risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 14/09/2025
Aceitação/Acceptance: 16/11/2025

StopEmailSpoofing: uma solução para detecção de vulnerabilidade de domínios à ataques falsificação de e-mail

Guilherme Dieguez Cândido[1], Igor Ramos Bezerra da Silva[1], Emílio Gonçalves[1], Leonardo de Paiva Souza[1], João Souza Neto[1], Rafael Rabelo Nunes[1]

guilherme.candido@aluno.unb.br; igorbramos1@unb.br; emilio.goncalves@aluno.unb.br; leonardops@unb.br; neto.joao@unb.br; rafaelrabelo@unb.br

[1] Departamento de Engenharia Elétrica, Universidade de Brasília (UnB), Campus Darcy Ribeiro, 70.910-900, Brasília – DF, Brasil

DOI: 10.17013/risti.60.57–73

Resumo: O e-mail permanece sendo o principal meio de comunicação contemporâneo, constituindo vetor frequente de ataques cibernéticos. Apesar da evolução dos sistemas de proteção, o fator humano continua sendo o elo mais fraco da segurança cibernética, sendo explorado por técnicas de engenharia social. Este trabalho apresenta a ferramenta de código aberto *StopEmailSpoofing*, desenvolvida para automatizar a detecção de vulnerabilidades de falsificação de e-mail em domínios. A ferramenta analisa todas as 295 combinações possíveis entre os protocolos SPF e DMARC, realizando consultas DNS para avaliar a suscetibilidade dos domínios. Diferentemente de soluções existentes, oferece cobertura completa dos protocolos de autenticação e sugere ações imediatas de correção. Uma validação foi realizada através de estudo de caso com instituições públicas de ensino superior brasileiras, demonstrando eficiência na identificação de falhas e contribuindo para o fortalecimento da resiliência das comunicações digitais organizacionais.

Palavras-chave: Falsificação de e-mail; SPF; DMARC; segurança cibernética; segurança das comunicações.

StopEmailSpoofing: a solution for detecting domains vulnerability to email spoofing attacks

Abstract: Email remains the primary means of contemporary communication, becoming a frequent vector for cyberattacks. Despite the evolution of protection systems, the human factor continues to be the weakest link in cybersecurity, being exploited by social engineering techniques. This work presents the open-source tool StopEmailSpoofing, developed to automate the detection of email spoofing vulnerabilities in domain names. The tool analyzes all 295 possible combinations between SPF and DMARC protocols, performing DNS queries to assess domain susceptibility. Unlike existing solutions, it offers complete coverage of authentication protocols and provides immediate corrective actions. Validation was performed through a case study with Brazilian public higher education institutions,

demonstrating efficiency in identifying failures and contributing to strengthening the resilience of organizational digital communications.

Keywords: Email spoofing; SPF; DMARC; Cybersecurity; Communications security.

1. Introdução

O e-mail tornou-se um dos principais meios de comunicação da sociedade contemporânea. Estima-se que, até 2027, cerca de 408,2 bilhões de mensagens sejam enviadas diariamente (Statista, 2025). Por ser fundamental na comunicação individual e corporativa, o e-mail também se torna um vetor de ataque amplamente explorado por fontes de ameaça (Shen et al., 2021).

A despeito da constante evolução da proteção de redes e sistemas, o fator humano permanece sendo o elo mais fraco da segurança cibernética. Em decorrência disso, atores maliciosos se valem cada vez mais de técnicas de engenharia social para conseguirem comprometer seus alvos (Hu & Wang, 2018). Neste sentido, a segurança de e-mails tem se tornado um tema central devido à dependência das comunicações digitais e ao surgimento de ameaças cada vez mais sofisticadas. Em um cenário em que grande parte das interações empresariais e pessoais ocorre via correio eletrônico, a garantia da autenticidade das mensagens e a proteção contra fraudes têm implicações diretas na continuidade dos negócios, na privacidade dos usuários e na salvaguarda de dados sensíveis (Carvalho et al., 2023).

Combinando conteúdo de e-mails de *phishing* sofisticados com técnicas de engenharia social, o ataque de falsificação de endereços de e-mail (também conhecido como *e-mail spoofing*) afeta bilhões de usuários em todo o mundo. Trata-se de uma atividade maliciosa que adultera o remetente de um e-mail e engana os destinatários, fazendo-os acreditar que a mensagem foi enviada por um remetente confiável, quando, na realidade, o remetente é o atacante (Yu et al., 2022). Desta forma, protocolos de autenticação, como SPF (*Sender Policy Framework*), DKIM (*DomainKeys Identified Mail*) e DMARC (*Domain-based Message Authentication, Reporting and Conformance*), tornaram-se ferramentas essenciais para organizações que buscam atestar a legitimidade de suas mensagens de e-mail (Carvalho et al., 2023).

1.1. Problema

Apesar da evolução das metodologias de detecção de mensagens com endereço de remetente falsificado, vulnerabilidades técnicas e operacionais persistem no que diz respeito à adoção e à correta configuração de protocolos como SPF e DMARC (Hu & Wang, 2018). Além disso, estudos como o de Nmachi (2023) destacam a importância de não concentrar esforços apenas nas características técnicas, mas também em como usuários e administradores compreendem o funcionamento desses mecanismos. Autores como Maroofi et al. (2021) apontam que grande parte das falhas decorre de implementações parciais ou configurações incorretas dos referidos protocolos, o que, em última análise, permite que invasores forjem remetentes de forma efetiva. Embora tenha havido avanços consideráveis, a elaboração de diretrizes práticas e de ferramentas

de suporte para a configuração e a manutenção desses protocolos ainda representam um desafio.

Neste trabalho, apresenta-se uma ferramenta de fácil utilização e de código aberto - denominada *StopEmailSpoofing* - que cobre todas as combinações possíveis entre as configurações dos referidos protocolos de autenticação, auxiliando administradores na automatização da detecção de vulnerabilidades de falsificação de e-mails em seus domínios e sugerindo ações detalhadas para a mitigação imediata do problema.

2. Referencial Teórico

Nesta seção, discorre-se sobre o funcionamento do ecossistema de correio eletrônico; mecanismos de autenticação de remetente em mensagens de e-mail; ataques de falsificação de endereço de e-mail e sua utilização em campanhas de *phishing*; e sobre as extensões *Simple Mail Transfer Protocol* (SMTP) criadas para a mitigação do problema. Por fim, elencam-se trabalhos correlatos.

