Task 2: Analyzing a Phishing Email

Phishing Email Analysis

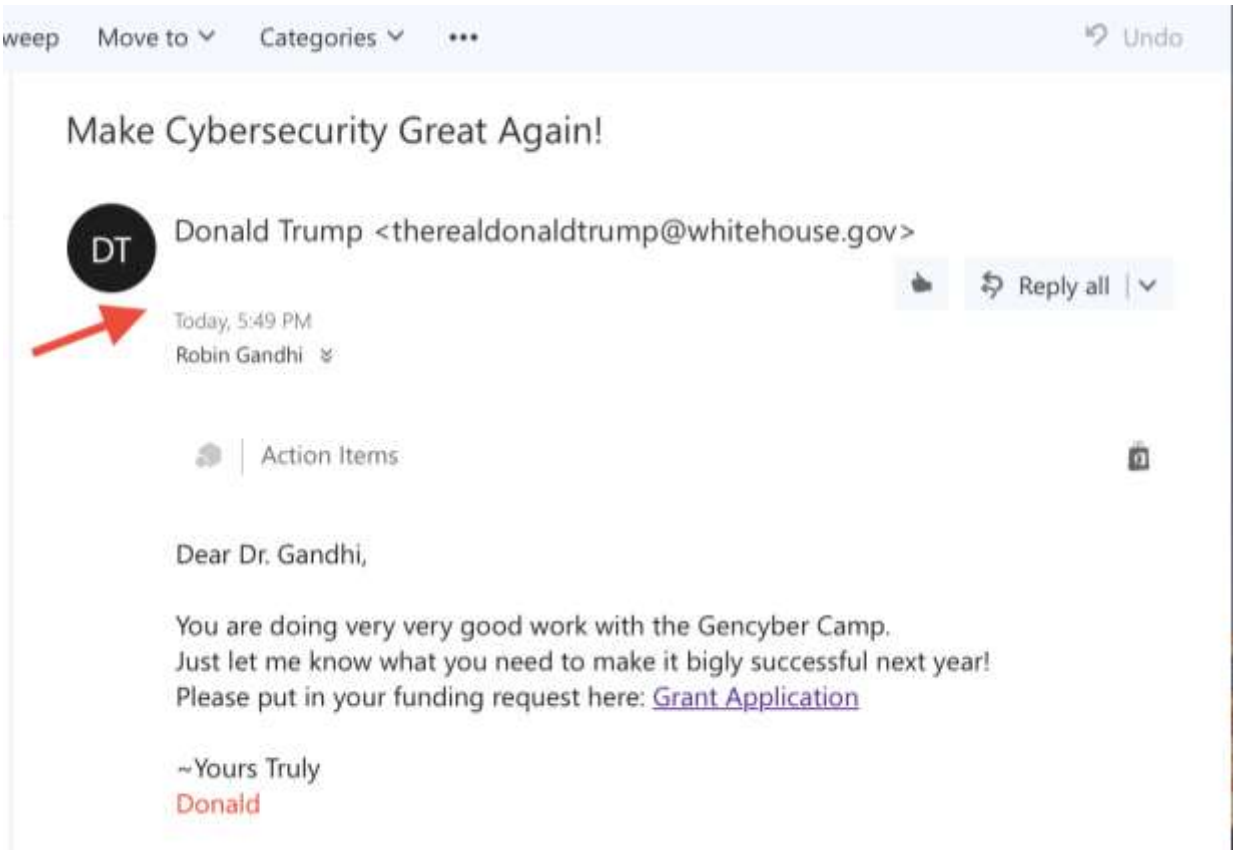
This email appears to be a phishing attempt designed to deceive recipients by impersonating an official communication. Below are key indicators of phishing:

1. **Spoofed Email Address: The sender's email address is crafted to appear legitimate. However, phishing attackers often use deceptive techniques to impersonate trusted sources.**

2. **Malicious Link: The email contains a link labelled "Grant Application," which may lead to a fraudulent website aimed at collecting sensitive user information.**

