SCIENCE
SCIENTIFIC JOURNAL

Detecção de Phishing por Análise Estrutural de E-Mails: Uma Abordagem Automatizada

Phishing Detection Through Structural Email Analysis: An Automated Approach

Mateus Cabral de Matos Dias[1]
Juliana Alves Vieira[2]

https://doi.org/10.5281/zenodo.17487612

Resumo: O crescimento das ameaças digitais consolidou o phishing como uma das estratégias mais recorrentes e perigosas utilizadas por cibercriminosos para obtenção de informações sensíveis, como senhas e dados bancários. Este artigo tem como objetivo propor uma metodologia para o desenvolvimento de uma ferramenta automatizada de detecção de phishing em e-mails e links suspeitos. A pesquisa busca responder: como a análise estrutural de mensagens eletrônicas pode contribuir para identificar indícios de phishing de forma automatizada? Para isso, a proposta metodológica contempla técnicas como verificação de remetentes, análise de domínios, detecção de erros textuais, validação de links e certificados digitais, bem como autenticação via SPF, DKIM e DMARC. Inclui ainda a verificação da geolocalização de IPs e consulta a listas negras. Espera-se que a ferramenta reduza a incidência de ataques, amplie a capacidade de detecção por parte dos usuários e ofereça base para futuras aplicações em segurança cibernética.
Palavras-chave: Phishing. Segurança Cibernética. Detecção de Phishing. Segurança de Emails.

Abstract: The growth of digital threats has consolidated phishing as one of the most recurrent and dangerous strategies used by cybercriminals to obtain sensitive information, such as passwords and banking data. This article aims to propose a methodology for the development of an automated tool for detecting phishing in emails and suspicious links. The research seeks to answer: how can the structural analysis of electronic messages contribute to automatically identifying phishing attempts? The methodological proposal includes techniques such as sender verification, domain analysis, detection of textual errors, validation of links and digital certificates, as well as authentication mechanisms through SPF, DKIM, and DMARC. It also considers IP geolocation checks and the use of blacklists. The expected results indicate that the tool may reduce the incidence of phishing attacks, enhance users detection capacity, and serve as a technical foundation for future applications and improvements in cybersecurity defense systems.
Keywords: Phishing. Cybersecurity. Phishing Detection. Email Security.

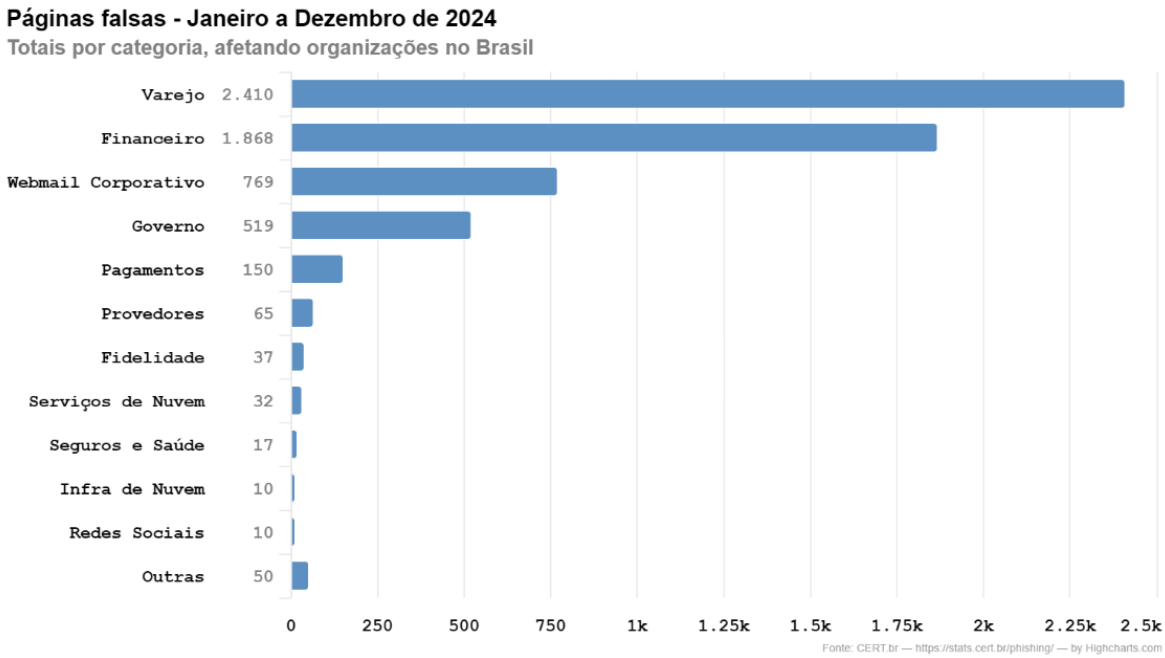
Introdução

Com o avanço da tecnologia e a crescente dependência de plataformas digitais, a segurança cibernética tornou-se uma preocupação essencial. Entre as diversas ameaças existentes, o phishing se destaca como uma das fraudes mais comuns, visando enganar usuários para obter informações confidenciais, como senhas e dados bancários. Esses ataques frequentemente se disfarçam como comunicações legítimas, o que dificulta sua detecção e coloca em risco tanto indivíduos quanto organizações. O phishing é uma técnica de engenharia

