ISSN: 2358-8829

CONCEITOS DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE ESCOLAR: SOBRE A NECESSIDADE DE CONHECER TÉCNICAS DE DEFESA VIRTUAL

Radamila Oliveira do Nascimento[1]
Danylla de Medeiros Souza[2]
Augusto César Oliveira de Almeida[3]
Anna Raquel da Silva Marinho[4]
Amanda Ohana Albuquerque Gomes[5]

RESUMO

As informações são de extrema importância para as sociedades desde os primórdios da civilização. No contexto contemporâneo, largamente influenciado pelo uso de computadores, os indivíduos estão constantemente divulgando seus dados, especialmente por meio da internet, o que resulta na vulnerabilidade destes usuários contra agentes maliciosos. Os mecanismos de proteção virtual, como os antivírus, as senhas complexas e as boas práticas ao navegar no ciberespaço são algumas formas de combater ataques, porém, os usuários da internet devem ser educados para empregar tais recursos adequadamente. Assim, recomenda-se que cursos e formações na área de informática dediquem também alguns momentos para instruir os aprendizes sobre práticas de segurança da informação. Nesse âmbito, o presente artigo tem como objetivos explorar literaturas acerca da segurança da informação, bem como relatar as constatações auferidas sobre esse tema em aulas de inclusão digital ministradas em telecentros na cidade de Natal/RN e em um questionário disponibilizado em redes sociais. Essa prática de ensino, sugerida pelos alunos do telecentro, abordou os diferentes tipos de programas maliciosos e as técnicas de prevenção contra vírus e golpes recebidos nos meios virtuais, como o email e o aplicativo de mensagens. Nessas aulas, os alunos foram orientados a observar características de informação falsa, por exemplo, o remetente da mensagem ou uma notificação de prêmio. Com as práticas de aula, o processo de pesquisa e a análise dos dados recolhidos, evidenciou-se a necessidade de ações que levem para o ambiente escolar as discussões sobre os conceitos de segurança da informação, sendo estas mediadas por profissionais habilitados, assim contribuindo para formar uma sociedade mais preparada para combater as ameaças existentes no meio digital. O referencial teórico, também, promove uma discussão sobre o contexto brasileiro no âmbito da segurança da informação e o seu ensino.

Palavras-chave: Segurança da informação, Telecentros, Inclusão digital, Softwares maliciosos.

[1] Especialista em Tecnologias Educacionais e Educação a Distância, IFRN, oliveiraradamila@gmail.com;
[2] Especialista em Mídias na Educação, UERN. Especialista em Docência para Educação Profissional e Tecnológica, IFES, medeirosdanylla@gmail.com;
[3] Especialista em Tecnologias Educacionais e Educação a Distância, Instituto Federal de Educação, Ciência e Tecnologia - RN.
Especialista em Docência para a Educação Profissional e Tecnológica , Instituto Federal de Educação, Ciência e Tecnologia - ES, augustotouya@gmail.com;
[4] Especialista em Psicopedagogia Clínica, Hospitalar e Institucional, UNINASSAU, raquelmarinho.linfor@gmail.com;
[5] Pós-graduanda em Games e Gamificação na Educação, UNINTER. Especialista em Formação Docente para EAD, UNINTER. ohana.albuquerque@gmail.com.

ISSN: 2358-8829

INTRODUÇÃO

Desde os primórdios da comunicação entre os seres humanos, existe o conceito de documentação, como exemplificado pelas pinturas rupestres. Com a escrita e a necessidade na segurança das mensagens em sociedades antigas, criaram-se métodos de codificação e decodificação e, com isso, também houveram esforços para decifrar códigos secretos (Cabral, 2015).

As inundações, o vandalismo, a falta de energia, os erros e as fraudes também são exemplos de ameaças contra a segurança da informação. Portanto, a preocupação com a segurança das informações não é um tema recente, mas entende-se que sua relevância tem crescido na sociedade moderna.

Portanto, os programas maliciosos de computador não são as únicas preocupações advindas do mundo virtual. Silva e Stein (2007) apontam que, enquanto as empresas estão cada vez mais conscientes e atentas para com suas vulnerabilidades, os usuários comuns geralmente não acreditam que podem sofrer ataques. Os meios de comunicação digitais e virtuais oferecem uma grande disponibilidade de informações, além de ser possível, e por vezes necessário, que o usuário compartilhe seus dados pessoais em sítios da internet ou tenha esses mesmos dados divulgados. É imprescindível a importância de instruir os indivíduos continuamente sobre métodos de proteção contra ataques e vazamento de informações no meio virtual.