2.1. Funcionamento do ecossistema de e-mail

O e-mail é amplamente utilizado em comunicações diárias, exercendo papel fundamental em conversas e transações confidenciais. Em muitos países e organizações, ele é o principal recurso para comunicações oficiais (Nmachi, 2023). Além disso, representa a ferramenta de comunicação mais adotada no mundo, sobretudo em ambientes empresariais (Gallo et al., 2024).

O SMTP é o principal protocolo para serviços de correio eletrônico. Quando um remetente redige uma mensagem, seu *Mail User Agent* (MUA) a transmite ao seu *Mail Transport Agent* (MTA) por meio dos protocolos SMTP ou HTTP. Em seguida, o MTA de origem encaminha o e-mail ao MTA de destino utilizando SMTP (Shen et al., 2021). Para isso, o servidor MTA de saída utiliza o *Domain Name System* (DNS) para encontrar o MTA do destinatário (Meshram et al., 2024). Por fim, o MTA de destino entrega a mensagem ao MUA do destinatário, usando protocolos como HTTP, IMAP ou POP3 (Shen et al., 2021).

2.2. Mecanismos de autenticação de remetente em mensagens de e-mail

A autenticação do remetente em uma troca de e-mails é fundamental para verificar se a mensagem realmente foi originada da fonte declarada (Maroofi et al., 2021).

Segundo Shen et al. (2021), a autenticação no processo de transmissão de e-mails envolve quatro etapas importantes: **(1) Autenticação no envio**: ao enviar um e-mail a partir do MUA via protocolo SMTP, o remetente precisa inserir seu nome de usuário e senha para autenticação. Nessa etapa, o MTA do remetente deve não apenas verificar a identidade do usuário, mas também garantir que o campo '*Mail From'* seja consistente com o '*Auth username*'; **(2) Verificação no recebimento**: o MTA do destinatário recebe o e-mail e valida a autenticidade do remetente por meio dos protocolos SPF, DKIM e DMARC; **(3) Renderização de interface**: o MUA fornece ao destinatário uma exibição amigável do e-mail. A maioria dos clientes de e-mail populares não

apresenta os resultados da verificação de autenticidade ao usuário; **(4) Verificação no encaminhamento de e-mails**: um servidor de encaminhamento reenvia automaticamente um e-mail, devendo verificar o endereço do remetente. Se a assinatura DKIM estiver ativa, o status original da verificação deve ser '*pass*' antes que uma nova assinatura DKIM seja adicionada.

2.3. Falsificação de endereço de e-mail em campanhas de *phishing*

As especificações do correio eletrônico datam da década de 1970, período em que aspectos de segurança não foram priorizados, deixando lacunas que persistem até hoje (Blechschmidt & Stock, 2023). Devido a sua importância e ampla utilização, o e-mail tornou-se um dos vetores de ataque mais explorados por atores maliciosos (Shen et al., 2021). As vulnerabilidades são exploradas de diversas maneiras, aproveitando tanto as fraquezas técnicas quanto as vulnerabilidades cognitivas dos usuários (Gallo et al., 2024).

Vítimas de ataques de *phishing* são frequentemente atraídas por mensagens que contêm anexos maliciosos ou levam a sites falsos cuidadosamente elaborados. A construção dos e-mails de *phishing* é a principal preocupação dos atacantes, que aplicam técnicas para aumentar a credibilidade de suas mensagens e utilizam estratégias para enganar as percepções da vítima (Gallo et al., 2024). Muitas vezes, as mensagens transmitem um senso de urgência ou autoridade, imitando comunicações de organizações conhecidas e confiáveis (D'Angelone, 2022).

Maroofi et al. (2020) classificam a falsificação de e-mail em dois tipos: **(1) Comprometimento de servidores legítimos**, quando os invasores comprometem servidores e utilizam seu MTA para enviar e-mails às vítimas; e **(2) Falsificação de domínio** (*domain spoofing*), quando os atacantes conseguem enviar e-mails, a partir de seus próprios servidores, em nome de domínios legítimos. A falsificação de endereços de e-mail é frequentemente utilizada por inúmeros cibercriminosos em tentativas de *phishing*. Ao criar uma mensagem, o ator malicioso pode fraudar os cabeçalhos '*From'* e *'Return-path'* da mensagem para que a mensagem pareça ter sido enviada de uma conta legítima e confiável (Sethuraman et al., 2024).

A segurança na transmissão de e-mails depende de uma cadeia de confiança multilateral, mantida por diversos serviços, o que aumenta sua vulnerabilidade sistêmica a ataques cibernéticos. No processo de comunicação via SMTP, as informações de identidade do remetente estão distribuídas de forma complexa em vários campos: **(1) *Auth username***, o nome de usuário utilizado no comando '*AUTH'* para autenticar o cliente no MTA de envio; **(2) *MAIL From***, o remetente que constará no envelope do e-mail, usado principalmente para verificação de identidade durante o processo de entrega da mensagem ao MTA de destino; **(3) *From***, o remetente exibido no corpo do e-mail, sendo o endereço que o MUA mostra ao destinatário; e; **(4) *Sender***, utilizado para identificar o remetente real quando há vários endereços no campo '*From'*. A inconsistência entre esses campos fornece a base para ataques de falsificação de endereços de e-mail (Shen et al., 2021).

2.4. Extensões SMTP: SPF, DKIM e DMARC

Para combater a falsificação de endereços e-mail, os servidores podem empregar extensões SMTP, como SPF, DKIM e DMARC para autenticar a identidade do remetente e exibir uma garantia de credibilidade para os usuários que lêem as mensagens (Chen, Paxson & Jiang, 2020). As extensões são publicadas em forma de registros TXT no DNS do domínio remetente. Como a implementação destes protocolos não é mandatória e depende exclusivamente do provedor de e-mails, os usuários finais não possuem influência sobre sua adoção (Hu & Wang, 2018).

Essas extensões definem regras sobre quem está autorizado a enviar mensagens em nome de um domínio e fornecem estratégias para combater e-mails falsificados. Quando configuradas adequadamente, podem eliminar o problema de falsificação de domínio por completo (Maroofi et al., 2020). Desta forma, a segurança de e-mail exige esforços bidirecionais: uma configuração correta dos protocolos por parte do remetente e uma validação rigorosa por parte do destinatário (Zhang et al., 2023). Configurações incorretas ou ausentes expõem as organizações a riscos de falsificação de domínios em ataques de *phishing* (Shen et al., 2021).