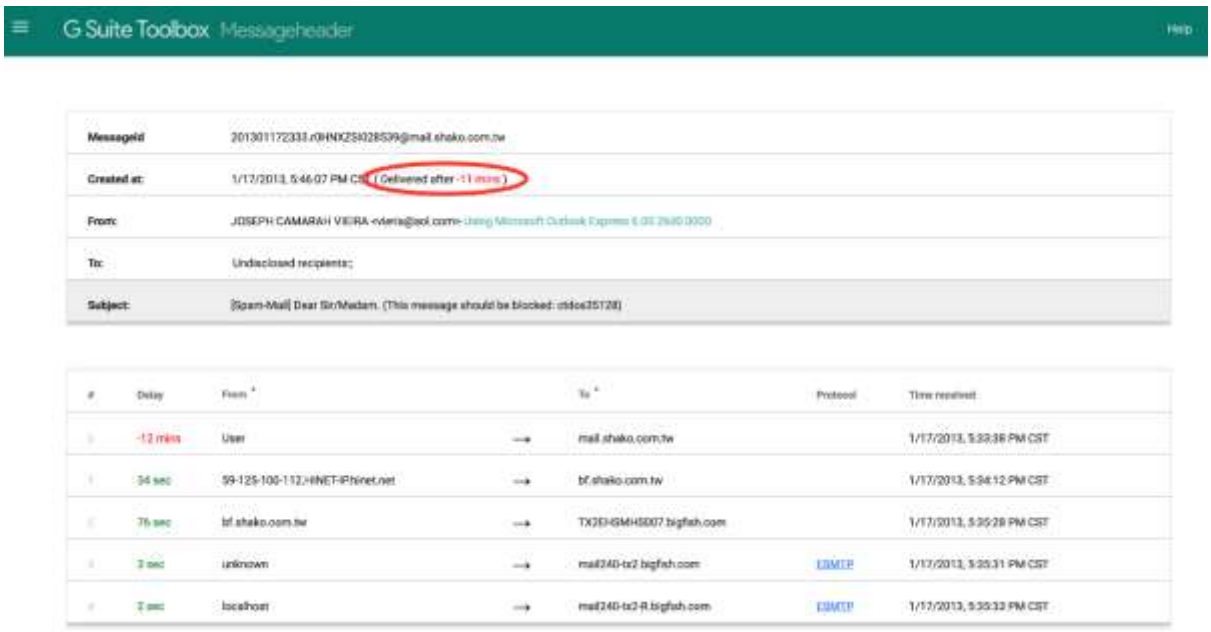
3. **Unusual Language and Tone: Official communications typically adhere to a formal style. Any deviation, such as slang or exaggerated claims, should raise concerns.**

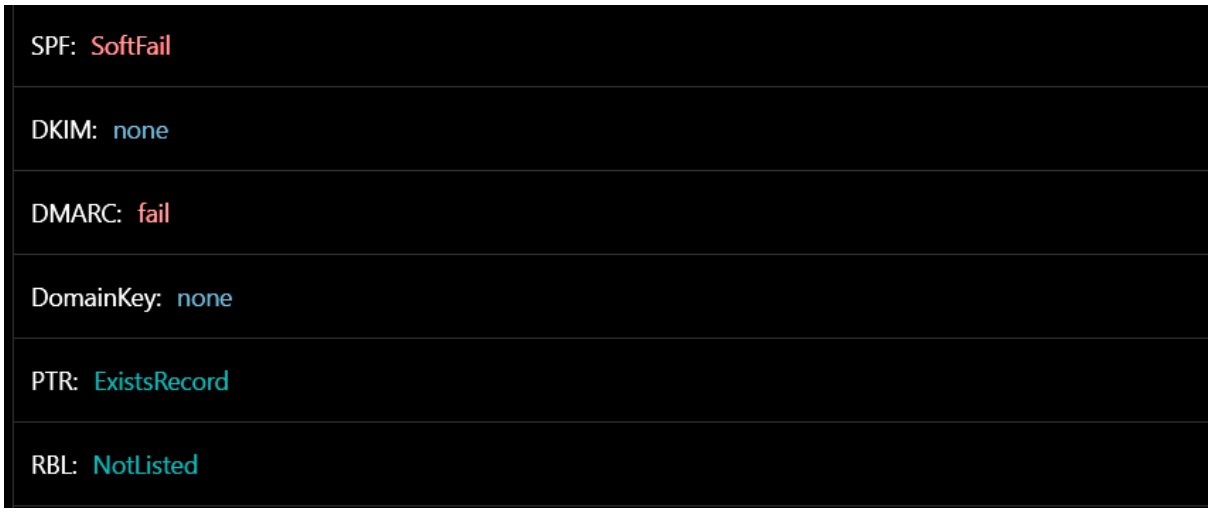
4. **Urgency and Incentive: Phishing emails frequently attempt to lure recipients with financial promises or urgent requests to elicit a quick response.**



