PERFIL DOS UNIVERSITÁRIOS USUÁRIOS DE REDES SOCIAIS DE MONTE CARMELO E REGIÃO

PROFILE OF UNIVERSITY STUDENTS SOCIAL NETWORK USERS IN MONTE CARMELO AND REGION

Danieli Aparecida da Silva[1]

Carlos Alberto Cordeiro Palhares [2]

RESUMO:

O trabalho apresenta um estudo feito por meio de um levantamento de dados sobre utilização das redes sociais por universitários residentes de Monte Carmelo, Minas Gerais. O principal objetivo é identificar o perfil desses jovens quanto á prática insegura de navegação na *internet* como postagem de fotografias, utilização de senhas fracas e excesso de informações pessoais. A iniciativa surgiu diante do crescente número de problemáticas geradas durante a utilização de redes sociais.

PALAVRAS-CHAVE: Internet; Segurança; Interações Virtuais.

ABSTRACT:

The paper presents a study through a data collection on use of social networks by under graduate students residents of Monte Carmelo, Minas Gerais. The main objective is to identify the profile of these young people like the unsafe practice of surfing the internet as photographs posting, use of weak passwords and excessive personal information. The initiative appeared observing the growing number of problems generated when using social networks.

KEYWORDS : internet; safety; virtual interactions.

1. Introdução

Os constantes avanços tecnológicos, anteriormente acessíveis apenas a uma pequena parte da população, apresentaram nas ultimas décadas uma enorme expansão,

1- Graduada em Sistemas para Internet- danieli.silvati@gmail.com

2- Professor Fucamp

principalmente a promovida pela *internet,* que associada à aquisição de microcomputadores, *notebooks, tabletes, smartphone* entre outros dispositivos eletrônicos, permitiram uma forma ampla e diferente nas interações sociais. Para Bohn et al (2011) Desde 1993 a *internet* tem atraído à atenção pública.

Desde então, as vendas de computadores tem aumentado, e um numero maior de pessoas tem tido contato com a rede, que segundo Dias (2011, p. 636),

> As redes sociais são ambientes *virtuais* nos quais sujeitos se relacionam instituindo uma forma de sociabilidade que está ligada à divulgação e à própria formulação do conhecimento.

As relações ganharam um novo universo nas redes sociais, um fenômeno coletivo que possibilita diversas vertentes de relacionamentos, interações e organizações, que precisam ser cuidadosamente analisadas e conhecidas devido ao seu crescente avanço e por abrangerem as diversas esferas do conhecimento.

É sobre a necessidade de se conhecer o ambiente virtual no qual estamos inseridos e a forma como nos comportamos nele, que esse trabalho pretende tratar.

1.1 Objetivos

O estudo em questão investigou os padrões de uso das redes sociais, focando nos hábitos, enquanto usuários das ferramentas de comunicação, por meio de perfis de estudantes universitários. Buscando identificar e descrever o comportamento desses jovens quanto á prática de navegação na *internet* como postagem de fotografias, utilização de senhas e exposição de informações pessoais, objetivando uma resposta satisfatória a questão de pesquisa. Pretende-se com os resultados levantados, contribuir com futuros estudos a respeito do tema, assim como propor meios viáveis para a interação virtual.

1.2 Objetivos Específicos

- Verificar se os universitários de Monte Carmelo usam senhas consideradas “fortes” para seus perfis nas redes sociais.
- Verificar se esses mesmos jovens, habitualmente, publicam fotos que podem ser usadas de forma indesejada por pessoas mal intencionadas ou publicam

informações pessoais que podem comprometer sua privacidade e a própria segurança pessoal.

- Levantar o percentual de participantes que já tiveram problemas de privacidade invadida devido ao mau uso das redes sociais
- Produzir um material de qualidade.
- Contribuir para futuros estudos.

1.3 Justificativa

Devido a grande disseminação da *internet,* e a enorme exposição de informações pessoais, a privacidade e consequentemente a intimidade vêm sendo negligenciadas. Observando-se o crescente número de problemáticas causadas às pessoas e instituições no ambiente virtual das redes sociais, como o excesso de informações pessoais e a divulgação de hábitos diários e recorrentes, comportamentos esses percebidos entre os jovens, usuários mais constantemente expostos em tais ocorrências. Observou-se que tais hábitos podem gerar transtornos sociais diversos, facilitados pelo excesso de informações. Percebeu-se a necessidade de estudos que ofereçam alternativas de prevenção a essa realidade social entre o publico em questão. Em busca de respostas para tais questões, surgiu o presente trabalho.

1.4 Hipóteses

Acredita-se que exista um alto número de jovens, que já tiveram algum problema de privacidade enquanto usuários de redes sociais, essa ocorrência, supõe-se estar ligada ao mau uso das mesmas. O estudo trabalhou com a hipótese de que os participantes usam as redes sociais de forma inadequada ou insegura. Sabe-se que usando senhas fracas e publicando informações pessoais, a segurança é comprometida, e se violadas, podem ser usadas de formas indevidas, prejudicando assim a privacidade e a segurança pessoal.

1.5 Metodologia

Para a execução do trabalho, foi realizado um levantamento bibliográfico a respeito do assunto, onde se buscou conhecer as formas de interação virtuais mais utilizadas atualmente, buscou-se também na literatura, compreender as causas, efeitos e consequências dos fenômenos que ocorrem no ciberespaço, assim como suas definições.

Para a realização da pesquisa, foi feita a coleta de dados por meio de um *survey*, ou seja, um método sistemático de coleta de informações de entidades (uma amostra), com finalidade de construir um resumo quantitativo das características dos atributos de uma população mais ampla, da qual as entidades são membros (GROVES et al., 2004). No *survey* os dados são coletados em um ponto no tempo, com base em uma amostra para descrever a população neste determinado momento.

A coleta de dados foi realizada em forma de questionário, respondido por estudantes universitários, nas duas instituições de ensino superior existentes na cidade de Monte Carmelo, sendo uma a FUCAMP, Fundação Carmelitana Mário Palmério e a UFU, Universidade Federal de Uberlândia, campus Monte Carmelo. A escolha dos alunos foi aleatória e espontânea. Faz se importante ressaltar que, apesar das instituições serem ambas situadas na cidade de Monte Carmelo, alguns alunos pode residir em cidades próximas ou serem natural de outras cidades e, apenas viverem em Monte Carmelo durante o período de conclusão dos estudos universitários.