SPF

O SPF é um protocolo de autenticação baseado em endereço IP. Ele registra o domínio do remetente e vincula esse domínio a um IP específico, permitindo que o destinatário verifique, por meio de consulta DNS, se o e-mail realmente veio de um servidor autorizado (Shen et al., 2021). Durante a entrega do e-mail via SMTP, o servidor do destinatário autentica o MTA do remetente com base na identidade fornecida nos campos '*HELO*' ou '*MAIL From*, comparando o registro SPF publicado com o endereço IP do remetente (Maroofi et al., 2020). Um registro SPF versão 1 válido deve começar com a string *v=spf1*, seguida por outros mecanismos, qualificadores e modificadores. Os mecanismos descrevem o conjunto de servidores de e-mail autorizados para um domínio e podem ser prefixados com um dos quatro qualificadores: + *(Pass)*, - *(Fail)*, ~ *(SoftFail)* e *? (Neutral)*. Os mecanismos SPF mais comuns são:

- **ip4** e **ip6**: especificam um endereço, ou um conjunto de endereços, IPv4 (ou IPv6) a serem comparados com o endereço IP do remetente;
- **a** e **mx**: instruem a realizar primeiro uma consulta DNS para registros A (ou MX) de um determinado domínio e, em seguida, comparar os endereços IP retornados com o endereço IP do remetente;
- **include**: instrui a incluir a regra SPF de outro domínio na avaliação; e
- **all**: sempre corresponde; ou seja, seu qualificador correspondente determina a decisão final.

DKIM

O DKIM, por sua vez, baseia-se em assinaturas digitais. Utilizando criptografia de chave assimétrica, o remetente insere uma assinatura digital no cabeçalho do e-mail, o que possibilita a identificação de tentativas de falsificação ou adulteração durante a transmissão. O destinatário, ao receber a mensagem, consulta o DNS do remetente para obter a chave pública e verificar a assinatura, atestando se o e-mail foi ou não adulterado (Shen et al., 2021).

DMARC

Já o DMARC é um mecanismo de autenticação que atua com base nos resultados de SPF e DKIM. Especificamente, o DMARC adota uma lógica de '*OR*': se a mensagem for aprovada em ao menos um dos protocolos (SPF ou DKIM) e o campo *From* estiver alinhado com o identificador autenticado, o e-mail será considerado válido (Shen et al., 2021). A extensão compara os domínios verificados pelo SPF aos que estão listados no campo '*From'* do cabeçalho do e-mail por meio de um mecanismo de alinhamento que exige que esses domínios correspondam totalmente ou parcialmente. Por exemplo, o DMARC verifica se o domínio em *'MAIL From'* e em '*From'* são ou não compatíveis. No caso de falha no teste de alinhamento, a política DMARC pode definir o que fazer com a mensagem: aceitar, rejeitar ou colocar em quarentena (Maroofi et al., 2020). A seguir, elenca-se as *tags* DMARC que, quando configuradas incorretamente, podem ser exploradas por um adversário:

- **aspf (alinhamento para SPF)**: especifica se o modo de alinhamento estrito *'s'* ou relaxado *'r'* é exigido pelo proprietário do domínio. O valor padrão é o modo relaxado. No modo estrito, o nome de domínio usado no SPF deve ser exatamente o mesmo que o domínio utilizado no campo *'From'* do cabeçalho. No modo relaxado, qualquer subdomínio pode ser usado no campo *'From'* e ainda assim resultar em uma checagem válida;
- **p (política)**: define a ação a ser tomada pelo destinatário caso o teste de alinhamento resulte em *'FAIL'*. Os valores possíveis para essa *tag* são (1) *none*, nenhuma ação específica; (2) *quarantine*, a mensagem é considerada suspeita e pode ser entregue como *spam*; e (3) *reject*, o proprietário do domínio deseja rejeitar e-mails ainda durante a transação SMTP; e
- **sp (política para subdomínios)**: possui a mesma sintaxe da *tag 'p'*, mas se aplica aos subdomínios do domínio principal. Na ausência da *tag 'sp'*, a política definida na *tag 'p'* deve ser aplicada a todos os subdomínios. Se os subdomínios não forem usados para enviar e-mails, o proprietário pode definir essa *tag* com o valor *reject* para evitar falsificação de endereços de e-mails a partir de subdomínios.

Autenticação no Recebimento

O processo completo de verificação de autenticidade no recebimento da mensagem inicia-se pelo SPF, que faz a extração do domínio presente no campo '*Return-Path*' do cabeçalho da mensagem, juntamente com o endereço IP do servidor remetente. Em seguida, realiza uma consulta DNS para identificar a existência de um registro SPF associado a esse domínio. Caso o registro não exista, o resultado da verificação é '*SPF=NONE*'. Se o registro estiver presente, procede-se à validação para determinar se o endereço IP está autorizado a enviar mensagens em nome do domínio, conforme as regras especificadas no próprio registro (*-all, ~all, ?all, +all*). Quando o endereço IP está explicitamente autorizado, a autenticação resulta em '*SPF=PASS*'; caso contrário, ou se o registro estiver malformado, o resultado é '*SPF=FAIL'*.

O fluxo de autenticação continua com a validação DKIM, que se inicia verificando a presença do cabeçalho '*DKIM-Signature*' na mensagem. Caso ele esteja ausente ou malformado, o resultado é '*DKIM=NONE/ERROR'*. Se o cabeçalho existir, prossegue-

se à consulta DNS para o domínio especificado no parâmetro '*d=*', utilizando o seletor '*s=*', a fim de obter a chave pública correspondente. A ausência desse registro ou de uma chave pública válida resulta em '*DKIM=FAIL*'. Quando o registro é encontrado, verifica-se a **integridade** da mensagem calculando o *hash* do corpo da mensagem e comparando-o com o valor indicado no campo '*bh=*'. Se houver divergência, o resultado é '*DKIM=FAIL*'. Em caso de correspondência, passa-se à etapa de **autenticidade**, na qual o valor do campo '*b=*' é descriptografado com a chave pública e comparado ao *hash* dos cabeçalhos especificados no campo '*h=*'. Se os valores coincidirem, a autenticação é bem-sucedida e *'DKIM=PASS'*; caso contrário, o resultado é *'DKIM=FAIL'*.

