Segurança Digital na Educação de Jovens e Adultos: Reflexões e Práticas Pedagógicas

Frank Pinto dos Santos[1], João da Mata Libório Filho[1], Luiz Sérgio de Oliveira Barbosa[1]

[1]Centro de Estudos Superiores de Itacoatiara (CESIT) – Universidade do Estado do Amazonas (UEA) – Itacoatiara – AM – Brasil

{fpds.lic22, jlfilho, lsergio}@uea.edu.br

Abstract. *This study presents research conducted with students from Youth and Adult Education (EJA) in a public school during the Supervised Internship in Computing II, addressing the theme of Identification and Prevention of Digital Scams. The research used a participatory approach and active methodology, providing relevant data. Among the 56 participants, 53.2% know someone who has suffered digital scams, and only 19.6% can recognize malicious links, highlighting the need for pedagogical approaches to digital security.*

Resumo. *Este trabalho apresenta um estudo realizado com alunos da Educação de Jovens e Adultos (EJA) de uma escola pública, durante as práticas do Estágio Supervisionado em Computação II, abordando a temática de Identificação e Prevenção de Golpes Virtuais. A pesquisa utilizou uma abordagem participante e metodologia ativa, trazendo dados relevantes. Dos 56 participantes, 53,2% conhecem alguém que já sofreu golpes digitais e apenas 19,6% conseguem reconhecer links maliciosos, evidenciando a necessidade de abordagens pedagógicas sobre segurança digital.*

1. Objetivos Geral e Específicos

1.1 Objetivo Geral

Desenvolver e avaliar uma estratégia pedagógica para conscientizar alunos da EJA sobre segurança digital, prevenção de golpes e identificação de *fake news*.

1.2 Objetivos Específicos

- Analisar o perfil dos estudantes da EJA em relação ao uso de tecnologias digitais;
- Identificar os principais tipos de golpes digitais que afetam esse público;
- Implementar uma atividade pedagógica que promova reflexão e ações preventivas;
- Avaliar o impacto da metodologia adotada.

2. Público-alvo

A atividade foi aplicada a estudantes da EJA nos anos finais do Ensino Fundamental e no Ensino Médio de uma escola pública em Itacoatiara-AM. O público atendido apresenta uma grande diversidade de faixas etárias e níveis de escolaridade, conforme apresentado na Tabela 1, caracterizando desafios pedagógicos específicos.

Tabela 1. Distribuição dos participantes da pesquisa por faixa etária e nível de escolaridade.

Características	Sujeitos	
	N (56)	%
Faixa etária		
18 - 22	34	60,71
23 - 26	10	17,86
27 – 38	6	10,71
39 - 63	6	10,71
Escolaridade		
9º ano	3	5,36
1º ano EM	10	17,86
2º ano EM	25	44,64
3º ano EM	18	32,14

3. Habilidade Trabalhada

A atividade desenvolveu habilidades previstas nas Normas sobre Computação na Educação Básica, de acordo com a BNCC [Brasil 2022]. As habilidades trabalhadas foram:

- EF04CO08 - Reconhecer a importância de verificar a confiabilidade das fontes de informações obtidas na internet.
- EF05CO08 - Acessar as informações na Internet de forma crítica para distinguir os conteúdos confiáveis dos não confiáveis.
- EM13CO08 - Entender como mudanças na tecnologia afetam a segurança, incluindo novas maneiras de preservar sua privacidade e dados pessoais on-line, reportando suspeitas e buscando ajuda em situações de risco.
- EM13CO14 - Avaliar a confiabilidade das informações encontradas em meio digital, investigando seus modos de construção e considerando a autoria, a estrutura e o propósito da mensagem.

Essas habilidades foram exploradas por meio de atividades práticas e discussões em grupo para desenvolver o letramento digital e a segurança dos alunos na internet.

