INTERNET SEGURA PARA JUVENTUDES VULNERÁVEIS: EDUCAÇÃO DIGITAL COMO FERRAMENTA DE CIDADANIA

SAFE INTERNET FOR VULNERABLE YOUTH: DIGITAL EDUCATION AS A TOOL FOR CITIZENSHIP

Helber Claudio Alves Lima[i]
Bernardo Gomes Olive[ii]
Gabriel Caetano Soares[iii]
Luis Henrick Oliveira da Silva[iv]
Humberto de Sousa Megda[v]

RESUMO

Esse trabalho foi desenvolvido para promover a conscientização sobre segurança digital entre jovens em situação de vulnerabilidade social, especialmente aqueles em cumprimento de medidas socioeducativas. A iniciativa surgiu da parceria entre o Grupo de Extensão, o SENAI e a subcomissão da CMDCA. A pesquisa investigou as principais ameaças cibernéticas enfrentadas por esses jovens e como oficinas educativas podem contribuir para uma navegação mais segura. Utilizando uma abordagem qualitativa, foram realizadas oficinas práticas que abordaram temas como senhas seguras, verificação em duas etapas, desinformação e atualização de dispositivos. Os resultados indicaram desconhecimento inicial sobre segurança digital, mas também mostraram alto engajamento e mudanças concretas de comportamento ao longo das atividades. A oficina sobre fake news teve destaque pela participação ativa dos jovens. Conclui-se que a metodologia adotada foi eficaz, mesmo sem instrumentos estatísticos formais, e recomenda-se a expansão do projeto para outros contextos, fortalecendo a cidadania digital e os direitos dos jovens.

Palavras-chave: Segurança Digital; Juventude Vulnerável; Educação Socioeducativa

ABSTRACT

This project was developed to raise awareness about digital security among socially vulnerable youth, especially those undergoing socio-educational measures. The initiative emerged from a partnership between the Extension Group, SENAI, and the CMDCA subcommittee. The research investigated the main cyber threats faced by these young people and how educational workshops can contribute to safer online navigation. Using a qualitative approach, practical workshops were conducted covering topics such as strong passwords, two-factor authentication, misinformation, and device updates. The results indicated an initial lack of knowledge about digital security, but also showed high engagement and concrete behavioral changes throughout the activities. The workshop on fake news stood out due to the active participation of the youth. It is concluded that the adopted methodology was effective, even without formal statistical instruments, and the expansion of the project to other social and educational contexts is recommended, strengthening digital citizenship and youth rights.

Keywords: Digital Security; Vulnerable Youth; Socio-educational Education

1. INTRODUÇÃO

A crescente digitalização da sociedade trouxe benefícios significativos, mas também expôs vulnerabilidades, especialmente entre jovens em situação de risco social. Esses jovens, muitas vezes em cumprimento de medidas socioeducativas, acessam a Internet sem orientação adequada, tornando-se alvos de ameaças cibernéticas como golpes, desinformação e exploração digital.

Diante desse cenário, o projeto “Internet Segura” foi desenvolvido pelo Grupo de Extensão em parceria com o SENAI e a subcomissão da CMDCA, com o objetivo de promover educação digital voltada à segurança online. A iniciativa, proposta pela Analista Tânia e apoiada pelo coordenador Fabrício, busca capacitar jovens vulneráveis por meio de oficinas práticas e educativas.

1.1. Problema de pesquisa

Quais são as principais ameaças cibernéticas que afetam jovens em situação de vulnerabilidade, e como práticas educativas podem contribuir para uma navegação mais segura e consciente?

1.2. Objetivo(s)

Geral:

- Promover a conscientização sobre segurança digital entre jovens em situação de vulnerabilidade social.

Específicos:

- Identificar as ameaças digitais mais recorrentes enfrentadas por esse público.
- Traduzir conceitos técnicos em práticas acessíveis e aplicáveis.
- Avaliar o impacto das oficinas educativas na mudança de comportamento digital dos participantes.

1.3. Justificativa

A inclusão digital sem educação sobre segurança expõe jovens a riscos graves. Este projeto busca preencher essa lacuna por meio de oficinas educativas baseadas em frameworks reconhecidos (como o NIST CSF 2.0) e dados nacionais (CERT.br), promovendo cidadania digital e proteção contra ameaças online.

2. REVISÃO DA LITERATURA

A literatura aponta uma evolução das ameaças digitais, desde vírus simples até ataques sofisticados com uso de inteligência artificial. Relatórios como o Verizon DBIR 2024 e o ENISA Threat Landscape destacam o crescimento de ataques por engenharia social, exploração de vulnerabilidades e desinformação.

O NIST CSF 2.0 propõe uma abordagem integrada à segurança digital, incluindo identidade, governança e cadeia de suprimentos. No Brasil, o CERT.br fornece dados sobre incidentes e capacitação, reforçando a necessidade de ações educativas

contextualizadas.

