CENTRO PAULA SOUZA

COMPETÊNCIA EM EDUCAÇÃO PÚBLICA PROFISSIONAL

GOVERNO DO ESTADO SÃO PAULO

ESCOLA TÉCNICA PROFESSOR MASSUYUKI KAWANO

TÉCNICO EM REDES DE COMPUTADORES

JEFERSON APARECIDO DA SILVA

JOSE ROBERTO DIAS JUNIOR

LEANDRO AFFONSO VIVALDINI

LUIS GUILHERME PEREIRA NISHIYAMA

RAYSSA THAINÁ KATAOKA DE CARVALHO SILVA

RONALDO KEIJI KOMAKOME

VIVIANE ZORATTO PINHEIRO DE MATOS

ENGENHARIA SOCIAL - SEGURANÇA DA INFORMAÇÃO

Tupã - SP

2016

CENTRO PAULA SOUZA
COMPETÊNCIA EM EDUCAÇÃO PÚBLICA PROFISSIONAL

ESCOLA TÉCNICA PROFESSOR MASSUYUKI KAWANO

TÉCNICO EM REDES DE COMPUTADORES

JEFERSON APARECIDO DA SILVA

JOSE ROBERTO JUNIOR

LEANDRO AFFONSO VIVALDINI

LUIS GUILHERME PEREIRA NISHIYAMA

RAYSSA THAINÁ KATAOKA DE CARVALHO SILVA

RONALDO KEIJI KOMAKOME

VIVIANE ZORATTO PINHEIRO DE MATOS

ENGENHARIA SOCIAL - SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado à ETEC Prof. Massuyuki Kawano, como requisito parcial para obtenção do título de **Técnico em Redes de Computadores.**
Orientador: Anderson Tukiyama Berengue

Tupã – SP

2016

ETEC PROF. MASSUYUKI KAWANO
TÉCNICO EM REDES DE COMPUTADORES

JEFERSON APARECIDO DA SILVA

JOSE ROBERTO JUNIOR

LEANDRO AFFONSO VIVALDINI

LUIS GUILHERME PEREIRA NISHIYAMA

RAYSSA THAINÁ KATAOKA DE CARVALHO SILVA

RONALDO KEIJI KOMAKOME

VIVIANE ZORATTO PINHEIRO DE MATOS

ENGENHARIA SOCIAL - SEGURANÇA DA INFORMAÇÃO

Dissertação para obtenção do título

BANCA EXAMINADORA:

_____

Prof. Orientador: Anderson Tukiyama Berengue

_____

Prof (a). Validador (a)

_____

Prof (a). Validador (a)

Tupã, 28 de junho de 2016.

É de inteira responsabilidade o conteúdo do trabalho apresentado pelo aluno. O Professor Orientador, a Banca de Validação e a Instituição não são responsáveis e nem endossam as ideias e o conteúdo do mesmo.

Dedicamos este trabalho primeiramente a Deus, aos nossos pais e a todos os amigos, a toda a equipe de professores competentes, por esse novo desafio que será mais uma conquista em nossas vidas!

Agradecemos a Deus pela força que nos tem dado até a conclusão do curso, aos Docentes do Curso Técnico de Redes de Computadores pela dedicação, sempre incentivando-nos e nos ensinando a desenvolver sempre o melhor para adquirirmos competências e habilidades; pela generosidade e confiança depositada em nós diante de todos os momentos difíceis e por compartilhar de seus conhecimentos profissionais e humanos.

Resumo

Nos últimos anos as tecnologias de informação e comunicação têm evoluído de forma rápida, fazendo com que pessoas e organizações tenham maior preocupação em tomar decisão, devido a este fato, as chances de pessoas a não usarem sistemas de informação tornou-se praticamente inválidas, a importância de se utilizar mecanismos de segurança e de armazenamento das informações é vital para a sobrevivência e competitividade destas pessoas e organizações, no passado a questão segurança da informação era uma preocupação não muito abordado, pois os arquivos contendo inúmeros papéis podiam ser trancados fisicamente, porém com a chegada das tecnologias da informação e a comunicação a questão ficou bem mais complexa, hoje, a maioria dos computadores conecta-se a internet e consequentemente a internet conecta-se a eles, além disto, sabemos que dados em formato digital são portáteis, este fato fez que estes ativos tornassem atrativos para pessoas com intuito malicioso, portanto podemos dizer que não existe segurança absoluta, torna-se necessário agirmos no sentido de descobrir quais são os pontos vulneráveis e a partir daí avaliar os riscos e impactos, e rapidamente providenciar para que a segurança da informação seja eficaz. Infelizmente o que acontece na prática é que muitas pessoas e empresas não dão o devido valor a esta questão e por muitas vezes o preço é muito alto, portanto este trabalho tem como intuito mostrar a fragilidade da segurança quando se diz respeito a dados de informações pessoais em Redes Sociais. Por mais que se tente privar esses dados, restringir informações, ainda é fácil descobrir quase tudo que quiser, principalmente em Redes Sociais, onde as pessoas acabam expondo imagens ou informações de onde estão com quem estão, onde mora, etc. Ficando assim mais vulneráveis, pessoas mal intencionadas utilizam as Redes Sociais, para conseguir essas informações e aplicar algum tipo de golpe virtual ou até mesmo fora da virtualidade. O objetivo deste projeto é alertar sobre os riscos que trazem a exposição dos dados nas Redes Sociais, mostrar que não se pode confiar em qualquer um ou qualquer tipo de informação dentro da Rede; o melhor caminho é reduzir ao máximo quaisquer riscos às informações, seguindo um trajeto no sentido único de manter a integridade.

Palavras chaves: Informação, Rede Social, Segurança, Integridade.

Índice de Figuras

Figura 1 – Ataques Hackers em empresas (Fonte ttp://www.psafe.com/blog/grandes-ataques-hackers-empresas-governos/) 27

Figura 2 – Redes de Blogs - (Fonte da imagem: Gawker Media) 30

Figura 3 – Central Intelligence Agency (Fonte da imagem: Governo dos Estados Unidos) 30

Figura 4 - Albert Gonzales (Fonte da imagem: Governo dos Estados Unidos) 32

Figura 5 –Redes Sociais mais utilizadas 33

Figura 6- Tempo conectado nas Redes Sociais 33

Figura 7- Postagem de fotos frequêntemente 34

Figura 8-Dados pessoais verdadeiros nas Redes Sociais 34

Figura 9-Troca de imagens intimas nas Redes Sociais 35

Figura 10-Pessoas que conhecem seus amigos das Redes Sociais pessoalmente 35

Figura 11- Pessoas que aceitam pedidos de amiazade de desconhecidos 36

Figura 12- Pessoas que sofreram algm tipo de vazamento de informaç 36

Figura 13-Prejuízos sofridos 37

SUMARIO

1. Introdução 10
2. Objetivos 11
2.1. Objetivo Geral: 11
2.2. Objetivo Específico: 12
3. Justificativa 12
4. Metodologia 12
5. Conceito de Rede Social 13
5.1. Redes Sociais Mais Utilizadas 14
5.1.1. Facebook 14
5.1.2. Twitter 14
5.1.3. Google Plus 15
5.1.4. YouTube 15
5.1.5. Linkedin 15
5.1.6. Whatsapp 16
5.1.7. MySpace 16
5.1.8. Instagram 16
5.2. Os Perigos nas Redes Sociais 16
5.2.1. O Alto Risco Nas Redes Sociais 17
5.2.2. Perigos Nas Redes Sociais 18
5.3. A Fragilidade Na Internet 19
5.4. Conceito Sobre Segurança 19
5.5. Segurança da Informação 20
5.6. Engenharia Social 20
5.7. Grandes Ataques Hackers 24
6. Pesquisa de Campo 33
7. Considerações Finais 38
8. Referências Bibliográficas 39

1. Introdução

Atualmente a internet é uma das grandes plataformas de conhecimento, entretenimento e interação entre as pessoas. Muitos usuários passam grande parte do dia conectada à Rede mundial de computadores para esses fins. Com a chegada dos smartphones, tablets e outros dispositivos móveis todos ligados a Redes sem fio, o acesso se propagou ainda mais.

