Ensino de Noções Básicas de Segurança da Informação nas Escolas Brasileiras

Emerson A. Carvalho[1], **Thales A. Reis**[2], **Fábio J. Alves**[1]

[1]IFSULDEMINAS – Campus Machado
Rodovia Machado – Paraguaçu – KM 3 – Santo Antônio – Machado – MG – Brasil

[2]Departamento de Engenharia da Computação
Universidade Federal de Itajubá (UNIFEI) – Itajubá – MG – Brasil

{emerson.carvalho,fabio.alves}@ifsuldeminas.edu.br, thalesreis57@gmail.com

Abstract. *The technology has been changing people's habits world wide, including in Brazil, with an estimation of having a computational device for each inhabitant by the end of this year (2017). Internet access also grows at a considerable pace (80% of Brazilian households already have Internet access). However, security regarding to the use of computing devices, especially the connected ones, is not treated properly. According to an UN's report, at its Conference on Trade and Development (UNCTAD), Brazil is one of the top five countries regarding to cyber crimes. Whereas this topic is relevant, this work shows that our school community needs improve its background on Information Security, as well as grounds the need for debates, training and even the creation of disciplines to properly address the subject.*

Resumo. *A tecnologia vem mudando os hábitos das pessoas mundo a fora. No Brasil não é diferente, com a estimativa de termos um dispositivo computacional para cada habitante até o final deste ano (2017). O acesso à Internet também cresce a uma velocidade considerável (80% dos domicílios brasileiros já possuem acesso). No entanto, a segurança no uso dos dispositivos computacionais, em especial os conectados em rede, não é tratada com a devida atenção. Segundo um relatório da ONU, em sua Conferência sobre Comércio e Desenvolvimento (UNCTAD), o Brasil é um dos cinco países com mais crimes cibernéticos. Considerando a relevância do tema, este trabalho mostra que nossa comunidade escolar precisa de um melhor embasamento sobre a Segurança da Informação, bem como fundamenta a necessidade de debates, capacitações e até mesmo a criação de disciplinas para tratar adequadamente o assunto.*

1. Introdução

Atualmente, a maioria das aplicações está *online*, sendo acessadas por meio da *Web*. Estamos em plena era digital, cujo bem durável que mais cresce nos lares brasileiros é o computador com acesso à *Internet* (crescimento de quase 40% entre 2009 e 2011, com aproximadamente 79,9 milhões de brasileiros [IBGE. 2011]. Aproximadamente 93% dos brasileiros já possuem um aparelho celular, 32% possuem um *laptop*, 25% possuem um computador pessoal e 19% possuem um *tablet*. A expectativa é termos um dispositivo computacional para cada habitante até o fim de 2017 [CGI.br. 2015].

DOI: 10.5753/cbie.wie.2017.765

O computador e a *Internet* têm sido considerados os principais recursos tecnológicos utilizados atualmente, superando os outros meios de comunicação, principalmente pela velocidade em que as coisas se realizam [Neitzel 2007]. Aproximadamente 80% dos domicílios brasileiros possuem algum dispositivo computacional com acesso à *Internet*, sendo os *smartphones* o tipo de aparelho mais usado para se conectar à rede a partir da propria residência [CGI.br. 2015]. A Pesquisa Nacional por Amostra de Domicílios mostra que, apesar de todos os grupos de idade apresentar aumento no uso da rede entre os anos de 2013 e 2014, o maior aumento no período, com 8%, foi entre os jovens de 20 a 24 anos de idade, que foi de 70,5% para 78,5%. A maior parcela de uso da rede, no ano de 2014, fica com os jovens de 15 a 17 anos de idade, com 81,8% [IBGE. 2014]. Considerando a faixa etária entre 15 e 24 anos, estamos falando de uma boa parte dos estudantes do ensino médio e superior do país.

A Pesquisa sobre o uso das tecnologias de comunicação e informação nos domicílios brasileiros ainda mostra que 89% das pessoas que acessaram a *Internet* o fizeram com algum propósito relacionado à Educação, seja para realizar atividades ou pesquisas escolares, atividades de Cursos à Distância (EaD) ou estudos gerais por conta própria [CGI.br. 2015]. Os resultados dessas pesquisas recentes apontam para um crescimento no uso da *Internet* e seus recursos para propósitos educacionais, o que é um bom indicador se considerarmos os avanços que podemos ter no processo de aprendizagem quando adotamos ferramentas tecnológicas [Santos et al. 2016]. No entanto, usar ferramentas tecnológicas, em especial as que fazem algum tipo de recurso da *Internet*, pode levar a uma série de riscos que nem todos estão preparados para identificar e se proteger.