3. METODOLOGIA

A pesquisa adotou uma abordagem qualitativa, com base em oficinas educativas realizadas com jovens em situação de vulnerabilidade. As atividades foram estruturadas em três etapas:

- Diagnóstico inicial informal: observação das práticas digitais dos participantes.
- Oficinas educativas: abordagens práticas sobre segurança digital, com dinâmicas interativas.
- Avaliação qualitativa: coleta de relatos espontâneos, observação de engajamento e mudanças de comportamento.

Não foram utilizados instrumentos estatísticos formais, mas os dados observacionais foram registrados e analisados para identificar padrões e impactos.

1. RESULTADOS ESPERADOS

Os resultados foram obtidos por meio da observação direta durante as oficinas e dos relatos espontâneos dos participantes. Destacam-se alguns pontos importantes:

Inicialmente, observou-se um desconhecimento generalizado entre os jovens sobre práticas básicas de segurança digital, como o uso de senhas fortes e a verificação em duas etapas. No entanto, ao longo das oficinas, houve um alto engajamento, especialmente em atividades práticas como simulações de mensagens falsas e a criação de senhas seguras.

Esse envolvimento contribuiu para mudanças concretas de comportamento. Alguns participantes relataram que passaram a revisar suas configurações de privacidade e a evitar o clique em links suspeitos. Conceitos técnicos mais complexos, como “gestão de vulnerabilidades”, foram adaptados para ações cotidianas, como manter o celular sempre atualizado.

A oficina sobre desinformação, focada em fake news, foi a que gerou maior participação, com intensos debates e exercícios de verificação de fontes, demonstrando o interesse dos jovens pelo tema.

Esses dados qualitativos reforçam as conclusões do projeto e evidenciam o alinhamento com os objetivos propostos, mostrando que a abordagem adotada foi eficaz na promoção da conscientização e da mudança de hábitos digitais.

5. CONCLUSÕES PRELIMINARES

O projeto demonstrou que oficinas educativas são eficazes para promover segurança digital entre jovens vulneráveis. A abordagem prática e contextualizada facilitou a compreensão e aplicação dos conceitos, gerando mudanças perceptíveis de comportamento.

A ausência de instrumentos estatísticos formais foi compensada por dados

observacionais consistentes, que indicam impacto positivo. A metodologia está alinhada aos objetivos e à hipótese, e os resultados sustentam as conclusões.

Recomenda-se a continuidade e expansão do projeto, com possibilidade de aplicação em outros contextos sociais e educacionais, fortalecendo a cidadania digital e os direitos dos jovens.

REFERÊNCIAS

Verizon. (2024). Data Breach Investigations Report (DBIR). Verizon Business. Disponível em: https://www.verizon.com/business/resources/T646/reports/2024-dbir-data-breach-investigations-report.pdf

ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

NIST. (2024). Cybersecurity Framework 2.0. National Institute of Standards and Technology. Disponível em: https://www.nist.gov/cyberframework

CERT.br. (2025). Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. NIC.br. Disponível em: https://www.cert.br/

SOBRE O(S)AUTOR(ES)

[i] **HELBER CLÁUDIO ALVES LIMA**

Graduando em Superior em Tecnologia de Automação Industrial pela Faculdade Senai Antônio de Souza Noschese (2026), formado em Técnico de eletrotécnica pela Escola Técnica Adélia Camargo Correia (2020). Com experiência na área de manutenção industrial em terminais portuários.

[ii] **BERNARDO GOMES OLIVE**

Possui graduação em Técnico de Eletrotécnica pela Instituição Etec Aristoteles Ferreira (2023), cursando atualmente o Tecnólogo de Automação industrial pela Faculdade SENAI de Tecnologia (2025). Tem experiência na área de Elétrica, com ênfase em Manutenção de equipamentos. Eletricista de manutenção na empresa Fm2c responsável pelos setores de elétrica.

iii GABRIEL CAETANO SOARES

Possui graduação em técnico em eletrotécnica, pela escola Grau Técnico (2023. Atualmente cursando Tecnólogo em automação industrial pela faculdade Senai (2025). Tenho experiência na área de manutenção elétrica a 8 meses no porto.

[iv] **LUIS HENRICK OLIVEIRA DA SILVA**

Aluno do Curso Superior em Automação Industrial do Senai de Santos

- **HUMBERTO DE SOUSA MEGDA**

Mestre e Graduado em Engenharia, Pós-graduado em Gestão de Energia e Eficiência Energética, Licenciado em Matemática e Técnico em Desenvolvimento de Sistemas e Eletrônica. Atualmente é Professor de Educação Superior na Faculdade SENAI e Engenheiro de Operação e Medição prestador de serviços da Petrobrás.