

# Tribunal Judicial de Lisboa

Juízo de Instrução Criminal n.º 4

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

## Prova Eletrónica

E-mail de Phishing – Mensagem Recebida em 18 de março de 2023

**Autor/Requerente:** Ministério Público, representado por **Dr<sup>a</sup>. Marta Santos**, Procuradora do Ministério Público (OA 54321)

**Réu/Requerido:** João da Silva, residente em Rua das Flores, 45, 1.º Dto., 1150-123 Lisboa

### 1. Identificação da prova

Campo	Conteúdo
<b>Tipo de prova</b>	Mensagem eletrónica (e-mail) – phishing
<b>Data de receção</b>	18 de março de 2023, às 09:42:17 (GMT+0)
<b>Remetente</b>	<i>admin@securebank-alert.com</i>
<b>Destinatário</b>	<i>maria.fernandes@email.pt</i>
<b>Assunto</b>	<b>“Alerta de Segurança – Ação Imediata Necessária”</b>
<b>Formato do ficheiro</b>	.eml (RFC 5322)
<b>Hash SHA-256</b>	<b>3F9A1C4E7B2D8C5F6A9E0B1D4C7F2A3E5D8C9B0A7E6F4D3C21</b>
<b>Procedimento de captura</b>	Extração forense com <b>FTK Imager 4.5</b> , preservação da cadeia de custódia, data de captura 05 de abril de 2023, hora 14:15:00 (GMT+0).
<b>Armazenamento</b>	Servidor de provas eletrónicas do Tribunal Judicial de Lisboa – pasta “2023/0456/PROVA-E-MAIL-20230318”.

### 2. Cabeçalho completo (RFC 5322)

From: "SecureBank Alert" <admin@securebank-alert.com>  
To: "Maria Fernandes" <maria.fernandes@email.pt>  
Date: Sat, 18 Mar 2023 09:42:17 +0000  
Subject: Alerta de Segurança - Ação Imediata Necessária  
Message-ID: <20230318094217.12345.securebank-alert.com@securebank-alert.com>  
MIME-Version: 1.0  
Content-Type: text/html; charset="UTF-8"  
X-Priority: 1 (Highest)  
X-Mailer: Microsoft Outlook 16.0  
Received: from mail.securebank-alert.com (mail.securebank-alert.com [185.23.45.67])  
by mail.lisboa.pt (Postfix) with ESMTPS id 7A9C3E01B3  
for <maria.fernandes@email.pt>; Sat, 18 Mar 2023 09:42:19 +0000 (UTC)

### 3. Conteúdo da mensagem (texto integral)

Prezada Sra. Maria Fernandes,

Detectámos uma atividade suspeita na sua conta bancária da **SecureBank** que requer a sua intervenção imediata.

**Detalhes da suspeita:**

- Tentativa de login a partir de um endereço IP desconhecido (185.23.45.78).
- Transferência de €5 000,00 pendente de validação.

Para evitar a suspensão da conta, **clique no link abaixo** e confirme a sua identidade:

[ <https://securebank-alert.com/verify?token=9f8e7d6c5b4a3> ]

Ao validar a sua identidade, a SecureBank garantirá a continuação do serviço e bloqueará quaisquer tentativas futuras de acesso não autorizado.

Caso não reconheça esta atividade, **não clique no link** e contacte imediatamente a nossa linha de apoio ao cliente 24h pelo número **800 123 456**.

Atenciosamente,

**Equipe de Segurança – SecureBank**  
admin@securebank-alert.com

*Nota:* O link acima redireciona para um site falsificado que reproduz a interface de login da SecureBank, recolhendo as credenciais da vítima para posterior transferência ilícita de fundos.

---

#### 4. Certificação de autenticidade

**Certifico**, ao abrigo do artigo 225.º do Código de Processo Civil, que a presente prova eletrónica foi extraída integralmente do servidor de correio eletrónico da vítima, **Maria Fernanda Fernandes**, NIF 123 456 789, com a sua autorização expressa, e que foram observados todos os requisitos de preservação da cadeia de custódia previstos no Decreto-Lei n.º 33/2008, de 5 de fevereiro, que regula a prova eletrónica nos processos judiciais.

A captura foi realizada mediante software de preservação forense reconhecido (FTK Imager 4.5), garantindo a integridade do ficheiro e a produção do hash SHA-256 acima indicado, que permite a verificação posterior da não-alteração da prova.

**Lisboa, 12 de abril de 2023**

---

**Dr<sup>a</sup>. Marta Santos** – Procuradora do Ministério Público (OA 54321)

---

#### 5. Relevância probatória

1. **Continuidade da campanha de phishing** – O e-mail demonstra a utilização de um modelo de mensagem padrão, idêntico a outras comunicações já analisadas nas diligências periciais, reforçando a tese de que o réu, João da Silva, coordenou ou participou na elaboração e distribuição da campanha.
  2. **Ligação ao crime de burla informática** – O link fraudulento, ao capturar credenciais da vítima, permitiu a posterior realização das transferências bancárias fraudulentas que totalizam €32 000, configurando a materialização da conduta descrita no artigo 217.º do Código Penal.
  3. **Identificação do remetente falsificado** – O domínio *securebank-alert.com* foi registado em 02 de janeiro de 2023, com dados de contacto falsificados, o que corrobora a intenção deliberada de enganar a vítima.
-

## 6. Conclusão

A presente prova eletrónica, devidamente autenticada e preservada, integra o conjunto de elementos probatórios que demonstram a prática de burla informática por phishing, sendo indispensável para a instrução do processo penal n.º 2023/0456.

---

*Documento elaborado e apresentado em conformidade com o disposto no Código de Processo Penal e nas normas de prova eletrónica aplicáveis.*