O CERT.br, nos anos de 2014 e 2015, registrou um total de 1.7 milhões de incidentes de segurança no Brasil. Desse total, 636.396 foram tentativas de fraude, que se caracteriza por um ato enganoso, de má fé, com intuito de lesar ou ludibriar alguém. É importante destacar os casos de páginas falsas de bancos e sites de comércio eletrônico, que cresceram 80% em 2014 se comparado ao ano de 2013 [Cert.br. 2017]. A Central Nacional de Denúncias de Crimes Cibernéticos (CNDCC), mantida pela SarferNet Brasil, recebe, diariamente, uma média de 2.500 denúncias envolvendo crimes de pornografia infantil ou pedofilia, racismo, neonazismo, intolerância religiosa, apologia e incitação a crimes contra a vida, homofobia e maus tratos contra os animais. No total, já foram mais de 3.861.707 denúncias recebidas pela CNDCC [SAFERNET 2017]. A Rede Nacional de Ensino e Pesquisa (RNP), por meio do Centro de Atendimento a Incidentes de Segurança (CAIS), criado para agir como um CSIRT (*Computer Security Incident Response Team*), que atua na detecção, resolução e prevenção de incidentes de segurança na rede Ipê (rede acadêmica brasileira), já detectou, até o final de 2013 (último relatório divulgado), 1.206.881 incidentes. Dos incidentes detectados no ano de 2013, 62% foram relacionados a códigos maliciosos, 8% foram tentativas de fraudes, com mais de 70% dessas tentativas referindo-se a algum tipo de *phishing*, técnica onde o atacante tenta se passar por outra pessoa ou instituição para obter informações que lhe permitirá obter algum tipo de benefício futuramente [CAIS 2013].

Devido a esse aumento no uso da *Internet*, os riscos de invasões e ataques se tornam maiores. Quanto mais aplicações em rede, maiores são as chances de ataques bem sucedidos contra seus usuários. Informações pessoais, profissionais e corporativas são os maiores ativos de uma pessoa, empresa ou instituição de ensino, que muitas vezes

negligenciam, por falta de conhecimento, os riscos que correm quanto ao acesso indevido a esses dados tão importantes. Os sistemas computacionais modernos são desenvolvidos pensando na segurança de suas informações. No entanto, muitas vezes esses sistemas seguros são alvos de ataques bem sucedidos devido ao mau uso por parte de seus usuários. Um conceito importante relacionado à Segurança da Informação é o de que não existe segurança absoluta. Ao invés de perseguir uma garantia absoluta na segurança por meio de *software*, é mais importante conscientizar as pessoas para que tenham atitudes seguras [Marçula and Filho 2013].

Em uma pesquisa realizada com professores e alunos do ensino fundamental e médio da rede pública do estado do Rio de Janeiro, foi constatado que mais de 90% dos professores tem medo do roubo de dados e golpes ou fraudes em compras, enquanto apenas 34% dos alunos se preocupam com esses riscos. Aproximadamente 63% do professores temem por encontrar conteúdos agressivos e 34% tem medo de ser difamado pela *Internet* (*Cyberbullying*) por alunos e/ou colegas de trabalho. Sobre os principais riscos aos quais seus alunos podem estar expostos, os professores temem por: 1) Conteúdos violentos ou criminosos (88%); 2) Pornografia (77%); 3) Aprender coisas que ferem os bons costumes (57%); 4) *Cyberbullying* (33%) e 5) Roubo de dados (21%). Um dado interessante da pesquisa mostra que apenas 26% do público pesquisado aprendeu a utilizar a *Internet* em capacitações formais, os demais aprenderam a utilizar a rede de alguma maneira informal (amigos, parentes etc) ou sozinhos. Aproximadamente 68% dos professores acreditam ser importante ter mais capacitação em relação ao uso seguro da tecnologia. Das medidas para prevenção dos perigos *online*, 56% dos educadores admitiram discutir com seus alunos os efeitos da tecnologia em sala de aula, para 65% deles é urgente a necessidade de as escolas tratarem o tema Segurança na *Internet* com mais frequência e 31% admitiram não ter nenhum recurso didático disponível para tratar do tema [SAFERNET. 2009].