1 Graduando. Iesgo. ORCID 0009-0006-4417-2199. E-mail: mateuscabral7575@gmail.com.
2 Especialista. Iesgo. ORCID 0009-0003-5902-4373. E-mail: juliana.vieira@iesgo.edu.br.

social que explora e-mails, páginas falsificadas e mensagens de texto para induzir a vítima a realizar ações que comprometam sua segurança. Mesmo com campanhas de conscientização e soluções de defesa, esses ataques continuam a crescer em número e sofisticação. Um levantamento da Redbelt Security (2024) revelou que, em 2023, pelo menos 3,5 milhões de brasileiros foram vítimas de phishing. Além disso, dados da Appgate (2024) apontam que o phishing representou 61% das atividades fraudulentas neutralizadas pelo Centro de Operações de Segurança (SOC) da companhia, seguido pelo uso indevido de marcas registradas (25%) e pelo redirecionamento para páginas maliciosas (10%). As estatísticas fornecidas pelo CERT.br (2024) demonstram quais áreas foram mais afetadas pelo phishing em 2024. A Figura 1 apresenta uma análise detalhada da distribuição desses ataques por categoria no Brasil, destacando os setores mais visados pelos cibercriminosos.

Figura 1 – Páginas falsas por categoria no Brasil (jan-dez 2024).



Fonte: CERT.br. Dados disponíveis em https://stats.cert.br/phishing/ (2024).

O crescimento desses ataques tem sido impulsionado por novas táticas de engenharia social e pelo uso de inteligência artificial, tornando-se essencial o aprimoramento das ferramentas de defesa cibernética. Diante desse cenário, este artigo propõe o desenvolvimento de uma ferramenta para detecção e prevenção de phishing, focada na análise de e-mails e links com base em boas práticas de segurança. A solução será projetada para auxiliar usuários e

organizações na identificação dessas ameaças, reduzindo os riscos associados ao roubo de credenciais, vazamento de dados, fraudes e comprometimento de sistemas. Este estudo também examina as técnicas e métodos atuais de detecção de phishing, identifica as limitações das soluções existentes e propõe melhorias para fortalecer a segurança digital.

Fundamentação Teórica

Os ataques de phishing tornaram-se cada vez mais sofisticados, representando um risco significativo para indivíduos e organizações. Apesar da existência de filtros de segurança, os criminosos continuam aperfeiçoando suas táticas para enganar usuários. O grande desafio está no fato de que essas ameaças se tornam mais convincentes e difíceis de detectar à medida que evoluem. Diante desse cenário, propõe-se uma ferramenta para identificação eficiente de tentativas de phishing. Em vez de depender exclusivamente de listas de domínios suspeitos ou filtros básicos, a solução sugerida examina múltiplos elementos presentes nos e-mails e links. Além de identificar ataques, a ferramenta oferecerá uma análise mais detalhada das possíveis fraudes, aprimorando a precisão na detecção. Com isso, espera-se fortalecer a proteção contra essas ameaças, reduzindo vulnerabilidades e ampliando a segurança digital para usuários e empresas. Compreender a natureza do phishing exige a análise das abordagens empregadas por cibercriminosos e das soluções disponíveis para sua mitigação. O phishing é um dos ataques cibernéticos mais recorrentes, explorando vulnerabilidades humanas por meio de técnicas de engenharia social. Nesse contexto, a presente seção tem como objetivo apresentar uma revisão das principais pesquisas sobre o tema, abordando as estratégias de detecção, prevenção e os desafios enfrentados pelas soluções atuais.

1) **Definição e Impacto do Phishing:** Segundo Bhavsar et al. (2018), o phishing é um crime cibernético que ocorre por meio de e-mails, chamadas telefônicas e mensagens de texto fraudulentas, visando a obtenção de informações pessoais e dados bancários das vítimas. Esse ataque segue um processo estruturado: (1) o invasor envia um e-mail fraudulento, (2) a vítima clica no link e é direcionada a um site falso, (3) suas credenciais são capturadas e (4) as credenciais capturadas são usadas para acessar serviços legítimos de forma indevida. Além disso, os atacantes costumam mascarar suas mensagens para que pareçam vir de fontes confiáveis, aumentando a taxa de sucesso dos golpes.