As Redes Sociais são uma ótima maneira de conhecer novas pessoas e assimilar gostos, é um dos ambientes mais visitados pelos internautas quando o assunto é interação, compartilhamento e relacionamento, mas, para navegar nesses espaços virtuais, é preciso manter alguns cuidados relacionados à segurança como captura de senhas, informações pessoais e imagens.

O trabalho vem mostrar o grande perigo que há por traz das Redes Sociais, por mais que as pessoas acham que tem privacidade pelo contrário não tem. Por mais que se restringe as informações, é muito fácil descobrir quase tudo uns dos outros na Internet, ainda mais em Redes Sociais em poucos minutos é possível saber onde uma pessoa foi, o que ela está fazendo, comendo, onde mora, com quem está, tudo através das fotos postadas, comentários, com tudo isso, as pessoas acabam ficando mais vulneráveis.

Este trabalho mostra a fragilidade que há por traz das Redes Sociais, por mais que há benefícios quando não sabemos usar, há pessoas que se aproveitam dessas fragilidades para enganar, extorquir, cometer diversos crimes em poder dessas informações.

Segurança da informação consiste na proteção de um conjunto de dados, sejam eles pessoais ou de uma empresa, para que não sejam consultados, copiados ou alterados por indivíduos não autorizados.

A segurança da informação está fundamentada em valores como a confidencialidade, integridade e disponibilidade, que pretendem preservar o valor da informação ou dados. Atualmente, a segurança da informação é mais falada no âmbito de sistemas informáticos, apesar de não ser exclusiva dessa área. No universo das informações eletrônicas, os hackers são conhecidos por conseguirem encontrar brechas em sistemas, violando a segurança da informação.

A segurança da informação diz respeito à proteção de determinados dados, com a intenção de preservar seus respectivos valores para uma organização (empresa) ou um indivíduo.

Atualmente, a informação digital é um dos principais produtos de nossa era e necessita ser convenientemente protegida. A segurança de determinadas informações podem ser afetadas por vários fatores, como os comportamentais e do usuário, pelo ambiente/infraestrutura em que ela se encontra e por pessoas que têm o objetivo de roubar, destruir ou modificar essas informações.

Confidencialidade, disponibilidade e integridade são algumas das características básicas da segurança da informação, e podem ser considerados até mesmo atributos.

Confidencialidade – Diz respeito à inacessibilidade da informação, que não pode ser divulgada para um usuário, entidade ou processo não autorizado;

Integridade – A informação não deve ser alterada ou excluída sem autorização;

Disponibilidade – Acesso aos serviços do sistema/máquina para usuários ou entidades autorizadas.

Toda vulnerabilidade de um sistema ou computador pode representar possibilidades de ponto de ataque de terceiros.

Esse tipo de segurança não é somente para sistemas computacionais, como imaginamos. Além de também envolver informações eletrônicas e sistemas de armazenamento, esse tipo de segurança também se aplica a vários outros aspectos e formas de proteger, monitorar e cuidar de dados.

2. Objetivos

2.1. Objetivo Geral:

Objetivo do tema é mostrar a vulnerabilidade para obter informações contidas na internet

2.2. Objetivo Específico:

O projeto possibilitara alertar sobre a vulnerabilidade das informações de uma pessoa com um simples nome, como essas Redes Sociais são muito famosas, hackers e spammers (Spamming é a prática de envio de mensagens em grande quantidade para milhares de pessoas ao mesmo) também estão ativos nesses lugares e podem usá-los para obter informações confidenciais. Sim, sites de Redes Sociais desempenham um papel importante na coleta de informações relevantes de uma pessoa. As questões de privacidade e segurança relacionadas a sites de Redes Sociais não é um assunto novo e também não é muito fácil de combater, devido ao grande número de usuários.

3. Justificativa

O trabalho demonstra o grande perigo que há por traz das Redes Sociais, por mais que se imagina que tem privacidade pelo contrário não temos.

Por mais que tente ocultar as informações, é muito fácil descobrir quase tudo uns dos outros na Internet, ainda mais em Redes Sociais, em poucos minutos é possível saber onde uma pessoa foi, o que ela está fazendo, comendo, onde mora, com quem está tudo através das fotos postadas, comentários, com isso nós ficamos cada vez mais vulneráveis sem nos darmos conta.

Através do trabalho será exposta a fragilidade que há por traz das Redes Sociais, por mais que há benefícios, há pessoas que se aproveitam dessas fragilidades para enganar, extorquir, cometer diversos crimes em poder dessas informações.

4. Metodologia

Para desenvolver o projeto, serão feitas pesquisas na internet sobre o assunto abordado em relação à falta de segurança em Redes Sociais, também será desenvolvido pesquisas de campo para verificar o conhecimento sobre os riscos que os usuários podem sofrer.

5. Conceito de Rede Social

Uma Rede Social é uma estrutura Social composta por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns. Uma das características fundamentais na definição das Redes é a sua abertura e porosidade, possibilitando relacionamentos horizontais e não hierárquicos entre os participantes.

Hoje a influência das Redes Sociais na sociedade é tão grande que além do relacionamento Social entre as pessoas, as empresas, profissionais autônomos, religiões, ONGs (Organizações Não Governamentais) e outros segmentos já marcam presença nas Redes Sociais.

Elas também exercem um papel fundamental quando ocorre um acidente, um desastre, um fenômeno natural ou qualquer outra notícia relevante no país ou no mundo! É pelas Redes Sociais que as pessoas se informam, postam fotos, vídeos, notícias sobre os acontecimentos e isso praticamente em tempo real.

Essa definição pura e simples, aparentemente, acaba por tornar mais complexa à compreensão perto do que viria a ser uma Rede Social e é perfeitamente compreensível essa confusão, pois o termo “Rede Social” ganhou visibilidade a partir do surgimento da internet, ou seja, quando se fala em Rede Social, muitas pessoas associam automaticamente a Redes de relacionamento online que têm se tornado muito popular ao longo dos anos e que, na verdade, são realmente vertentes de uma Rede Social.

Diariamente, milhões de pessoas em todo o mundo usam as Redes Sociais para todo o tipo de atividades: de partilha de informação, notícias, fotos ou vídeos; para networking empresarial, para dar a conhecer uma empresa, um projeto ou iniciativa, privada, pública ou Social. Todas as grandes empresas, incluindo as principais de comunicação Social, têm hoje canais nas principais Redes, criando plataformas multimídia que crescentemente são acedidas fora dos espaços tradicionais, mercê da explosão dos aparelhos celulares de última geração e, mais recentemente, dos tablets.

5.1. Redes Sociais Mais Utilizadas

5.1.1. Facebook

Criada por Marck Zuckerberg em 2004, é uma Rede Social que permite a criação de um perfil Social. Neste espaço, você pode adicionar pessoas conhecidas e interagir com elas (e elas com você) por meio de postagens de texto, fotos e vídeos. No Facebook é possível seguir perfis de seu interesse (celebridades, veículos de comunicação, marcas, dentre outros) e acompanhar em tempo real as notícias que são disponibilizadas por eles. Dentro do próprio Facebook existem as fanpages, um perfil mais utilizado para empresas. Funciona como um meio de aproximar consumidores de clientes e, atualmente, tem se tornado uma ferramenta de serviço de atendimento ao cliente. Graças a disseminação rápida da informação na internet, as empresas têm medo da repercussão negativa de algum comentário e não deixam seus clientes esperando. É possível ganhar dinheiro com as fanpages (páginas de fãs), desde que sua página cair no gosto do público, adquirindo opções de curtir muito facilmente. Quanto mais pessoas curtirem a sua página, mais destaque ela adquire. Existem inúmeras páginas atualmente que tem parcerias com grandes empresas, já que passam da casa de um milhão de likers.

5.1.2. Twitter

O Twitter foi fundado em março de2006 por Jack Dorsey, Evan Williams e Biz Stone como um projeto paralelo da Odeo. A ideia surgiu de Dorsey durante uma reunião de discussão de ideias (brainstorming) em que ele falava sobre um serviço de troca de status, como um SMS. Trata-se de um micro blog que permite apenas 140 caracteres por postagem. Cheio de funcionalidades permite as mesmas funções do item anterior. O Twitter possui quase que um dicionário próprio.