A educação é uma maneira econômica de empresas e instituições de ensino alcançar uma segurança mínima. Sendo assim, este artigo tem o objetivo de demostrar a necessidade da formação e conscientização de docentes, discentes e toda comunidade escolar no que tange às noções básicas sobre Segurança da Informação e os principais fatores de riscos aos quais os usuários, principalmente os não técnicos, estão sujeitos ao desempenhar suas atividades diárias que envolvem o uso de dispositivos computacionais conectados em rede. Por meio dos resultados apresentados neste trabalho é possível justificar ações educativas, disciplinas e/ou cursos, direcionados ao público analisado e tratando dos fatores de maior risco. Difere das pesquisas realizadas anteriormente pelo fato de direcionar a pesquisa aos riscos e vulnerabilidades atualmente mais identificados, uma vez que é sabido que o uso da *Internet* é uma realidade em nossa sociedade.

2. Métodos

O trabalho fundamentou-se numa pesquisa aplicada, objetivando gerar conhecimentos para tomada de ações relacionadas ao uso seguro de dispositivos computacionais conectados em rede. Foi desenvolvido sobre uma abordagem não experimental, e sim por um levantamento realizado por questionários *online* para sua elaboração e execução. Discentes e docentes de diversos cursos e campi da instituição formaram o espaço amostral. Baseado nos índices por tipos de ataques reportados ao CERT.br, à CNDCC e ao CAIS, foram selecionados ataques e vulnerabilidades de maior risco, considerando o público alvo, para comporem os tópicos da pesquisa.

Foi aplicado a todos os participantes da pesquisa, um questionário (questionário 1) com questões de múltipla escolha que considerou situações do cotidiano das pessoas durante suas atividades que envolvem o uso de dispositivos computacionais, de forma que os riscos inerentes pudessem ser avaliados naturalmente. O objetivo foi verificar se as pessoas saberiam identificar situações de risco que nos são apresentadas a todo momento, tais como: fraudes de antecipação de recursos, rastreamento de atividades, falsificações de *e-mails*, furtos de identidade, *Cyberbullying*, códigos maliciosos (vírus, *worms*, cavalos de tróia etc), criação de senhas seguras, *sexting*, uso de criptografia (https) etc.

As questões do questionário 1 foram elaboradas de forma a simularem situações cotidianas de risco as quais os usuários de sistemas conectados em rede podem vivenciar. As questões e suas respectivas alternativas estão listadas abaixo:

1. Você recebe um *e-mail* dizendo que você está prestes a receber uma herança e para que ela seja liberada é necessário pagar uma certa quantia de dinheiro. Isso caracteriza um(a): ( ) Fraude de antecipação de recursos; ( ) *Pharming*; ( ) Fraude de comércio eletrônico; ( ) *Spam*.
2. Você recebe um *e-mail* de uma pessoa dizendo que trabalha no seu banco e que necessita dos dados de sua conta, pois ocorreu um erro no sistema. Isso caracteriza um(a): ( ) Vírus; ( ) *Phishing*; ( ) *Pharming*; ( ) Falsificação de *e-mail*.
3. *E-mails* com assuntos diversos, oriundos de remetentes desconhecidos, recebidos sem se solicitar e que, na maiorias das vezes, são propagandas ou alguma tentativa de fraude são classificados como? ( ) Falsificação de *e-mail*; ( ) *Spams*; ( ) Virús; ( ) *Cookies*.
4. Há alguns dias atrás você pesquisa um celular que deseja comprar. Em seguida você começa a observar que as propagandas que estão aparecendo em redes sociais, *blogs* e em outros *sites* acessados são daquele mesmo modelo de celular ou de algum similar. Isso acontece graças aos(as): ( ) *Spams*; ( ) Janelas de *pop-up*; ( ) *Cookies*; ( ) Códigos maliciosos.
5. Alguém cria um perfil em uma rede social com o seu (você leitor) nome e sua foto. Isso caracteriza um(a): ( ) Vírus; ( ) Fraude de identidade; ( ) Fraude de antecipação de recursos; ( ) Janela de *pop-up*.
6. Você percebe que seu computador está realizando tarefas que você não iniciou ou está rodando alguns programas sem sua permissão. Isso acontece graças aos(as): ( ) *Spams*; ( ) Fraudes de antecipação de recursos; ( ) *Pharmings*; ( ) Códigos maliciosos (vírus, *worms*, cavalo de troia).
7. Para realizar uma compra segura na *Internet*, além de conhecer a reputação da empresa, é importante: ( ) Observar se o site usa criptografia de dados (https); ( ) Observar se o site usa criptografia dos dados (http); ( ) Não pagar com cartão de crédito; ( ) Não comprar pela *Internet*, pois não é seguro.
8. Ao praticar ofensas a uma pessoa através da *Internet*, você está praticando: ( ) Fraude de identidade; ( ) *Cyberbullying*; ( ) Invasão a privacidade; ( ) *Pharming*.
9. São medidas para criação de uma senha segura, exceto. ( ) Não usar dados pessoais (nome, data de nascimento, dados de familiares etc); ( ) Não usar sequências (alfabeto ou teclado) de letras ou números; ( ) Usar senhas pequenas, para não correr o risco de esquecer; ( ) Usar combinações de letras, números, símbolos e letras capitalizadas; ( ) Não utilizar senhas muito pequenas.
10. Ao praticar *sexting*, as pessoas estão sujeitas a: ( ) Ser contaminado(a) com vírus; ( ) Ter sua privacidade roubada; ( ) Sofrer fraudes de identidade; ( ) *Phishing*.