No Brasil, 81% das escolas públicas possuem salas de informática e conexão com a internet (Varella, 2017). Existem ainda os centros municipais de formação profissional equipados com telecentros. Contudo, a falta de professores qualificados para atuar neste ambiente resulta na subutilização dos recursos. Assim, a presença de licenciados em informática nestes ambientes de ensino, desenvolvendo atividades voltadas para esta área de conhecimentos, beneficiaria as comunidades e os usuários das Tecnologias da Informação e da Comunicação (TICs).

Nesta perspectiva, o presente trabalho reúne uma pesquisa bibliográfica sobre a importância de se trabalhar conceitos de segurança da informação nos ambientes de ensino, tendo-se o licenciado em informática como o profissional com formação adequada para atuar neste sentido. Para complementar o embasamento literário, é traçado um paralelo com atuações docentes realizadas pelos autores deste artigo em turmas de inclusão digital.

ISSN: 2358-8829

Analisa-se também um questionário disponibilizado acerca da presença dos conceitos relacionados à segurança da informação nos ambientes de ensino.

O artigo divide-se da seguinte forma: na segunda seção discutem-se dados sobre a segurança da informação no contexto brasileiro. Na terceira, faz-se um levantamento sobre a importância das TICs e o papel das instituições de ensino na propagação de boas práticas no meio virtual. Na quarta seção descrevem-se práticas de ensino em um telecentro na cidade de Natal/RN envolvendo conceitos de proteção e cuidados nos ambientes virtuais. Por fim, são apresentadas as considerações finais.

METODOLOGIA

Este artigo traz uma descrição de experiência e apresenta o relato de forma qualitativa, incluindo a subjetividade dos autores no processo de análise. Busca-se, ainda, criar uma ponte entre a vivência e as literaturas publicadas sobre a segurança da informação e o ensino de informática. (Souza, 2022)

REFERENCIAL TEÓRICO

Sobre as informações e a segurança virtual no contexto brasileiro

Queiroz e Moura (2015) apontam que a preocupação com a segurança das informações tem se tornado mais intensa desde o século XVI até os dias atuais, devido ao aumento de publicações acadêmicas e à troca de correspondências entre autores do meio científico.

De acordo com Cabral (2015, p. 17),

> A segurança da informação implica em garantir que as informações (em qualquer formato: mídias eletrônicas, papel e até mesmo em conversações pessoais ou por telefone) estejam protegidas contra o acesso por pessoas não autorizadas (confidencialidade), estejam sempre disponíveis quando necessárias, e que sejam confiáveis (não tenham sido corrompidas ou adulteradas por atos de pessoas mal-intencionadas).

O conceito exposto pelo autor abrange tanto os dados corporativos quanto de conteúdo pessoal. No âmbito das TICs e da segurança no meio virtual, Silva e Stein (2007, p. 49) apontam que a motivação de alguns hackers é o "lucro financeiro, outros procuram segredos corporativos, outros ainda estão atrás do fascinante desafio de encontrar a chave para o

ISSN: 2358-8829

território proibido das informações confidenciais de outros". Para as autoras (2007), devido à elevada capacidade de processamento dos computadores pessoais modernos, a quebra de senhas se tornou um ato trivial, havendo inclusive softwares com essa finalidade acessíveis gratuitamente na internet.

Em matéria online, o jornal UOL apresenta dados de um relatório da Norton Cyber Security, revelando que em 2017 o Brasil passou a ser o segundo país com maior índice de crimes cibernéticos, os quais atingiram de alguma forma mais de 62 milhões de pessoas, alcançando um prejuízo total de 22 bilhões de dólares. O site aponta o smartphone como o maior foco de ataque e o crescente números de usuários deste aparelho como um dos principais fatores para o aumento no número de crimes cibernéticos, chegando-se a "236 milhões de aparelhos no Brasil, ou 113,52 para cada 100 habitantes". (UOL, 2018)

Entretanto, seria a popularidade crescente dos celulares a real causa do grande número de cibercrimes bem sucedidos? Para Silva e Stein (2007) existem poucas pesquisas sobre o que leva aos comportamentos inadequados do fator humano, ou seja, o usuário, mas este é o responsável pela maior quantidade de erros e falhas de segurança e entendê-lo é determinante para evitar incidentes.

