**Aluno(a):** Fernanda Alves Fahl

**Orientador(a):** Daniele Caroline Lima Da Silva

**Curso: MBA em Engenharia de Software**

**Segurança Cibernética para Todos: Um Programa Educacional Interativo para Conscientização e Proteção Digital**

**Introdução**

No cenário atual, a segurança cibernética emergiu como uma preocupação crítica, não apenas para empresas e governos, mas também para indivíduos comuns. Com o aumento exponencial do uso de dispositivos conectados e a digitalização de serviços, o público geral está cada vez mais exposto a riscos cibernéticos, como phishing, roubo de identidade, malware e violações de privacidade. No entanto, a maioria das iniciativas educacionais em segurança cibernética é voltada para profissionais de tecnologia ou estudantes da área, deixando uma lacuna significativa na conscientização do público leigo.

Este projeto, intitulado "Segurança Cibernética para Todos: Um Programa Educacional Interativo para Conscientização e Proteção Digital", busca preencher essa lacuna, oferecendo um programa educacional acessível, prático e envolvente, que não exige conhecimentos prévios em programação ou tecnologia. A proposta é desenvolver e implementar um programa educacional interativo, voltado para o público geral, com o objetivo de ensinar conceitos básicos de segurança cibernética e práticas essenciais de proteção digital.

A relevância deste estudo reside na crescente necessidade de capacitar indivíduos a identificar ameaças cibernéticas, proteger suas informações pessoais e adotar hábitos seguros no uso de tecnologias digitais. Ao promover a conscientização e a educação em segurança cibernética, espera-se contribuir para a criação de uma cultura de proteção digital em larga escala, reduzindo a vulnerabilidade de pessoas leigas a ataques cibernéticos e, consequentemente, promovendo uma sociedade mais segura e informada.

**Objetivo**

Desenvolver e implementar um programa educacional acessível e interativo, voltado para o público geral, com o objetivo de ensinar conceitos básicos de segurança cibernética e práticas essenciais de proteção digital. O projeto busca capacitar pessoas leigas em programação a identificar ameaças cibernéticas, proteger suas informações pessoais e adotar hábitos seguros no uso de tecnologias digitais.

Com o aumento do uso de dispositivos conectados e a digitalização de serviços, o público geral está cada vez mais exposto a riscos cibernéticos, como phishing, roubo de identidade, malware e violações de privacidade. No entanto, a maioria das iniciativas educacionais em segurança cibernética é voltada para profissionais de tecnologia ou estudantes da área, deixando uma lacuna significativa na conscientização do público leigo. Este projeto busca preencher essa lacuna, oferecendo um programa educacional acessível, prático e envolvente, que não exige conhecimentos prévios em programação ou tecnologia.

**Metodologia ou Material e Métodos**

               **Pesquisa Inicial:**

* Realizar uma pesquisa com o público-alvo para entender suas principais preocupações e lacunas de conhecimento em segurança cibernética.
* Identificar os tipos de ameaças mais comuns enfrentadas por pessoas leigas, como golpes online, fraudes bancárias e invasões de contas.

 **Desenvolvimento do Conteúdo:**

* Criar módulos educacionais simples e interativos, abordando temas como:
  + O que é segurança cibernética e por que ela é importante.
  + Como criar senhas fortes e gerenciá-las.
  + Identificação de golpes online (phishing, scams, etc.).
  + Proteção de dispositivos pessoais (antivírus, atualizações, etc.).
  + Privacidade online e uso seguro de redes sociais.
* Utilizar linguagem acessível e evitar jargões técnicos.

 **Plataforma de Ensino:**

* Desenvolver uma plataforma online ou aplicativo móvel com recursos interativos, como:
  + Vídeos explicativos curtos.
  + Quiz e jogos educativos para reforçar o aprendizado.
  + Simulações de cenários reais (ex.: identificar um e-mail de phishing).
  + Certificados de conclusão para motivar os participantes.

 **Implementação Piloto:**

* Testar o programa com um grupo pequeno de pessoas leigas em tecnologia, coletando feedback para ajustes.

 **Divulgação:**

* Promover o programa em redes sociais, escolas, ONGs e comunidades locais.
* Parcerias com empresas e instituições para alcançar um público maior.

 **Avaliação:**

* Aplicar questionários antes e depois do curso para medir o aumento no conhecimento e na adoção de práticas seguras.
* Coletar feedback qualitativo dos participantes sobre a relevância e aplicabilidade do conteúdo.

**Resultados Esperados**

* Conscientização: Aumento significativo na compreensão do público geral sobre segurança cibernética.
* Mudança de Comportamento: Maior adoção de práticas seguras, como uso de senhas fortes e cuidado ao clicar em links suspeitos.
* Impacto Social: Redução de incidentes cibernéticos entre os participantes do programa.
* Escalabilidade: Um modelo educacional que pode ser replicado em diferentes comunidades e regiões.

