ISBN: 9786588884447

SEGURANÇA COMPUTACIONAL NO ENSINO-APRENDIZAGEM

ADEMIR GOULART; MILENA CRISTINA FRANÇA; WALESKA RAITZ

RESUMO

Com o grande aumento de dispositivos conectados à Internet, a exposição digital das gerações mais jovens tem aumentado, alertando para a necessidade de intensificar a educação sobre a segurança da informação nas escolas. No entanto, existem alguns obstáculos ao ensino e a aprendizagem em segurança da informação, tais como: A abrangência do tema e seus vários campos; Novas tecnologias possibilitam técnicas de ataques mais sofisticadas e os conteúdos educacionais não são observados nos livros do ensino de educação. Este artigo tem como objetivo compreender a importância da segurança da informação para alunos do ensino médio, bem como, discutir o estado da arte nos esforços de propor técnicas e ferramentas para aplicação prática de atividades de ensino-aprendizagem em segurança computacional. Para a produção desta pesquisa foi realizado uma revisão de literatura sobre o estado da arte no que se refere a educação da segurança computacional, nomeadamente, segurança cibernética para alunos do ensino médio. Como resultado, foi possível identificar que vários trabalhos apresentam a preocupação com questões de segurança computacional em específico a educação em segurança cibernética. A apresentação dos estudos revela temas que precisam ser introduzidos nos programas educacionais do ensino médio, tais como: cyberbullying, spam, phishing, vírus, senhas fortes, criptografia e segurança de dados, transferência segura de dados, proteção de dados pessoais, aliciamento sexual, contas falsas em redes sociais, e privacidade cibernética. Também, algumas escolas já incluíram cursos de segurança cibernética em seu currículo, enquanto outras não. O estudo enfatizou a importância de estratégias eficazes para incentivar os estudantes a se envolver com a segurança cibernética. Apesar da necessidade evidente do desenvolvimento de cursos interativos bem como jogos para a educação em segurança cibernética, se requer uma avaliação específica de tais ferramentas pois nem todos os jogos disponíveis no mercado são concebidos com objetivos educacionais e públicos-alvo muito claros.

Palavras-chave: Cibersegurança; Educação; Ensino Médio; Currículo; Jogos.

1 INTRODUÇÃO

Com o grande aumento de dispositivos conectados à Internet, a exposição digital das gerações mais jovens tem aumentado, alertando para a necessidade de intensificar a educação sobre a segurança da informação nas escolas (Antunes et.al, 2021).

No entanto, existem alguns obstáculos ao ensino e a aprendizagem em segurança da informação. A segurança da informação abrange vários campos, tais como: segurança computacional, segurança de rede, segurança de banco de dados, criptografia, gerenciamento de segurança, computação forense e ética computacional. E cada campo, requer diversos conhecimentos e habilidades. Por exemplo, a ética informática educa os usuários de computador para evitar cometer crimes de informática e ajudar a proteger os sistemas informáticos. No entanto, na ética computacional existem diferentes visões filosóficas envolvidas. Desse modo, ensinar segurança da informação com eficácia para jovens passa a ser um desafio.

DOI: 10.51189/ensipex2024/30421

ISBN: 9786588884447

Segundo Diana et.al, 2022, dados da União Internacional de Comunicação (UIT), mostram que os adolescentes são o grupo de pessoas que mais usam a Internet globalmente, o que corresponde a mais de 70%. E normalmente os adolescentes estão entre os estudantes de ensino médio.

Com o surgimento de novas tecnologias, técnicas de ataques mais sofisticadas são utilizadas pelos hackers, com o objetivo de obtenção de lucro através de suas vítimas. (Jung; Park, 2021).

Os conteúdos educacionais de segurança da informação se limitam apenas a proteção da informação pessoal e as medidas preventivas da segurança computacional não são observadas nos livros do ensino de educação básica (Kim, 2020).

Também, o campo de segurança da informação inclui diversos conteúdos interdisciplinares e devido a essa natureza diversificada, faz-se necessário a adoção de técnicas e ferramentas para o ensino-aprendizagem de segurança computacional na educação de ensino médio.

O presente estudo está organizado da seguinte forma: Na seção 2 apresenta a metodologia de pesquisa, bem como trabalhos correlatos relacionados a aspectos de segurança computacional em específico a segurança cibernética. A seção 3 aborda os resultados e discussões, onde são abordadas soluções possíveis para aplicação em atividades de ensino-aprendizagem no ensino médio. A seção 4 são apresentadas as conclusões e sugestões de trabalhos futuros.

Este artigo tem como objetivo compreender a importância da segurança da informação para alunos do ensino médio, bem como, discutir o estado da arte nos esforços de propor técnicas e ferramentas para aplicação prática de atividades de ensino-aprendizagem em segurança computacional.

