

# Relatório Técnico – Análise de Cabeçalhos de E-mail

**Processo:** Processo Penal n.º 2023/0456 – Burla Informática por Phishing – Transferências Fraudulentas de €32 000

**Data:** 15 de março de 2024

**Emitente:** Peritório de Informática Forense – Unidade de Perícias do Tribunal Judicial de Lisboa

**Peritos Responsáveis:** Eng. Carlos Mendes (N.º de Perito 00123), Eng. Sofia Ribeiro (N.º de Perito 00124)

---

## 1. Identificação do Objeto

O presente relatório tem por finalidade **detalhar a análise dos cabeçalhos dos e-mails de phishing** que foram utilizados pelo réu **João da Silva**, residente em Lisboa, no âmbito da prática tipificada no artigo 217.º do Código Penal (burla informática). A análise visa identificar eventuais falsificações de remetente (spoofing) e outras manipulações que permitiram a ilusão de legitimidade junto das vítimas, resultando em transferências bancárias fraudulentas no montante total de **€32 000**, efetuadas entre 10 e 25 de março de 2023.

---

## 2. Contexto Processual

| Campo                        | Informação   |
|------------------------------|--|
| <b>Autor/Requerente</b>      | Ministério Público – Secção de Instrução Criminal, Tribunal Judicial de Lisboa |
| <b>Réu/Requerido</b>         | João da Silva, residente na Rua da Palma, 45, 1.º Esq., 1150-064 Lisboa        |
| <b>Mandatários da Defesa</b> | Dr. Ana Pereira (OA 12345), Dr. Luís Carvalho (OA 67890)                       |
| <b>Mandatária do MP</b>      | Dr. Marta Santos (OA 54321)  |
| <b>Juiz de Instrução</b>     | Juiz de Instrução Criminal nº 4 do Tribunal Judicial de Lisboa                 |
| <b>N.º do Processo</b>       | 2023/0456  |
| <b>Objeto da Perícia</b>     | Análise dos cabeçalhos dos e-mails enviados entre 10/03/2023 e 25/03/2023      |

---

## 3. Metodologia

- Aquisição dos e-mails** – Os e-mails foram extraídos dos servidores de correio eletrónico das vítimas (Banco Português de Investimento – BPI, e-mail corporativo **conta@bpi.pt**) mediante ordem judicial de preservação de dados.
- Preservação da Cadeia de Custódia** – Cada mensagem foi armazenada em formato **.eml** com hash SHA-256, garantindo a integridade da prova.
- Ferramentas de Análise** – Utilizou-se o software **MailXplorer 5.2**, complementado por scripts **Python** (bibliotecas **email**, **dkimpy**, **spf**) para extração e validação dos campos de cabeçalho.
- Verificação de Autenticidade** – Foram efetuados testes de:
  - SPF (Sender Policy Framework)** – comparação do endereço IP de envio com os registos DNS autorizados.
  - DKIM (DomainKeys Identified Mail)** – validação da assinatura digital.
  - DMARC (Domain-based Message Authentication, Reporting & Conformance)** – análise da política de alinhamento.

5. **Cross-checking** – Correlation with logs de servidores de correio (SMTP) da vítima e do suposto remetente (domínio **bpi.pt**).

#### 4. Análise dos Cabeçalhos

A seguir, apresentamos um exemplo representativo de um dos e-mails analisados (Mensagem ID 20230315.123456@bpi.pt), com destaque para os campos críticos.

| Campo               | Valor Extraído  | Observação  |
|---------------------|---|---|
| <b>Received (1)</b> | from <b>mail.outlook.com</b> (209.85.220.41) by <b>mx.bpi.pt</b> (212.150.10.5) with <b>SMTP</b> id <b>A1B2C3D4</b> ; Fri, 15 Mar 2023 09:12:34 +0000 | IP de origem <b>não</b> pertence ao range autorizado pelos registos SPF de <i>bpi.pt</i> .              |
| <b>Received (2)</b> | from [10.0.0.5] (unknown [10.0.0.5]) by <b>mail.outlook.com</b> with <b>ESMTPS</b> id <b>X9Y8Z7</b> ; Fri, 15 Mar 2023 09:12:33 +0000                 | Endereço interno não resolvido publicamente – indica origem interna de um cliente Outlook comprometido. |
| <b>From</b>         | <b>conta@bpi.pt</b>   | Domínio aparenta ser legítimo, porém <b>não</b> corresponde ao endereço IP de envio.                    |
| <b>Reply-To</b>     | <b>seguranca@bpi.pt</b>   | Endereço válido, mas não utilizado no fluxo de entrega.   |
| <b>Subject</b>      | <b>Urgente – Atualização de Dados de Segurança</b>  | Título genérico, comum em campanhas de phishing.  |
| <b>Message-ID</b>   | <20230315.123456@bpi.pt>  | Formato coerente, porém o domínio do Message-ID não tem assinatura DKIM.                                |

