

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.

G Suite Toolbox: Messageheader						
Help						
Messageid:	201301172332.r0HNK25428539@mail.shako.com.tw					
Created at:	1/17/2013, 5:46:07 PM CST (Delivered after -11 mins)					
From:	JOSEPH CAMARAH VERA <vera@ed.com> using Microsoft Outlook Express 6.00.2600.0000					
To:	Undisclosed recipients;					
Subject:	[Spam-Mail] Dear Sir/Madam, (This message should be blocked: info:25728)					

#	Delay	From *	To *	Protocol	Time received
1	-12 mins	User	mail.shako.com.tw		1/17/2013, 5:38:38 PM CST
2	34 sec	99-125-100-112.HINET-IP.hinet.net	bf.shako.com.tw		1/17/2013, 5:34:12 PM CST
3	76 sec	bf.shako.com.tw	TX2E3GMH5007.bigfish.com		1/17/2013, 5:35:28 PM CST
4	3 sec	unknown	mail240-tx2-bigfish.com	EDMTP	1/17/2013, 5:35:31 PM CST
5	3 sec	localhost	mail240-tx2-R.bigfish.com	EDMTP	1/17/2013, 5:35:32 PM CST

SPF: **SoftFail**

DKIM: **none**

DMARC: **fail**

DomainKey: **none**

PTR: **ExistsRecord**

RBL: **NotListed**

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.

```
Report-Id: 01e9eda5
Sender: <therealdonaldtrump@whitehouse.gov>
Header-From: <therealdonaldtrump@whitehouse.gov>
HELO-Domain: CY1PR0701MB1819.namprd07.prod.outlook.com
Source-IP: 2a01:111:f400:7e42::203
SSL/TLS: unencrypted
Validator-Version: 1.22
```

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