2) **Técnicas de Phishing e Engenharia Social:** A engenharia social é um elemento central nos ataques de phishing. Estudos como o de Khadka (2024) analisam o uso de técnicas de persuasão nesses ataques, demonstrando como os atacantes manipulam emoções e comportamentos dos alvos. Em um estudo complementar, Khadka et al. (2023) realizam uma revisão sobre princípios de persuasão utilizados em golpes de phishing, abordando como estratégias psicológicas são aplicadas para enganar as vítimas. Os ataques de phishing podem ser classificados em diferentes tipos, dependendo da abordagem utilizada pelos atacantes. Segundo Salviano, Santos e Silva (2021), alguns dos principais tipos incluem:
    a) **Scam:** tentativa de enganar usuários para que forneçam informações pessoais por meio de links ou arquivos maliciosos.
    b) Blind Phishing: envio massivo de e-mails fraudulentos sem um alvo específico, contando com a probabilidade de que algumas vítimas caiam no golpe.
    c) Spear Phishing: ataques direcionados a grupos específicos, como funcionários de uma empresa ou órgãos governamentais, com o objetivo de obter informações sigilosas.
    d) Clone Phishing: clonagem de sites legítimos para capturar credenciais dos usuários desavisados.
    e) Whaling: ataques voltados para altos executivos, frequentemente disfarçados de comunicações empresariais ou notificações judiciais falsas.
    f) Vishing: golpes realizados via chamadas telefônicas, muitas vezes combinados com SMS (Short Message Service) falsos para induzir a vítima a ligar para um número controlado pelos criminosos.
    g) Pharming: manipulação de servidores DNS (Domain Name Servers) para redirecionar usuários a páginas falsas sem que percebam a fraude.
    h) **Smishing:** variante do phishing focada em mensagens SMS (Short Message Service), geralmente envolvendo golpes que pressionam a vítima a agir rapidamente, como falsas dívidas ou prêmios inexistentes.
3) **Métodos de Detecção e Prevenção de Phishing:** A prevenção do phishing envolve soluções tecnológicas e a educação do usuário. Segundo Agazzi (2020), cinco camadas de proteção são essenciais: Ferramentas automatizadas, Ferramentas de

auxílio à decisão, Conhecimento, Proteção externa e Autenticação Multifator (MFA). Diversas abordagens têm sido propostas para a detecção de ataques de phishing. Venturi et al. (2022), analisaram mais de 2.000 kits de phishing, classificando-os com base em técnicas de evasão e ofuscação. Esses kits são ferramentas utilizadas por atacantes para criar páginas falsas que imitam serviços legítimos. Outra abordagem relevante é a proposta por Xiong et al. (2019), que demonstram que o treinamento de usuários embutido em alertas de segurança melhora significativamente a capacidade de identificar páginas fraudulentas. Além disso, Tanti (2024) destaca a importância da adoção de múltiplas camadas de defesa, como a utilização de infraestrutura de e-mails baseada em IPv6. O IPv6 permite a autenticação nativa do remetente por meio do cabeçalho de origem, o que dificulta técnicas de falsificação de endereços spoofing, muito comuns em ataques de phishing. Essa tecnologia proporciona maior rastreabilidade e integridade na comunicação entre servidores. O autor também enfatiza que soluções como filtragem de URLs (Uniform Resource Locator) e inspeção de tráfego criptografado são essenciais para mitigar ameaças ocultas em conexões seguras.

4) **Limitações das Soluções Atuais:** Embora existam diversas estratégias para a detecção e prevenção de phishing, os sistemas anti-phishing ainda enfrentam desafios. Silva e Andrade (2018) discutem que “elas evoluíram desde suas origens, estão mais sofisticadas e adaptaram seus objetivos e capacidades de infectar os computadores de forma prejudicial e, muitas vezes, silenciosa.” Diante dessas limitações, torna-se necessário estabelecer objetivos claros para o desenvolvimento de soluções mais eficazes.

Diante dos desafios identificados na literatura, destaca-se a necessidade de desenvolver soluções mais eficazes para a detecção de phishing. Considerando os estudos analisados, a próxima seção apresenta a metodologia adotada para construção da ferramenta proposta neste trabalho.

Metodologia

Nesta seção, são apresentados os materiais e metodologias que serão utilizados para o desenvolvimento da ferramenta de detecção e prevenção de ataques de phishing. Para que a ferramenta de detecção de phishing seja eficiente, é fundamental extrair e analisar elementos

presentes em mensagens suspeitas, como remetente, assunto, links e conteúdo textual. A metodologia propõe o uso de bibliotecas e ferramentas automatizadas para realizar essa extração a partir do texto bruto ou estruturas de e-mails fornecidas diretamente pelos usuários. A Figura 2 apresenta um módulo de extração utilizando a linguagem de programação Python com uso de algumas bibliotecas.