Hastag – palavra seguida do símbolo jogo da velha para expressar sentimentos

Tuíte – A frase que você escreve chama-se tuíte

Retuíte – Quando você compartilha o tuíte de alguém

Trending Topics – É uma lista com os assuntos mais falados na Rede.

5.1.3. Google Plus

Fundado em 4 de setembro de 1998, por Larry Page e Sergey Brin, também conhecida como Google +, a Rede Social da Google veio para ser concorrente do Facebook. Apesar de não possuir tantos perfis quanto o Facebook, contudo, por ser uma Rede Social da gigante das buscas é de suma importância para aqueles que precisam ser facilmente encontrados na internet, principalmente, os que precisam tornar público seus trabalhos, como os blogueiros, por exemplo.

5.1.4. YouTube

Teve início em uma garagem de San Francisco (Califórnia, EUA), em fevereiro de 2005. Lá, os funcionários de uma empresa de tecnologia Chad Hurley e Steve Chen, Integrante da Google é a maior Rede de compartilhamento do mundo. Criando um canal no Youtube, você pode favoritar páginas de cantores ou programas preferidos, além de assistir tutoriais, vídeos logs, cursos e outras infinidades de conteúdos que surgem na web. É possível faturar uma grana com o Youtube, desde que você se cadastre no Google Adwords, programa que permite a inserção de anúncios em seus vídeos e, quando acessados, você ganha uma fatia do montante repassado pelas empresas pelo Google. Outro meio é o sistema de parceria. Mais criterioso esse programa monetiza seus vídeos-desde que sejam criações próprias e não infrinjam nenhuma regra de direito autoral.

5.1.5. Linkedin

Foi fundada em 2002 por Reid Hoffman, porem só foi lançado em 2003 na Califórnia, voltado para a criação de perfis profissionais, o LinkedIn atua como um currículo online, conectando pessoas a fim de aumentar o networking. Nesse perfil, é possível prospectar novos empregos, já que empresas compartilham suas vagas por este canal.

O segredo deste perfil é manter a página atualizada com suas habilidades, experiências profissionais e indicações de conhecidos que já trabalharam ou estudaram com você.

5.1.6. Whatsapp

O WhatsApp foi fundado em 2009 por duas pessoas Brian Acton (americano) e Jan Koum (ucraniano), foi comprado por Mark Zuckerberg em 2014, o aplicativo, possibilita o bate-papo e interação com usuários, de forma privada ou pela criação de grupos, através de smartphone, tablet e também podendo acessar a mídia pelo computador.

5.1.7. MySpace

O MySpace foi fundado em 2003 por Chris DeWolfe e Tom Anderson. Começou como um site de relacionamentos, já foi a mais popular do mundo.

5.1.8. Instagram

Foi criado por Mike Krieger e seu sócio Kevin Systrom, ele criou em 2010 o Instagram, é uma Rede Social de fotos para usuários de Android e iPhone. Basicamente se trata de um aplicativo gratuito que pode ser baixado e, a partir dele, é possível tirar fotos com o celular, aplicar efeitos nas imagens e compartilhar com seus amigos. Há ainda a possibilidade de postar essas imagens em outras Redes Sociais, como o Facebook e o Twitter. No Instagram, os usuários podem curtir e comentar nas suas fotos e há ainda o uso de hashtags (#) para que seja possível encontrar imagens relacionadas a um mesmo tema, mesmo que as pessoas que tiraram essas fotos não sejam suas amigas.

5.2. Os Perigos nas Redes Sociais

Na falta de cuidado de muitos de seus membros ao exporem sua intimidade e informações particulares, as quais os tornam presas fáceis para pessoas mal intencionadas;

Na falta de moderação da grande maioria delas, onde todo tipo de conteúdo é livremente postado, haja vista que a produção de conteúdos ocorre de forma não centralizada, onde não há assim por dizer o chamado controle editorial;

Nos links embutidos em fotos e imagens ou abertos mesmo, que contém códigos maliciosos capazes de contaminarem os computadores com malwares ou que levem os membros das Redes Sociais a sites perigosos;

Na falta de limite que deveria ser imposta pelo próprio internauta, onde passa horas e horas nas Redes Sociais, ficando sujeito a tornar-se um viciado ou até mesmo adquirir doenças pelo uso ininterrupto do computador.

5.2.1. O Alto Risco Nas Redes Sociais

A chamada "Era Digital" trouxe inúmeros benefícios à sociedade. E não apenas no campo das comunicações. O avanço tecnológico foi o ponto de partida para mais um passo na evolução da humanidade, proporcionando conforto, segurança e melhoria de serviços, não só na área da informática, mas também na medicina e na agricultura, por exemplo. Por outro lado, esse avanço foi responsável por criar maus hábitos nos usuários, como sedentarismo e perda de horas de sono.

Um dos impactos mais preocupantes do uso das tecnologias da informação está relacionado à influência que ela pode ter no comportamento dos usuários, em especial de jovens e crianças. Um problema que se potencializa com o uso das Redes Sociais, acessadas por dispositivos móveis que, cada vez mais, dificultam o acompanhamento por parte das famílias.

Esta é uma questão que preocupa educadores e familiares. Mas, o fato de o monitoramento ser mais difícil não quer dizer que os pais devem ignorar a forma como os filhos usam as Redes Sociais ou o que acessam na internet. Por mais complexo que possa ser, é possível prevenir problemas que jovens e crianças possam ter com o uso da internet e das Redes Sociais, como ressalta a professora Tânia Zagury, que é professora, filósofa, conferencista e escritora, com 22 livros publicados no Brasil e no exterior.

A professora observa que muitos jovens têm compartilhado links de fotos e vídeos em Redes como Twitter, Facebook, Youtube e Instagram sem se preocuparem com as repercussões futuras, gerando uma exposição desnecessária.

Para ela, os adolescentes não tem conhecimento das consequências que isto pode trazer. Há empresas, por exemplo, que utilizam a análise da Rede Social de um candidato como etapa complementar de seus processos de seleção.

5.2.2. Perigos Nas Redes Sociais

Exposição nas Redes Sociais é comum postar fotos e dados pessoais, tais como o endereço da casa, local onde estuda, telefones, etc. Este tipo de ação pode parecer inofensivo, afinal, quem se importaria com a exposição desses dados? Infelizmente, há pessoas que podem utilizá-las para os mais diferentes fins. Por isso, é muito importante analisar o tipo de informação que posta nas Redes Sociais e refletir se toda esta exposição é realmente necessária.

Privacidade na maioria das Redes Sociais é possível determinar quem pode visualizar e ter acesso a dados pessoais. Se isso for possível, o mais indicado é autorizar somente os amigos, familiares e conhecidos, pessoas em que realmente confiam. Hoje, existe uma certa competição entre os jovens e adolescentes sobre quem possui mais amigos ou mais seguidores nesses espaços. Antes de adicionar qualquer contato é recomendado analisar sua origem, o motivo pelo qual a pessoa está te adicionando e quais as relações com o seu perfil.

Publicações:- Além dos perigos com relação à exposição, tem que cuidar também das opiniões que expressam e publicam nas Redes Sociais. Atualmente, existem Leis que categorizam certas publicações como criminosas e, nestes casos, as pessoas devem responder por aquilo que divulgam.

Cyberbullying:- pode ser considerada toda prática que utiliza a internet e dispositivos tecnológicos para divulgar na Rede textos e imagens com a intenção de constranger, humilhar ou perseguir pessoas. Infelizmente, assim como o bullying, esse tipo de ação tem se tornado comum, principalmente entre os jovens. Nas Redes Sociais, o que pode começar com uma simples brincadeira, pode gerar graves consequências.

5.3. A Fragilidade Na Internet

As fragilidades da internet e as brechas de segurança existentes nos mais diversos programas e sites que permitem aos crackers[1] (tipos de hackers[2] mal-intencionados) invadam sistemas e obtenham dados e informações que deveriam estar protegidos.

Diversos casos nos últimos anos acenderam o sinal vermelho entre os especialistas de segurança, que temem casos mais graves. Muito se tem debatido sobre o tema, e há quem diga que a próxima guerra mundial será cibernética.