Por fim, o DMARC verifica se existe um registro DMARC associado ao domínio que consta no campo '*From*'. Caso o registro esteja ausente ou malformado, o resultado é *'DMARC=NONE'*. Se o registro existir, o mecanismo avalia os resultados de SPF e DKIM. Quando ambos falham, ou seja, *'SPF=FAIL'* e *'DKIM=FAIL'*, a autenticação é considerada mal-sucedida e *'DMARC=FAIL'*. Contudo, se pelo menos um deles tiver sucesso e estiver alinhado com o domínio em '*From*' — isto é, se *'SPF=PASS'* e simultaneamente o domínio em '*Return-Path*' corresponder ao domínio em '*From*'; ou se '*DKIM=PASS*' e simultaneamente o domínio no parâmetro '*d=*' também corresponder ao de '*From*' —, o resultado é '*DMARC=PASS*'. Com base nesse resultado e na política *'p=*' definida no registro DMARC, o servidor de e-mail aplicará a ação especificada: ***reject*** (mensagem rejeitada), ***quarantine*** (mensagem enviada para quarentena ou pasta de *spam*) ou ***none*** (nenhuma ação específica, permitindo a entrega). Destaca-se que outras regras de filtragem *antispam* do servidor ou de ferramentas externas podem complementar o tratamento da mensagem, inclusive se sobrepondo à decisão final de DMARC.

Desta forma, observa-se ser fundamental que os domínios estabeleçam políticas apropriadas de SPF e DMARC para reduzir a chance de ataques bem-sucedidos. Por exemplo, a inexistência ou a definição de uma política fraca junto à extensão DMARC pode colocar um servidor de e-mails em uma posição difícil, pois nenhuma instrução para rejeitar um e-mail é dada quando SPF, DKIM ou ambos falham durante o processo de autenticação (Maroofi et al., 2021). Além disso, se o MTA do destinatário não oferecer suporte à verificação de SPF ou DMARC, independentemente do quão rigorosas sejam as regras adotadas pelo domínio remetente, elas não serão eficazes. Uma configuração incorreta de SPF ou DMARC é tão perigosa quanto a ausência dessas regras, pois o resultado da avaliação não levará a uma decisão acertada (Maroofi et al., 2020).

2.5. Trabalhos Correlatos

Diversas ferramentas para detecção de vulnerabilidades relacionadas à falsificação de endereços de e-mail já foram propostas. A solução *MXToolbox SuperTool*[1], por exemplo, constitui um utilitário unificado de avaliação de serviços de e-mail e DNS, integrando múltiplas funcionalidades de verificação em uma interface web. O sistema aceita domínios, endereços IP ou *hostnames* como entrada, mantendo histórico cronológico dos resultados para referência futura.

[1] https://mxtoolbox.com/SuperTool.aspx

D'Angelone (2022) desenvolveu uma ferramenta de medição em larga escala para pesquisas sobre adoção dos protocolos SPF e DMARC. O sistema, implementado em Python com arquitetura modular, opera através de um *crawler* de domínios que coleta dados de mais de 1,4 milhão de domínios utilizando APIs comerciais ou arquivos CSV. A ferramenta executa consultas DNS automatizadas para verificar a presença, configuração e políticas dos registros SPF e DMARC, normalizando os resultados e identificando erros de configuração. Os dados são processados e armazenados em formato CSV padronizado, permitindo análises comparativas e reprodução experimental.

Porém, a ferramenta de maior destaque é o *Spoofy*[2] (2023). Desenvolvida e disponibilizada em código-aberto por Matthew Keeley, é uma evolução das soluções *SpoofCheckSelfTest*[3] (2015) e *SpoofCheck*[4] (2016) da empresa Bishop Fox e oferece um diagnóstico automatizado da vulnerabilidade de domínios à falsificação de e-mail através da análise das configurações SPF e DMARC. O sistema executa consultas DNS autoritativas e implementa um algoritmo de decisão para determinar a suscetibilidade dos domínios à falsificação. Os resultados são processados através de uma tabela de combinações SPF e DMARC. Contudo, a referida tabela foi construída a partir de testes empíricos que consistiram no envio de mensagens falsificadas utilizando a ferramenta *EmailSpoofTest.com*[5] e na observação do comportamento de serviços como Gmail, ProtonMail e Microsoft 365 ao receber estas mensagens. Esta abordagem apresenta algumas limitações metodológicas.

Haja vista o objetivo de detectar a vulnerabilidade de domínios (e não de MTAs/MUAs), as medidas efetivas para reduzir a exposição a ataques de *spoofing* baseiam-se unicamente na correta configuração das extensões SMTP no DNS do domínio. Realizar o diagnóstico a partir do comportamento específico de determinados MTAs/MUAs pode levar a uma falsa conclusão de segurança. Isso porque o destinatário das mensagens falsificadas pode utilizar qualquer outro MTA/MUA que não tenha sido contemplado nos testes. É válido ressaltar que as decisões de autenticação de cada MTA/MUA podem diferir das orientações configuradas pelas extensões SMTP e serem complementadas, ou mesmo sobrepostas, por mecanismos de filtragem *antispam*.

Na mesma linha, a partir da abordagem escolhida, o *Spoofy* agrupa os estados de vulnerabilidade em 8 categorias, sendo algumas dessas classificadas como "Dependendo do *Mailbox*". Repisa-se que não se pode depender do comportamento do MTA/MUA para a avaliação da vulnerabilidade intrínseca a um domínio. Logo, uma ferramenta com o objetivo de avaliar a vulnerabilidade de um domínio a *spoofing* deveria concentrar-se unicamente nas configurações declaradas no DNS por meio das extensões SMTP, sem requerer resultados observados a partir da interpretação de MTAs/MUAs específicos. Somente assim seria possível fornecer uma avaliação alinhada às reais possibilidades de intervenção por parte dos administradores de domínio. Por fim, a tabela de combinações

[2] https://github.com/MattKeeley/Spoofy

[3] https://github.com/BishopFox/SpoofcheckSelfTest

[4] https://web.archive.org/web/20220211170519/https://github.com/BishopFox/spoofcheck

[5] https://emailspooftest.com/

do *Spoofy* não leva em consideração todas as combinações possíveis entre '*all*', '*aspf*', '*p*' e '*sp*'.