2 MATERIAIS E MÉTODOS

O procedimento metodológico adotado é a pesquisa bibliográfica e o método utilizado é a revisão sistemática de literatura. (Chung; Burns; Kim, 2006).

Os estudos de revisão e/ou pesquisas relacionadas foram encontrados em diferentes bases de dados, incluindo Springer, Elsevier, Science Direct, IEEE dentre outras, com os seguintes termos de pesquisa: Computer security; Computer security basic education; Computer segurity high scholl, Computer security teaching-learning; com data de publicação de 2022 e 2023. O número total de artigos por termos de pesquisas é apresentado conforme a tabela 1 abaixo:

Tabela 1. Palavras-chave de pesquisa.

Palavra-chave	**Total**
“computer security”	9310
"computer security" basic education	263
“computer security” high school”	123
"computer security" teaching-learning	5

Com os resultados de análise da tabela 1, é possível observar que apenas 2,8% do número de estudos de revisão/pesquisas sobre segurança computacional estão relacionados à educação básica, e que desses, 1,8% estão relacionados ao ensino médio, e 0,05% discutem o ensino-aprendizagem, indicando a carência de estudos de segurança computacional no ensino-aprendizagem. Os artigos relevantes são descritos a seguir:

DOI: 10.51189/ensipex2024/30421

ISBN: 9786588884447

2.1. Exploring IoT Vulnerabilities in a Comprehensive Remote Cybersecurity Laboratory

Em 2022, Delgado, et.al., propõem o desenvolvimento de um laboratório online remoto, permitindo aos alunos adquirir experiência prática na identificação e mitigação de ameaças à segurança cibernética num contexto de IoT (Internet of Things). Este ambiente virtual simula ecossistemas reais de IoT, permitindo que os alunos interajam com dispositivos e protocolos reais enquanto praticam diversas técnicas de segurança. O laboratório IoT consiste em três placas Arduino interconectadas. Cada placa é equipada com vários sensores e atuadores, para uma representação realista. Como um servidor Web, um Raspberry PI 3 é conectado às 3 placas de Arduino. Uma interface de software foi criada para fins educacionais para os alunos interagirem com as placas. Os resultados mostraram o laboratório remoto não só aborda os desafios atuais na educação em segurança cibernética da IoT, mas também, oferece uma estrutura para preparar profissionais de segurança cibernética para combater ameaças futuras.

2.2. Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity.

Em 2022, Jerman e Jerman, propõem levantar através de questionários e entrevistas o nível de conhecimentos e competências em cibersegurança dos estudantes europeus do ensino secundário, recolhendo dados dos alunos, seus professores e pais. A pesquisa revelou os temas necessários da área de segurança cibernética, tais como: cyberbullying, spam, phishing, vírus, senhas fortes, criptografia e segurança de dados, transferência segura de dados, proteção de dados pessoais, aliciamento sexual, contas falsas em redes sociais, e privacidade cibernética que precisam ser introduzidos nos programas educacionais do ensino médio e metodologias de ensino mais adequadas, como vídeos e jogos sérios. Uma seleção de treze jogos sérios como relacionados à segurança cibernética foi avaliada e apresentada a uma turma de alunos do ensino médio. O estudo mostrou que o processo de avaliação que teve como objetivo encontrar jogos que pudessem ser aplicados no contexto do ensino médio, resultou em um conjunto menor de três jogos: Targeted Attack,, Permission Impossible, e Keep Tradition Secure. Como resultado, existe um grande interesse em segurança cibernética entre professores, pais e alunos, mas existe uma lacuna entre a educação e a comunidade de especialistas em segurança cibernética, e o público do ensino médio é de alguma forma negligenciado. Também, os participantes concordam com a necessidade de introdução de cursos interativos na educação, com o apoio de jogos, tais como similares a quiz e jogos de aventuras com temas relevantes de segurança cibernética.

2.3. Cybersecurity Issues among High School Students: A Thematic Review

Em 2023, Diana, et.al. enfatiza elementos que incentivam os estudantes de ensino médio a incorporar a segurança cibernética em seu cotidiano, principalmente no uso da internet. O estudo utilizou uma revisão bibliográfica de literatura nas bases de dados Scopus e Science Direct. Como resultado, a partir das 27 publicações de pesquisas examinadas, foram identificados quatro elementos: elemento demográfico, elemento psicológico, elemento familiar e elemento social. Também, os dois termos mais utilizados nos artigos foram bullying e cyberbullying.