Ainda mencionando a matéria da UOL, o entrevistado André Miceli, professor e coordenador do MBA em Marketing Digital da Fundação Getúlio Vargas em todo o Brasil, explica que algumas técnicas para navegar com mais segurança na internet envolvem alterar a senha com frequência, ter senhas diferentes para acessar cada site, evitar o uso de redes públicas, não instalar softwares de procedência desconhecida e ter cuidado com e-mails de desconhecidos (UOL, 2018).

É importante tratar sobre este tema constantemente, pois cada vez mais os dispositivos estarão passíveis de sofrer ataques e estes mesmos aparelhos farão parte das nossas vidas. Enquanto a tecnologia caminha para oferecer aos usuários um maior controle sobre seus dispositivos, a falta de práticas de segurança pode ser danosa para os indivíduos (UOL, 2018).

Percebe-se que a tecnologia (excluindo-se o seu uso malicioso por hackers e crackers) não é realmente o fator decisivo que proporciona um cyber ataque bem sucedido, mas sim a desinformação dos usuários quanto aos perigos do mundo virtual e as atitudes de prevenção e proteção contra os ataques.

O usuário constante de ambientes online também deve estar preparado para lidar com a veiculação de notícias falsas. Balem (2017) aponta que cada vez mais brasileiros residentes

ISSN: 2358-8829

em grandes centros urbanos têm utilizado as redes sociais como fonte de notícias, mas muitas vezes, a leitura é rasa e se resume à manchete, sem que o leitor ao menos verifique o conteúdo e sua veracidade.

As fake news se apresentam muitas vezes com manchetes sensacionalistas, atingindo fortemente a emotividade do leitor.

> Embora o acesso universal à informação e à opinião, graças à Internet, devam ser bem-vindos, também fizeram com que os meios de comunicação passassem não apenas a informar e opinar, mas com que qualquer pessoa possa dar publicidade a todo tipo de afirmações, verdadeiras ou não. Daí surgem as fake news – notícias na forma, mas não no conteúdo. (Pina, 2017, p. 41)

Balem (2017) aponta que a expressão fake news ganhou destaque graças a uma eleição realizada anualmente pelo Dicionário Oxford para definir a palavra de maior destaque na língua inglesa, revelando-se que, em 2017, o termo foi citado milhões de vezes e em três idiomas diferentes. Segundo Pina (2017), fake news não se trata, por si só, de um conceito novo, o problema se encontra na divulgação massificada e no compartilhamento indiscriminado de informações difamatórias e prejudiciais a determinadas pessoas.

> Declarações ambíguas, enviesadas, ou derivadas de enganos são na prática equiparadas a mentiras inventadas pelos mais diversos motivos: ganhar dinheiro dos anunciantes, alcançar resultados eleitorais específicos, formar e influenciar correntes de opinião, induzir metas de politicas públicas, reforçar vínculos de identificação coletiva e, até mesmo, denegrir a imagem de uma coletividade ou segmento social, étnico ou racial. (Balem, 2017, p. 3)

A citação complementa a reflexão de Pina (2017) que afirma confundir-se muitas vezes a liberdade de expressão e o discurso de ódio, ou seja, a disseminação de ideias preconceituosas. Para a autora, no entanto, aumentar a quantidade de regulamentações para a comunicação na rede de computadores implicaria em limitar a liberdade individual, gerando um clima de censura. Balem (2017) afirma que o método mais efetivo contra as fake news deve ser a educação do usuário para avaliar e processar a veracidade das informações que lê.

> Com efeito, a cada oportunidade em que nos deparamos com alguma notícia polêmica, há que se por em prática o juízo crítico com o fito de avaliar, mesmo que superficialmente, a credibilidade de tal informação. O exercício pleno da liberdade de expressão, capaz de contribuir positivamente na construção da democracia, passa pela responsabilidade individual de cada na disseminação das “fake news”. (Balem, 2017, p. 5)

Percebe-se que existe uma grande procura pelas inovações tecnológicas. Porém não há no país uma cultura que prepare o consumidor/cidadão para utilizar essas tecnologias. Não é costume discutir sobre os riscos ao usar um aparelho conectado em rede. A fim de verificar esta situação, os autores deste artigo disponibilizaram nas redes sociais um questionário

ISSN: 2358-8829

criado por meio do Google Forms. O público-alvo desta pesquisa foi qualquer pessoa usuária da internet, portanto, não há outras delimitações.