Desta forma, o presente estudo propõe um aprimoramento das soluções já existentes por: (1) cobrir todas as 295 possibilidades de combinação entre *'all'*, *'aspf'*, *'p'* e *'sp'* que podem influenciar na suscetibilidade de um domínio principal, bem como de seus subdomínios, à falsificação; (2) oferecer sugestões imediatas e precisas de mitigação personalizadas para cada domínio avaliado; e (3) verificar a possível adoção de DKIM e *Catch-All*.

3. Metodologia

Esta é uma pesquisa de natureza aplicada, haja vista ser uma investigação científica que busca resolver um problema prático e desenvolver uma solução específica para uma questão concreta, visando a aplicação imediata do conhecimento gerado. Tem caráter utilitário, direcionado a melhorias tecnológicas, processos ou intervenções em contextos reais.

A partir desta perspectiva, optou-se por uma abordagem qualitativa, que dispensa o uso de métodos e técnicas estatísticas, concentrando-se principalmente no seu processo e significado. Dessa forma, busca-se interpretar e atribuir sentido a um fenômeno do mundo real (Silva e Menezes, 2005).

Este estudo possui caráter exploratório, uma vez que tem como objetivo proporcionar maior familiaridade com o problema da falsificação de endereços de e-mail, com vistas a torná-lo mais explícito e construir hipóteses, aprimorando ideias e soluções (Gil, 2017).

4. Método, Resultados e Discussões

Com o objetivo de ajudar administradores a automatizar a detecção de vulnerabilidades a ataques de falsificação de endereço de e-mail contra seus domínios, propõe-se a ferramenta de código-aberto *StopEmailSpoofing*[6].

Os usuários podem fornecer uma lista ou um único domínio para a avaliação. Por meio de consultas DNS, além de verificar se os domínios fornecidos são principais ou subdomínios e obter registros SOA (*Start of Authority*), NS (*Nameserver*) e MX (*Mail Exchange*), a ferramenta coleta os registros SPF e DMARC e, considerando a configuração combinada desses registros, realiza conclusões quanto à suscetibilidade dos domínios analisados às categorias de vulnerabilidade à falsificação dispostas na Tabela 1. Por fim, a partir da conclusão quanto à vulnerabilidade do domínio, a ferramenta aponta ações detalhadas de mitigação para que o administrador possa sanar o problema, como exemplificado na Figura 1.

As conclusões sobre o estado de vulnerabilidade e as sugestões de mitigação são feitas a partir do que se dispõe em uma tabela[7] que relaciona todas as 295 combinações possíveis

[6] https://github.com/v1sc0/stopemailspoofing

[7] https://github.com/v1sc0/stopemailspoofing/blob/main/ULTIMATE_TABLE.xlsx

entre o mecanismo *'all'* do registro SPF e as *tags 'p', 'aspf'* e *'sp'* do registro DMARC, tanto para domínio principal quanto para subdomínios, conforme mostrado na Figura 2.

Para testes e confirmações empíricas, dois domínios foram adquiridos: um para agir como remetente e outro como destinatário. As extensões SMTP do domínio remetente foram configuradas no DNS de acordo com cada caso analisado. O domínio destinatário foi vinculado a um servidor de e-mails *mailcow*[8] com a solução *antispam Rspamd*[9] embutida, o que permitiu o controle personalizado da autenticação, análise e regras de processamento das mensagens.

	Categoria
1	A falsificação do domínio principal e de subdomínios é possível
2	Apenas a falsificação do domínio principal é possível
3	Apenas a falsificação de subdomínios é possível
4	Condição desconhecida (possivelmente vulnerável devido a erro de sintaxe nos registros)
5	A falsificação não é possível

Tabela 1 – Categorias de vulnerabilidade à falsificação consideradas pela ferramenta