2. Referencial Teórico

A rede mundial de computadores transformou o dia a dia das pessoas, revolucionando a maneira de se relacionarem, inserindo a tecnologia à rotina de maneira fantástica por meio das redes sociais, entre as quais se incluem *Facebook, Twiter, youtube* entre outras. O *ciberespaço* integra atividades individuais que, ao se misturarem, influenciam mutuamente a realidade social na qual são inseridas.

Em uma conhecida rede social, podemos perceber através da apresentação da própria pagina que, ela não foi feita para uma comunicação fechada entre duas pessoas, e o conteúdo exposto por ela pode ser acessado por inúmeras outras.

Os perigos que as pessoas correm por não saber usar corretamente essas redes sociais são reais, qualquer pessoa pode obter uma conta no *Facebook* a partir de um cadastro de usuário, embora possua restrições de idade, os usuários podem não estarem sendo sinceros quanto a isso, e é nesse ponto que tantas vezes, se inicia uma serie de problemas.

Castells (2007, p. 459) no trecho a seguir, nos oferece uma ideia de como se apresenta uma forma virtual e individual.

> [...] um sistema em que a própria realidade (ou seja, a experiência simbólica/material das pessoas) é inteiramente captada, totalmente imersa

> em uma composição de imagens virtuais no mundo do faz-de-conta, no qual as aparências não apenas se encontram na tela comunicadora da experiência, mas se transformam na experiência.

Ainda nas palavras de Castells, em seu livro, A Galáxia da *Internet*, afirma que a *internet* é, acima de tudo, uma criação cultural. Uma pesquisa realizada pelo Ibope/Nielsen em 2012 demonstra que, no primeiro semestre do ano da pesquisa, o numero total de pessoas com acesso a *internet*, em qualquer ambiente (profissional, domiciliar, escolar) atingiu a marca de 82,4 internautas no Brasil, mostrando a abrangência e potencial social que a *internet* possui no cotidiano das pessoas.

O espaço virtual estende-se à frente como um universo com infinitas possibilidades. Percebe-se que, independente do ambiente, há sempre alguém conectado, seja em casa, na escola, nas lanchonetes, no trabalho, na igreja ou em qualquer outro lugar, as formas de comunicações estão presentes na vida de jovens e crianças, em sua maioria.

As relações interpessoais ganharam um novo universo nas redes sociais, um fenômeno coletivo, que possibilitam diversas vertentes de relacionamentos, interações e organizações, que precisam ser cuidadosamente analisadas e conhecidas, devido ao seu crescente avanço, e por abrangerem as diversas esferas do conhecimento. Este fenômeno interliga de forma quase direta com o mundo virtual, cada uma das atividades comuns ao cotidiano.

A *internet* é, em muitos aspectos, uma novidade, e como no mundo real, as interações feitas por meio dela impõem limites sensíveis, permeados por questões de ordens jurídicas, sociais e morais, liberdade de expressão, o direito a privacidade, entre outros, limites que foram sendo impostos diante dos riscos que as interações virtuais apresentam tais como fraude financeira, envio de vírus, rouba de senhas, crimes contra a honra, calúnia, injúria, difamação, *cyberbullying* e, talvez o crime mais preocupante, a pedofilia.

Em meio a todos esses riscos, é importante saber que, existem meios seguros de se usar a rede, apesar de que ela, muitas vezes, é usada equivocadamente sem cuidados. Segundo a SaferNet Brasil, a Central Nacional de Denúncias de Crimes Cibernéticos recebe uma média de 2.500 denúncias por dia, envolvendo páginas suspeitas de conter evidências de crimes de Pornografia Infantil, Racismo, Neonazismo, Intolerância

Religiosa, Apologia e/ou Incitação a crimes contra a vida, Homofobia e Maus tratos contra os animais.

Para Paganella (2012), o emprego da tecnologia sempre levanta uma indagação a respeito de quais limites devem ser respeitados, e de quais devem ser superados. Esses limites são necessários, pois não se trata apenas de uma grande rede interativa neutra ou sem efeito, mas sim de uma construção cultural que, embora construída em um espaço "invisível" seus reflexos afetam o espaço social. De acordo com Martin-Barbero (2008 apud Souza; Ribeiro, 2011, p.4),

> O mundo está diante de juventudes cujas sensibilidades respondem às alternativas de sociabilidade que permeiam tanto as atitudes políticas quanto as pautas morais, práticas culturais e gostos estéticos.

2.1 Privacidade na *internet*

A virtualização não é nem boa, nem má, nem neutra (Levy, 1996, p.11) se usada de forma adequada. Assim como no cotidiano, a interação virtual necessita de regras e muito bom senso, pois todo o conteúdo exposto na rede se torna de conhecimento e de domínio público. Com a propagação volumosa de computadores, a proteção à privacidade tornou-se um fator de preocupação para as pessoas e organizações, sobre como garantir a segurança das suas informações.

Qualquer individuo pode criar um espaço na *internet,* e interagir socialmente de maneira rápida e abrangente, entretanto, esta riqueza de possibilidades tem o seu preço, e requer cuidados. Alguns deles dizem respeito à sua intimidade. O que você revela sobre si na *internet* pode ser acessado por um número incontável de pessoas, independentemente das barreiras geográficas.

A Constituição Federal de 1988 assegura a cada individuo o direito de poder resguardar a sua intimidade e privacidade. O inciso X, do artigo 5° da CF/88 garante que:

> *São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.*

No entanto, devido à disseminação da *internet* e a enorme exposição de informações pessoais, a privacidade e a intimidade vêm sendo constantemente negligenciadas.

É comum observar as pessoas expondo todo tipo de informações em suas redes sociais, cursos que frequentam e academia, faculdade, escola e mesmo seu estado emocional ou de relacionamentos, suas preferências politicas e opiniões, muitas vezes polêmicas a respeito de si mesmas ou dos outros.