Será que você utiliza as Redes Sociais com segurança? Quando nos cadastramos em sites como as Redes Sociais, somos responsáveis pelos dados que disponibilizamos nesses espaços. Navegar na internet com responsabilidade é um dever de todos. E nunca é demais receber dicas e orientações sobre como utilizar esses recursos. Navegar pela internet é como caminhar na rua, temos as leis de trânsito, as normas e os cuidados com a sinalização. Apesar da Internet pareça um local onde "tudo é possível", também tem que seguir certas regras e cuidados.

5.4. Conceito Sobre Segurança

O termo segurança vem do latim “*securitas*” e implica minimizar ou eliminar qualquer tipo de risco na vida. Implica os diversos agentes Sociais nos processos de avaliação e prevenção de qualquer tipo de risco.

A qualidade do meio ambiente, a segurança no trabalho; são conceitos que devem ser abordados de forma relacionada entre si para poder chegar a um bom nível de segurança em todos os setores da sociedade.

A qualidade da segurança nos pode dizer que viver sem nenhum tipo de medo, despreocupados, sem temor algum.

A segurança é um conjunto de medidas assumidas para proteger-se de quaisquer atos de violência, como pode ser ataques, roubos, espionagens, sabotagens, etc. A segurança implica a qualidade ou o estado de estar seguro. Com

[1] Hacker são indivíduos que elaboram e modificam softwares e hardwares de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas.
[2] Cracker é o termo usado para designar quem pratica a quebra (ou cracking) de um sistema de segurança.

a seguridade se tenta evitar as exposições a situações perigosas e a devida atuação para estar protegido diante de situações adversas.

5.5. Segurança da Informação

Segurança da informação consiste na proteção de um conjunto de dados, sejam eles pessoais ou de uma empresa, para que não sejam consultados, copiados ou alterados por indivíduos não autorizados.

A segurança da informação está fundamentada em valores como a confidencialidade, integridade e disponibilidade, que pretendem preservar o valor da informação ou dados. Atualmente, a segurança da informação é mais falada no âmbito de sistemas informáticos, apesar de não ser exclusiva dessa área. No universo das informações eletrônicas, os hackers são conhecidos por conseguirem encontrar brechas em sistemas, violando a segurança da informação.

5.6. Engenharia Social

Em Segurança da informação, chama-se Engenharia Social, as práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio da enganação ou exploração da confiança das pessoas.

Para isso, o golpista pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, etc.

É uma forma de entrar em organizações que não necessita da força bruta ou de erros em máquinas. Explora as falhas de segurança das próprias pessoas que, quando não treinadas para esses ataques, podem ser facilmente manipuladas.

Engenharia Social compreende a inaptidão dos indivíduos manterem-se atualizados com diversas questões pertinentes a tecnologia da informática, além de não estarem conscientes do valor da informática que eles possuem e, portanto, não terem preocupação em proteger essa informação conscientemente. É importante salientar que, a engenharia Social é aplicada em diversos setores da segurança da informação independente de sistemas computacionais, software e ou plataforma utilizada, o elemento mais vulnerável de qualquer sistema de segurança da

informação é o ser humano, o qual possui traços comportamentais e psicológicos que o torna suscetível a ataques de engenharia Social.

Dentre essas características, pode-se destacar:

• Vaidade pessoal e ou profissional: O ser humano costuma ser mais receptivo a avaliação positiva e favorável aos seus objetivos, aceitando basicamente argumentos favoráveis à sua avaliação pessoal ou profissional ligada diretamente ao benefício próprio ou coletivo de forma demonstrativa.

• Autoconfiança: Busca transmitir em diálogos individuais ou coletivos o ato de fazer algo bem, coletivamente ou individualmente, buscando transmitir segurança, conhecimento, saber e eficiência, buscando criar uma estrutura base para o início de uma comunicação ou ação favorável a uma organização ou indivíduo.

• **Formação profissional:** Busca valorizar sua formação e suas habilidades adquiridas nesta faculdade, buscando o controle em uma comunicação, execução ou apresentação seja ela profissional ou pessoal buscando o reconhecimento pessoal inconscientemente em primeiro plano.

• **Vontade de ser útil:** Comumente, procura agir com cortesia, bem como ajudar outros quando necessário.

• **Busca por novas amizades:** Costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a dar informações.

• **Propagação de responsabilidade:** Trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades.

• **Persuasão:** Compreende quase uma arte a capacidade de persuadir pessoas, onde se busca obter respostas específicas. Isto é possível porque as pessoas possuem características comportamentais que as tornam vulneráveis a manipulação.

A engenharia Social não é exclusivamente utilizada em informática, a engenharia Social é uma ferramenta onde explora - se falhas humanas em organizações físicas ou jurídicas onde operadores do sistema de segurança da informação possuem poder de decisão parcial ou total ao sistema de segurança da informação seja ele físico ou virtual porém, deve-se considerar que as informações pessoais, não documentadas, conhecimentos, saber, não são informações físicas ou virtuais, elas fazem parte de um sistema em que possuem características comportamentais e psicológicas na qual a engenharia Social passa a ser auxiliada por outras técnicas como: leitura fria, linguagem corporal, leitura quente, termos usados no auxílio da engenharia Social para obter informações que não são físicas ou virtuais mas sim comportamentais e psicológicas.

A Engenharia Social é uma das técnicas utilizadas por Crackers para obter acesso não autorizado a sistemas, Redes ou informações com grande valor estratégico para as organizações. Os Crackers que utilizam desta técnica são conhecidos como Engenheiros Sociais.

Quando é abordo Engenharia Social, tem-se que evidenciar Kevin D. Mitnick que foi um dos mais famosos crackers de todos os tempos, e boa parte dos seus ataques foram originados das técnicas de Engenharia Social, como analise de lixo, contato telefônico, abordagem pessoal e falhas humanas.

A seguir serão apresentadas as técnicas mais utilizadas pelos Engenheiros Sociais:

Analise do Lixo: Provavelmente poucas organizações tem o cuidado de verificar o que está sendo descartado da empresa e de que forma é realizado este descarte. O lixo é uma das fontes mais ricas de informações para os Engenheiros Sociais. Existem muitos relatos e matérias publicadas na Internet abordando este tipo de ataque, visto que através das informações coletadas no lixo podem conter nome de funcionários, telefone, e-mail, senhas, contato de clientes, fornecedores, transações efetuadas, entre outros, ou seja, este é um dos primeiros passos para que se inicie um ataque direcionado à empresa.

Internet e Redes Sociais: Atualmente muitas informações podem ser coletadas através da Internet e Redes Sociais sobre o alvo. Quando um Engenheiro Social precisa conhecer melhor seu alvo, esta técnica é utilizada, iniciando um

estudo no site da empresa para melhor entendimento, pesquisas na Internet e uma boa consulta nas Redes Sociais na qual é possível encontrar informações interessantes de funcionários da empresa, cargos, amizades, perfil pessoal, entre outros.

Contato Telefônico: Com as informações coletadas nas duas técnicas acima, o Engenheiro Social pode utilizar uma abordagem via telefone para obter acesso não autorizado, seja se passando por um funcionário da empresa, fornecedor ou terceiros. Com certeza neste ponto o Engenheiro Social já conhece o nome da secretária, nome e e-mail de algum gestor, até colaboradores envolvidos na TI. Com um simples telefonema e técnicas de Engenharia Social se passando por outra pessoa, de preferência do elo de confiança da vítima, fica mais fácil conseguir um acesso ou coletar informações necessárias da organização.

Abordagem Pessoal: Está técnica consiste de o Engenheiro Social realizar uma visita na empresa alvo, podendo se passar por um fornecedor, terceiro, amigo do diretor, prestador de serviço, entre outros, no qual através do poder de persuasão e falta de treinamento dos funcionários, consegue sem muita dificuldade convencer um segurança, secretária, recepcionista a liberar acesso ao datacenter onde possivelmente conseguirá as informações que procura. Apesar de esta abordagem ser arriscada, muitos Crackers já utilizaram e a utilizam até hoje.