Figura 2 – Trecho do código para extração de dados de e-mails.

```python
import re
import ipaddress
from email import policy
from email.parser import BytesParser
from email.utils import parsedate_to_datetime

def extrair_info_eml(caminho_arquivo):
    with open(caminho_arquivo, 'rb') as f:
        msg = BytesParser(policy=policy.default).parse(f)

    remetente = msg['From']
    assunto = msg['Subject']
    data = parsedate_to_datetime(msg['Date']) if msg['Date'] else None

    headers = msg.as_string()
    spf = re.search(r"spf=(\w+)", headers)
    dkim = re.search(r"dkim=(\w+)", headers)
    dmarc = re.search(r"dmarc=(\w+)", headers)

    """ --------- TRECHO OMITIDO --------- """

    return {
        'Remetente': remetente,
        'Assunto': assunto,
        'Data': str(data) if data else None,
        'SPF': spf.group(1).upper() if spf else 'N/A',
        'DKIM': dkim.group(1).upper() if dkim else 'N/A',
        'DMARC': dmarc.group(1).upper() if dmarc else 'N/A',
        'IPs_detectados': list(set(ips_validos)),
        'Links_encontrados': links,
        'Anexos': anexos
    }
```

Fonte: Elaborado pelos autores (2025).

A validação do remetente é uma etapa fundamental na detecção de e-mails maliciosos, pois permite verificar se a mensagem foi enviada de forma legítima por um domínio autorizado. Para isso, a metodologia sugere a verificação dos três principais mecanismos de autenticação de e-mails: SPF, DKIM e DMARC.

a) **SPF (Sender Policy Framework):** Verifica se o endereço IP do servidor de envio está autorizado a enviar mensagens em nome do domínio do remetente.
b) **DKIM (DomainKeys Identified Mail):** Analisa a assinatura digital presente no cabeçalho do e-mail, garantindo a integridade do conteúdo.
c) **DMARC (Domain-based Message Authentication, Reporting & Conformance):** Válida se o domínio do remetente possui uma política explícita para proteger contra spoofing, combinando os resultados do SPF e DKIM.

Além disso, é possível consultar a reputação do domínio por meio de serviços reconhecidos como PhishTank, Google Safe Browsing e SiteConfiavel.com.br. Essas fontes permitem verificar se o domínio está presente em listas negras ou possui histórico de atividades fraudulentas. A Figura 3 apresenta um trecho do código utilizado para realizar verificações de forma automatizada.

Figura 3 – Trecho do código para validação de SPF, DKIM e DMARC.

```python
# SPF
import spf
resultado, codigo, explicacao = spf.check2(i='203.0.113.1', s='usuario@exemplo.com', h='exemplo.com')
print("SPF:", resultado)

# DKIM
import dkim
with open("email.eml", "rb") as f:
    raw_email = f.read()
verificado = dkim.verify(raw_email)
print("DKIM:", "PASS" if verificado else "FAIL")

# DMARC
import dns.resolver
dominio = "exemplo.com"
registro = "_dmarc." + dominio
try:
    resposta = dns.resolver.resolve(registro, 'TXT')
    for rdata in resposta:
        print("DMARC:", rdata.to_text())
except:
    print("DMARC: Não configurado")
```

Fonte: Elaborado pelos autores (2025).

Outra questão importante a ser considerada é a análise de links e anexos presentes no corpo dos e-mails. Essa etapa é fundamental na identificação de tentativas de phishing, já que esses elementos são frequentemente utilizados para redirecionar as vítimas a páginas fraudulentas ou distribuir malware.

a) **Extração de URLs no Corpo do e-mail e Anexos:** O sistema analisará o corpo da mensagem e os arquivos anexados para identificar endereços web (URLs), utilizando expressões regulares para localizá-los. O conteúdo dos anexos também será examinado, caso contenham redirecionamentos ou hiperlinks.
b) **Expansão de Endereços Encurtados:** Endereços web encurtados são frequentemente utilizados para ocultar destinos maliciosos. É possível fazer uso da ferramenta Unshorten.me ou utilizando a biblioteca requests do Python para revelar qual o destino do link.
c) **Análise de Certificados SSL/TLS:** A verificação dos certificados digitais será realizada com base na validade, na cadeia de confiança e na impressão digital (SHA-256). Caso o domínio do link não possua um certificado válido ou apresente sinais de falsificação, será classificado como suspeito.
d) **Verificação de Extensões de Arquivos Perigosas:** Arquivos anexados com extensões como .exe, .js, .vbs, entre outras, serão identificados como de alto risco. Para fortalecer a análise, o sistema poderá integrar-se à API do VirusTotal, um serviço amplamente utilizado para a verificação de arquivos e URLs, permitindo detectar anexos que contenham códigos maliciosos conhecidos.

Na Figura 4 é apresentado um trecho de código que permite verificar se os links utilizam conexões seguras, informando o nome comum (CN), validade do certificado e impressão digital SHA-256.