Ao analisar o questionário, observa-se que mesmo em um ambiente escolar o tema segurança da informação muitas vezes é esquecido totalmente, inclusive em escolas estruturadas com equipamentos computacionais concedidos por programas governamentais.

O questionário mostra que 69,8% dos respondentes nunca tiveram aulas ou conhecimentos sobre segurança da informação, 9,3% já discutiram pontualmente esse tema em sala e 39,5% não sabem o que estuda a segurança da informação. Dos participantes, 60,5% já foram ou conhecem vítimas de crimes virtuais. Quanto às fake news, 9,6% sabem que elas existem, porém 43,3% não sabem como proceder para identificar uma notícia falsa.

Os dados observados no questionário demonstram uma necessidade real de se discutir sobre segurança da informação na escola, concordando com os 97,7% dos respondentes que acreditam que essa discussão deve estar presente na escola para que a população possa estar mais preparada para proteger-se contra os ataques virtuais e saber identificar fake news.

Sobre ensinar com a tecnologia e ensinar acerca da tecnologia

Kensky (2003) advoga que cada época é uma "era da tecnologia", todas com um tipo diferente de tecnologia e que essas novas tecnologias sempre modificaram a sociedade, alterando não somente os padrões comportamentais de interação social, mas também outros setores como novas formas de golpes financeiros e novas formas de crimes.

O uso mal intencionado das TIC's, e em específico das ferramentas computacionais, fez com que essas novas roupagens criminais tomassem novas características e maior poder de alcance, fazendo-se necessário o estudo de segurança da informação para que a população mantenha-se preparada para ataques mediados pelas TIC's.

No Brasil, o Programa Nacional de Informática na Educação (Proinfo), criado em 1997, trouxe às escolas públicas estrutura para formação de salas de informática, equipadas com computadores e internet para servir a comunidade escolar. Tal programa torna visível que a sociedade brasileira passou por um processo de inclusão digital, porém para De Almeida et al (2020, s/p),

> Seu documento de Diretrizes (BRASIL/MEC, 1997) apresenta uma variedade de possibilidades para a sala de informática, tais como, até dois períodos de aula na sala por semana, cursos na área da informática para a comunidade. [...] O documento de Diretrizes do PROINFO (BRASIL/MEC, 1997) advoga em favor de uma revolução na escola e no processo de ensino-aprendizagem. Contudo, mais de 17 anos após sua

ISSN: 2358-8829

> construção o que encontramos nas escolas públicas são salas de informática sucateadas, pouco usadas, sem profissionais com formação para assumir sua responsabilidade e professores que, muitas vezes, não estão envolvidos com as evoluções tecnológicas e não tem apoio pedagógico para planejamento e realização de atividades com o uso do computador.

A inatividade da sala de informática na escola, além de limitar o aluno quanto ao uso das tecnologias computacionais para sua subordinação, deixa a sociedade à mercê da ignorância quanto aos ataques cibernéticos que ocorrem de inúmeras maneiras, sem conhecimento para a prevenção e cuidados após exposição ao risco.

Esses riscos podem, como exposto anteriormente, tomar a forma de fake news ou ataques de malwares. O ensino de segurança em informação, portanto, permite que a sociedade esteja mais preparada para lidar com essas situações e, assim, diminuam as estatísticas para crimes virtuais. Entretanto ao retomarmos Kenski (2003. p. 5) percebemos que

> As tecnologias têm suas especificidades. É preciso saber aliar os objetivos de ensino com os suportes tecnológicos que melhor atendam a esses objetivos. [...] Não é possível pensar que o simples conhecimento da maneira de uso do suporte (ligar a televisão ou o vídeo ou saber usar o computador e navegar na Internet) já qualificam o professor para a utilização desses suportes de forma pedagogicamente eficiente em atividades educacionais.