A declaração universal do direito do homem em seu artigo 19 dispõe que:

> *Todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão.*

O Brasil aderiu essa declaração expressa em nossa constituição no artigo 5º, inciso IV:

> *É livre a manifestação do pensamento, sendo vedado o anonimato, bem como no inciso IX: é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença.*

A liberdade de expressão, como qualquer outro direito fundamental, não é absoluta. O direito a livre expressão não é o mesmo que direito a ofensa e desacato, os tribunais de todo o mundo nos provam que, a *internet* não é uma terra sem lei, no entanto muitos usuários se escondem por traz de um perfil, para ofender e humilhar aos outros.

2.2 Crimes na *internet*

Juntamente com as vantagens advindas com a *internet*, nasceram também inúmeras praticas de crimes, esses por sua vez, penalizados pela legislação vigente. Em 1960 surgiu na literatura cientifica e na mídia, as primeiras ocorrências de crimes informáticos.

Nesse contexto é importante ressaltar que existem crimes cometidos com o computador, que seriam estelionatos, ameaças, roubos de informações, e os cometidos contra o computador, como roubos de direitos intelectuais e propriedades sobre softwares.

Os crimes de informática se dividem em duas categorias: Atos cometidos contra o próprio sistema de informática, também conhecido como crime virtual puro, e atos cometidos contra valores sociais (Bueno e coelho 2011).

2.3 *Cyberbullying*

Faustino e Oliveira (2008) definem *cyberbulling* como sendo uma agressão praticada discursivamente, via meios de comunicações virtuais. Segundo Fante (op. Cit, p. 46) o *bullying* não é um crime, mas a manifestação de vários crimes. Quando há ocorrência de *bullying*, pode-se denunciar o agressor por calúnia e difamação, agressão física ou moral, danos à propriedade privada, etc.

2.4. Pornografia Infantil

Se antes, o crime como o de pornografia infantil era instrumentalizado por meio de vídeos ou revistas, atualmente, dá-se por salas de bate-papo, como também pela troca de fotos por e-mail entre pedófilos, e divulgação em sites. Mudou a forma, mas a essência do crime permanece a mesma. (Bueno e Coelho 2011).

A Organização das Nações Unidas define pornografia infantil como

> *A exibição, por quaisquer meios de uma criança envolvida em atos sexuais explícitos, reais ou simulados, ou qualquer exposição da genitália da criança com intenção libidinosa.*

2.5 Roubos de dados

Utilizar dados pessoais como senha, perfil, comunidade, *avatar*, personagem ou e-mail de um usuário sem autorização ou consentimento do dono para qualquer fim, pode ser considerado crime. Esse tipo de ocorrência é muito comum em organizações, no entanto, os ataques ocorrem com certa frequência em contas de e-mail ou em redes sociais pessoais, que possam estar de alguma forma vulneráveis.

2.6 Vírus

Vírus são programas de computador criados com intenções maliciosas, como roubo de dados e danificar ou invadir sistemas. Mesmo sem percebermos, eles se espalham para infectar os computadores e dispositivos por meio de e-mails, trocas de arquivos e programas. Por terem capacidade de se multiplicarem, esses programas receberam o apelido de vírus. Dentre os "vírus" o Cavalo de Tróia (*trojan horse*) é uns dos mais comuns. O usuário pode recebê-lo de várias maneiras, na maioria das vezes ele vem anexado a algum e-mail. (Bueno e Coelho 2011).

Segundo a cartilha de segurança na *internet*, percebemos algumas atitudes importantes, que podem ser adotadas como práticas para preservar usuários de atitudes nocivas a sua segurança na rede. Segundo ela é importante não esquecer que as relações estabelecidas na *Internet* são relações interpessoais e, por isso, é importante ter os mesmos cuidados tomados no contato pessoal do dia a dia, como não revelar a desconhecidos informações pessoais que possam comprometê-lo.

Ainda orienta a jamais deixar-se fotografar em cenas comprometedoras, através de webcam, celular etc., através da *Internet* ou enviar imagens que possa comprometê-lo. (SAFERNET).

2.7 Senhas

A abordagem mais usada para autenticação de usuários legítimos, consiste de sistemas de senhas. Contudo, os requisitos para uma senha segura esbarram nas capacidades cognitivas de seus usuários, dando origem a inúmeros problemas (SILVA E STEIN, 2007).

Uma senha forte deve ser formada de números, letras e sinais gráficos, sem apresentar relação direta com informações dos seus usuários, o que as torna difíceis de serem lembradas e, portanto, com grande probabilidade de serem anotadas por seus usuários em locais de fácil acesso, favorecendo os ataques de engenharia social (MITNICK; SIMON, 2003 apud SAMPAIO; SIQUEIRA, 2010 et al).

Sasse et al (2001) diz que, senhas fortes consistem de itens sem sentido e assim são inerentemente difíceis de se lembrar. Nielsen (2004) diz que é indispensável treinar os

usuários, embora essa medida, isoladamente, não seja suficiente para erradicar os problemas relacionados ao uso de senhas.

Basta que o hacker disponibilize um cadastro ofertando brindes ou outras formas de premiação, que receberá, sem maiores dificuldades, uma gama de usuários e senhas (GRANGER, 2002 apud POPPER, 2010).

Segundo Silva e Stein (2007), os ataques de hackers vêm sendo noticiados com frequência, e em números cada vez maiores. As vítimas de tais ataques não se restringem apenas a grandes companhias ou departamentos governamentais, considerando que hoje, qualquer indivíduo pode ser alvo de um ataque virtual.

3. Resultados e Discursões

Através de uma definição pré-estabelecida, a pesquisa indagou a respeito da utilização de senhas consideradas fortes, divulgação de informações pessoais e problemas vividos na rede aos entrevistados. Os resultados obtidos com a entrevista realizada em forma de um questionário, contendo dez questões, respondida por 317 estudantes universitários da cidade de Monte Carmelo, MG podem ser vistos nos gráficos representados pelas figuras a seguir.