Os docentes também responderam a um segundo questionário (questionário 2) visando identificar a atuação dos mesmos em relação à tópicos sobre Segurança da Informação. As questões do questionário 2 e suas respectivas respostas estão listadas abaixo:

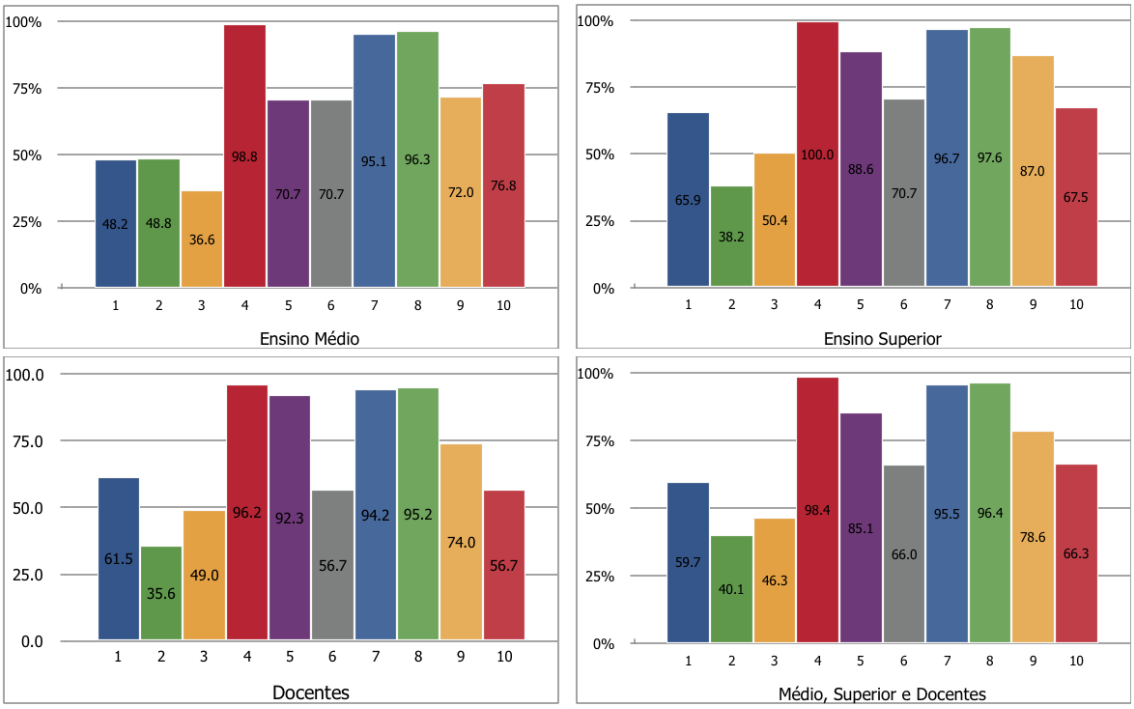
1. Em suas disciplinas, independente da área e/ou curso, já conversou com ou ensinou aos seus alunos sobre o uso seguro da *Internet* e seus recursos? ( ) Sim; ( ) Não.
2. Por que nunca conversou com ou ensinou aos seus alunos sobre o uso seguro da *Internet* e seus recursos? ( ) Por não achar que isso seja importante; ( ) Por não considerar que há riscos ou que os riscos não demostram perigo real; ( ) Por não me sentir preparado para falar sobre o assunto; ( ) Outro [especificar]. Essa pergunta foi respondida apenas por quem respondeu **Não** na primeira questão.
3. Considera importante uma capacitação para docentes (independente de sua área de atuação) sobre o uso seguro da *Internet* e seus recursos? ( ) Sim; ( ) Não.
4. Considera importante a adição desse tema (uso seguro da *Internet* e seus recursos) em disciplinas de Informática Básica no Ensino Médio/Superior ou até mesmo a criação de uma disciplina exclusiva para tratar o assunto? ( ) Sim; ( ) Não.