Assim, é preciso um profissional qualificado para lecionar as disciplinas da área da informática. E quem seria esse profissional? O Projeto Pedagógico de Curso (BRASIL/IFRN, 2012, p. 12) da Licenciatura em Informática do Campus Natal Zona Norte do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (LI-IFRN/ZN) apresenta o licenciado em informática como um profissional que atribui em sua atuação

> Desenvolvimento de atividades de docência e pesquisa em computação e educação.
>
> [...]
>
> Planejamento e execução de currículos e programas de capacitação profissional, em organizações diversas, que empreguem a Informática como suporte e apoio educativo.
>
> Elaboração e participação em projetos na área de Educação a Distância ou atividades educativas com a mediação de Tecnologias de Informação e Comunicação.
>
> Desenvolvimento de materiais educacionais através do emprego da Informática.
>
> [...]

Dessa maneira, o licenciado em informática tem em sua formação habilidades para trabalhar conteúdos da informática em diferentes níveis de ensino, usando de metodologias

ISSN: 2358-8829

diversificadas e adaptadas a realidade em que exerce sua função. Ainda pode tratar os conteúdos de forma que quebre os limites do ensino de informática, assim, podendo trabalhar de maneira interdisciplinar e integrando os conteúdos com problemáticas sociais, como as discussões sobre segurança da informação.

ENSINANDO CONCEITOS DE SEGURANÇA DA INFORMAÇÃO NOS TELECENTROS

Com tantas influências da informática na sociedade, o mundo do trabalho não é diferente. As empresas buscam a tecnologia para poupar gastos e, principalmente, otimizar seus serviços: softwares de mensagens instantâneas que trabalham online, por exemplo, são usados tanto para comunicação interna quanto para com os clientes. O próprio computador invadiu esse ambiente e não encontramos mais uma empresa que não tenha um computador, ao contrário, agora temos empresas que funcionam exclusivamente na internet.

Ao que podemos perceber, em nosso modelo social, nos é exigido o mínimo de conhecimento de informática não somente para socialização, como também para o mundo do emprego. Os chamados “analfabetos digitais” acabam por perder muitas oportunidades pela falta de algum conhecimento na área, passando a sentir-se obsoletos e desestimulados como profissionais.

Visando a importância que a informática tem no meio do trabalho, a Secretaria Municipal de Trabalho e Assistência Social de Natal (SEMTAS) disponibiliza cursos de formação e iniciação às ferramentas da informática para as comunidades da cidade do Natal por meio dos Telecentros espalhados pela capital.

Criados para possibilitar o acesso ao computador e internet a todos, os Telecentros também adquiriram a função de inclusão digital oferecendo cursos de informática básica para essas comunidades, incentivando e instigando os participantes a tomarem propriedade das ferramentas da informática. Os cursos geralmente contam com 20 alunos por turma e são oferecidos aos cidadãos da cidade, incluindo a terceira idade, tornando seu caráter social ainda maior.

Para manter a qualidade dos cursos foi aberto, pela SEMTAS em diário oficial, edital em 2016 para suprir a demanda de professores para os telecentros, assim, a chamada pública 01/2016 convocou Licenciandos da área de Informática para atuarem como

ISSN: 2358-8829

Professores/Instrutores de caráter eventual para cursos com carga horária de 100 horas. Dessa seleção, os licenciandos foram convocados a participar de oficinas pedagógicas de formação continuada, socialização dos selecionados e equipe pedagógica responsável e reconhecimento de instrumentos. Durante as oficinas a proposta dos telecentros foi apresentada, assim como, a realidade a ser enfrentada e equipamentos disponíveis para cada localidade.

Os cursos oferecidos pelos Telecentros são cursos de iniciação à informática que, em seus conteúdos, ensinam manipulação de arquivos (criar pastas, copiar, colar, etc), editores de texto (criar documento de texto, formatação de texto e página, etc) e navegação na internet (pesquisa em sites, busca na internet, redes sociais, download, etc), entretanto os instrutores têm autonomia para acrescentar conteúdos extras no decorrer do curso, caso possa atender uma demanda dos alunos.

Em turmas que os autores deste trabalho ministraram aulas, lhes foi solicitado pelos alunos discussões acerca de segurança da informação. Segundo os estudantes, existia uma necessidade de aprender sobre como se proteger de vírus, visto que sofriam constantemente com ataques do tipo, sendo uma explicação dada pelos técnicos onde levavam suas máquinas para manutenção.

Por ter uma carga horária de curso bem limitada aos conteúdos programáticos, os instrutores não ofereceram prática em softwares antivírus, já que demandaria muito tempo e mesmo com as práticas, os programas antivírus tornam-se obsoletos facilmente e explicar essa dinâmica poderia tomar uma parte considerável do curso. Assim, os instrutores focaram em ensinar técnicas básicas de reconhecimento de arquivos, programas, páginas da internet e links maliciosos levando em consideração o fator humano por trás das falhas de segurança. Essa discussão estendeu-se para o tema das Fake News quando foram trabalhadas as redes sociais.

