Phishing Email Analysis Report

|  |  |  |  |
| --- | --- | --- | --- |
| Indicator Category | Phishing Indicator Found | Supporting Evidence / Header Field | Corresponding Hint |
| I. Technical Authentication Failure | SPF Failure | Authentication-Results: spf=none and Received-SPF: None. The sending IP (57.128.69.202) is unauthorized for the claimed domain (dturm.de). | Hint 3 |
|  | DKIM Failure | Authentication-Results: dkim=none (message not signed). The email lacks a valid digital signature. | Hint 3 |
|  | Header Spoofing Confirmed | Authentication-Results: compauth=fail reason=001. Explicitly states the sender failed alignment/authentication. | Hint 3 |
| II. Sender Discrepancy (Spoofing) | Mismatched Sender and Reply-To Domains | From: <zonnepaneel@appjj.serenitepure.fr> Reply-To: <news@aichakandisha.com> (Two different, non-reputable domains). | Hint 2 |
| III. Social Engineering (Urgency) | Use of Urgent/Scarcity Language | Text pressures the user to act immediately ('Wacht daarom niet langer en meld u nu aan!') by claiming high demand. | Hint 5 |
| IV. Malicious Links | Mismatched URL / Link Misdirection | The visible link text (e.g., 'JA, ik wil zonnepanelen offertes') leads to a suspicious tracking/redirect domain (http://go.nltrck.com/...) instead of a legitimate company website. | Hint 6 |
| V. Low Quality / Errors | Spelling and Grammar Mistakes | Errors such as 'Het de moeite waard s...' (The word 'is' is missing or misspelled) indicate unprofessionalism. |  |

Generated automatically for phishing analysis.