Os dados coletados por meio dos questionários *online*, que totalizaram 104 docentes e 206 discentes, foram analisados estatisticamente para identificar os riscos menos conhecidos, estimar o conhecimento do público em relação a cada vulnerabilidade estudada e, principalmente, fundamentar a necessidade de um tratamento mais adequado ao tema em nossas instituições de ensino.

3. Resultados e Discussões

Os resultados foram analisados fundamentando-se nas vulnerabilidades, as quais foram separadas em três grupos. Aquelas cujo percentual médio de acerto (considerando todo o público) foi superior a 90% (grupo 3), aquelas cujo percentual médio de acerto foi inferior a 90%, porém superior a 70% (grupo 2) e aquelas cujo percentual médio de acerto foi inferior a 70% (grupo 1). Classificou-se dessa forma por entender que esse agrupamento pode ser usado para direcionar e aprofundar a análise e priorizar ações específicas direcionadas a cada grupo de vulnerabilidades. Não objetivou-se determinar que, por ser ou não mais conhecido, uma determinada vulnerabilidade representa maior ou menor risco. Foi considerado que o grau de risco não depende somente do tipo de vulnerabilidade, pois são muitas as variáveis a se considerar em uma situação real do cotidiano. A Figura 1 exibe o percentual de conhecimento (na vertical) em relação às vulnerabilidades analisadas (numeradas na horizontal com legenda abaixo). O grupo 1 é composto por cinco vulnerabilidades: *Cookies*, Falsificação de *e-mail*, Antecipação de recursos, Senhas seguras e *Sexting* e privacidade. O grupo 2 é composto por duas vulnerabilidades: *Spam* e Criptografia(https). O grupo 3 é composto por três vulnerabilidades: Furto de identidade, Códigos maliciosos e *Cyberbullying*.

A análise dos dados foi realizada considerando o público como um todo, com ressalvas relacionadas a algum perfil específico quando houve alguma variação significativa. Observa-se que há um bom entendimento das vulnerabilidades do grupo 3, que demonstra o conhecimento do público sobre os riscos iminentes de antigas e tradicionais vulnerabilidades, tais como, *Malwares*, falsificações ideológicas e *Cyberbullying*. Vale ressaltar o entendimento do público em relação ao fato de que o *Bullying* realizado por meio da



1) *Cookies*; **2)** Falsificação de email; **3)** Antecipação de recursos; **4)** Furto de identidade; **5)** *Spam*; **6)** Senhas seguras; **7)** Códigos maliciosos; **8)** *Cyberbulling*; **9)** Criptografia (https); **10)** *Sexting* e privacidade

Figura 1. Porcentagem de acerto por público e vulnerabilidade (questionário 1)

Internet não descaracteriza o ato. No entanto, o fato de saber o que são *malwares*, parece não significar ser capaz de evitá-los, pois, segundo o site *Check Point*[1], só o *malware Fireball*, que assume o controle dos navegadores da vítima e os transforma em zumbis, infectou, em junho de 2016, aproximadamente 24 milhões de computadores no Brasil, o segundo país mais infectado pelo *malware*. Segundo uma pesquisa da *Gemalto*[2], o roubo de identidade representou 64% de todas as violações de dados no primeiro semestre de 2016.