*Inovações do Projeto:*

* Gamificação: Incorporar elementos de jogos para tornar o aprendizado mais envolvente e divertido.
* Simulações Práticas: Criar cenários interativos onde os participantes possam praticar a identificação de ameaças cibernéticas.
* Acessibilidade: Garantir que o programa seja acessível para pessoas com diferentes níveis de alfabetização digital, incluindo idosos e jovens.
* Educação Comunitária: Promover workshops presenciais em comunidades com acesso limitado à internet.

Este projeto tem o potencial de transformar a forma como o público geral percebe e lida com segurança cibernética, promovendo uma cultura de proteção digital em larga escala. Ele pode ajudar a reduzir a vulnerabilidade de pessoas leigas a ataques cibernéticos, contribuindo para uma sociedade mais segura e informada.

**Cronograma de Atividades**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Atividades planejadas** | **Mês** | | | | | |
| **Abril** | **Maio** | **Junho** | **Julho** | **Agosto** | **Setembro** |
| Pesquisa Inicial | x |  |  |  |  |  |
| Desenvolvimento do Conteúdo | x | x |  |  |  |  |
| Plataforma de Ensino |  | x | x |  |  |  |
| Implementação Piloto |  |  | x |  |  |  |
| Divulgação |  |  |  | x |  |  |
| Implementação Completa |  |  |  | x | x |  |
| Avaliação |  |  |  |  | x |  |
| Análise de Resultados |  |  |  |  | x |  |
| Relatório Final |  |  |  |  |  | x |
| Planejamento Futuro |  |  |  |  |  | x |

**Referências**

 Segurança Cibernética:

SCHNEIER, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company.

ANDERSON, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.

STALLINGS, W., & Brown, L. (2018). *Computer Security: Principles and Practice*. Pearson.

RAMOS, R. B. (2024). *Metodologias de análise integrada de segurança crítica e segurança cibernética em sistemas ciber físicos* (Dissertação (Mestrado). Universidade de São Paulo, São Paulo. Recuperado de https://www.teses.usp.br/teses/disponiveis/3/3141/tde-12072024-091247/pt-br.php

RAMOS, R. B. (2024). *Metodologias de análise integrada de segurança crítica e segurança cibernética em sistemas ciber físicos* (Dissertação (Mestrado). Universidade de São Paulo, São Paulo. Recuperado de https://www.teses.usp.br/teses/disponiveis/3/3141/tde-12072024-091247/pt-br.php

 Educação e Metodologias de Ensino:

BROWN, T. (2017). *Design Thinking*. Alta Books, Rio de Janeiro, RJ, Brasil.

AMBROSE, G., & HARRIS, P. (2015). *Design Thinking*. Brookman, Porto Alegre, RS, Brasil.

PRENSKY, M. (2010). *Teaching Digital Natives: Partnering for Real Learning*. Corwin Press.

RADFAHRER, L. (2011). Ferramentas para o ensino digital. *Folha de São Paulo*. São Paulo: Escola de Comunicações e Artes, Universidade de São Paulo. Recuperado de https://www.eca.usp.br/acervo/acervo-local/producao-academica/002186826.pdf

MUNIZ, S. R. (2016). Ferramentas digitais para personalizar o ensino. In *Programação*. São Paulo: Universidade de São Paulo - USP, Pró-Reitoria de Graduação - PRG. Recuperado de http://biton.uspnet.usp.br/cgrad/wp-content/uploads/2016/07/Programacao\_CONGRESSO\_GRAD\_2016.pdf

 DESENVOLVIMENTO DE PROGRAMAS EDUCACIONAIS:

COHN, M. (2011). *Desenvolvimento de software com Scrum*. Bookman, Porto Alegre, RS, Brasil.

SUTHERLAND, J. (2014). *Scrum: a arte de fazer o dobro de trabalho na metade do tempo*. Leya, São Paulo, SP, Brasil.

MASSARI, V.L. (2018). *Gerenciamento ágil de projetos*. 2ed. Brasport. Rio de Janeiro, RJ, Brasil.

 Gamificação e Aprendizagem Interativa:

KAPP, K. M. (2012). *The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education*. Pfeiffer.

GEE, J. P. (2007). *What Video Games Have to Teach Us About Learning and Literacy*. Palgrave Macmillan.

BAUER, Adriana e FERNANDES, Fabiana Silva. *Avaliação de projetos, programas e políticas educacionais*. Estudos em Avaliação Educacional, v. 33, 2022

TODA, A. M. (2021). *Contributions for Gamification Design in Educational Contexts* (Tese (Doutorado). Universidade de São Paulo, São Carlos. Recuperado de https://www.teses.usp.br/teses/disponiveis/55/55134/tde-23062021-114011/

PEDRO, L. Z., & ISOTANI, S. (2016). *Explorando o impacto da gamificação na redução do gaming the system em um ambiente virtual de aprendizagem*. In *Anais*. Porto Alegre, RS: SBC. doi:10.5753/cbie.wcbie.2016.81

 Avaliação de Programas Educacionais:

Kirkpatrick, D. L., & Kirkpatrick, J. D. (2006). *Evaluating Training Programs: The Four Levels*. Berrett-Koehler Publishers.

Guskey, T. R. (2000). *Evaluating Professional Development*. Corwin Press.