Figura 4 – Trecho do código para análise de certificado digital SSL/TSL de URLs.

```python
import ssl
import socket
import hashlib
from urllib.parse import urlparse

def verificar_certificado(url):
    try:
        dominio = urlparse(url).hostname
        if not dominio:
            print("URL inválida.")
            return

        contexto = ssl.create_default_context()
        with socket.create_connection((dominio, 443), timeout=5) as sock:
            with contexto.wrap_socket(sock, server_hostname=dominio) as ssock:
                cert_bin = ssock.getpeercert(binary_form=True)
                cert = ssock.getpeercert()

                sujeito = dict(x[0] for x in cert['subject'])
                cn = sujeito.get('commonName', 'N/A')
                validade_de = cert['notBefore']
                validade_ate = cert['notAfter']
                sha256 = hashlib.sha256(cert_bin).hexdigest()

                print("Certificado encontrado.")
                print(f"Domínio: {dominio}")
                print(f"Nome comum (CN): {cn}")
                print(f"Validade: {validade_de} até {validade_ate}")
                print(f"SHA-256: {sha256}")
    except Exception as e:
        print("Nenhum certificado encontrado ou erro:", str(e))

# Exemplo
verificar_certificado("https://google.com")
```

Fonte: Elaborado pelos autores (2025).

Complementando a análise estrutural, a análise textual é uma técnica importante na identificação de e-mails fraudulentos, uma vez que mensagens de phishing frequentemente contêm erros gramaticais, ortográficos e padrões linguísticos que podem servir como indicadores de risco. Embora ainda não tenha sido implementado neste estágio da pesquisa, o módulo poderá utilizar ferramentas como language_tool_python ou serviços de análise linguística online para realizar essa verificação, futuramente complementando os demais critérios de avaliação. Além disso, a origem geográfica do e-mail pode fornecer informações valiosas sobre sua legitimidade. Muitos domínios e remetentes legítimos estão associados a regiões geográficas específicas. A localização do IP do remetente pode ser obtida por APIs como IPinfo.io ou GeoLite2. A Figura 5 apresenta uma requisição a API IPinfo.io, obtendo dados como país, cidade e organização associada ao IP.

Figura 5 – Trecho do código para consulta de geolocalização de IP utilizando a API do IPinfo.io.

```python
import requests

ip = '8.8.8.8'  # exemplo

url = f'https://ipinfo.io/{ip}/json'
resposta = requests.get(url)

if resposta.status_code == 200:
    dados = resposta.json()
    print("IP:", ip)
    print("Cidade:", dados.get('city'))
    print("Região:", dados.get('region'))
    print("País:", dados.get('country'))
    print("Org:", dados.get('org'))
else:
    print("Não foi possível obter informações do IP.")

```

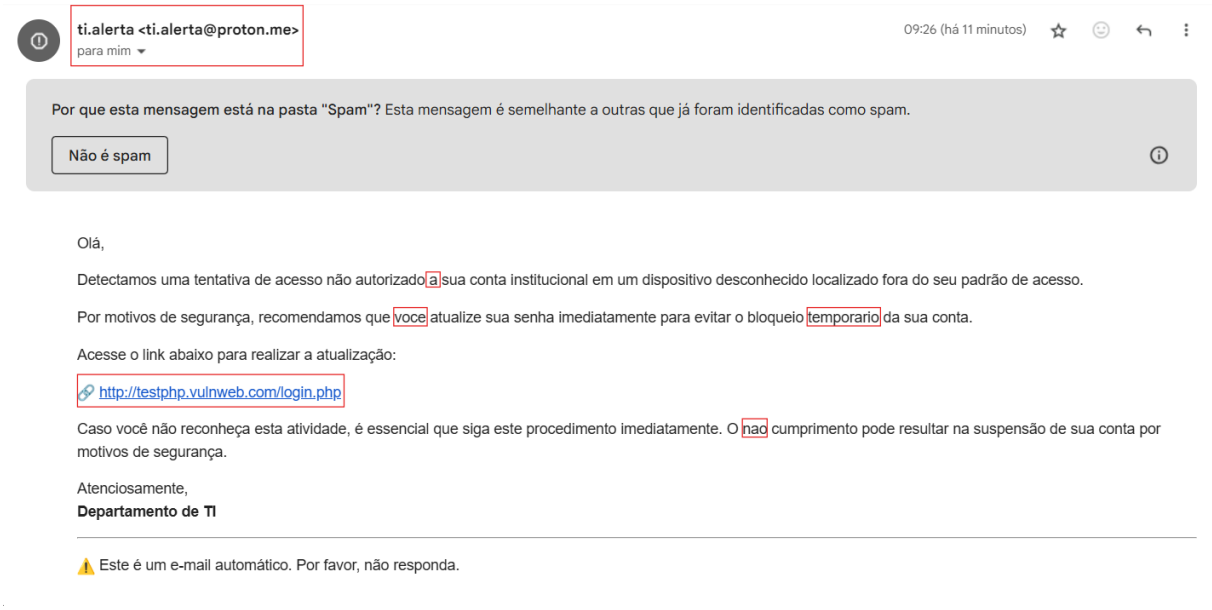
Fonte: Elaborado pelos autores (2025).