O percentual de acerto das vulnerabilidades do grupo 2, apesar de alto, mostra que 15% do público geral não souberam identificar uma situação onde um *e-mail* (*Spam*) deveria ser considerado suspeito. O público adolescente mostrou um conhecimento menor, com aproximadamente 30% das pessoas não sabendo identificar tais situações, o que é preocupante se considerarmos que somente de janeiro a dezembro de 2015 foram denunciados 711.467 *spams* ao CERT.br, que o número estimado de usuários de *e-mail* em todo o mundo é de 3.7 bilhões e a quantidade de *e-mails* enviados por dia (em 2017) é de aproximadamente 269 bilhões, dos quais 49.7% são *spams* [Cert.br. 2017, Radicati 2017]. Aproximadamente 22% do público não associaram o protocolo *https* à criptografia das informações que trafegam pela rede. Um número que merece atenção se considerarmos que o não uso do mecanismo pode expor dados sensíveis do usuário, tais como número de cartões de créditos, senhas de acesso, número de documentos etc. Dos 10 principais riscos que afetam as aplicações *web*, a exposição de dados sensíveis está em 6º (sexto)

[1]FIREBALL – The Chinese Malware of 250 Million Computers Infected (https://goo.gl/4pTkGQ)
[2]Data breach statistics 2016: First half results are in (https://goo.gl/BvAPCJ)

lugar [OWASP 2017]. Um dado que melhora a situação dos internautas brasileiros nesse aspecto é que, segundo o *Google*[3], aproximadamente 95% do tráfego oriundo do Brasil está criptografado.

Os índices de acertos em relação às vulnerabilidades do grupo 3 são mais preocupantes. Do público total respondente, 34% não relacionaram *sexting* ao risco de possíveis exposições públicas de sua privacidade. O público adolescente demonstrou um conhecimento maior sobre o tema, com aproximadamente 77% das pessoas identificando corretamente o tema. O fato dos adolescentes conhecerem mais o tema pode não ser positivo, pois, segundo o *GuardChield*[4], em suas estatísticas sobre *sexting* entre adolescentes americanos, 17% das pessoas que recebem algum tipo de *sexting* compartilham as mensagens com outras pessoas e 55% delas as compartilham com mais de uma pessoa. Quase 40% de todos os adolescentes já publicaram ou enviaram algum tipo de mensagem sexualmente sugestiva, mas essa prática é mais comum entre adolescentes do sexo masculino. No entanto, enviar fotos nus(as) ou seminus(as) é uma prática mais comum entre adolescentes do sexo feminino, 22% das meninas adolescentes relatam o envio de imagens desta natureza, enquanto aproximadamente 18% dos meninos o faz.

Aproximadamente 40% das pessoas avaliadas não mostraram domínio sobre como criar uma senha segura. A situação entre o público docente é ainda pior, com apenas 57% das pessoas identificando corretamente como criar senhas seguras. Um dado alarmante se considerarmos que, no ano de 2014, segundo a *TeleSign*[5], duas em cada cinco pessoas tiveram alguma conta invadida ou alguma senha roubada. Aproximadamente 73% das contas de serviços *online* usam senhas duplicadas, possibilitando que, ao roubar uma senha, um atacante tenha acesso a mais de uma conta do usuário. Outra informação importante é que 90% das contas corporativas (de empregados de empresas) podem ser invadidas em menos de 6 horas e 65% das pessoas usam a mesma senha para todos os seus sistemas.

Em relação às fraudes de antecipação de recursos, aproximadamente 54% do público pesquisado não puderam identificar uma situação típica de antecipação de recursos, entre o público adolescente esse percentual chegou a 63%. Esse tipo de fraude foi responsável, no ano de 2013, segundo o *Advance Fee Fraud Statistics* da *Ultrascan AGI*[6], por mais de 12.7 bilhões de dólares em perdas financeiras de pessoas ou instituições em todo o mundo. No Brasil, o valor em perdas financeiras foi de aproximadamente 179 milhões de dólares para esse mesmo ano, o que reforça a necessidade de uma melhor política de disseminação do conhecimento em relação a esse tipo de fraude em específico.

A fraude de falsificação de *e-mail* também não foi bem reconhecida, com aproximadamente 60% das pessoas não reconhecendo esse tipo de ataque. Segundo a *Phishing.org*[7], mais da metade dos usuários da *Internet* recebem pelo menos um *e-mail phishing* por dia. Um estudo conduzido pela *Intel Security*[8] mostrou que 97% das pessoas no mundo todo não podem identificar corretamente um *e-mail phishing* sofisticado.

[3]HTTPS at Google (https://goo.gl/Rzvzw7)
[4]Teenage Sexting Statistcs (https://goo.gl/X5UENW)
[5]TeleSign (https://goo.gl/bQNTF5)
[6]419 Advance Fee Fraud Statistics 2013 (https://goo.gl/wIo49n)
[7]Phishing.org (https://goo.gl/syHcSG)
[8]Intel Security study shows that 97% of people can't identify phishing e-mails (https://goo.gl/oenOLN)

O estudo da *Intel Security* apresentou 10 *e-mails* questionando as pessoas sobre quais *e-mails* eram *phishing*, objetivando roubar dados pessoais e quais eram *e-mails* legítimos. O estudo coletou dados em 144 países, com aproximadamente 19 mil pessoas pesquisadas.