Phishing: Sem dúvidas esta é a técnica mais utilizada para conseguir um acesso na Rede alvo. O Phishing pode ser traduzido como “pescaria” ou “e-mail falso”, que são e-mails manipulados e enviados a organizações e pessoas com o intuito de aguçar algum sentimento que faça com que o usuário aceite o e-mail e realize as operações solicitadas. Os casos mais comuns de Phishing são e-mails recebidos de supostos bancos, nos quais afirma que sua conta está irregular, seu cartão ultrapassou o limite, ou que existe um novo software de segurança do banco que precisa ser instalado senão irá bloquear o acesso. Outro exemplo de phishing pode ser da Receita Federal informando que seu CPF está irregular ou que o Imposto de Renda apresentou erros e para regularizar consta um link, até as situações mais absurdas que muitas pessoas ainda caem por falta de conhecimento, tais como, e-mail informando que você está sendo traído (a) e para ver as fotos

consta um link ou anexo, ou que as fotos do churrasco já estão disponíveis no link, entre outros. A maioria dos Phishings possuem algum anexo ou links dentro do e-mail que direcionam para a situação que o Cracker deseja.

Falhas Humanas: O Ser Humano possui várias vulnerabilidades que são exploradas pelos Engenheiros Sociais, tais como, confiança, medo, curiosidade, instinto de querer ajudar, culpa, ingenuidade, entre outros. No livro “Segredos do H4CK3R Ético”, escrito por Marcos Flávio Araújo Assunção, é abordada uma passagem interessante no capitulo “Manipulando Sentimentos” no qual, através do sentimento de Curiosidade, um Cracker instalou um outdoor na frente da empesa alvo com as palavras “Compre seu celular de última geração de modo fácil: entregue seu aparelho antigo e, com mais um real, escolha aquele que você quiser ter” e, abaixo, o link do site. Claro que este site estava com códigos maliciosos no qual foi possível acessar vários computadores da organização através de vulnerabilidade de softwares e sistemas operacionais.

Este é somente um exemplo de como o Engenheiro Social consegue obter êxito no ataque através de falhas humanas. A maioria dos ataques por Phishing visam explorar alguma falha humana para obter sucesso.

5.7. Grandes Ataques Hackers

Ao longo dos últimos anos, criminosos virtuais estão vendo suas opções de ataques se multiplicarem com a variedade de plataformas e possibilidades de se conectar a internet. Por isso, não é raro lermos notícias quase que diárias de ações de hackers, principalmente a grandes empresas e a governos. Alguns casos ganham enormes proporções devido à ousadia ou ao número de vítimas afetadas.

Alguns ataques:

Foi em 2014 que o mundo teve alguns de seus maiores ataques virtual da história. Entre o final de fevereiro e o início de março, hackers acessaram o banco de dados do eBay e roubaram registros de nada menos que 145 milhões de usuários cadastrados.

A crise teve início mais especificamente no PayPal, propriedade do eBay. Usuários do site de pagamentos foram aconselhados a mudar suas senhas, sendo o

aviso dado por meio de um post no blog oficial, contendo apenas o título com a advertência, sem texto. Na época, o aviso causou uma queda de 1,73% nas ações da empresa.

O ataque ao eBay, segundo especialistas, foi a segunda maior brecha em segurança já detectada. Só perde para o caso com a Adobe em 2013, quando 152 milhões de contas tiveram seus dados acessados.

De acordo com um comunicado da empresa na época, os hackers tiveram acesso à informação codificada que continha as senhas, data de fim de licenças e números de cartões de crédito e débito dos utilizadores.

Entre 2007 e 2010, hackers usaram um malware que compartilhava logins, senhas e dados bancários de clientes que tinham ações investidas na bolsa americana Nasdaq. Eles filtraram suas buscas por pessoas que tinham grande volume de dinheiro em conta.

Segundo informações do governo americano, cerca de 800 mil contas bancárias foram atingidas, gerando um prejuízo de aproximadamente US$ 300 milhões. Além disso, 160 milhões de cartões de crédito tiveram os dados comprometidos.

Como consequência, quatro cidadãos russos e ucranianos foram acusados, em 2013, de comandar a sofisticada organização de hackers que, por anos, penetrou as Redes de computação de mais de uma dúzia de grandes empresas norte-americanas e internacionais.

A Heartland Payment Systems, sediada em Nova Jersey, nos Estados Unidos, processa pagamentos com cartões de crédito e débito para pequenas e médias empresas, e foi identificada como a principal vítima do esquema iniciado em 2007, com o roubo de mais de 130 milhões de números de cartões de crédito e prejuízos de mais de US$ 200 milhões.

A Global Payment Systems, de Atlanta, outra grande empresa de processamento de pagamentos por cartão, teve quase um milhão de números de cartões roubados, com prejuízos de quase US$ 93 milhões, segundo os promotores.

O ano de 2014 não foi tão bom para o Sony quando o assunto é segurança digital. Por meio de um post no Playstation Blog, a empresa confirmou que os servidores sofreram ataques DDoS (quando vários bots propositalmente acessam o

serviço de uma vez, causando instabilidade), o que fez com as funções da PSN ficassem fora do ar durante todo o dia.

Apesar de garantir que nenhuma informação pessoal dos clientes foi acessada ou comprometida pelo ataque, o presidente da Sony Online Entertainment, John Smedley, chegou a ser ameaçado. O grupo informou que o avião em que Smedley estava viajando continha bombas, o que deve ter assustado bastante a todos, a ponto do trajeto do voo ter sido desviado por “questões de segurança”, segundo mensagem do executivo.

Não só os serviços da Sony ficaram fora do ar em 2014. Servidores da Blizzard e da Riot também sofreram com instabilidade após ataques. Em determinado momento do ano, três grandes empresas de games tiveram problemas em pouco tempo.

Neste ataque, o site do estúdio de Phil Fish, o Polytron, foi invadido por hackers e várias informações pessoais do desenvolvedor foram divulgadas. O mesmo aconteceu com Zoe Quinn, desenvolvedora de Depression Quest.

É difícil mensurar quantos ataques acontecem diariamente, e quais suas consequências. O gráfico abaixo (em inglês) e os enlaces, do início de 2014, mostra quais foram as empresas mais atingidas em 2013. Ele foi desenvolvido pelo site

Information is Beautiful, no artigo **World's biggest data breaches**.

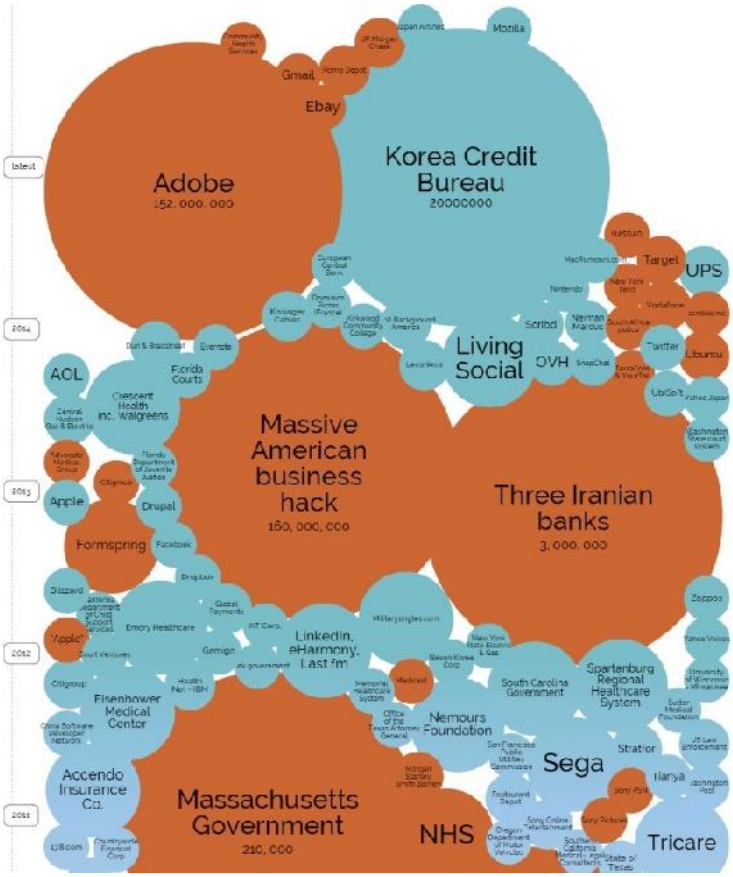

Figura 1 – Ataques Hackers em empresas (Fonte http://www.psafe.com/blog/grandes-ataques-hackers-empresas-governos/)

Outra notícia é a invasão aos servidores do LastPass, que pode ter comprometido os dados pessoais de uma grande quantidade de usuários. A preocupação, neste caso, é ainda maior do que no caso da PSN, já que o serviço é responsável por concentrar os dados de acesso usados em serviços como e-mails, jogos e Redes Sociais.