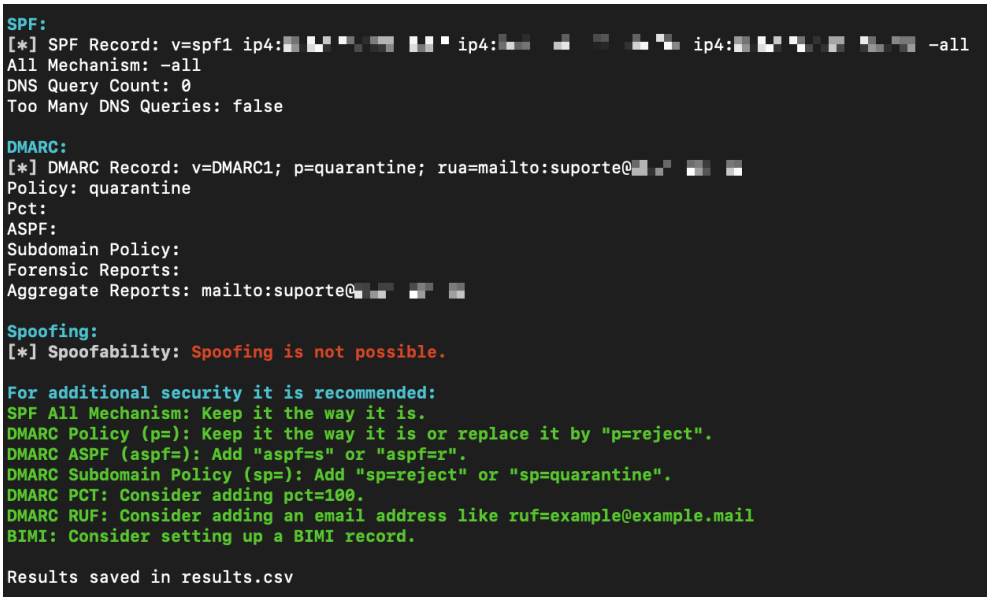

Figura 1 – Exemplo de saída da ferramenta com sugestões de mitigação

[8] https://mailcow.email/

[9] https://rspamd.com/

	ALL	P	ASPF	SP	DOMAIN TYPE	RESULT	SPOOFABILITY
261	~all	none	No aspf=	quarantine	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
					SUBDOMAIN	QUARANTINE	
262	~all	none	No aspf=	reject	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
					SUBDOMAIN	REJECT	
263	~all	none	r	No sp=	ORG. DOMAIN	INBOX	Organizational domain spoofing and subdomain spoofing are possible.
					SUBDOMAIN	INBOX	
264	~all	none	r	none	ORG. DOMAIN	INBOX	Organizational domain spoofing and subdomain spoofing are possible.
					SUBDOMAIN	INBOX	
265	~all	none	r	quarantine	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
					SUBDOMAIN	QUARANTINE	
266	~all	none	r	reject	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
					SUBDOMAIN	REJECT	
267	~all	none	s	No sp=	ORG. DOMAIN	INBOX	Organizational domain spoofing and subdomain spoofing are possible.
					SUBDOMAIN	INBOX	
268	~all	none	s	none	ORG. DOMAIN	INBOX	Organizational domain spoofing and subdomain spoofing are possible.
					SUBDOMAIN	INBOX	
269	~all	none	s	quarantine	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
					SUBDOMAIN	QUARANTINE	
270	~all	none	s	reject	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
					SUBDOMAIN	REJECT	
271	~all	quarantine	No aspf=	No sp=	ORG. DOMAIN	QUARANTINE	Spoofing is not possible.
					SUBDOMAIN	QUARANTINE	
272	~all	quarantine	No aspf=	none	ORG. DOMAIN	QUARANTINE	Only subdomain spoofing is possible.
					SUBDOMAIN	INBOX	
273	~all	quarantine	No aspf=	quarantine	ORG. DOMAIN	QUARANTINE	Spoofing is not possible.
					SUBDOMAIN	QUARANTINE	
274	~all	quarantine	No aspf=	reject	ORG. DOMAIN	QUARANTINE	Spoofing is not possible.
					SUBDOMAIN	REJECT	

Figura 2 – Exemplo de combinações de mecanismos e *tags* SPF/DMARC e a situação de vulnerabilidade correspondente consideradas pela ferramenta

Incrementalmente, a ferramenta também coleta os registros DKIM e BIMI (*Brand Indicators for Message Identification*). Ressalta-se que para a coleta de DKIM é necessário que se conheça o seletor *'s='* utilizado, o que somente seria possível com acesso a uma mensagem de e-mail legítima enviada a partir do domínio analisado. Desta forma, a ferramenta utiliza uma lista de 100 seletores conhecidos para realizar as consultas DNS e tentar identificar a presença de DKIM. Logo, a conclusão da ferramenta refere-se a ter ou não encontrado o registro DKIM e, em caso negativo, sugerir que o administrador certifique-se de ter configurado a extensão, uma vez que não é possível determinar com certeza que ela não foi adotada.

A ferramenta ainda verifica se o servidor de e-mail do domínio adota uma política de *catch-All*. *Catch-all* é uma configuração que permite que o servidor aceite mensagens enviadas para endereços inexistentes dentro do domínio. Em vez de rejeitar ou devolver as mensagens que foram enviadas para endereços errados, o servidor redireciona todas essas mensagens para uma conta de e-mail designada, chamada de *catch-all*. Isso pode ser útil para reduzir a enumeração e validação de endereços de e-mail por parte de atacantes, uma vez que a resposta dada pelo servidor SMTP não permitirá aos atacantes confirmarem a existência de endereços de e-mail coletados e que se tornariam alvos em uma campanha de *phishing*.

Todos os resultados das avaliações feitas pela ferramenta são apresentados em interface textual e exportados em formato CSV, permitindo integração com outras aplicações de tratamento e análise de dados. A ferramenta foi desenvolvida em Go (Golang), por ser uma linguagem de programação que oferece vantagens quanto a utilização, alteração e acréscimo de módulos. Um fluxograma da solução e uma descrição dos módulos desenvolvidos para a aplicação podem ser encontrados na Figura 3 e Tabela 2, respectivamente.