4. Recursos e Materiais Utilizados

Para a realização da atividade, utilizou-se o laboratório de informática da escola, que possui acesso à internet, além de computadores e dispositivos móveis dos próprios alunos. Foram preparadas apresentações multimídia para abordar a temática de golpes virtuais, acompanhadas de impressos contendo exemplos de *fake news* e sites maliciosos, a fim de proporcionar uma experiência prática de análise crítica. Além disso, questionários diagnósticos foram aplicados para avaliar o nível de conhecimento

prévio dos alunos e, ao final da atividade, utilizou-se um questionário de avaliação para medir o impacto da intervenção pedagógica.

5. Metodologia Detalhada

A pesquisa seguiu os seguintes passos metodológicos, baseando-se em análises sobre o impacto das metodologias ativas na Educação de Jovens e Adultos e pesquisas realizadas em contextos similares [Santos et al. 2024, González 2020, Pereira and França 2023, Fonseca, Liborio Filho and Reis 2025].

5.1 Diagnóstico Inicial

Foi aplicado um questionário para mapear o perfil socioeconômico e os hábitos digitais dos alunos. O questionário abordou acesso à internet, conhecimento sobre golpes virtuais e experiências prévias com *fake news*.

5.2 Desenvolvimento da Atividade

A estratégia pedagógica baseou-se em metodologias ativas, inspirados em diversos estudos [Da Silva and Pereira 2023, Rocha, Da Silva Brandão and Ramos 2023], incluindo:

- **Roda de Conversa:** Discussão sobre golpes digitais e *fake news*, compartilhamento de experiências.
- **Análise de Exemplos:** Avaliação de *prints* de golpes reais e *fake news* para desenvolver senso crítico.
- **Aprendizagem Baseada em Problemas (ABP):** Os alunos acessaram *links* diferentes para identificar elementos suspeitos e discutir sua segurança, conforme registro apresentado na Figura 1.

Figura 1. Registros da realização da atividade ABP com os alunos.

6. Avaliação

A avaliação foi feita por meio de observação participativa [Velloso et al. 2022] e questionário final, verificando:

- Evolução no reconhecimento de golpes virtuais;
- Percepção da importância da segurança digital;
- Impacto da atividade na mudança de comportamento dos alunos.

A Tabela 2 apresenta a percepção dos 56 participantes em relação a golpes virtuais, *fake news* e segurança de dados. Os dados incluem o nível de familiaridade com golpes digitais, experiências diretas ou indiretas com fraudes, identificação de notícias falsas e compreensão sobre proteção de informações pessoais. Observa-se que 17% dos alunos já foram vítimas de golpes virtuais, como fraudes no PIX, redes sociais e compras *online*. Além disso, 53,2% conhecem alguém que enfrentou situações semelhantes, reforçando a vulnerabilidade do grupo.

Quando o tema é *fake news*, 37,5% já as receberam ou compartilharam, sendo a identificação geralmente feita por meio de pesquisas ou consulta a fontes confiáveis. Sobre segurança de dados, metade dos participantes demonstra algum conhecimento, mencionando práticas como proteção de informações pessoais e uso de senhas fortes. Esses dados destacam a necessidade de ações educativas voltadas à segurança digital, fundamentais para formar cidadãos mais conscientes e protegidos no ambiente virtual.

Tabela 2. Conhecimento e experiência dos participantes sobre segurança digital.

Questão	**Sujeitos**	
	N (56)	**%**
Você já ouviu falar sobre golpes virtuais?		
Sim	47	83,9
Não	9	16,1
Se sim, já foi vítima de algum golpe?		
Sim	9	17
Não	44	83
Se não, conhece alguém que já foi?		
Sim	25	53,2
Não	22	46,8
Você já recebeu ou compartilhou notícias falsas?		
Sim	21	37,5
Não	35	62,5
Você sabe o que significa segurança de dados?		
Sim	28	50
Não	28	50

A Tabela 3 apresenta as práticas adotadas pelos 56 participantes para proteger suas informações ao utilizar a internet e redes sociais. Inclui medidas preventivas, como uso de senhas fortes e verificação da origem de sites, além de experiências com problemas de segurança, como invasão de contas ou roubo de dados.

Tabela 3. Hábitos de segurança digital dos participantes.