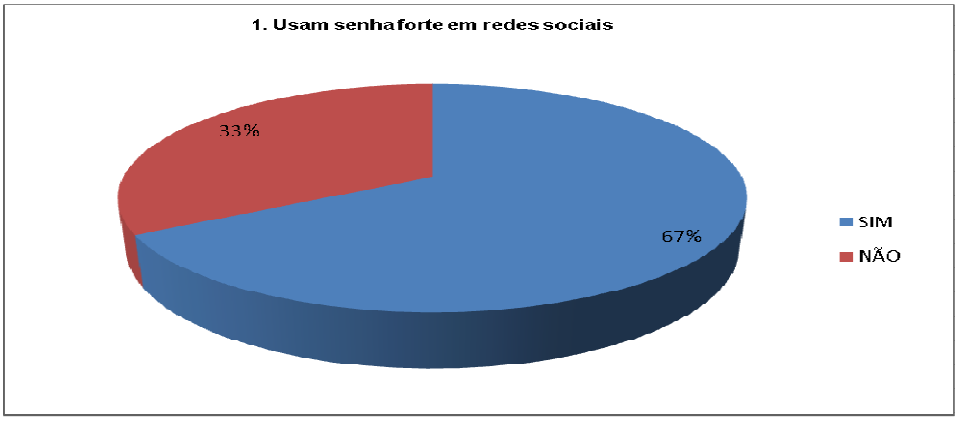

Gráfico 1- Resposta pergunta 01

Esse primeiro gráfico ilustra a resposta obtida na questão que levantou o percentual de participantes que utilizavam frequentemente as redes sócias. Foi especificada uma definição para senha segura e buscou-se com isso, avaliar se suas senhas pessoais em redes sociais, e-mail ou cadastros de sites na web (fóruns, comunidades, chats, etc.) atendiam todos esses pré-requisitos. Verificou-se com esses resultados, que o grupo pesquisado, em sua maioria, possui hábitos de segurança corretos em relação às senhas que etilizam para assegurar suas páginas. O resultado reflete a conscientização dos usuários com a

necessidade de manter seguras não só a privacidade das informações trocadas online, como as informações que são disponibilizadas por seus perfis na rede. Durante as entrevistas, alguns dos participantes demostraram não terem conhecimento a respeito de como seria uma senha adequada, oque pode justifica o percentual de respostas negativas.

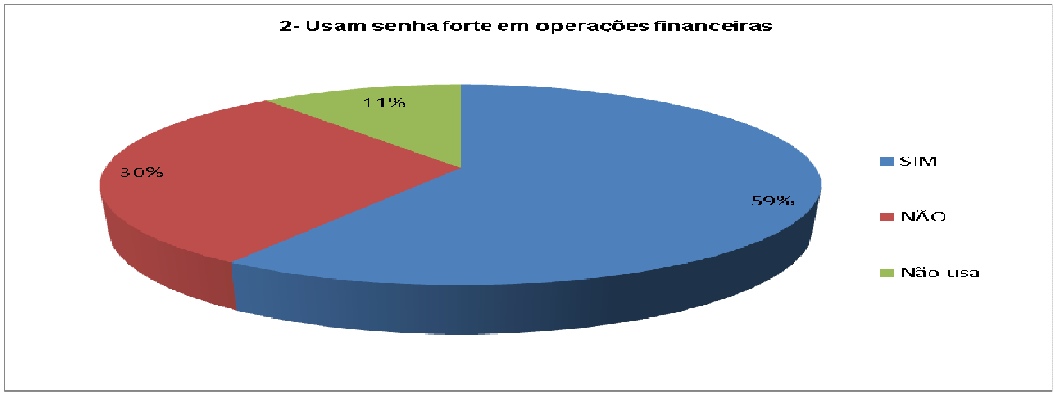

Gráfico 2 - Resposta pergunta 02

Essa questão usou a mesma definição de uma senha adequada da questão anterior, com o objetivo de investigar os hábitos dos usuários em relação às demais transações que necessitam de segurança como cartões, bancos etc. para comparar com o perfil dos mesmos em relação às redes sociais, e oque se verificou foi que um valor menor de participantes lida com a mesma seriedade com dados bancários, por exemplo, com que lida com as questões virtuais, enquanto um perceptual de 11% do total dos entrevistados não utiliza a web para transações financeiras por não confiarem nos meios de segurança disponíveis.

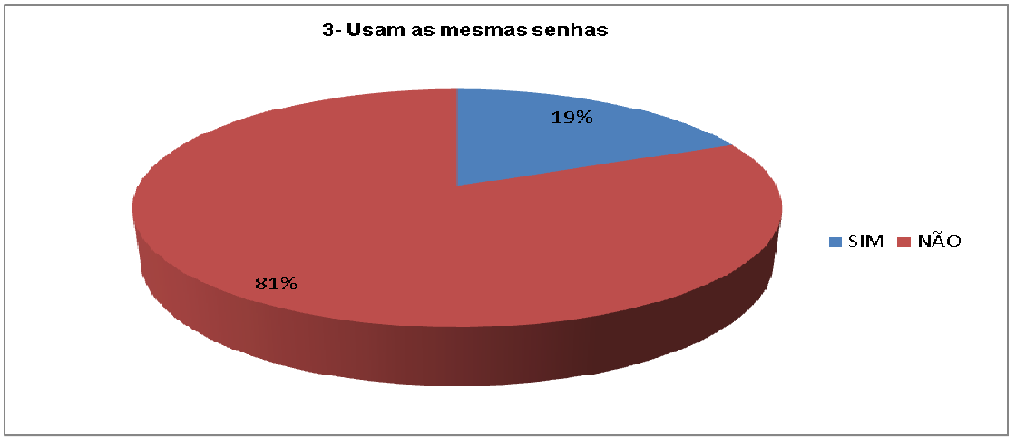

Gráfico 3- Resposta pergunta 03

Na questão três do questionário, buscou-se compreender se os estudantes reutilizavam o mesmo padrão de senhas para as diferentes transações como contas

bancarias, cartões de credito e sites. Não repetir a mesma senha para diversas contas é fundamental para manter sua segurança e evitar invasões. Os resultados mostraram que 81% dos participantes não possuem o habito de repitir os códigos de segurança, contra um percentual bem baixo, de apenas 19% dos entevistados que preferem repetir as mesmas senhas.