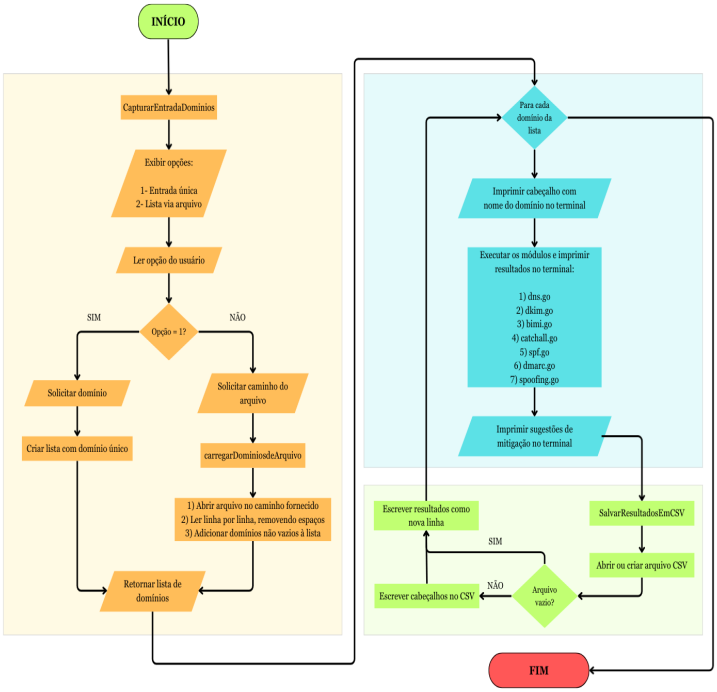

Figura 3 – Fluxograma de funcionamento da ferramenta proposta

Módulo	Descrição
dns.go	Classifica o nome informado como domínio ou subdomínio usando a biblioteca **publicsuffix**. Em seguida, **ObterSOARecord** consulta o registro SOA do domínio; se encontrado, armazena o nome do *nameserver* e procura seu endereço IP. Já **ObterMXRecords** busca registros MX para listar os servidores de e-mail associados.
catchall.go	Usa a biblioteca **AfterShip/email-verifier** para verificar se um domínio aceita e-mails para qualquer endereço. A função **NovoCatchAllVerifier** cria um verificador com checagem SMTP habilitada. O método **VerificarCatchAll** consulta se o domínio possui registro MX; em caso afirmativo, faz uma verificação SMTP para determinar se a caixa é *catch-all* e preenche a estrutura **CatchAllResult**.
dkim.go	Define a estrutura **DKIMResult** e a lista de 100 seletores padrão usados por muitos provedores. A função **VerificarDKIM** recebe uma lista de domínios, valida o nome de cada domínio e, para cada seletor padrão, monta uma consulta do tipo **seletor._domainkey.<domínio>**; se encontrar um registro TXT contendo a chave DKIM, marca o resultado como "SIM" e armazena o registro. Caso nenhum seletor retorne, indica que o DKIM não foi encontrado.
bimi.go	Define a estrutura **BIMI** com campos para domínio, servidor DNS e informações extraídas do registro BIMI. O construtor **NovoBIMI** consulta **default._bimi.<domínio>** via DNS, salvando o registro textual se este contiver "v=BIMI" e extraindo a versão, a localização do logotipo e a autoridade por meio das funções **ExtrairVersao**, **ExtrairLocalizacao** e **ExtrairAutoridade**. Caso o registro não exista, o campo **BIMIRecord** é definido como "BIMI não encontrado".

Módulo	Descrição
spf.go	A estrutura **SPF** inclui o domínio, registro SPF e informações derivadas. **NovoSPF** chama **ObterSPFRecord**, que procura nos registros TXT um início com "v=spf1"; se encontrado, armazena o registro. Depois, **ObterMecanismoAll** identifica o mecanismo ***all***; **ContarConsultasDNS** analisa recursivamente as diretivas *include* e *redirect*, bem como mecanismos **a**, **mx**, **ptr** e **exists**, para contar quantas consultas DNS o SPF realiza. Se esse número exceder 10, **TooManyDNSQueries** é marcado como verdadeiro.
dmarc.go	A estrutura **DMARC** guarda o domínio, servidor DNS e campos extraídos. **NovoDMARC** chama **ObterDMARCRecord** para consultar **_dmarc.<domínio>**; se o domínio for um subdomínio sem registro DMARC, tenta o domínio organizacional (eTLD+1). Após localizar um registro contendo "DMARC1", a estrutura extrai política (**p=**), percentual (**pct=**), alinhamento SPF (**aspf=**), política para subdomínios (**sp=**) e endereços para relatórios forenses e agregados.
spoofing.go	Define a estrutura **Spoofing** para combinar informações de SPF e DMARC. A função **CheckSpoofing** verifica várias combinações dessas configurações para determinar se é possível falsificar o domínio. Ela usa a tabela de condições para identificar cenários em que *spoofing* não é possível, é possível apenas para o domínio organizacional ou apenas para subdomínios, ou é totalmente possível. Retorna uma mensagem explicativa indicando o nível de vulnerabilidade.
suggestion.go	Oferece recomendações de segurança. A função **Suggestion** avalia o mecanismo *all* do SPF e as opções DMARC (*p*, *aspf* e *sp*). Dependendo dos valores, sugere manter, corrigir ou adicionar configurações

Tabela 2 – Módulos

As pesquisas sobre engenharia social e *phishing* têm levado ao desenvolvimento de técnicas de prevenção e capacitação em empresas, mas ainda existem áreas inexploradas, como ataques a instituições educacionais e abordagens específicas voltadas para docentes e estudantes (Camacho Coronel et al., 2024). Considerando-se que a segurança cibernética vem ganhando papel de destaque e mostrando-se imprescindível para os avanços na transformação digital brasileira, inclusive no setor público (Georg et al., 2022), realizou-se um estudo de caso com os domínios relacionados a todas as instituições públicas de ensino superior brasileiras a fim de validar a eficiência da ferramenta desenvolvida. Este grupo específico de instituições foi escolhido por constituir uma área da administração pública que desenvolve pesquisas, tecnologias e conhecimentos sensíveis, sendo flagrante a importância da mitigação de vulnerabilidades de falsificação de endereços de e-mail para combater campanhas de *phishing* que possam comprometer esta produção.

Uma lista das instituições de ensino superior brasileiras foi obtida a partir do *website* do Ministério da Educação[10]. A lista foi filtrada para conter apenas as instituições públicas, resultando num universo de 345 instituições. Os nomes de domínio destas instituições foram coletados utilizando-se técnicas de Inteligência de Fontes Abertas (OSINT). Por fim, a lista final com os 345 nomes de domínio foi submetida à ferramenta *StopEmailSpoofing*. Os resultados são apresentados na Tabela 3 e referem-se a agosto de 2025. Nota-se que cerca de 80% dos nomes de domínio das instituições públicas de ensino superior brasileiras estão vulneráveis a falsificação de e-mail. Isso comprova

[10] https://dadosabertos.mec.gov.br/images/conteudo/Ind-ensino-superior/2022/PDA_Lista_Instituicoes_Ensino_Superior_do_Brasil_EMEC.csv

a persistência do problema e implica dizer que, na grande maioria destas instituições, atacantes podem enviar mensagens de e-mail se passando por reitores, alunos, professores e pesquisadores para aumentar a credibilidade de campanhas de *phishing* e obter acesso a conhecimentos e tecnologias sensíveis produzidos por institutos e universidades.

		Parâmetros	Quantidade	Porcentagem
Nome de Domínio		Domínio	288	83,48%
Subdomínio			57	16,52%
SPF		Inexistente	71	20,58%
+all			0	0,00%
-all			106	30,72%
~all			151	43,77%
?all			16	4,64%
DKIM		Encontrado	155	44,93%
Não encontrado			190	55,07%
DMARC	p	Inexistente	136	39,42%
		none	113	32,75%
		quarantine	77	22,32%
		reject	18	5,22%
	sp	Inexistente	291	84,35%
		none	37	10,72%
		quarantine	11	3,19%
		reject	6	1,74%
Vulnerabilidade		Não vulnerável	71	20,58%
Apenas domínio principal vulnerável			0	0,00%
Apenas subdomínios vulneráveis			23	6,67%
Domínio principal e subdomínios vulneráveis			249	72,17%
Erro de sintaxe (vulnerável)			2	0,58%

Tabela 3 – Análise dos domínios de instituições públicas federais brasileiras de ensino superior a partir da ferramenta proposta (ago. 2025)

5. Conclusões

Este trabalho teve como objetivo desenvolver uma ferramenta para detecção da vulnerabilidade de domínios a ataques de falsificação de endereços de e-mail, ataques estes que - a despeito de configurarem um problema antigo - ainda são muito explorados atualmente. A ferramenta foi projetada para avaliar a implementação e configuração de protocolos como SPF, DKIM e DMARC, oferecendo diagnósticos detalhados sobre

a exposição de domínios a ataques de *spoofing*. Os testes demonstraram que a solução é oportuna e que pode auxiliar administradores e equipes de segurança na detecção de falhas e na pronta adoção de medidas corretivas. A principal contribuição deste estudo está na automatização e na completude da verificação das extensões de autenticação de e-mails, fornecendo um mecanismo eficiente e acessível para fortalecer a segurança e a resiliência das comunicações digitais. Entretanto, algumas limitações foram observadas. A solução apresentada cobre apenas a autenticação no recebimento de mensagens de e-mail. Ataques avançados - que não foram considerados na atual abordagem da ferramenta - exploram falhas durante a renderização do remetente pelo MUA do destinatário.