Com base nessas informações, é possível verificar se o e-mail está sendo enviado de uma região condizente com o domínio do remetente. Um exemplo seria um domínio registrado no Brasil, mas com o IP do remetente apontando para outro país, o que poderá indicar que o e-mail é suspeito.

Resultados

Apesar da ferramenta proposta ainda estar em fase de desenvolvimento, alguns testes foram realizados com scripts isolados, a fim de validar a viabilidade técnica das funcionalidades propostas, nesta seção iremos simular em um ambiente controlado uma tentativa de ataque de phishing. Os resultados simulados apresentados a seguir têm como objetivo ilustrar o funcionamento esperado de cada módulo da ferramenta. Durante os testes, o e-mail simulado foi automaticamente direcionado para a caixa de SPAM. Isso ocorreu, possivelmente, devido à combinação de fatores como: remetente com domínio genérico, ausência de autenticação SPF/DKIM/DMARC e presença de um link externo com linguagem de urgência no conteúdo. Esses elementos são comumente associados a tentativas de phishing e ativam os filtros antispam do provedor. No entanto, é importante destacar que nem todos os e-mails de phishing são automaticamente classificados como spam, especialmente aqueles mais sofisticados, com ofuscação de conteúdo, links encurtados, remetentes legítimos comprometidos ou engenharia social mais refinada. A Figura 6 apresenta um e-mail simulado utilizado no experimento. O teste realizado foi um projeto experimental controlado, sem técnicas de evasão, apenas para validar a estrutura básica da ferramenta.

Figura 6 – E-mail simulado de tentativa de phishing simples.



Fonte: Elaborado pelos autores (2025).

Na figura, observam-se alguns indicadores típicos de phishing:

- O nome de exibição do remetente é “ti.alerta”, mas o domínio real é @proton.me;
- Há erros ortográficos simples, como a ausência de acentuação em palavras como “à”, “você”, “temporário” e “não”;
- O link fornecido direciona para um domínio considerado vulnerável, pertencente ao site de testes mantido pela Acunetix.

Utilizando um arquivo de e-mail no formato .eml, o módulo de extração foi capaz de identificar corretamente os principais elementos da mensagem. A Figura 7 apresenta os dados extraídos de um e-mail simulado de phishing.

Figura 7 – Dados extraídos do e-mail simulado de phishing.

```
Remetente: "ti.alerta" <ti.alerta@proton.me>
Assunto: Alerta de segurança: atividade suspeita detectada em sua conta
Data: 2025-05-21 12:26:18+00:00
SPF: PASS
DKIM: PASS
DMARC: PASS
IPs_detectados: ['79.135.106.102']
Links_encontrados: ['http://testphp.vulnweb.com/login.php', 'http://testphp.vulnweb.com/login.php', 'http://testphp.vulnweb.com/login.php</a></p><p']
Anexos: []
```

Fonte: Elaborado pelos autores (2025).

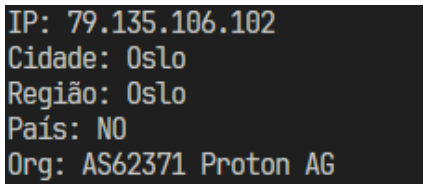
Utilizando dos links extraídos do e-mail, fazemos a verificação se há um certificado digital válido no site. A Figura 8 apresenta a verificação de certificado SSL presente no link, também foi utilizado o link https://gmail.com que contém certificado válido e vamos fazer a comparação.

Figura 8 –Verificação e comparação de certificados digitais em links.

Fonte: Elaborado pelos autores (2025).

Utilizando o IP extraído do cabeçalho do e-mail, foi realizada a análise de sua localização geográfica. A Figura 9 exibe o resultado da consulta por meio da API IPinfo.

Figura 9 –Resultado da geolocalização do IP do remetente.



Fonte: Elaborado pelos autores (2025).

Discussão

Os testes realizados com módulos isolados da ferramenta proposta permitiram validar, ainda que de forma preliminar, a viabilidade técnica da abordagem sugerida. A extração automatizada de informações a partir de arquivos .eml demonstrou ser eficaz para identificar remetente, assunto, links e anexos suspeitos. Essa funcionalidade é essencial, uma vez que grande parte dos ataques de phishing explora elementos simples do e-mail para enganar o usuário. Durante a simulação de um e-mail de phishing, observou-se que, embora os mecanismos de autenticação SPF, DKIM e DMARC tenham retornado resultados positivos (PASS), a mensagem foi automaticamente classificada como spam pelo provedor de e-mail.

Esse resultado evidencia que, embora importantes, esses protocolos de autenticação não são suficientes, de forma isolada, para atestar a legitimidade do conteúdo do e-mail nem impedem que filtros antispam avancem sobre outros fatores, como linguagem de urgência, presença de links suspeitos e reputação do domínio. Isso reforça a necessidade de um sistema que vá além das autenticações formais e análise aspectos estruturais e contextuais do e-mail.

