para passear. Este resultado mostra a força das redes sociais nos dispositivos móveis e evidencia a alta quantidade de usuários adeptos desta prática favorável à engenharia social.

7. Você conversa assuntos da empresa com os seus colegas de trabalho via *Facebook*?

A) Sim, através de postagens no mural.

B) Sim, falando em tempo real através do chat.

C) Sim, utilizando um grupo fechado somente com colegas da empresa.

D) Não converso.

Caso sinta necessidade de complementar sua resposta, faça abaixo.

Esta questão é para constatar se o usuário fala sobre assuntos de trabalho no *Facebook* e como ele o faz. Esta constatação é fundamental para classificar o perfil do usuário, já que falar sobre assuntos de trabalho via rede social seria uma prática que facilitaria muito o trabalho do engenheiro social no caso do alvo do ataque ser a empresa em que esta pessoa trabalha.

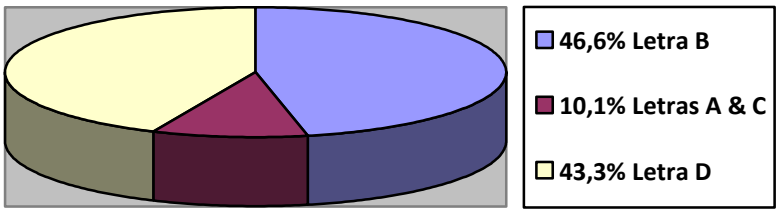

Gráfico 2 – Comentar assuntos da empresa via *Facebook*.

Como observado no Gráfico 2, 46,6% responderam a letra B. Esta opção foi a mais votada dentre aqueles que afirmaram conversar sobre assuntos de trabalho na rede social. Aparentemente conversar pelo chat do *Facebook* é a maneira mais segura e confidencial de trocar informações pela rede social, mas isso não quer dizer que as pessoas que se utilizam disso estejam invulneráveis a ataques e violações. Combinando as alternativas A, B e C, chega-se a um total de 56,7% de pessoas que conversam assuntos de trabalho na rede social por estes diferentes meios, ou seja, a maioria das pessoas estaria propiciando pelo Fecebook a oportunidade de atuação de um engenheiro social na sua área profissional. 43,3% responderam a letra D.

8. Alguém postou um *link* com uma matéria do seu interesse (política, saúde, lazer, trabalho, etc), este alguém é um amigo que interage frequentemente com você, porém você não o conhece pessoalmente. O que você faz?

A) Clico e vejo a matéria normalmente, pois é do meu interesse.

B) Só clico se conhecer pessoalmente quem postou.

C) Clico se eu conhecer o site, não importa quem postou.

D) Não clico.

Caso sinta necessidade de complementar sua resposta, faça abaixo.

Esta é sobre a questão de clicar em *links* enviados por pessoas que não conhece pessoalmente, além de também servir para analisar a confiança que os usuários têm nessas pessoas.

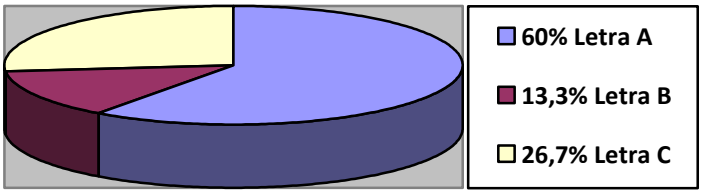

Gráfico 3 – Clicar em *links* enviados por pessoas não conhecidas pessoalmente.

De acordo com o Gráfico 3, observa-se que 60% das pessoas responderam letra A. Isso mostra que a maioria delas não se preocupa com o risco de clicar em *links* enviados por

desconhecidos. Ao atacante, bastaria camuflar o *link* com algo que lhes interessasse e estes usuários clicariam. Mais uma vez, um alto número de pessoas está expondo vulnerabilidades e facilitando o trabalho do engenheiro social.

Conhecer pessoalmente a pessoa que postou o *link* (letra B) é significante para 13,3% dos usuários. No entanto, isso não garante nada pois um engenheiro social poderia acessar a conta de um amigo e enviar um *link* para esta pessoa de modo que não pareça *spam*.