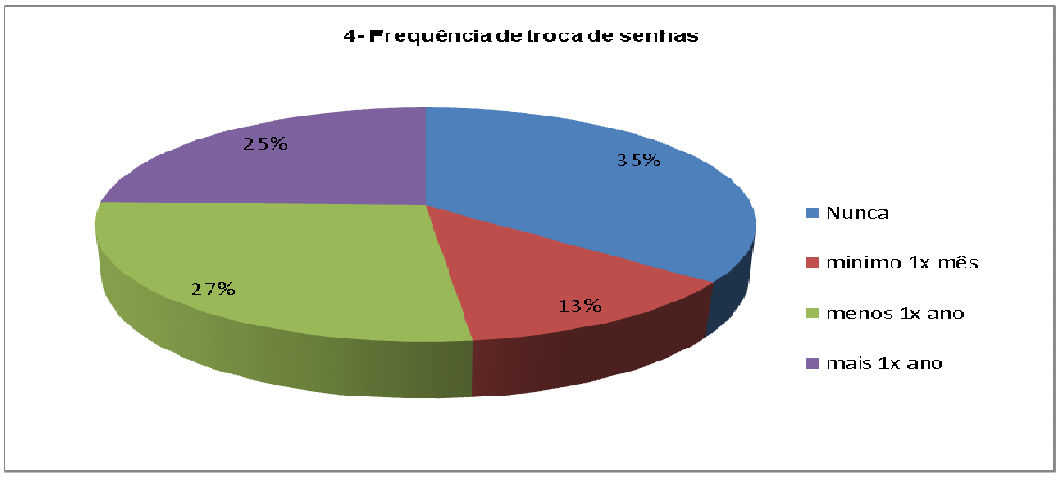

Gráfico 4 - Resposta pergunta 04

O grupo entrevistado mostrou que usam senhas fortes e não costumam repetir essas mesmas senhas, no entanto, a frequencia com que trocam o códigos de segurança de suas páginas mostrou-se abaixo do ideal. Foi elaborado quatro opções com diferentes intervalos de tempo para investigar de que forma os participantes mantinham suas senhas seguras através dos periodos que as mesmas são alteradas. Os resultados mostram que 35% dos usuarios entrevistados nunca trocaram suas senhas e apenas 13% desse total tem o hábito seguro de troca-las no intervalo minimo de uma vez ao mês. Entende-se que, quanto mais vezes uma senha de acesso é alterada, mais reduz-se as probabilidades de que ela seja decodificada ou mesmo descoberta. Esse quesito de segurança, mostrou ser um ponto fraco para a segurança dos esttudantes ouvidos.

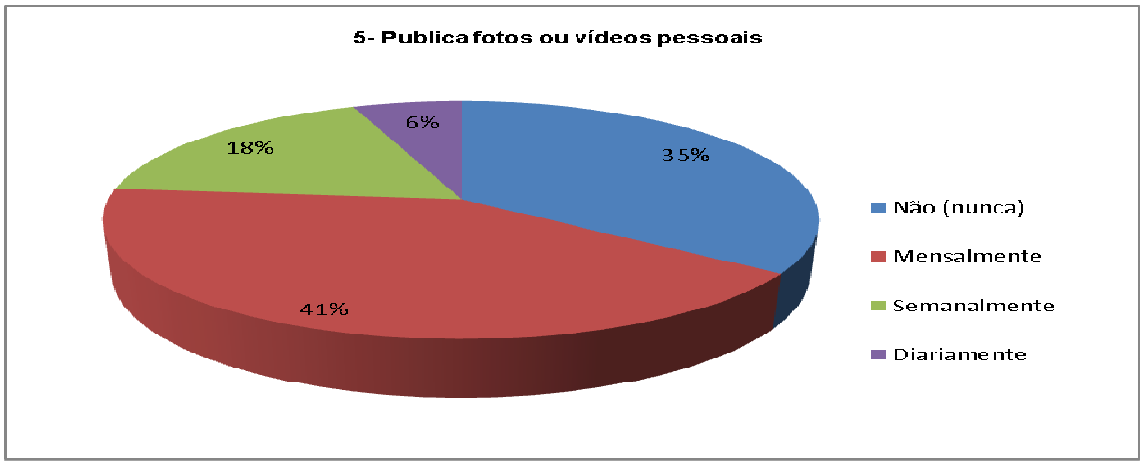

Gráfico 5 –Resposta a pergunta 05

A questão cinco da entrevista indagou a respeito da frequência com que os participantes divulgavam fotos ou vídeos pessoais de suas viagens de férias ou trabalho, assim como sua localização. 41% dos entrevistados relataram que mensalmente disponibilizam informações pessoais em redes sociais, 35% disseram que nunca expões esse tipo de informação, 18% publica essas informações semanalmente, e um percentual de 6% tem o habito de divulga-las diariamente em suas páginas. Podemos concluir através dos resultados que os estudantes pesquisados produzem uma quantidade considerável de informações para o publico que poderiam ser usadas de forma nociva conta eles mesmos, se houver tal intenção.

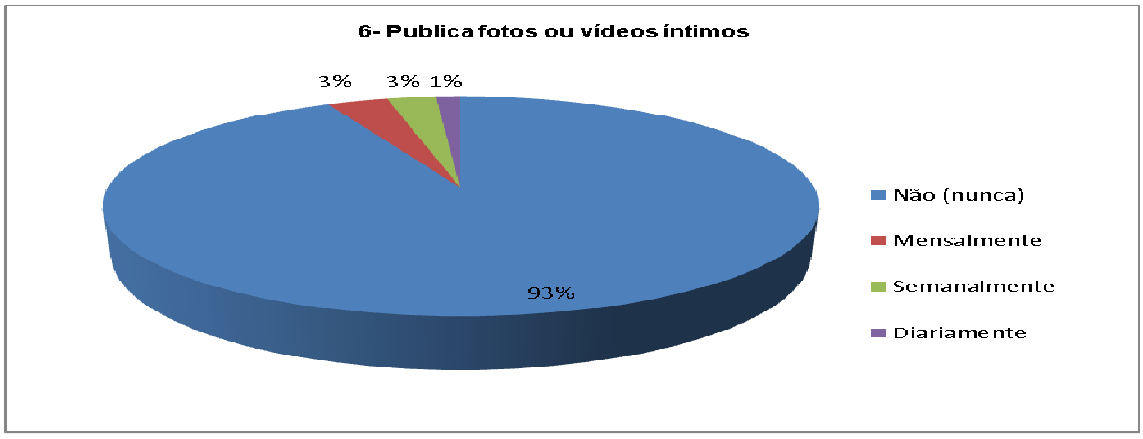

Gráfico 5 - Resposta pergunta 06

Essa quetão perguntou especificamente sobre fotos ou videos de carater intimo como beijos, roupas íntimas, relacionamentos íntimos ou poses sinuosas. Tem sido frequente na mídia a ocorrência de exposições de pessoas em momentos íntimos, causando irreparáveis constrangimentos a mesma por terem tido fotos ou vídeos muito íntimos divulgados por terceiro. Dos entrevistados, 3% publicam mensalmente, 1% diariamente e

outros 3% semanalmente. 93% disseram que não publicam esse tipo de material. É importante ressaltar que não foi investigado se esses participantes produzem esse tipo de material ou sua forma de armazena-lo e mantê-los em segurança, mas somente se eles próprios divulgam sobre si esse tipo de informação.