O primeiro conceito discutido com os alunos foi Malwares, abordou-se o que são os vírus de computadores e as classificações dos programas maliciosos. Assim, os alunos puderam compreender como trabalham os vírus, os spywares, os ransomware e os trojans e perceber as intenções de quem os cria.

Com as explicações sobre o comportamento desses tipos de malwares, foi mais fácil para as turmas entenderem alguns processos de prevenção. Entre os métodos de prevenção destacou-se o descarte de arquivos e links suspeitos, como anúncios que prometem “milagres” ou dinheiro fácil, evitar sites pouco conhecidos e destinados ao público adulto ou com muitos

ISSN: 2358-8829

anúncios, assim como a criação de senhas mais seguras para suas contas. Os instrutores usaram, com auxílio de imagens, exemplos reais para demonstrar como pode ser comum uma exposição aos ataques virtuais. Assim, os alunos puderam desenvolver meios de identificar ações que os colocariam em risco.

Em seguida, iniciou-se discussões sobre engenharia social, pois como advoga Fonseca (2009, p. 2)

> Um dos grandes problemas, se não o maior, com relação a Segurança da Informação do ponto de vista humano é uma técnica chamada de Engenharia Social, pois através dela o engenheiro social utiliza diversos métodos para obter acesso as informações confidenciais das empresas.

Seguindo esse preceito, as discussões buscaram fazer com que os alunos identificassem a engenharia social como o conhecimento do comportamento humano sendo utilizado para fazer pessoas atuarem segundo o desejo do engenheiro, sendo diferente das técnicas de controle da mente e hipnose, usada também para todos os tipos de fraudes e invasão de sistemas eletrônicos (Peixoto, 2006).

Assim, os conceitos trazidos por Peixoto (2006) foram abordados durante os encontros, tais como: o uso do telefone para passar-se por outra pessoa; por internet com sites que disponibilizam dados do usuário, ou perfis públicos; e-mail's e mensagens suspeitos; a interação com engenheiro social (pessoalmente, chat, etc) possibilitando descobrir informações pessoais; mergulho no lixo (dumpster diving); e surfar sobre os ombros.

Ao iniciarem os conteúdos sobre redes sociais, os instrutores retomaram as discussões sobre segurança da informação, dessa vez, focando nas fake news. Primeiramente, os alunos foram questionados sobre o que seria uma fake news, ao abordar a tradução literal do termo, os alunos puderam conceituar o tema muito facilmente. Dessa maneira discutiu-se o porquê existirem essas notícias falsas, trazendo em sala uma temática sobre o poder manipulador das mídias. Os estudantes trouxeram para o debate suas próprias experiências vivenciadas em redes sociais como o Facebook e o Whatsapp, que abordavam assuntos como política e difamação. Os alunos perceberam que é necessário pesquisar sobre as notícias vindas de fontes como as redes sociais ou desconhecidas antes de serem tomadas como verdadeiras.

Segundo os estudantes, depois das discussões promovidas em sala, eles tornaram-se mais confiantes em acessar a internet, pois agora teriam maior "suporte para saber a diferença entre links ou páginas com vírus" (Alunos do Telecentro).

ISSN: 2358-8829

CONSIDERAÇÕES FINAIS

As inovações tecnológicas influenciam profundamente a sociedade e trazem consigo uma nova cultura, o que exige uma nova postura dos indivíduos. Na era contemporânea há uma grande ênfase no valor da informação, portanto, é necessário que os usuários conheçam e pratiquem métodos de segurança virtual.

Sem conhecimento, uma mudança nos hábitos dos usuários das ferramentas computacionais não especializados na área, que representam uma grande massa desses usuários, não acontecerá e cada vez mais os dados sobre crimes virtuais crescerão. O simples fato de descobrir como se comportam os malwares e os engenheiros sociais pode dar aos que utilizam o computador uma maior segurança em seu acesso às ferramentas e diminuir as ocorrências nas assistências técnicas devido a máquinas infectadas.