O funcionamento dos *cookies*, utilizados, geralmente, para rastrear a navegação do usuário, não foi identificado por 40% das pessoas pesquisadas, com esse percentual chegando a 52% entre os alunos do Ensino Médio. Considerando que nem todo tipo de *cookie* é seguro, essa é uma estatística perigosa. Segundo o *W3techs*[9], 50.2% de todos os *sites* usam *cookies* e 97.3% desses *sites*, que usam *cookies*, usam *cookies* não seguras.

A pesquisa sobre as percepções dos docentes em relação à Segurança da Informação (Figura 2) mostra que quase 56% deles nunca abordou o tema com seus alunos, uma porcentagem ainda maior comparado aos resultados de [SAFERNET. 2009], com 44%. A principal justificativa é o fato de não se sentir preparado para debater o assunto (76%), seguida da isenção de responsabilidade por dar aula em outra área (12%) ou julgar que o assunto foi tratado em alguma outra disciplina (3%). Além de aproximadamente 9% alegar que nunca havia pensado sobre essa questão. Por outro lado, 95% dos docentes consideram ser importante uma capacitação docente sobre o uso seguro da *Internet* e seus recursos, independente de sua área de atuação e 90% dos docentes também consideram ser importante a adição do tema em disciplinas de Informática Básica no Ensino Médio/Superior ou até mesmo a criação de disciplinas exclusivas para abordar o assunto.

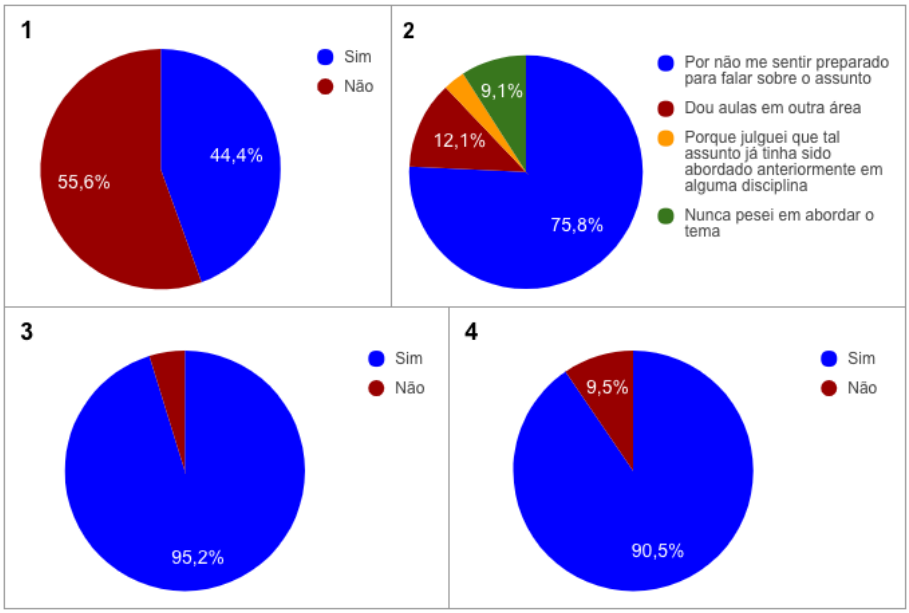


Figura 2. Percepções dos docentes em relação à Segurança da Informação (questionário 2)

1) Já abordou o uso seguro da *Internet* com seus alunos? **2)** Por que nunca abordou o tema com seus alunos? **3)** Considera importante uma capacitação para os docentes sobre o uso seguro da *Internet*? e **4)** Considera importante a adição do tema em disciplinas de Informática no Ensino Médio ou até mesmo a criação de disciplina específica?

[9]Usage of Cookies for websites (https://goo.gl/zRQk49)

4. Conclusões

É inegável que a tecnologia está cada vez mais presente em nosso cotidiano. Conforme visto anteriormente, a tendência é de um crescimento ainda maior para os próximos anos. A presença da tecnologia em nosso dia a dia nos trás inúmeros benefícios, no entanto, nos apresenta também diversos riscos aos quais devemos estar preparados para enfrentar, para que possamos utilizar o que de melhor a tecnologia nos proporciona sem que possamos sofrer perdas e/ou prejuízos de qualquer natureza.