As pessoas que não se importam com quem postou desde que conheçam o site do *link* representam 26,7%. A alternativa C pode parecer completamente segura, todavia existem redutores de *links* como o *meu.ms* que dificultam a identificação do *site*. Além disso, o *Facebook* permite que um *link* seja postado com a logo de qualquer outro *site*. É necessário apenas colocar um *link* (*site* confiável) no campo *status*, como se fosse postá-lo, em seguida o *Facebook* irá gerar uma visualização com a logo desse *link*. Após essa visualização ter sido gerada, bastaria trocar o *link* da visualização por outro *link* reduzido (*link* malicioso) e a postagem seria exibida com o *link* trocado, mas com a logo do primeiro *link* (*site* confiável). Esta seria mais uma forma do engenheiro conseguir que a vítima clicasse no *link* já que ele aparentaria ser totalmente seguro por ser de um site confiável.

9. Um dos seus melhores amigos no trabalho está com uma dúvida urgente sobre um processo importante na empresa, porém no momento vocês não estão próximos fisicamente, então ele recorre ao *chat* do *Facebook* para lhe pedir ajuda com a tal dúvida. O que você faz?

A) Conversa tranquilamente, pois você está falando em modo privado e ele é um amigo de confiança.

B) Apesar de o amigo ser de confiança, você responde apenas o básico por não ficar à vontade falando de assuntos importantes via chat do *Facebook*.

C) Não responde, pois você só fala sobre esses assuntos pessoalmente.

Caso sinta necessidade de complementar sua resposta, faça abaixo.

Através desta questão, verifica-se se os usuários estão propensos a trafegar informações importantes da empresa pelo *Facebook*. O resultado mostra que mais da metade das pessoas, 53,3% responderam a letra A, falaria tranquilamente sobre processos importantes da empresa com um amigo de trabalho pelo *Facebook*.

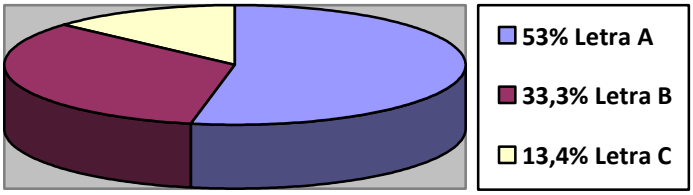

Gráfico 4 – Divulgar informações importantes da empresa via *Facebook*.

A alternativa B foi escolhida por 33,3% dos usuários e eles responderam que falariam sobre processos importantes da empresa com um colega de trabalho pelo *Facebook*, porém não se aprofundariam na conversa por não se sentirem completamente seguros em realizá-la via rede social. Já outros 13,4% responderam que falariam apenas pessoalmente.

Mais uma vez, um alto número de pessoas que conversaria informações da empresa via *Facebook*, no entanto neste caso há o agravante de serem informações importantes. Nesse caso, um engenheiro social poderia atacar uma pessoa amiga deste usuário, conseguir acesso ao *Facebook* dela e se passar por esta pessoa. Dessa forma, o engenheiro poderia pedir informações sigilosas ao usuário que pensa estar falando com a pessoa amiga.

10. Você está com um problema, no entanto é algo que pode ser solucionado facilmente com algumas dicas de alguém que entenda do assunto. Para solucionar esse problema você pediria ajuda a um amigo do *Facebook* que você não conhece pessoalmente, mas que você sabe que ele está capacitado para te ajudar?

Esta é útil para completar a avaliação da confiança que os usuários do *Facebook* têm em pessoas que eles não conhecem. Essa questão também é uma das técnicas da engenharia social usada na fase da exploração da confiança. Ela consiste em manipular a vítima para que ela peça ajuda ao engenheiro social. Isso pode ser conseguido após o atacante demonstrar conhecimento na área em questão, em seguida, o próprio engenheiro causaria o problema para que a vítima solicitasse ajuda a dele.

O sim foi maioria, 73,3% das pessoas afirmaram que pediriam ajuda a alguém que conhecem somente pelo *Facebook*. É claro que existem diversas gravidades de problemas, talvez se a pergunta especificasse um tipo de problema sigiloso este percentual fosse menor, correto? Errado, segundo Mitnick (2003, p.140) a gravidade do problema não afeta a decisão

do usuário de pedir ajuda, isso depende exclusivamente da capacidade do engenheiro social de construir sua imagem de forma convincente na área que deseja atacar.

11. A empresa possui política de segurança da informação definida e divulgada?

As questões onze e doze são para verificar se as vulnerabilidades oriundas do comportamento do funcionário estão presentes mesmo quando a empresa possui política de segurança.

O resultado aponta que 46,6% das pessoas responderam que a empresa em que trabalham não tem uma política de segurança da informação definida e divulgada. Este despreparo das empresas corrobora com os altos índices de práticas errôneas dos funcionários ao compartilhar informações da empresa sem o devido sigilo.