A verificação dos links, por exemplo, possibilitou identificar certificados SSL/TLS válidos ou ausentes e fornecer informações como validade, emissor e impressões digitais. Já a análise da geolocalização do IP mostrou-se útil ao detectar discrepâncias entre o país de registro do domínio e a origem do IP, um indício recorrente em ataques sofisticados.

Esses testes demonstraram que uma solução multifatorial, baseada em diferentes critérios técnicos, pode aumentar significativamente a precisão na identificação de tentativas de phishing. Ao agregar múltiplas camadas de verificação, ao invés de depender apenas de listas negras ou filtros heurísticos, a ferramenta tem o potencial de reduzir tanto os falsos positivos quanto os falsos negativos. Outro diferencial da proposta é sua implementação local, sem dependência de nuvem, o que garante maior controle dos dados analisados e amplia sua aplicabilidade em ambientes corporativos e pessoais. Mesmo em fase de desenvolvimento, os resultados obtidos até aqui demonstram que a estrutura da ferramenta está alinhada com os principais desafios apontados pela literatura e representa uma abordagem promissora para ampliar a segurança digital dos usuários.

Considerações Finais

O desenvolvimento da ferramenta proposta neste trabalho tem como principal objetivo contribuir na mitigação de ataques de phishing, que permanecem entre as ameaças cibernéticas mais comuns e perigosas. Ao focar na análise técnica de e-mails e links suspeitos, a solução se apresenta como uma alternativa prática e eficiente para auxiliar na detecção de fraudes. É importante destacar que embora a tecnologia desempenhe um papel fundamental, ela sozinha não é capaz de garantir a prevenção completa; é igualmente necessária a conscientização dos usuários. Assim, a ferramenta atua não apenas na identificação de ameaças, mas também como instrumento de educação e alerta sobre os riscos da engenharia social. Espera-se que esta proposta incentive o desenvolvimento de soluções mais eficazes e acessíveis, além de promover maior atenção à segurança da informação em ambientes pessoais e corporativos

1) **Limitações:** Embora a ferramenta apresentada tenha como objetivo identificar e-mails e links suspeitos, ela possui algumas limitações. Em certos casos, ela poderá não ser capaz de detectar todos os tipos de phishing, especialmente aqueles baseados em técnicas de engenharia social mais sofisticadas ou métodos que ainda não foram documentados. Além disso, a precisão da ferramenta depende de fontes externas, como listas de domínios e IPs (Internet Protocol) confiáveis, que podem não estar sempre atualizadas ou completas. Outro ponto a ser considerado é que, por ser uma solução local, a ferramenta não possui integração com sistemas de defesa em tempo real, os quais poderiam aprimorar a detecção de ameaças à medida que estas surgem. Além disso, as soluções atuais de anti-phishing enfrentam diversas limitações que comprometem sua eficácia:

   a) **Eficácia Reduzida de Listas Negras:** Conforme observado por Moore e Clayton (2011), embora listas negras de URLs maliciosas ajudem na mitigação de ameaças, a relutância das empresas em compartilhar dados por questões de concorrência atrasa a remoção de sites fraudulentos, aumentando a exposição dos usuários a ataques.

   b) **Aproveitamento de Emoções Humanas:** Como apontado por Chaudry et al. (2016), ataques de phishing frequentemente utilizam estratégias de engenharia social para manipular emoções como medo, empatia e curiosidade, o que reduz a efetividade de soluções puramente técnicas.

   c) **Dificuldade na Detecção de Spoofing Avançado:** Jakobsson (2007) ressalta que os atacantes passaram a utilizar domínios legítimos com subdomínios enganosos ou domínios semelhantes (cousin domains), dificultando a detecção automática baseada em padrões de URL — um desafio que persiste até hoje, mesmo com a evolução dos mecanismos de detecção, destacado por D'Angelone (2023).

   d) **Sites Falsos de Curta Duração e Hospedagem Rotativa:** Outro apontamento feito por Jakobsson (2007) é o uso de botnets para hospedar sites falsos com tempo de vida muito curto (técnica conhecida como distributed phishing) que dificulta a ação de listas negras e mecanismos de bloqueio tradicionais.

e) **Limitações dos Sistemas de Segurança Tradicionais:** Bhardwaj et al. (2020) destacam que sistemas tradicionais de segurança de e-mail não são eficazes contra os ataques sofisticados como spear-phishing, whaling e fraudes com QR Codes, permitindo que essas ameaças avancem mesmo em ambientes corporativos protegidos.