| Campo                         | Valor Extraído  | Observação  |
|-------------------------------|---|---|
| <b>DKIM-Signature</b>         | <i>Ausente</i>  | Falta de assinatura digital – violação da política DMARC de <i>bpi.pt</i> .                                 |
| <b>SPF-Result</b>             | <b>softfail</b> (domain of sender does not designate 209.85.220.41 as permitted sender)   | Indicador de possível falsificação.   |
| <b>Authentication-Results</b> | mx.bpi.pt; spf=softfail (google.com: domain of bpi.pt does not designate 209.85.220.41 as permitted sender) ; dmarc=fail (p=reject) | Falha nas três camadas de autenticação.   |
| <b>X-Originating-IP</b>       | <b>209.85.220.41</b>  | IP público da Google (serviço de envio de Outlook.com) – incompatível com a política SPF de <i>bpi.pt</i> . |

#### 4.1. Principais Indícios de Spoofing

1. **Desalinhamento entre o domínio “From” e o IP de origem** – O endereço IP que efetuou a entrega (209.85.220.41) pertence a servidores da Microsoft (Outlook.com) e não consta nos registos SPF de *bpi.pt*.
2. **Ausência de assinatura DKIM** – O domínio *bpi.pt* utiliza DKIM (selector **mail**); a mensagem não apresenta o cabeçalho **DKIM-Signature**, indicando que não foi assinada pela infraestrutura oficial.
3. **Falha DMARC** – A política DMARC de *bpi.pt* está configurada para **p=reject**; o relatório de resultados indica **dmarc=fail**, confirmando a tentativa de falsificação.
4. **Uso de “Reply-To” legítimo** – Estratégia típica de phishing para reforçar a credibilidade, mas não tem efeito na autenticação do remetente.

#### 5. Conclusões

1. **Falsificação de remetente confirmada** – A análise dos cabeçalhos demonstra, de forma inequívoca, que os e-mails foram enviados a partir de servidores externos (Outlook.com) que não estão autorizados pelos registos SPF do domínio *bpi.pt*, não possuem assinatura DKIM e violam a política DMARC. Estas circunstâncias configuram falsificação de remetente (spoofing) nos termos do artigo 217.º, n.º 1, alínea b) do Código Penal.
2. **Relação causal com as transferências fraudulentas** – O conteúdo do e-mail, ao solicitar “atualização de dados de segurança”, induziu as vítimas a aceder a um portal falsificado que recolheu credenciais bancárias, permitindo a execução das transferências de €32 000 entre 10 e 25 de março de

2023.

3. **Responsabilidade do réu** – Os registos de IP internos (10.0.0.5) apontam para um equipamento que, segundo a perícia de rede, estava associado ao utilizador **João da Silva** (MAC 00-1A-2B-3C-4D-5E). A correlação temporal entre o acesso ao equipamento e o envio dos e-mails reforça a imputação de autoria.

---

## 6. Recomendação ao Tribunal

1. **Acrescer o laudo pericial ao processo** como prova documental de falsificação de remetente e de manipulação de credenciais.
2. **Ordenar a preservação dos logs de SMTP** dos servidores de correio da Microsoft (Outlook.com) para eventual cooperação internacional, caso se revele necessário.
3. **Recomendar à entidade bancária BPI a implementação de filtros avançados** (SPF, DKIM, DMARC reforçados) e a consciencialização dos seus clientes quanto a e-mails de solicitação de dados sensíveis.

---

## 7. Anexos

### Anexo A – Cabeçalho completo da Mensagem ID 20230315.123456@bpi.pt

Delivered-To: conta@bpi.pt  
Received: from mail.outlook.com (209.85.220.41) by mx.bpi.pt (212.150.10.5) with SMTP id A1B2C3D4; Fri, 15 Mar 2023 09:12:33 +0000  
Received: from [10.0.0.5] (unknown [10.0.0.5]) by mail.outlook.com with ESMTPS id X9Y8Z7; Fri, 15 Mar 2023 09:12:33 +0000  
Date: Fri, 15 Mar 2023 09:12:33 +0000  
From: conta@bpi.pt  
Reply-To: seguranca@bpi.pt  
Subject: Urgente - Atualização de Dados de Segurança  
Message-ID: <20230315.123456@bpi.pt>  
MIME-Version: 1.0  
Content-Type: text/html; charset=UTF-8  
X-Originating-IP: 209.85.220.41  
Authentication-Results: mx.bpi.pt; spf=softfail (google.com: domain of bpi.pt does not designate 209.85.220.41)

### Anexo B – Registo SPF do domínio *bpi.pt* (consultado em 12/03/2024)

bpi.pt. IN TXT "v=spf1 ip4:212.150.0.0/16 ip4:185.23.0.0/16 -all"

---

## Assinaturas

---

Eng. Carlos Mendes – Perito de Informática Forense  
N.º de Perito 00123

---

Eng. Sofia Ribeiro – Perito de Informática Forense  
N.º de Perito 00124

*Documento emitido eletronicamente em conformidade com o artigo 26.º do Código de Processo Civil.*