Apesar de preocupantes, esses ataques são pequenos comparados a outras ações perpetuadas por outros hackers durante a história. O ponto comum das ações, que incluem roubo de códigos militares e divulgação de números de cartões de crédito, é que todos causaram grandes prejuízos financeiros, mesmo que de forma indireta.

A Sony Pictures foi vítima de um grandioso ataque cibernético em novembro de 2014 que deixou todos os seus computadores fora do ar. Além disso, houve um roubo de 100 terabytes de dados confidenciais que incluíam informações de funcionários e até filmes que não haviam sido lançados.

O grupo GOP (Gardian of Peace, supostamente da Corea do Norte) assumiu a autoria do ataque que, segundo o FBI (a Polícia Federal dos Estados Unidos), foi promovido pela Coreia do Norte. Um dos supostos motivos seria o lançamento do filme "A Entrevista", em que dois jornalistas são instruídos a assassinar o líder do país, Kim Jong-un, após conseguirem uma entrevista com ele.

Como forma de represália, o governo americano aplicou sanções. Os prejuízos estimados da Sony são de aproximadamente 200 milhões de dólares.

Um dos ataques mais graves de todos aconteceu em julho de 2015 e atingiu a empresa italiana Hacking Team, que trabalha para diversos clientes e governos oferecendo serviços de vigilância digital. Nada menos que 400 GB de arquivos internos, códigos e outros documentos vazaram na internet.

Nenhum grupo cracker se manifestou ou foi apontado como responsável pelo ataque. O vazamento das informações apontou também muitos dos clientes que contratavam os serviços do Hacking Team, incluindo Coreia do Sul, Alemanha, Emirados Árabes e Estados Unidos.

Isso inclui órgãos ou seções de alguns países, como o FBI e o Departamento de Defesa estadunidense, além do próprio ministro da Etiópia, que aparece em um dos documentos agradecendo os serviços da companhia.

Depois do vazamento, foi descoberto que o grupo usava aplicativos populares para se infiltrarem smartphones com iOS, como WhatsApp, Facebook, Viber, Chrome, Telegram, Skype e WeChat.

Isso era feito através de uma falha descoberta no iOS 8 (já corrigida) que permitia que criminosos “atualizassem” apps já instalados no iPhone da vítima com uma versão alterada que escondia o código malicioso. Assim, era possível roubar uma série de informações, incluindo fotos, localização precisa de GPS em tempo real e outras.

O site de encontros extraconjugais Ashley Madison foi atacado pelo grupo cracker “Impact Team”, que roubou e divulgou informações pessoais dos usuários na internet. Entre os dados divulgados estão nomes verdadeiros, endereços, números de cartão de crédito e "todas as fantasias sexuais".

Atualmente, o site conta com 37 milhões de inscritos, mas, de acordo com o especialista em segurança Brian Krebs, apenas uma pequena parcela desse total teve seus dados divulgados. Segundo rumores, o roubo dessas informações está

relacionado a uma funcionalidade do próprio site de apagar completamente todos os dados do usuário.

Mediante o pagamento de US$ 17, as informações cadastradas podem ser definitivamente excluídas, algo que não acontece de fato. Essa falha no serviço aparentemente foi o que motivou o grupo cracker a providenciar o ataque.

Uma vulnerabilidade encontrada no iCloud – o serviço de armazenamento em nuvem da Apple – permitiu que crackers conseguissem obter diversas fotografias de celebridades completamente nuas. O caso foi conhecido posteriormente como The Fappening, ou Celebgate.

Entre as atrizes e cantoras vítimas do ataque estão Jennifer Lawrence, Kim Kardashian, Kirsten Dunst e Avril Lavigne. Todo o conteúdo havia sido posto no Reddit e no 4Chan. A Apple se isentou da culpa, afirmando que foi vítima de um phishing.

Um teste realizado pela revista Wired conseguiu comprovar que uma brecha no sistema conectado da Fiat Crysler permite que crackers invadam e controlem veículos remotamente.

A vulnerabilidade que um sistema dessa natureza tem dá espaço para crackers executarem uma série de ações ousadas, inclusive desligar o motor e, no caso de câmbios automáticos, desabilitar a aceleração e os freios.

Os pesquisadores Charlie Miller e Chris Vasalek demonstraram as fraquezas de um sistema de automóvel com conectividade de celular instalada em mais de 470 mil veículos daquele país. Mas a demonstração foi mais vívida do que muitos poderiam imaginar: os caras exploraram a vulnerabilidade do sistema atacando um Jeep Cherokee equipado com uma Rede Uconnect remotamente.

A fabricante ficou bastante preocupada com a repercussão do caso e rapidamente disponibilizou uma atualização de software para corrigir o problema. Contudo, como o update só pode ser instalado via USB, a Fiat Chrysler decidiu tomar medidas mais agressivas para garantir a segurança de seus consumidores e acionou um recall. No total, estima-se que mais de 1,4 milhão de veículos tenham sido cadastrados no programa.

Figura 2 – Redes de Blogs - (Fonte da imagem: Gawker Media)

Uma das principais Redes de blogs do mundo, e serviço responsável por hospedar alguns dos veículos online mais respeitados do mundo, a Gawker Media sofreu um duro ataque em dezembro de 2010. As informações de login e emails pessoais de milhões de usuários foram comprometidas, gerando preocupação em todos que possuíam contas em serviços populares com o Wordpress.

O ataque serviu para mostrar as brechas de segurança no sistema usado pela Gawker Media para armazenar as senhas dos usuários. Como muitas das informações roubadas também são usadas para fazer o login em Redes Sociais e no Twitter, não demorou para que os invasores começassem a usar esses meios como forma de espalhar mensagens de spam.

A empresa não divulgou o número de contas afetadas, se limitando a recomendar que todos os usuários trocassem as senhas. Porém, a invasão foi bem sucedida ao revelar a fragilidade do sistema de proteção utilizado, mostrando que nem mesmo os grandes sites da internet estão imunes a ataques simples.

Figura 3 – Central Intelligence Agency (Fonte da imagem: Governo dos Estados Unidos)

Em 1982, um ataque perpetuado pela CIA mostrou o estrago físico que um simples código de comando corrupto pode fazer. Hackers da agência do governo

norte-americano conseguiram fazer com que o sistema de controle de um gasoduto soviético enlouquecesse e começasse a operar de forma estranha.

O resultado, segundo um membro da força aérea que participou da operação, foi uma das explosões mais impressionantes já vistas do espaço tudo isso sem que nenhuma arma fosse disparada. Com o número cada vez maior de sistemas controlados exclusivamente pelo computador, a cada dia que passa, ataques do tipo têm um potencial destrutivo cada vez maior.

Em março de 2011, as companhias de segurança Symantec e Kaspersky reportaram diversas tentativas de invasão aos seus bancos de dados. Porém, o grande afetado pela onda de ataques criminosos foi a RSA Security, que teve diversos de seus dados roubados por hackers não identificados.

A situação é especialmente preocupante quando se leva em conta que a empresa é a responsável pelo desenvolvimento de ferramentas que prometem blindar milhares de sistemas contra invasões. Se nem mesmo as companhias que dispõe da última palavra em segurança estão protegidas, quais as esperanças que um usuário comum pode ter contra a ação dos criminosos virtuais?

