Título:	**CIBERSEGURANÇA INCLUSIVA: ASSISTENTE VIRTUAL PARA IDENTIFICAÇÃO DE ENGENHARIA SOCIAL NO WHATSAPP**		
Autores:	Lucas Oliveira Dias Evandro Franzen		
Área	[ ] Humanas [ ] Sociais Aplicadas [ ] Biológicas e da Saúde [X] Exatas, da Terra e Engenharias	Dimensão:	[ ] Ensino [X] Pesquisa [ ] Extensão [ ] Inovação

Resumo:
A popularização massiva do WhatsApp no cenário nacional transformou a plataforma no principal vetor de comunicação diária, mas também no terreno ideal para a proliferação de fraudes financeiras estruturadas via engenharia social. Uma vez que as abordagens tradicionais de segurança digital se concentram majoritariamente na mitigação de vulnerabilidades técnicas, o fator humano permanece frequentemente desprovido de defesas contra a manipulação psicológica. Nesse contexto, a segurança digital inclusiva direciona seus esforços para o desenvolvimento de soluções voltadas a grupos vulneráveis e com menor letramento digital, que figuram como os alvos preferenciais de golpistas devido à ausência de familiaridade técnica com a tecnologia. O presente trabalho tem como objetivo principal desenvolver e validar a arquitetura de um assistente virtual integrado à plataforma de mensageria WhatsApp, amparado por técnicas de Processamento de Linguagem Natural (PLN), com a capacidade de identificar e alertar usuários com baixo letramento digital sobre tentativas de ataques baseados em engenharia social em tempo real. A metodologia caracteriza-se como uma pesquisa de natureza exploratória e descritiva, conduzida por meio de um estudo bibliográfico e de testes em ambiente de laboratório computacional. Os procedimentos metodológicos incluem o levantamento de dados documentais a partir de bases públicas de relatórios de incidentes cibernéticos (como CERT.br e e-farsas) para reunir históricos textuais de golpes, visando estruturar uma base de dados conversacional robusta para o treinamento de modelos classificadores. A implementação do pipeline de Processamento de Linguagem Natural fará uso da linguagem de programação Python e de frameworks de Inteligência Artificial, culminando em um estudo de caso simulado para emular as interações da API do WhatsApp. A pesquisa adota uma abordagem mista, combinando avaliações quantitativas das métricas de desempenho do modelo classificador (como acurácia, precisão e F1-score) com análises qualitativas voltadas à adequação contextual da linguagem dos alertas gerados, assegurando que os parâmetros de acessibilidade cognitiva sejam plenamente satisfeitos para o público-alvo. Como principais resultados esperados, almeja-se a criação de um modelo arquitetural de software inovador que atue como uma barreira defensiva proativa para os usuários mais suscetíveis à manipulação psicológica. Espera-se que a ferramenta demonstre a viabilidade técnica de integrar módulos de segurança nativos em interfaces de conversação sem comprometer a usabilidade prática. Conclui-se, de forma preliminar, que o desenvolvimento desta tecnologia

assistiva possui um forte potencial de impacto social, contribuindo ativamente para a redução de prejuízos financeiros e emocionais decorrentes de fraudes digitais. Além disso, a iniciativa alinha-se aos Objetivos de Desenvolvimento Sustentável (ODS) da ONU, promovendo a educação de qualidade (ODS 4), a inovação tecnológica (ODS 9), a redução das desigualdades (ODS 10) e a promoção de instituições eficazes (ODS 16), garantindo que utilizadores marginalizados pela exclusão tecnológica tenham acesso a camadas essenciais de proteção cibernética no seu cotidiano digital.

Link do Vídeo: https://drive.google.com/file/d/1Y_KpeN-F1BQPEGf9p4UFz6GGJoxpsm05/view?usp=sharing