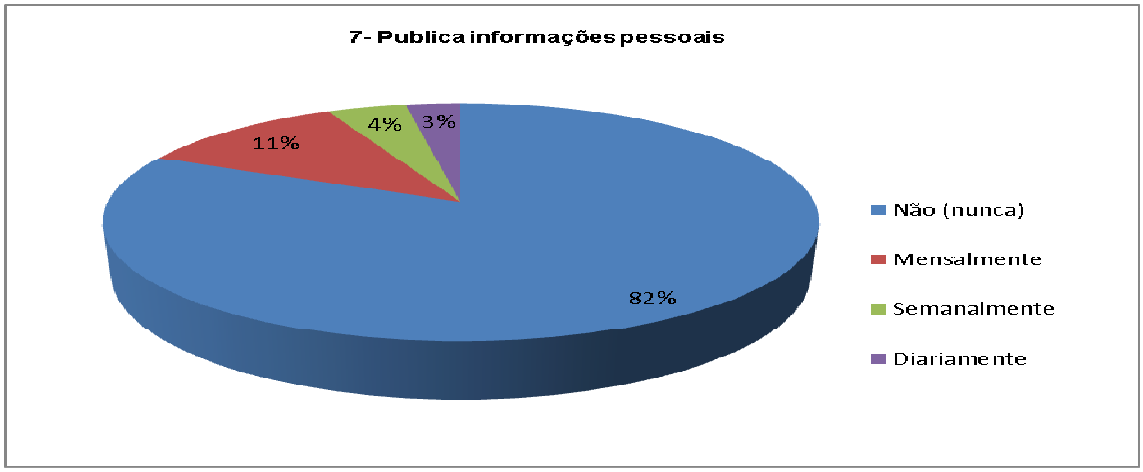

Gráfico 6 - Resposta pergunta 07

Esse gráfico ilustra a quantidade de entrevistados que publicam informações pessoais como horário de trabalho/escola, data de viagens, endereços ou números de telefones em redes sociais. A grande maioria 82%, disseram que nunca disponibilizam essas informações, 11% mensalmente, 4% semanalmente e 3% as disponibilizam diariamente. Quanto a essa questão, o grupo mostrou um nível de maturidade sobre manter sua privacidade na rede.

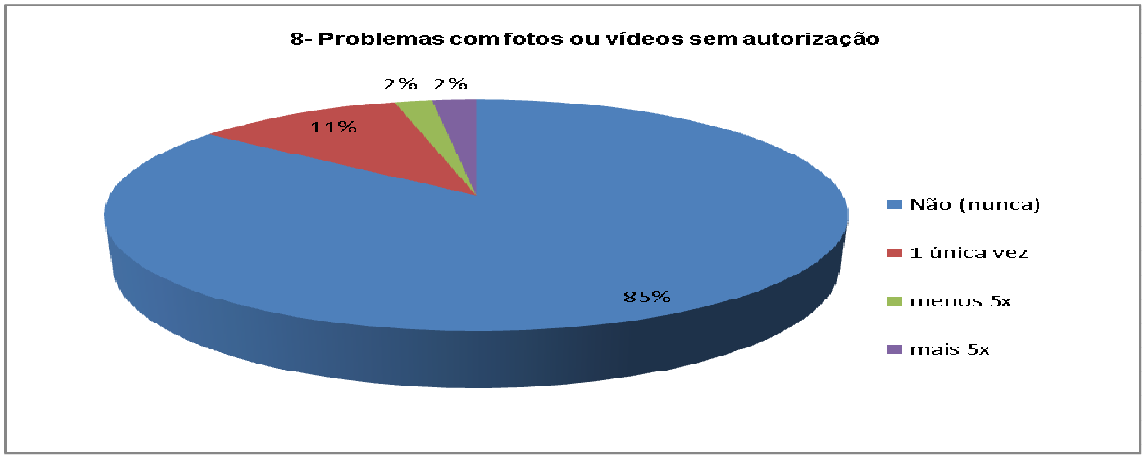

Gráfico 7 - Resposta pergunta 08

Enquanto as questões anteriores buscaram entender a forma como os participantes se comportavam em relação a manutenção da segurança de suas contas e a quantidade e frequencia de informaçoes que produziam sobre si mesmos. Esse tópico buscou numeros que demosntrassem quantos dos universitários ouvidos vivenciaram problemas relacionados com fotografias, vídeos ou assuntos pessoais divulgados **sem a sua autorização** nas redes sociais (*facebook, twiter, instagram* ou similares) ou aplicativos de troca de mensagens (*e-mail, whatsapp, MSN* ou similares); 85% dos participantes afirmaram que nunca tiveram problemas com isso, e 11% sofreram esse tipo de invasão uma única vez, 2% menos de cinco vezes e outros 2% mais de cinco vezes tiveram informações pessoais divulgadas sem o seu consentimento.

