**Faculdade de Informática e Administração Paulista - Aclimação   
Curso Defesa Cibernética   
  
  
  
  
  
  
  
Av. Lins de Vasconcelos, 1222 - Aclimação, São Paulo - SP, 01538-001  
  
  
  
  
  
  
Relatório Challenge AXUR:  
Detector de Phishing no WhatsApp Business   
  
Integrantes do grupo:  
Lucas Andrade Barbosa da Silva (RM99955),  
Matheus Casarini Dias (RM99965).  
  
  
  
  
  
  
  
  
  
  
  
SUMÁRIO**

1. **INTRODUÇÃO** 3

2. **FUNDAMENTAÇÃO TEÓRICA** 4

3. **METODOLOGIA** 4

4. **DESENVOLVIMENTO** 7

4.1 Configuração do Sistema de DeTECÇÃO 7

4.2 Ferramentas 8

4.3 Implementação e Testes 9  
5. **CONCLUSÃO** 11  
6. **REFERÊNCIAS** 12  
  
  
  
1. **INTRODUÇÃO**

Este relatório foi elaborado no âmbito de um challenge proposto pela empresa Axur, que visa desenvolver uma solução eficaz para detectar e alertar sobre tentativas de phishing. A motivação deste trabalho reside na crescente necessidade de proteger os clientes contra ataques de phishing, que são uma das formas mais comuns e prejudiciais de cibercrime.   
  
Visando um melhor entendimento dos princípios de segurança contra phishing, a importância de proteger as comunicações e dados dos clientes, bem como a necessidade de identificar e mitigar tentativas de phishing em tempo real, elaboramos um projeto de TI focado na proteção de clientes contra essas ameaças. Este projeto é composto por um sistema de detecção e alerta em tempo real, análise de mensagens suspeitas e com o objetivo de proporcionar um ambiente digital mais seguro e confiável.

**FUNDAMENTAÇÃO TEÓRICA**

**O que é Phishing?**

Phishing é uma técnica de engenharia social usada por cibercriminosos para enganar usuários e obter informações sensíveis, como senhas, números de cartões de crédito e outros dados pessoais. Os ataques de phishing geralmente são realizados através de e-mails, mensagens instantâneas ou sites falsos que se passam por entidades legítimas.

**METODOLOGIA**

Com base nas informações fornecidas por profissionais especializados em phishing, identificamos que as tentativas de phishing frequentemente utilizam textos padrões que buscam induzir o usuário a fornecer informações sensíveis. Alguns exemplos comuns incluem:

Solicitação de Dados Pessoais: "Precisamos que você confirme seu nome de usuário e senha para continuar acessando sua conta."

Urgência Falsa: "Sua conta será bloqueada em 24 horas, a menos que você verifique suas informações agora."

Ofertas Irresistíveis: "Você foi selecionado para ganhar um prêmio exclusivo. Clique aqui para reivindicar seu prêmio."

Ameaças e Medo: "Detectamos uma atividade suspeita em sua conta”.  
**Apoio Profissional**

O desenvolvimento da nossa solução contou com o apoio de profissionais da área de cibersegurança e especialistas em phishing, que forneceram informações críticas sobre as práticas comuns de phishing e os métodos mais eficazes para detectar e prevenir esses ataques. Este conhecimento especializado foi fundamental para a criação de uma ferramenta robusta e eficiente.

A fundamentação teórica e o apoio profissional embasaram o desenvolvimento da nossa solução contra phishing. A utilização de textos padrões, palavras-chave, e a verificação de links e números de telefone não oficiais, combinada com a expertise dos profissionais consultados, garantiram uma abordagem abrangente e eficaz na detecção e alerta de tentativas de phishing. Esta solução visa aumentar significativamente a segurança dos usuários contra uma das ameaças cibernéticas mais comuns e prejudiciais. **Metodologia da Prova de Conceito**

A prova de conceito foi conduzida em um ambiente simulado, utilizando a biblioteca streamlit de python para interface gráfica e usando uma variedade de mensagens e cenários para testar a eficácia da solução. Foram realizados os seguintes passos:

Preparação do Ambiente: Configuração dos dispositivos e ambientes de testes, incluindo computadores e smartphones, em uma rede controlada.

Implantação da Solução: Instalação e configuração da ferramenta de detecção e alerta contra phishing em um servidor dedicado.

Testes de Funcionalidade: Realização de testes para verificar a detecção de mensagens e links suspeitos, envio de alertas de phishing e resposta tentativas simuladas de phishing.

**Resultados da Prova de Conceito**

Durante os testes, a solução de detecção e alerta contra phishing demonstrou os seguintes resultados positivos: Detecção Precisa de Links Suspeitos: A ferramenta identificou corretamente links e mensagens que continham possíveis tentativas de phishing.

Envio Eficiente de Alertas: Os alertas de phishing foram enviados rapidamente para os usuários, permitindo ações preventivas imediatas.

Interface de Gerenciamento Intuitiva: A interface de gerenciamento foi fácil de usar, permitindo que os testes realizados fossem monitorados e gerenciados de maneira eficaz.

**Conclusão**

Com base nos resultados da prova de conceito, podemos concluir que a solução de ferramenta voltada à detecção e alerta contra phishing é eficaz na proteção de clientes contra tentativas de phishing. Ela oferece recursos que podem ser valiosos para empresas e organizações que desejam fortalecer sua postura de segurança cibernética.

**Agradecimentos**

Gostaríamos de agradecer à nossa faculdade, professores e colegas de turma pelo apoio e orientação durante a realização desta prova de conceito. Em especial, agradecemos à empresa Axur pela proposição do challenge e pela oportunidade de desenvolver uma solução que contribui significativamente para a segurança dos usuários.