Nosso principal objetivo foi analisar o entendimento do público pesquisado sobre os principais riscos de segurança aos quais estão expostos, bem como descrever as percepções dos professores sobre o tema. Dessa forma, poderíamos justificar ações educativas, disciplinas e/ou cursos, direcionados ao público analisado e tratando dos fatores de maior risco. Os resultados obtidos mostra que há uma certa uniformidade em relação ao não conhecimento de alguns riscos por parte do público analisado. Isso evidencia a necessidade da elaboração de ferramentas, disciplinas, treinamentos, palestras e materiais diversos, tanto para a capacitação de professores quanto para a preparação de nossos alunos.

Como visto em nossa pesquisa, bem como na pesquisa da [SAFERNET. 2009], nossos professores e alunos, do Ensino Médio e, pelos nossos resultados, também do Ensino Superior, demonstram estar expostos a diversas vulnerabilidades perigosas quando de suas atividades *online*. É clara a necessidade de ações que aumentem o entendimento e a capacidade das pessoas em lidar com situações de riscos, tais como: senhas fracas, a troca de informações íntimas, falta de conhecimento das ferramentas, protocolos, riscos relacionados ao ambiente de *e-mail*, o funcionamento básico dos sistemas *Web* e fraudes de antecipação.

Considerando os prejuízos, perdas e traumas que pessoas despreparadas poderiam sofrer se vítimas de alguma das fraudes estudadas, bem como o uso universal e praticamente inevitável da tecnologia, acredita-se ser de fundamental importância um debate maior sobre como abordar a questão da Segurança da Informação e consequentemente dos usuários de tecnologia. Em um ambiente onde a educação é o objetivo maior, é necessário educar, constantemente, educadores e educandos em relação ao uso mais consciente das ferramentas tecnológicas. Conforme descrito por [Garcia et al. 2011], a prática pedagógica moderna que contempla os recursos tecnológicos exige novas competências para tratar a cultura de aprendizagem que se instaura por meio do uso das tecnologias no processo de ensino e aprendizagem. A Segurança da Informação e de seus usuários certamente fará parte dessas novas competências.

5. Agradecimentos

À FAPEMIG, pela concessão de bolsa de Iniciação Científica e pelo apoio para participação e apresentação do trabalho no Congresso Brasileiro de Informática da Educação (CBIE) de 2017.

Ao Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais (IFSULDEMINAS), campus Passos, MG e campus Machado, MG, por disponibilizar a infraestrutura necessária para realização deste trabalho.

Referências

CAIS (2013). Relatório anual de incidentes de segurança da informação. [Online. Acesso em 19 de maio de 2017].

Cert.br. (2017). Centro de estudos, resposta e tratamento de incidentes de segurança no brasil. [Online. Acesso em 19 de abril de 2017].

CGI.br. (2015). Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros. [Online. Acesso em 7 de abril de 2017].

Garcia, M. F., Rabelo, D. F., da Silva, D., and do Amara, S. F. (2011). Novas competências docentes frente às tecnologias digitais interativas.

IBGE. (2011). Pesquisa nacional por amostra de domicilio. [Online. Acesso em 29 de abril de 2017].

IBGE. (2014). Pesquisa nacional por amostra de domicilio. [Online. Acesso em 15 de abril de 2017].

Marçula, M. and Filho, P. A. B. (2013). *Informática - Conceitos e aplicações*. Érica, São Paulo, 4 edition.

Neitzel, L. C. (2007). A rede digital na rede educacional: um re-encantamento. [Online. Acesso em 15 de maio de 2017].

OWASP (2017). Owasp top 10 application security risks - 2017. [Online. Acesso em 19 de maio de 2017].

Radicati (2017). Email statistics report, 2017-2021. [Online. Acesso em 03 de maio de 2017].

SAFERNET. (2009). Hábitos de navegação na internet: será que nossos alunos e educadores navegam com segurança na internet no estado do rio de janeiro? [Online. Acesso em 07 de maio de 2017].

SAFERNET (2017). Central nacional de denuncias de crimes ciberneticos. [Online. Acesso em 11 de abril de 2017].

Santos, N. L., Santos, L. S., Pontes, D. P. N., and Hounsell, J. (2016). Softwares educacionais: O papel do licenciado em computação na escola.