Com as TICs, o cidadão comum se torna também produtor de notícias, não apenas consumidor. É possível compartilhar suas opiniões, principalmente nas redes sociais, o que demanda maturidade para interagir com opiniões divergentes, além da necessidade de checar as fontes de notícias veiculadas nesses meios. Os professores licenciados em informática conseguem, devido a sua formação, se manter atualizados sobre as ameaças virtuais e transmitir esses saberes em sua prática.

A atuação nos telecentros evidenciou a crescente preocupação dos alunos com a segurança no meio digital. Contudo, isso deve ser constantemente desenvolvido por meio de ações educativas para incentivar a autocrítica, tendo em vista que o fator humano está mais suscetível a cometer falhas.

Por fim, percebe-se que a cultura com as TIC's, por vezes, ignora o (des)conhecimento dos usuários quanto ao lado negativo das tecnologias computacionais, tornando-os muito mais vulneráveis a ataques virtuais, assim, sendo necessárias atuações educativas que discutam sobre segurança da informação. Nesse sentido, a escola torna-se um ambiente propício para essas discussões, visto que, além de um ambiente de ensino, existem políticas públicas que as equipam com as ferramentas computacionais para serem trabalhadas com os alunos.

REFERÊNCIAS

BALEM, I. F.. O Impacto das Fakenews e o Fomento dos Discursos de Ódio na Sociedade em

ISSN: 2358-8829

Rede: A Contribuição da Liberdade de Expressão na Consolidação Democrática. 2017. **Anais do 4º Congresso Internacional de Direito e Contemporaneidade**: mídias e direitos da sociedade em rede.

BRASIL, Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte. **Projeto Pedagógico do Curso Superior de Licenciatura em Informática na modalidade presencial**. 2012. Disponível em <http://portal.ifrn.edu.br:8888/ensino/cursos/cursos-de-graduacao/licenciatura/licenciatura-plena-em-informatica/at_download/coursePlan> Acessado em: 30 de Junho de 2018.

CABRAL, I.. **Segurança da Informação em Bibliotecas universitárias federais**: um levantamento sobre ferramentas e técnicas utilizadas. 2015. 80 f. TCC (Graduação) - Curso de Biblioteconomia, Centro de Ciências da Educação, Universidade Federal de Santa Catarina, Florianópolis, 2015.

DE ALMEIDA, A. C. O. et al. Observando a Sala de Informática: O Licenciado em Informática e Novas Perspectivas com o Scratch como Objeto de Aprendizagem. In: Congresso sobre Tecnologias na Educação (CTRL+E), 5., 2020, Evento Online. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2020. p. 500-509.

FONSECA, P. F. **Gestão de Segurança da Informação**: o fator humano. 2009. 23 f. Monografia (Especialização) - Curso de Pós Graduação em Redes e Segurança de Computadores, Pontifícia Universidade Católica do Paraná, Curitiba, 2009.

KENSKI, V. M.. O que são tecnologias? Como convivemos com as tecnologias? In: **Tecnologias de ensino presencial e a distância**. Campinas, SP: Papirus, 2003.

PEIXOTO, M. C. P. P.. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

PINA, C.. Amigos da Verdade: Os limites jurídicos das fake news. **UNO**, São Paulo, n. 27, p. 41-43, mar. 2017.

QUEIROZ, D. G. C.; MOURA, A. M. M.. Ciência da Informação: história, conceitos e características. **Em Questão**, Porto Alegre, v. 21, n. 3, p. 25-42, ago/dez. 2015.

SILVA, D. R. P.; STEIN, L. M.. Segurança da informação: uma reflexão sobre o componente humano. **Ciências & Cognição**, Rio de Janeiro, v. 10, p. 46-53, mar. 2007.

SOUZA, J. **Saiba quais são os principais métodos de pesquisa**. Doity. 2022. Disponível em: <https://doity.com.br/blog/metodos-de-pesquisa/>. Acesso em: 15 de novembro de 2023.

UOL. **Brasil é o segundo país no mundo com maior número de crimes cibernéticos**. 2018. Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm>. Acesso em: 5 de Novembro de 2023.

VARELLA, G.. **Há laboratórios de informática em 81% das escolas públicas, mas somente 59% são usados**. Época. 2017. Disponível em:

ISSN: 2358-8829

<https://epoca.globo.com/educacao/noticia/2017/08/ha-laboratorios-de-informatica-em-81-das-escolas-publicas-mas-somente-59-sao-usados.html>. Acesso em: 5 de Novembro de 2023.