2) **Trabalhos Futuros:** Como a área de segurança cibernética está em constante evolução, os próximos passos envolverão a expansão e aprimoramento das funcionalidades da ferramenta para lidar com novos tipos de ataques de phishing. Isso incluirá a integração com sistemas de defesa em tempo real e o aperfeiçoamento do algoritmo de detecção, por meio de técnicas como Machine Learning, com foco na adaptação às novas estratégias utilizadas pelos atacantes. Além disso, a ferramenta poderá ser estendida para analisar não apenas e-mails e links, mas também anexos e outras formas de comunicação, como mensagens de texto. Dessa forma, pretende-se evoluir continuamente os recursos da ferramenta, garantindo que ela acompanhe o surgimento de novas ameaças e proporcione os mecanismos de proteção adequados para enfrentá-las.

Referências:

AGAZZI, Alessandro Ecclesie. **Phishing and Spear Phishing: examples in Cyber Espionage and techniques to protect against them**. arXiv preprint, arXiv:2006.00577, 2020. Disponível em: https://doi.org/10.48550/arXiv.2006.00577.

BHARDWAJ, Akashdeep et al. **Why is phishing still successful?** Computer Fraud & Security, [S.l.], v. 2020, n. 9, p. 15-19, set. 2020. DOI: https://doi.org/10.1016/S1361-3723(20)30098-1.

BHAVSAR, Vaishnavi; KADLAK, Aditya; SHARMA, Shabnam. **Study on phishing attacks**. International Journal of Computer Applications, v. 182, n. 33, p. 27-29, 2018.

CHAUDHRY, Junaid; CHAUDHRY, Shafique Ahmad; RITTENHOUSE, Robert G. **Phishing attacks and defenses**. International Journal of Security and Its Applications, v. 10, n. 1, p. 247-256, 2016. Disponível em: http://dx.doi.org/10.14257/ijsia.2016.10.1.23.

D'ANGELONE, Marcello. **Email spoofing defence techniques: a comprehensive review and development of a novel measurement tool**. 2023. 80 f. Dissertação (Mestrado em Cyber Security) – National College of Ireland, Dublin, 2023. Disponível em: https://norma.ncirl.ie/id/eprint/7116.

JAKOBSSON, Markus. **The human factor in phishing**. Privacy & security of consumer information, v. 7, n. 1, p. 1-19, 2007.

KHADKA, Kalam. **Persuasion and phishing: analysing the interplay of persuasion tactics in cyber threats**. arXiv preprint arXiv:2412.18485, 2024. Disponível em: https://doi.org/10.48550/arXiv.2412.18485

KHADKA, Kalam et al. **A survey on the principles of persuasion as a social engineering strategy in phishing**. In: 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Exeter, United Kingdom, 01-03 Nov. 2023. Piscataway: IEEE, 2023. p. 1631-1638. DOI: 10.1109/TrustCom60117.2023.00222. Disponível em: https://doi.org/10.1109/TrustCom60117.2023.00222.

MOORE, Tyler; CLAYTON, Richard. **The impact of public information on phishing attack and defense**. Communications and Strategies, n. 81, p. 45-68, 2011. Disponível em: https://ssrn.com/abstract=2020325.

REDBELT SECURITY. **3,5 milhões de brasileiros foram vítimas de phishing em 2023, estima Redbelt Security.** 2024. Disponível em: https://www.cisoadvisor.com.br/35-milhoes-de-brasileiros-foram-vitimas-de-phishing-em-2023/.

SALVIANO, Edgard Mesquita; SANTOS, João Pedro Ribeiro; SILVA, Matheus Almeida. **Principais tipos de ataques Phishing e mecanismos de segurança**. 2022. Centro Universitário do Planalto Central Apparecido dos Santos (UNICEPLAC), 2022.

SECURITY LEADERS. **Pesquisa indica phishing como líder do ranking global dos ciberataques em 2024**. 2024. Disponível em: https://securityleaders.com.br/pesquisa-indica-phishing-como-lider-do-ranking-global-dos-ciberataques-em-2024/.

SILVA, Jhovana Cristina da; ANDRADE, Larissa Biasi de. **Estudo e aplicação do Phishing visando a conscientização da segurança cibernética entre usuários e organizações**. 2018. 73 f. Trabalho de Conclusão de Curso (Graduação em Tecnologia em Análise e Desenvolvimento de Sistemas) – Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, Catanduva, 2018. Disponível em: https://repositorio.ifsp.edu.br/handle/123456789/1182.

TANTI, Rajesh. **Study of phishing attack and their prevention techniques**. International Journal of Scientific Research in Engineering and Management, v. 8, n. 10, p. 1-8, 2024. DOI: 10.55041/IJSREM38042.

VENTURI, Andrea et al. **Classification of web phishing kits for early detection by platform providers**. arXiv preprint arXiv:2210.08273, 2022. Disponível em: https://doi.org/10.48550/arXiv.2210.08273.

XIONG, Aiping et al. **Embedding training within warnings improves skills of identifying phishing webpages**. Human Factors, v. 61, n. 4, p. 577-595, 2019. DOI: 10.1177/0018720818810942. Disponível em: https://doi.org/10.1177/0018720818810942.