Este artigo de revisão destaca que aspectos psicológicos raramente são abordados na educação em cibersegurança, deixando uma lacuna em como aumentar a sensibilização dos alunos para a cibersegurança. No que se refere ao elemento demográfico, faltam estudos para discutir como um grupo demográfico específico influencia os alunos a praticarem segurança

DOI: 10.51189/ensipex2024/30421

ISBN: 9786588884447

cibernética. Além disso, a incapacidade de discutir questões familiares tem dificultado os esforços para resolver problemas de ataques cibernéticos entre estudantes do ensino secundário e aumentado problemas psicológicos. Além disso, indivíduos ou grupos podem ser afetados por aspectos sociais que também podem diferir entre comunidades. O uso problemático da internet também faz parte do elemento social que pode aumentar o envolvimento dos alunos com os problemas cibernéticos. O objetivo é resolver ameaças de ataques cibernéticas e melhorar a qualidade de vida das pessoas.

3 RESULTADOS E DISCUSSÃO

Em comparação com os artigos abordados nesta *survey*, foi possível identificar que vários trabalhos apresentam a preocupação com questões de segurança computacional em específico a educação em segurança cibernética. Foram realizadas pesquisas para identificar os elementos que incentivam os estudantes de ensino médio a incorporar a segurança cibernética em seu cotidiano.

Além disso, são apresentadas metodologias e ferramentas no intuito de preparar profissionais capazes de resolver ameaças de ataques cibernéticos.

Com a apresentação dos estudos que revelam temas que precisam ser introduzidos nos programas educacionais do ensino médio, conforme pode ser observado na figura 1, foram propostos jogos do tipo Quiz no intuito de aumentar o interesse dos estudantes em segurança cibernética.

Figura 1. Temas relevantes da área de segurança cibernética.

Conforme visto na figura 1, um dos ataques cibernéticos mais expressivos entre os jovens é o Cyberbullying.

Referente aos artigos pesquisados, na proposta do laboratório online remoto por Delgado, et.al. (2023), foi constatado que o acesso ao meio é a vulnerabilidade mais comum para redes com e sem fio. Com isso, envolve ameaças de colisão, ataques de negação de serviço (DoS) etc. Para minimizar isso, os autores sugerem realizar um monitoramento continuo para detecção de anomalias. Também, a pesquisa proposta por (Jerman; Jerman, 2023), forneceu observações gerais sobre a situação da segurança cibernética não somente no nível de educação cibernética, mas em diferentes institutos. Algumas escolas já incluíram cursos em seu currículo, enquanto outras não. No estudo de Diana, et.al. (2023), ao analisar os artigos referentes ao elemento demográfico a discussão é mínima carecendo de argumentos para relacionar com a segurança cibernética.

DOI: 10.51189/ensipex2024/30421

ISBN: 9786588884447

4 CONCLUSÃO

Este artigo de revisão bibliográfica destaca a carência de estudos recentes em segurança computacional no ensino-aprendizagem para estudantes de ensino médio, considerando que os adolescentes são o grupo de pessoas que mais usam a Internet globalmente, e que por isso, estão expostas a ataques cibernéticos. O estudo também enfatizou a importância de estratégias eficazes para incentivar os estudantes a se envolver com a segurança cibernética. Apesar da necessidade evidente do desenvolvimento de cursos interativos bem como jogos para a educação em segurança cibernética, se requer uma avaliação específica de tais ferramentas pois nem todos os jogos disponíveis no mercado são concebidos com objetivos educacionais e públicos-alvo muito claros.

REFERÊNCIAS

ANTUNES, Mário; SILVA, Carina; MARQUES, Frederico. An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context. **Applied Sciences**, v. 11, n. 23, p. 11269, 2021.

KIM, Choungbae. An Analysis of Information Security Curriculum in Elementary School practical arts, Secondary School Informatics Teaching and Suggestions for Improvement. **Journal of the Korea Society of Computer and Information**, v. 25, n. 10, p. 69-75, 2020.

CHUNG, Kevin C.; BURNS, Patricia B.; KIM, H. Myra. A practical guide to meta-analysis. **The Journal of hand surgery**, v. 31, n. 10, p. 1671-1678, 2006.

DELGADO, Ismael et al. Exploring IoT Vulnerabilities in a Comprehensive Remote Cybersecurity Laboratory. **Sensors**, v. 23, n. 22, p. 9279, 2023.

DIANA, Intan; ISMAIL, Ismi Arif; ZAIRUL, Mohd. Cyber Risk among High School Students: A Thematic Review. **Malaysian Journal of Social Sciences and Humanities (MJSSH)**, v. 8, n. 4, p. e002251-e002251, 2023.

JERMAN BLAŽIČ, Borka; JERMAN BLAŽIČ, Andrej. Cybersecurity skills among European high-school students: A new approach in the design of sustainable educational development in cybersecurity. **Sustainability**, v. 14, n. 8, p. 4763, 2022.

JUNG, Yujin; PARK, Namje. "Design of Unplugged Learning Tools for Cyber Attack and Defence Hacking Principle," **The Journal of Korean Institute of Information Technology**, vol. 19, no. 5, pp. 111-119, 2021.

DOI: 10.51189/ensipex2024/30421