12. A empresa orienta seus funcionários como deve ser feita a comunicação fora do espaço físico da empresa?

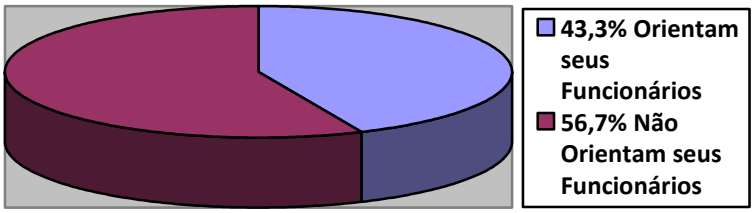

Gráfico 5 – Orientação dos funcionários nas empresas.

O Gráfico 5 mostra que 56,7% das empresas não orientam como os funcionários devem se comunicar fora dela. Nota-se um acréscimo no percentual desta questão em relação à questão anterior. Isso mostra que uma grande parcela das empresas analisadas não prepara os seus funcionários contra o vazamento de informações.

Foi visto na questão sete que 56,7% das pessoas conversam assuntos da empresa via *Facebook*. Exatamente o mesmo percentual que afirmou que a empresa não os orienta sobre a comunicação dos funcionários fora dela. Coincidência? Claro que não, esta é uma evidência clara da importância de uma boa política de segurança da informação nas empresas.

13. Sua função na empresa em que trabalha é gerencial, operacional ou terceirizado?

Esta questão mostra que a pesquisa alcançou diversos perfis em que o mais frequente foi o operacional. No entanto, cada um deles pode ser alvo de Engenharia Social no ataque à empresa e quanto maior o cargo, mais sensíveis são as informações.

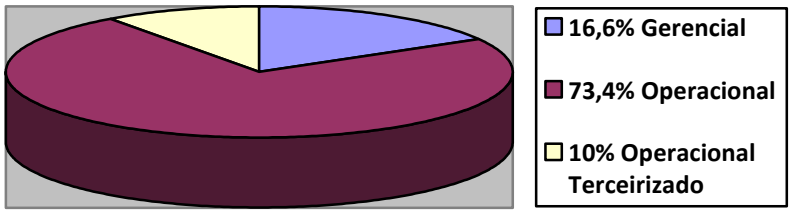

Gráfico 6 - Funções das pessoas nas empresas em que trabalham.

4.3 Análises Finais

Após a análise das páginas dos usuários no *Facebook*, foi observada uma alta quantidade de informações pessoais exibidas e da baixa privacidade atribuídas a elas. Observando o Quadro 3, nota-se que o *Facebook* se mostra um grande banco de dados aberto ao engenheiro social em que as informações estão à disposição de todos. Sejam quais for os motivos que levam as pessoas a divulgarem tantas informações, a realidade é que este cenário evidencia o despreparo dos usuários em relação à segurança da informação.

Deixar informações pessoais abertas ao público e aceitar como amigo gente desconhecida são dois pontos chave, pois mesmo se a pessoa bloqueasse suas informações ao público isso de nada adiantaria se ela adicionasse pessoas desconhecidas na rede de amigos. E foram estas as atitudes avaliadas no trabalho. Foram vistos altos percentuais de pessoas que se comportam erroneamente na rede social, atitudes que vão da falta de atenção com possíveis *links* maliciosos à divulgação de informações importantes da empresa. Diante de tantos resultados negativos e de tanta falta de segurança uma frase do Mitnick é confirmada: “o ser humano é o elo mais fraco da segurança”. Este trabalho ajudou a compreender um pouco mais a relevância desta afirmação.

> É incrível como é fácil para um engenheiro social convencer as pessoas a fazerem as coisas com base no modo como ele estrutura a solicitação. A tese é acionar uma resposta automática com base nos princípios psicológicos e utilizar os atalhos mentais que as pessoas usam quando percebem que o interlocutor é um aliado (MITNICK, 2003, p. 4).

5. CONSIDERAÇÕES FINAIS

Este trabalho apresentou um levantamento da fragilidade da segurança de um universo específico de pessoas em relação ao comportamento na rede social *Facebook.* Os resultados foram apresentados de forma objetiva e não só apontaram as falhas e vulnerabilidades deste universo de pessoas como também quantificaram e qualificaram cada uma delas.

A principal dificuldade deste trabalho foi elaborar um questionário que não fosse tendencioso. Outra dificuldade foi conseguir que pessoas desconhecidas participassem da pesquisa. Para isso, foram feitos contatos através de amigos e de amigos de amigos para que os participantes fossem escolhidos da forma mais aleatória possível dentro do universo de pessoas proposto.