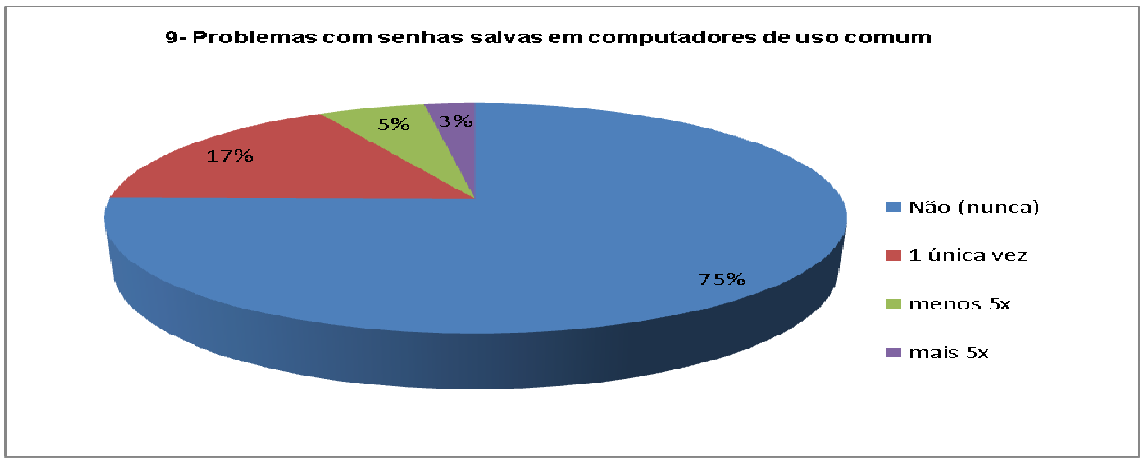

Gráfico 8 - Resposta pergunta 09

Esse questão pesquisou um fato muito comum, principalmente na universidades, onde os alunos acessam suas contas o tempo todo em diferentes computadores e nem sempre fazem o logout adequado. Buscou-se numeros que mostrassem quantos dos participantas já tiveram algum problema por terem deixado suas senhas salvas ou seu perfil conectado em algum computador de uso comum como *lan houses,* bibliotecas, faculdades ou em computadores que outras pessoas utilizam. 75% dos estudantes nunca tiveram esse problema, 17% passaram por isso uma única vez, 5% menos de cinco vezes e 3% por mais de cinco vezes tiveram problemas por deixarem suas contas abertas em maquinas de uso comum.

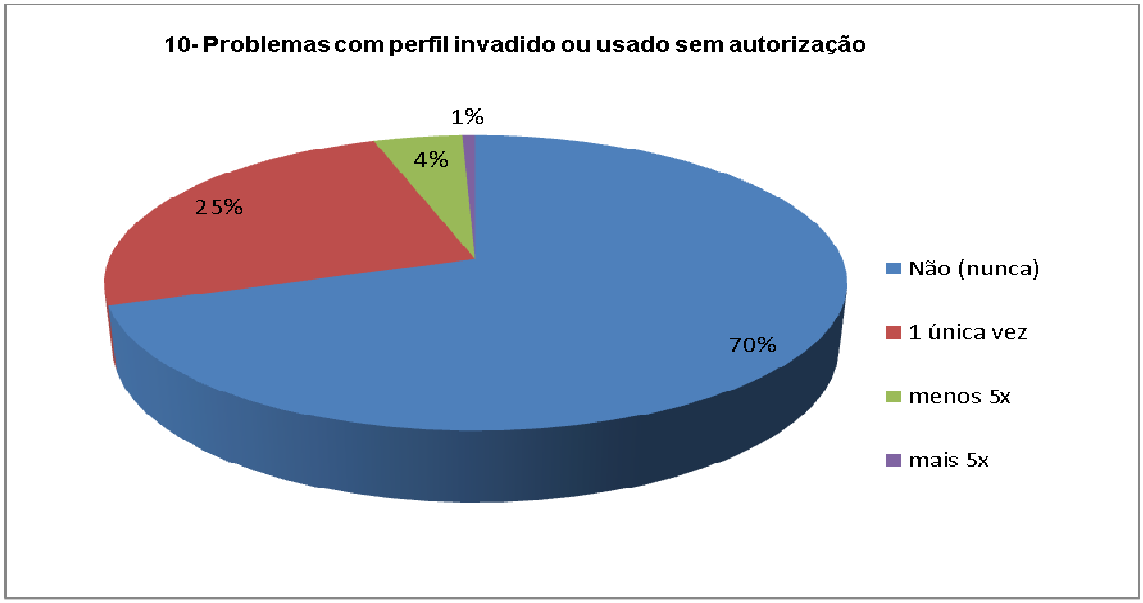

Gráfico 9 - Resposta pergunta 10

Esse gráfico representa de forma direta a quantidade de entrevistados que tiveram suas páginas pessoais ou perfil de rede social invadido ou usado por outra pessoa sem sua autorização. Essa foi a ultima questão da pesquisa, e o resultado encontrado reflete os resultados anteriores, onde os participantes apresentaram hábitos corretos em relação a senhas seguras, não repetição de senhas e mínimo de divulgações pessoais. Um total de 70% nunca tiveram suas páginas invadidas, enquanto 25% dos participantes tiveram esse problema, 4% das páginas forma invadidas menos de cinco vezes e 1% mais de uma vez.

Conclusão

A *internet*, como uma rede mundial de computadores, representa uma infinidade imensurável de cultura e informação, sem a qual, não estaríamos no atual estágio de desenvolvimento. O estudo trabalhou com a hipótese de que os participantes usavam as redes sociais de forma insegura, com senhas fracas e publicando informações que podem ser usadas inadequadamente, prejudicando assim sua privacidade e segurança pessoal. Acreditava-se também que existia um alto número desses jovens, que em algum momento de suas vidas, já tiveram algum problema de privacidade violada devido ao mau uso das redes sociais, oque de fato, pode ser verificado com os números apresentados.

A pesquisa tinha como objetivo inicial, conseguir ouvir 500 universitários sobre seus hábitos e comportamentos enquanto usuários de redes sociais, focando nos hábitos de

uso das ferramentas de comunicação por meio de perfis desses universitários e identificar o comportamento destes quanto á prática de navegação na *internet,* como postagem de fotografias, utilização de senhas e informações pessoais. Por se tratar de um trabalho onde a amostra é material humano, e por tanto, fatores variáveis, não foi possível prever com exatidão quantas pessoas se disporiam a participar, não conseguindo assim, encerrar os estudos com o numero proposto, realizando o trabalho com uma amostra de 317 participantes.

A hipótese inicial não foi totalmente comprovada, considerado que os resultados apresentados definiram um perfil de navegação seguro em sua maioria, embora se possa afirmar que uma parte das pessoas entrevistadas ainda não se conscientizou a respeito dos limites considerados adequados para manter-se protegido no mundo virtual, no entanto ao analisarmos os dados e compararmos a quantidade de entrevistados que já tiveram sua privacidade invadida e cruzarmos essa informação com seus hábitos de navegação e segurança, podemos concluir que o perfil desses usuários demostra um nível de maturidade e conscientização acima do esperado pelos pesquisadores, levando-se a acreditar que o grupo pesquisado possui uma cultura virtual mais esclarecida e equilibrada.