Um simples teste para determinar o tamanho da internet realizado em 1988 fez com que Robert Tappan Morris gravasse seu nome na história como o criador de uma das maiores pragas virtuais existentes. O worm criado pelo então estudante da Universidade Cornell saiu de controle e infectou milhares de computadores, que em pouco tempo deixavam de funcionar corretamente.

Como resultado, várias empresas reportaram perdas na casa dos milhões de dólares. Além disso, o governo norte-americano foi forçado a criar um plano de contingencia para futuros ataques do tipo, ação que ficou conhecida como CERT.

As ações de Morris renderam ao estudante uma multa de US$ 10 mil e a obrigatoriedade de cumprir 400 horas de serviço comunitário. Atualmente, o código fonte do worm está armazenado em um disquete exibido em destaque no Museu de Ciência de Boston.

. Uma declaração feita em 2007 pelo ex-oficial de segurança da informação do governo norte-americano, Paul Strassman, apontava a existência de cerca de 750 mil máquinas zumbis somente na China.

O número de máquinas infectadas cresce a cada ano, se aproveitando da falta de conhecimento de usuários que não tomam as medidas de seguranças necessárias para proteger seus dados pessoais.

Esses computadores são perigosos, pois podem ser usados como armas para sobrecarregar sites e outras máquinas com o envio intenso de dados conhecidos como DDOS. Além disso, os zumbis são armas perfeitas para o envio de mensagens indesejadas por e-mail.

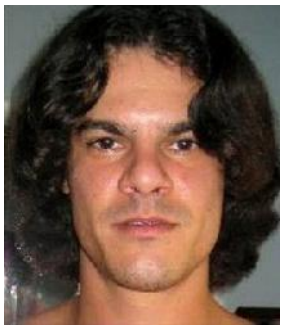

Figura 4 - Albert Gonzales (Fonte da imagem: Governo dos Estados Unidos)

Entre 2005 e 2007, o hacker Albert Gonzalez conseguiu roubar os dados de mais de 45 milhões de números de cartões de crédito e débito acumulados pela loja de departamento TJ Maxx & Marshalls. Durante a sua carreira, que durou até a captura pela polícia em 2008, o criminoso conseguiu acumular informações confidenciais de mais de 170 milhões de pessoas.

Em 2010, o hacker foi condenado a cumprir 40 anos de prisão devido a suas ações. Como é padrão nesse tipo de caso, não foram revelados os números do prejuízo causado pelo roubo das informações. Porém, a festa de aniversário promovida pelo hacker, no qual foram gastos US$ 75 mil, dá uma boa ideia do prejuízo.

Embora existam hackers cujas ações de invasão tenham o objetivo de fortalecer Redes de segurança e avisar administradores sobre problemas com servidores, a maioria dos grupos especialistas em acessar dados confidenciais não trabalha de forma tão nobre.

Qualquer pessoa que participa de forma ativa da internet corre o risco de sofrer a ação de criminosos, mesmo que de maneira indireta. Para se proteger, ainda valem as antigas regras: evite usar a mesma senha em diferentes serviços, escolha sempre códigos complexos e desconfie de qualquer conteúdo suspeito.

6. Pesquisa de Campo

Pesquisa realizada com os alunos da escola Técnica Professor Massuyuki Kawano, no ano de 2016.
Abaixo as perguntas utilizadas na pesquisa de campo.