O trabalho chega ao seu final deixando contribuições para as pessoas que estão presentes nas redes sociais virtuais e para as que não estão. Evidencia-se aqui o alerta sobre os perigos e ameaças que os usuários estão submetidos nestes ambientes e como devem se portar nestas redes sociais.

REFERÊNCIAS

AGUIAR, S. Redes sociais e tecnologias digitais de informação e comunicação., Rio de Janeiro, mar./ago. 2006. Disponível em: <http://www.observatoriodaimprensa.com.br/download/redes_sociais_e_tecnologias_digitais%20.pdf>. Acesso em: 10 nov. 2011.

E-COMMERCE NEWS. Redes sociais já conquistam 81,4% de todos os internautas do mundo, diz comScore, [Matéria publicada em 27 de setembro de 2011, na Internet].

Disponível em: <http://ecommercenews.com.br/noticias/pesquisas-noticias/redes-sociais-ja-conquistam-814-de-todos-os-internautas-do-mundo-diz-comscore>. Acesso em: 10 nov. 2011.

E-DIALOG. A primeira mídia social, [Matéria publicada em 27 de setembro de 2010, na Internet]. Disponível em: <http://www.edialog.com.br/midia-social/a-primeira-midia-social/>. Acesso em: 10 jul. 2013.

GARTON, Laura; HARTHORNTHWAITE, Caroline; WELLMAN, Barry. **Studying Online Social Networks.** *Journal of Computer Mediated Communication*, V 3, issue 1 (1997). Disponível em: <http://www.ascusc.org/jcmc/vol3/issue1/garton.html>. Acesso em 12/04/2004.

G1. Facebook tem o mesmo número de usuários que o total da web em 2004, [Matéria publicada em 05 de outubro de 2011, na Internet]. Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/10/facebook-tem-o-mesmo-numero-de-usuarios-que-o-total-da-web-em-2004.html>. Acesso em: 10 nov. 2011.

G1. Facebook alcança um bilhão de usuários ativos mensais, [Matéria publicada em 04 de outubro de 2012, na Internet]. Disponível em: <http://g1.globo.com/tecnologia/noticia/2012/10/facebook-atinge-1-bilhao-de-usuarios-ativos-mensais.html>. Acesso em: 31 jul. 2013.

G1. O que é: Facebook, [Matéria publicada em 17 de abril de 2008, na Internet]. Disponível em: <http://g1.globo.com/Noticias/0,,MUL394773-15524,00.html>. Acesso em: 10 nov. 2011.

KIOSKEA.NET. O fenômeno Facebook, [Matéria publicada em 31 de março de 2010, na Internet]. Disponível em: <http://pt.kioskea.net/faq/3621-o-fenomeno-facebook>. Acesso em: 10 nov. 2011.

MITNICK, Kevin D.; SIMON, Willian L. **The art of deception: controlling the human element of security.** São Paulo: Pearson Education, 2003. 284p.

OLIVEIRA M. C. *Quantificação de vulnerabilidades em segurança da informação avaliando maturidade de pessoas*. 2011. 20 f. TCC (Bacharelado em Redes de Computadores) - Universidade Luterana do Brasil (Ulbra), Canoas, Rio Grande do Sul. 2011.

RECUERO, Raquel da Cunha. **Redes Sociais da Internet.** São Paulo: Sulina, 2009. 191p.

RECUERO, R. C. Comunidades Virtuais em Redes Sociais na Internet: Uma proposta de estudo. Ecompos, Internet, Pelotas, v. 4, n. dez. 2005. Disponível em: <http://www6.ufrgs.br/limc/PDFs/com_virtuais.pdf>. Acesso em: 10 nov. 2011.

REZENDE, Denis A.; ABREU, Aline F. **Tecnologia da Informação Aplicada a Sistemas de informações Empresariais**. São Paulo: Atlas, 2000.

SILVA, D. R. P.; STEIN, L. M. Segurança da informação: uma reflexão sobre o componente humano., Porto Alegre, V. 10: 46-53, mar. 2007. Disponível em: <http://www.sumarios.org/sites/default/files/pdfs/52416_6138.PDF> Acesso em: 10 nov. 2011.

TOMAÉL, M. I. et al. Das redes sociais à inovação. Ci. Inf., Brasília, v. 34, n. 2, p. 93-104, mai/ago. 2005. Disponível em: <http://www.scielo.br/pdf/ci/v34n2/28559.pdf> Acesso em: 10 nov. 2011.