Para trabalhos futuros, sugere-se a ampliação do escopo da ferramenta para poder atuar como um MTA destinatário e avaliar mensagens de e-mail submetidas pelos usuários. Além disso, a integração de técnicas de aprendizado de máquina na detecção de padrões suspeitos em tráfego de e-mail também se apresenta como uma possibilidade futura de estudo. Essas melhorias poderão tornar a ferramenta *StopEmailSpoofing* ainda mais robusta e eficaz na mitigação e no combate a ameaças associadas à falsificação de endereços de e-mail.

Referências

Blechschmidt, B., & Stock, B. (2023). Extended Hell(o): A comprehensive large-scale study on email confidentiality and integrity mechanisms in the wild. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23) (pp. 4895–4912). USENIX Association. https://www.usenix.org/conference/usenixsecurity23/presentation/blechschmidt

de Carvalho, F. N., Tramontina, P. R., da Silva, W. R., & Misaghi, M. (2023). O emprego de DMARC para aprimoramento de proteção de e-mail: Um relato de caso. Revista Foco, 16(10), e3123. https://doi.org/10.54751/revistafoco.v16n10-074

Chen, J., Paxson, V., & Jiang, J. (2020). Composition kills: A case study of email sender authentication. In Proceedings of the 29th USENIX Security Symposium (USENIX Security 20) (pp. 2183–2199). USENIX Association. https://www.usenix.org/conference/usenixsecurity20/presentation/chen-jianjun

Camacho Coronel, A., Erazo Ayón, J. M., Salazar Tovar, C., & Pardo Centanaro, B. (2024). Ingeniería social: Revisión sistemática de phishing y pretexting en plataformas académicas. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (E72), 122–136. https://www.risti.xyz/issues/ristie72.pdf

D'Angelone, M. (2022). Email spoofing defence techniques: A comprehensive review and development of a novel measurement tool. School of Computing, National College of Ireland. https://norma.ncirl.ie/7116/1/marcellodangelone.pdf

Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. Computers & Security, 139, 103671. https://doi.org/10.1016/j.cose.2023.103671

Georg, M. A. C., Rodrigues, W. M. S., Alves, C. A. M., Silveira Junior, A., & Nunes, R. R. (2023). Os desafios da segurança cibernética no setor público federal do Brasil: Estudo sob a ótica de gestores de tecnologia da informação. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (E54), 602–616. https://doi.org/10.5281/zenodo.7855320

Gil, A. C. (2017). Como elaborar projetos de pesquisa (6th ed.). Atlas.

Hu, H., & Wang, G. (2018). End-to-end measurements of email spoofing attacks. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18) (pp. 1095–1112). https://www.usenix.org/conference/usenixsecurity18/presentation/hu

Maroofi, S., Korczyński, M., & Duda, A. (2020). From defensive registration to subdomain protection: Evaluation of email anti-spoofing schemes for high-profile domains. In Traffic Monitoring and Analysis. https://api.semanticscholar.org/CorpusID:219956390

Maroofi, S., Korczyński, M., Hölzel, A., & Duda, A. (2021). Adoption of email anti-spoofing schemes: A large-scale analysis. IEEE Transactions on Network and Service Management, 18(3), 3184–3196. https://doi.org/10.1109/TNSM.2021.3065422

Meshram, B. B., Mendhe, V., & Singh, M. K. (2024). Tracing the invisible threads: A deep dive into email security and forensics. International Journal of Enhanced Research in Science, Technology & Engineering, 13(1), 14-42. https://doi.org/10.55948/IJERSTE.2024.0104

Nmach, W. P. (2023). A framework for securing email entrances and mitigating phishing impersonation attacks. International Journal of Network Security & Its Applications, 15(6), 15-35. https://doi.org/10.5121/ijnsa.2023.15602

Silva, E. L., & Menezes, E. M. (2005). Metodologia da pesquisa e elaboração de dissertação. Universidade Federal de Santa Catarina.

Sethuraman, S. C., V. S., D. P., Reddi, T., Reddy, M. S. T., & Khan, M. K. (2024). A comprehensive examination of email spoofing: Issues and prospects for email security. Computers & Security, 137, 103600. https://doi.org/10.1016/j.cose.2023.103600

Shen, K., Wang, C., Guo, M., Zheng, X., Lu, C., Liu, B., Zhao, Y., Hao, S., Duan, H., Pan, Q., & Yang, M. (2021). Weak links in authentication chains: A large-scale analysis of email sender spoofing attacks. In Proceedings of the 30th USENIX Security Symposium (USENIX Security 21) (pp. 3201–3217). https://www.usenix.org/conference/usenixsecurity21/presentation/shen-kaiwen

Statista. (n.d.). Daily number of e-mails worldwide. Retrieved April 5, 2025, from https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide

Yu, B., Li, P., Liu, J., Zhou, Z., Han, Y., & Li, Z. (2022). Advanced analysis of email sender spoofing attack and related security problems. In 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud) / 2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 80–85). IEEE. https://doi.org/10.1109/CSCloud-EdgeCom54986.2022.00023

Zhang, H., Chen, L., Liu, M., Shi, Y., Wu, S., & Xue, Z. (2023). Both sides needed: A two-dimensional measurement study of email security based on SPF and DMARC. In 2023 19th International Conference on Mobility, Sensing and Networking (MSN) (pp. 855–861). IEEE. https://doi.org/10.1109/MSN60784.2023.00126