

Phishing Email Analysis Report

Basic Details

Subject: British Airways £300 Travel Voucher


Sender Name (Displayed): British Airways

Recipient Name: John (personalized)


Attachment/Link: Voucher attachment claimed; login URL shown

Step-by-Step Analysis


Step 1: Examine the Sender's Email Address

- Screenshot Limitation: The actual email address of the sender is not visible.
- Reason for Concern: Phishing emails often spoof brand names and display legitimate-looking names like "British Airways" but use fraudulent domains (e.g., @british-airways-voucher.com).
-  What to Check: Always inspect the full sender address for suspicious or unfamiliar domains.

Step 2: Check the Email Headers

-  Recommended Tool: Google Admin Toolbox or MXToolbox Email Header Analyzer
- Headers not provided, but in real-world analysis, check for:
 - SPF, DKIM, DMARC authentication failures
 - IP addresses that do not match known British Airways mail servers
 - Mismatched "From" and "Reply-To" domains

Step 3: Analyze the Link (URL)

- Visible Link: <https://accounts.britishairways.com/flight-credit/login>
-  Tip: Hover over the link in the real email client.
- Phishing Behavior:
 - Display a legitimate URL while the real destination redirects to a malicious clone site.
 - These clone sites harvest login credentials or install malware.

Step 4: Attachment Mention

- Red Flag: The email claims a voucher is attached.
- 🚩 Warning: Phishing attachments may include:
 - PDFs with malicious links
 - Word/Excel files with macros
 - Executable files (.exe or .scr)

Step 5: Language & Tone Analysis

- Positive & Reassuring Language: 'We hope this message finds you well.'
- ⚠️ Tactic Identified: Psychological manipulation using sympathy and compensation.
- ✅ No obvious grammatical/spelling errors, which makes it more convincing.

Step 6: Look for Urgent or Enticing Offers

- The core hook is: £300 British Airways travel voucher.
- 🚩 Red Flag: High-value rewards are commonly used to lure users into clicking or downloading files.

Step 7: Inspect Branding and Signature

- ✅ Logo is present (but logos can be easily copied).
- ❌ No official footer, contact address, or customer support details.
- ❌ No legal disclaimer or privacy/security statements typical of British Airways emails.

☑️ Summary of Phishing Indicators

Indicator	Status	Details
Suspicious sender email	⚠️ Likely	Email address not shown – must verify
No verifiable contact info or address	✅ Present	Missing in the footer
Unverified link (possible redirect)	⚠️ Suspect	URL might differ from shown text
Enticing compensation offer	✅ Present	£300 voucher offer to create urgency
Attachment warning	✅ Present	Potential

		phishing/malware file
Language & tone	⚠ Manipulative	Overly friendly and persuasive
Grammatical errors	✗ None	Text is well written
Branding mismatch	⚠ Lacks official design	No contact info or official format
Missing authentication metadata (headers)	⚠ Unknown	Cannot assess without header file