Tool Analysis Results:

Google has an online tool that helps to examine the "hops" and the time delay between them. Large delays in accepting email by the first server may be a sign of overloaded and resource constrained spam servers. Here's what the tool shows about email-header1.txt. There is a suspicious 12-minute delay right at the beginning, which may indicate an overloaded spam sending email server. Sometimes, the time difference between servers may cause false positives.

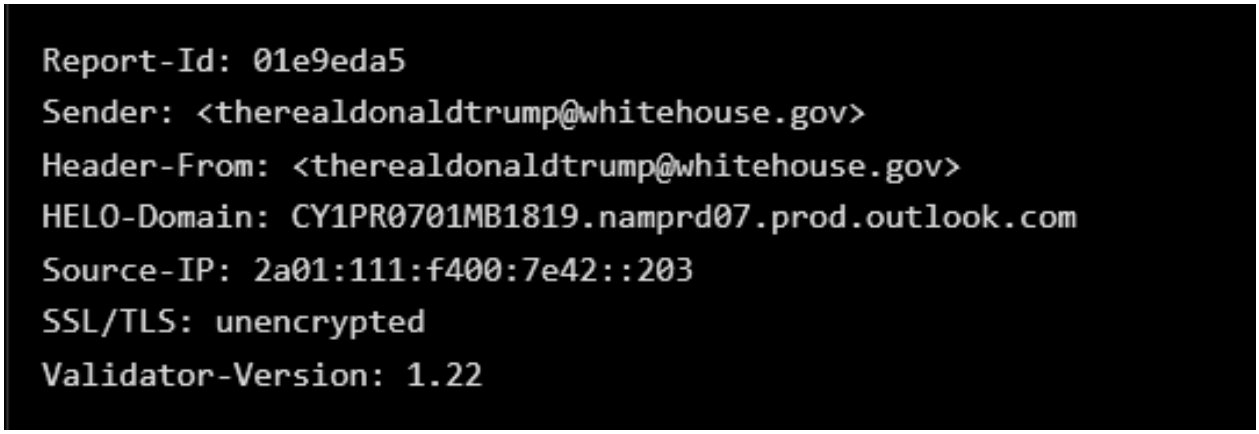




The above image is a result generated from DKIM/SPF/DMARC/DomainKey/RBL test tool provided by AdminSystem Software Limited

Phishing Traits

- **Authentication Failures:** The email failed key authentication checks, including SPF (SoftFail), DKIM (None), and DMARC (Fail), indicating it may not be from an authorized sender.
- **DomainKey Absence:** The lack of DomainKeys makes it impossible to verify the email's authenticity.
- **Suspicious Links:** The inclusion of a questionable "Grant Application" link suggests an attempt to redirect recipients to a fraudulent website.
- **Urgency & Incentive:** The email uses urgency (potential financial benefits) to manipulate recipients into taking quick action without verifying legitimacy.
- **Inconsistent Language & Tone:** Official government or corporate emails maintain formal tone—this email deviates from expected professionalism.
- **Unusual Sender Address:** The sender's address mimics a trusted domain but could be slightly altered, a common phishing strategy.
- **Unexpected Attachments:** Phishing emails often contain attachments that may deliver malware.
- **Lack of Encryption:** If the email is unencrypted, attackers could intercept or modify its contents.
- **Social Engineering Techniques:** The email aims to exploit human emotions—such as curiosity or trust—to encourage interaction.



The above image is a result generated from DKIM/SPF/DMARC/DomainKey/RBL test tool provided by AdminSystem Software Limited