1. Você se conecta em alguma Rede Social?

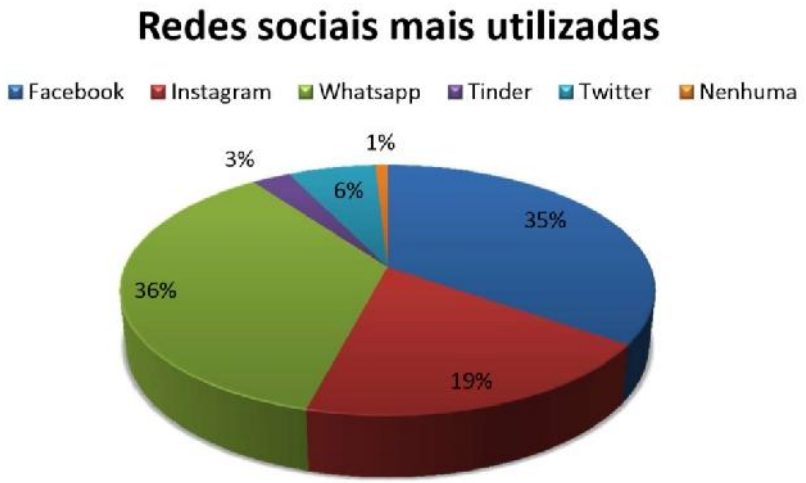

Figura 5 –Redes Sociais mais utilizadas

2. Quanto tempo você passa conectado em uma Rede Social?

Figura 6- Tempo conectado nas Redes Sociais

3. Costuma postar fotos de onde frequenta?

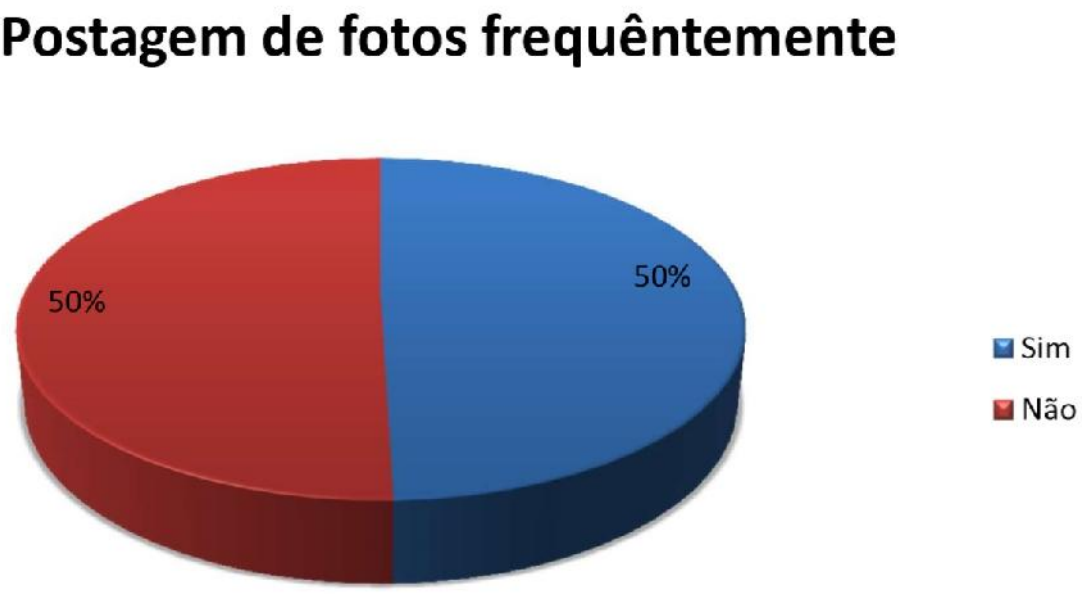

Figura 7- Postagem de fotos frequêntemente

4. Todos os dados pessoais em seu cadastro na Rede Social são verdadeiros?

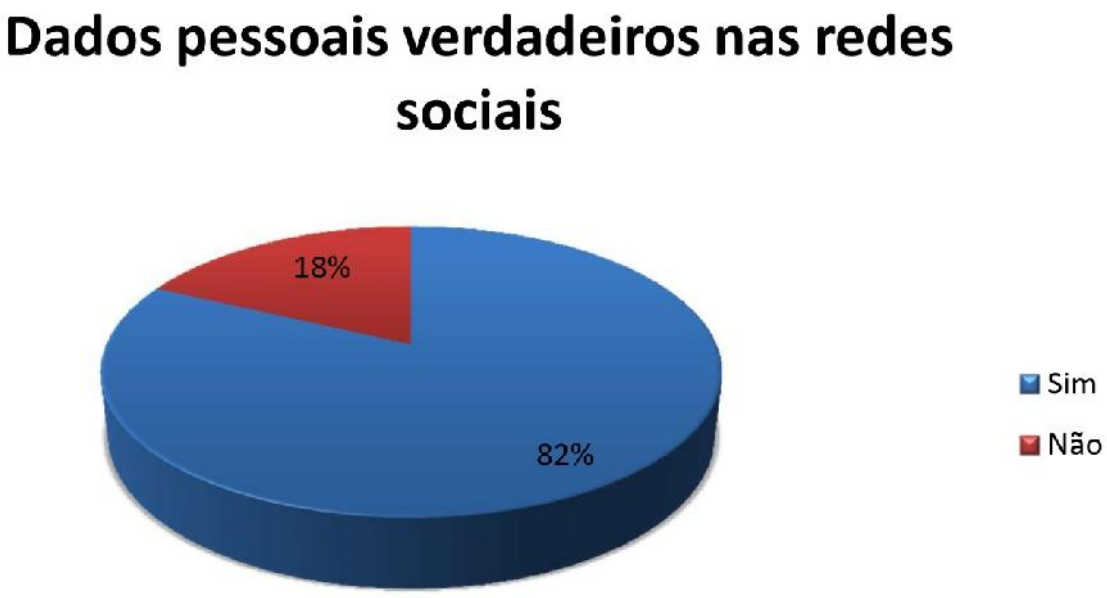

Figura 8-Dados pessoais verdadeiros nas Redes Sociais

5. Costuma trocar fotos comprometedoras com pessoas que conhecem apenas pela internet?

Figura 9-Troca de imagens intimas nas Redes Sociais

6. Você conhece todos seus amigos nas Redes Sociais pessoalmente?

Figura 10-Pessoas que conhecem seus amigos das Redes Sociais pessoalmente

7. Você costuma aceitar pedidos de amizade de desconhecidos?

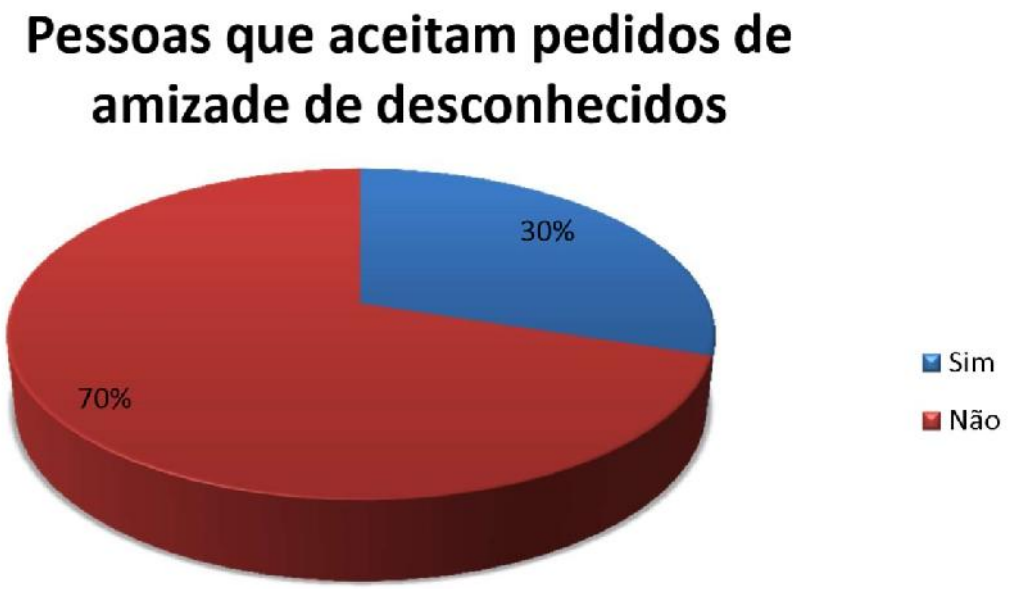

Figura 11- Pessoas que aceitam pedidos de amiazade de desconhecidos

8. Você já sofreu com algum tipo de vazamento de informação?

Figura 12- Pessoas que sofreram algm tipo de vazamento de informaç

9. Se sim, qual o tipo de prejuízo sofrido?

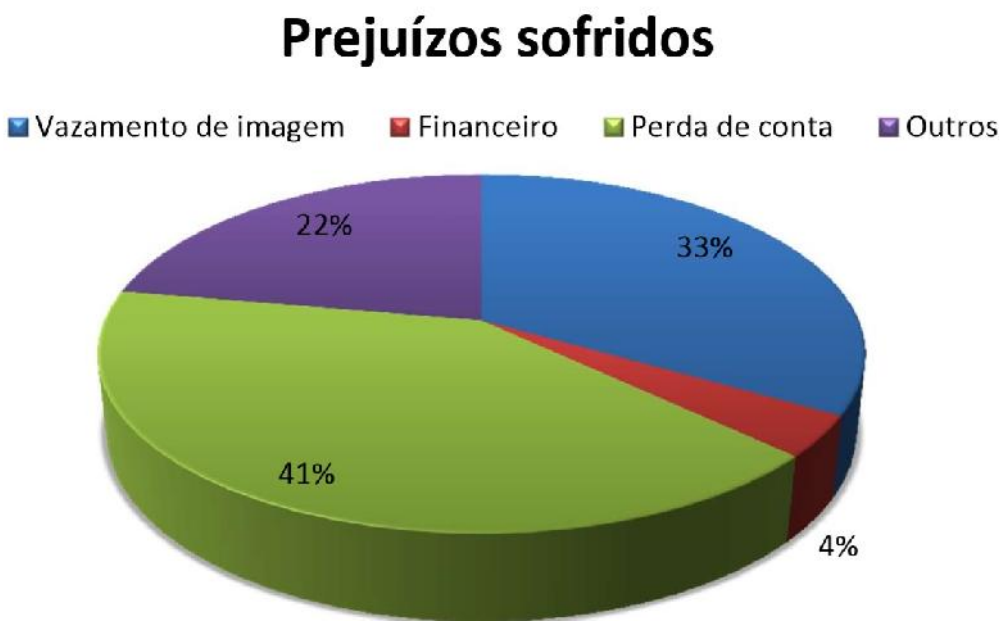

Figura 13-Prejuízos sofridos

7. Considerações Finais

O objetivo desse trabalho foi mostrar a fragilidade de muitos usuários deixam em suas contas Sociais como: dados pessoais, fotos intimas, entre outros a mercê de qualquer um. Foi demonstrado através de uma pesquisa de campo e bibliográfica que muitas pessoas passam mais tempo conectado no mundo virtual discutindo relações, amizades e até brigando, ao invés de ter uma conversa pessoalmente, e que usam deste meio para demonstrar todo seus sentimentos, como alegria, amor, ódio, indignação, felicidades uns pelos outros, porém se esquecem que a Rede Social não e um simples papel e lápis que você escreve e não gostou e simplesmente consegue apagar, mas sim algo que foi escrito com caneta e não é possível apagar, sendo assim ganha uma proporção gigantesca na Rede Sociais. Por outro lado a Rede Social traz bastante beneficio como a aproximação de pessoas distantes, informações de utilidades públicas, e várias outro benefício basta saber utilizar com consciência e segurança.

Portanto antes de colocar qualquer tipo de informação em uma Rede Social, devem-se pensar quais as consequências que essas informações possam alcançar no mundo atual.

8. Referências Bibliográficas

Leite Marcos, Luis; Em O Que São Redes Sociais http://ogestor.eti.br/o-que-sao-Redes-Sociais/ Acessado pela última vez em 28/02/16

Ucha, Florenci; de Oliveira, Dimauro Marcelo; de Andrade, Maria Paz; Bembibre, Cecilia; Yanover David; Em Conceito em Segurança http://queconceito.com.br/seguranca/ Acessado pela última vez em 28/02/16

Drubscky, Luiza; Em Redes mais acessadas. http://marketingdeconteudo.com/Redes-Sociais-mais-usadas-no-brasil/___Acessado pela última vez em 29/02/16

Novaes, Rafael; Em Grande Ataques http://www.psafe.com/blog/grandes-ataques-hackers-empresas-governos/ Acessado pela última vez em 11/04/16

Muller, Leonardo; Em Ataque Hacker http://www.tecmundo.com.br/seguranca/9971-os-maiores-ataques-hackers-da-historia.htm/ Acessado pela última vez em 11/04/16