Questão	**Sujeitos**	
	N (56)	**%**
Quais os cuidados que você costuma tomar ao usar internet ou redes sociais?		
Não compartilha dados	20	35,7
Usa senhas fortes	13	23,2
Outras medidas	23	41, 1
Você sabe o que é um *link* malicioso?		
Sim	11	19,6
Não	45	80,4
Costuma verificar a origem de um site antes de acessar?		
Sim	33	58,9
Não	23	41,1

Já teve algum problema de segurança (como invasão de conta ou roubo de dados)?		
Sim	23	41,1
Não	33	58,9

Constata-se que, em relação aos hábitos de segurança *online*, 58,9% dos alunos verificam a confiabilidade de *links* antes de abri-los, demonstrando preocupação com possíveis ameaças virtuais. Contudo, apenas 19,6% reconhecem *links* maliciosos, evidenciando comportamentos que os tornam vulneráveis a golpes. Além disso, 41,1% relataram verificar a origem dos *sites* antes de acessá-los, o que reflete um conhecimento moderado sobre segurança digital.

Com base nos dados apresentados acima, chegamos à conclusão de que os alunos da EJA possuem um perfil diverso, marcado por desafios socioeconômicos e lacunas em conhecimento tecnológico. Embora demonstrem interesse em segurança digital, muitos ainda carecem de informações essenciais, como a identificação de *links* maliciosos, e familiaridade com ferramentas tecnológicas, revelando a necessidade urgente de ampliar a educação para práticas que envolvam recursos computacionais. Além disso, a pesquisa mostrou a relevância de práticas pedagógicas voltadas à segurança digital para alunos da EJA, promovendo conhecimento crítico e prevenção contra golpes virtuais. Isso corrobora os achados de Pereira and De França (2023) sobre o impacto do *cyberbullying* na segurança digital e a necessidade de medidas educativas eficazes.

Referências

Brasil. Ministério da Educação. (2022). Complemento à Base Nacional Comum Curricular. Disponível em: http://portal.mec.gov.br/docman/fevereiro-2022-pdf/236791-anexo-ao-parecer-cneceb-n-2-2022-bncc-computacao/file. Acesso em 29 de janeiro de 2025.

Fonseca, A. K. A., Liborio Filho, J. da M., and Reis, A. B. A. (2025). Residência Pedagógica e o ensino de computação: experiências formativas no Ensino Fundamental. Revista Delos, 18(63), e3481. https://doi.org/10.55905/rdelosv18.n63-016.

González, F. E. (2020). Reflexões sobre alguns conceitos da pesquisa qualitativa. Revista Pesquisa Qualitativa, 8(17), 155-183.

Pereira, W., and França, R. (2023). Cyberbullying na Escola: Entendendo e Lidando com a Crueldade Online. In Anais do III Simpósio Brasileiro de Educação em Computação, (pp. 359-368). Porto Alegre: SBC. doi:10.5753/educomp.2023.228374.

Rocha, T. B., Da Silva Brandão, C. W. G., and Ramos, E. N. (2023). Cibercultura e educação básica: plano de aula sobre fake news para educação de jovens e adultos. Revista Docência e Cibercultura, 7(2), 52-66.

Santos, F. P., Sá, J. M. N., Melo, J. P. P., Silva, G. N., Oliveira, E. S., and Trindade, G. M. (2024). Depoimentos invisíveis: transformando relatos em ações contra o cyberbullying, bullying e os riscos on-line no ensino fundamental. Revista Ibero-Americana de Humanidades, Ciências e Educação, 10, 3046-3056.

Silva, L. M. da ., and Pereira, V. B. (2023). As Tecnologias Digitais da Informação e da Comunicação e suas Contribuições para a Metodologia Ativa e Inclusão Digital na

Educação de Jovens e Adultos. Boletim De Conjuntura (BOCA), 15(45), 229–242. https://doi.org/10.5281/zenodo.8347212.

Velloso, L. R. S., et al. (2022). Pesquisa participante na Educação Física Escolar: o estado da arte. Movimento, 28, e28059.