Os resultados mostram que o numero de participantes que responderam a pesquisa, e que lidaram com problemas de privacidade na rede é menos que 50% dos entrevistados, dados que refletem hábitos de navegação seguros do grupo pesquisado.

Referências Bibliográficas

BENNATON, Leandro. Segurança digital, uma batalha diária. Disponível em: http://corporate.canaltech.com.br/noticia/seguranca/Seguranca-digital-uma-batalha-diaria/. Acesso em 20 de novembro de 2014.

BUENO, James Nogueira. COELHO, Vânia Maria Bemfica Guimarães. Crimes na *Internet*. Faculdade de Direito de Varginha. Disponível em: < http://www.egov.ufsc.br/portal/sites/default/files/crimes_na_internet1.pdf. > Acesso em 17 de Fevereiro de 2015.

Cartilha da OAB: Recomendações e boas práticas para o uso seguro da *internet* para toda a família. Cartilha da OAB. 1º edição. Disponível em http://www.opiceblum.com.br/download/OABMack_UsoSeguroInternetFamilia.pdf. Acessado dia 20 de Abril de 2014.

CASTELLS, M. A sociedade em rede. A era da informação: Economia, Sociedade e Cultura. 10 ed., v. 1. São Paulo: Editora Paz e Terra, 2007.

CASTELLS, M. A Galáxia da *Internet*: reflexões sobre a *Internet*, os negócios e a sociedade. Tradução. Maria Luiza X. De A. Borges. Rio de Janeiro: Editora Zahar, 2003. 244 p. (original: La Galaxia *Internet*. Reflexiones sobre *Internet*, empresa y sociedad. Madrid: Arete. (2001). Disponível em: www.edrev.info/reviews/revp49.pdf: acesso Em 09 de Setembro de 2014.

DIAS, Cristiane; COUTO, Olivia Ferreira do. As redes sociais na divulgação e formação do sujeito do conhecimento: compartilhamento e produção através da circulação de ideias. Campinas: Unicamp, Otubro/ 2011. Disponível em: http://www.scielo.br/scielo.php?pid=S151876322011000300009&script=sci_abstract&tlng=pt. Acesso em 29 de outubro de 2013.

FAUSTINO, Raquel. OLIVEIRA, Tamires Morete de. O Ciberbullying no orkut: A agressão pela linguagem. Língua, literatura e ensino, Maio/2008 – Vol. III. Disponível em: http://revistas.iel.unicamp.br/index.php/lle/article/view/124/105. Acesso em: 17/02/2015.

FANTE, C. (2005). Fenômeno Bullying. São Paulo, SP: Verus Editora.

IBOPE. Disponível em: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=30874&sid=4 Acesso em 23 de Junho de 2014.

MARTÍN-BARBERO, Jesus. A mudança na percepção da juventude: sociabilidades, Tecnicidades e subjetividades entre jovens In: BORELLI, Sílvia H. S. e FILHO, João Freire, Culturas Juvenis no século XXI. São Paulo, EDUC, 2008.

Marco Civil da *Internet*: Projeto de Lei nº 2126/2011, conhecida como Marco Civil da *Internet*, apresentadas por José Eduardo Martins Cardoso, Miriam Aparecida Belchior, Aloizio Mercadante Oliva e Paulo Bernardo Silva.

MITNICK, Kevin; SIMON, William L. A arte de enganar. São Paulo: Pearson, 2003.

NIELSEN, J. (2004). User education is not the answer to security problems. Disponível em:< http://www.useit.com/alertbox/20041025.html > Acessado em 26/01/05.

PAGANELLA, W.R. Ética e Tecnologia**.** Universidade de Caxias do sul. Rio grande do sul. 2012. Disponível em: http://www.google.com.br/ Acesso em: 29 de Setembro de 2013.

POPPER, Marcos Antônio; BRIGNOLI, Juliano Tonizetti. Engenharia social – um perigo iminente. Disponível em: < http://fabricio.unis.edu.br/SI/Eng_Social.pdf > Acesso em: 20 de Abril. 2014.

ROSSINI, Augusto Eduardo de Souza. "Brevíssimas Considerações Sobre Delitos Informáticos". Caderno Jurídico. Julho/02. Ano 2.nº 4. ESMP.

Suporte Google. Como criar uma senha segura. Disponível em: https://support.google.com/accounts/answer/32040?hl=pt-BR. Acesso em 21/10/014.

Suporte Microsoft. Dicas para criar uma senha forte. Disponível em: http://windows.microsoft.com/pt-br/windows-vista/tips-for-creating-a-strong-password. Acesso em 21/10/2014.

SAMPAIO, Salustiano Campelo; SIQUEIRA, Jorge Eduardo Andrade; FILHO, José Bezerra Da. Engenharia Social, suas ameaças para a segurança da informação e formas de proteção embasadas nos controles da norma NBR ISO/IEC 27002 – Estudo de caso. Disponível em: http://www.youblisher.com/p/96562-Engenharia-Social-suas-ameacas-para-a-seguranca-e-formas-de-protecao, Acesso em 21 de Abril de 2014.

SAFERNET. Disponível em: www.SaferNet.org.br/cartil. Acesso em Abril 2014.

Sete de cada dez aparelhos da *Internet* das Coisas são vulneráveis a ataques. Disponível em: < http://corporate.canaltech.com.br/noticia/seguranca/Sete-de-cada-dez-aparelhos-da-*Internet*-das-Coisas-e-vulneravel-a-ataques > Acesso em 20 de Novembro de 2014.

SILVA, Denise Ranghetti Pilar da; STEIN Lilian Milnitsky. **Segurança da informação:** uma reflexão sobre o componente humano. Ciênc. cogn. vol.10 Rio de Janeiro mar. 2007. Disponível em: < http://pepsic.bvsalud.org/scielo.php?pid=S1806-58212007000100006&script=sci_arttext. >. Acesso em: 17 de fevereiro de 2015.

SASSE, M.A., Brostoff, S. e Weirich, D. (2001). Transforming the "weakest link" - a human/computer interaction approach to usable and effective security. BT Technology Journal, 19, 122-131 .