CODE
ALPHA

INTRODUCTION TO PHISHING ATTACK

AN OVERVIEW OF PHISHING

AHMED SAEED AHMED
ID CA/MY3/4222

HISTORY OF PHISHING ATTACK

The history of phishing dates back to the early 1990s, when the term "Phishing" began to be used to refer to the technique of using fake emails to compromise users' personal login information. The attacks were originally aimed at users of AOL systems, but have evolved to include all types of email and websites.

Since then, phishing techniques have evolved to include many modern methods such as social phishing and social engineering, where the trust and ignorance of victims are exploited to obtain confidential information or money.

Phishing has become a major threat to individuals and organizations alike, which has led to stricter security measures being taken to reduce these attacks and educate users on how to recognize and avoid them.

× × × ×

TYPES OF PHISHING ATTACKS

CODE
ALPHA

- Email Phishing: Fraudulent emails that appear to be from reputable sources.
- Website Phishing: Fake websites designed to look like real ones to deceive users.
- Phone Phishing (Vishing): Impersonating calls to gather sensitive information.
- SMS Phishing (Smishing): Fraudulent text messages aimed at collecting data or installing malware.

HOW PHISHING ATTACKS WORK

- Target Identification: Choosing the victim.
- Creating the Bait: Crafting a convincing message or website.
- Sending the Bait: Delivering the bait to the victim.
- Victim Response: Tricking the victim into revealing information.

CODE
ALPHA

RECOGNIZING PHISHING EMAILS

- **Unfamiliar Email Addresses: Check the sender's address.**
- **Suspicious Links: Hover over links to verify their destination.**
- **Grammatical Errors: Phishing emails often contain spelling and grammar mistakes.**
- **Requests for Sensitive Information: Be wary of unusual requests for personal information.**

AVOIDING PHISHING ATTACKS

CODE ALPHA

- Verify the Source: Confirm the identity of the sender before interacting.
- Use Antivirus Software: Ensure it is up-to-date.
- Do Not Click Suspicious Links: Be cautious with unknown links.
- Enable Two-Factor Authentication: Add an extra layer of security.

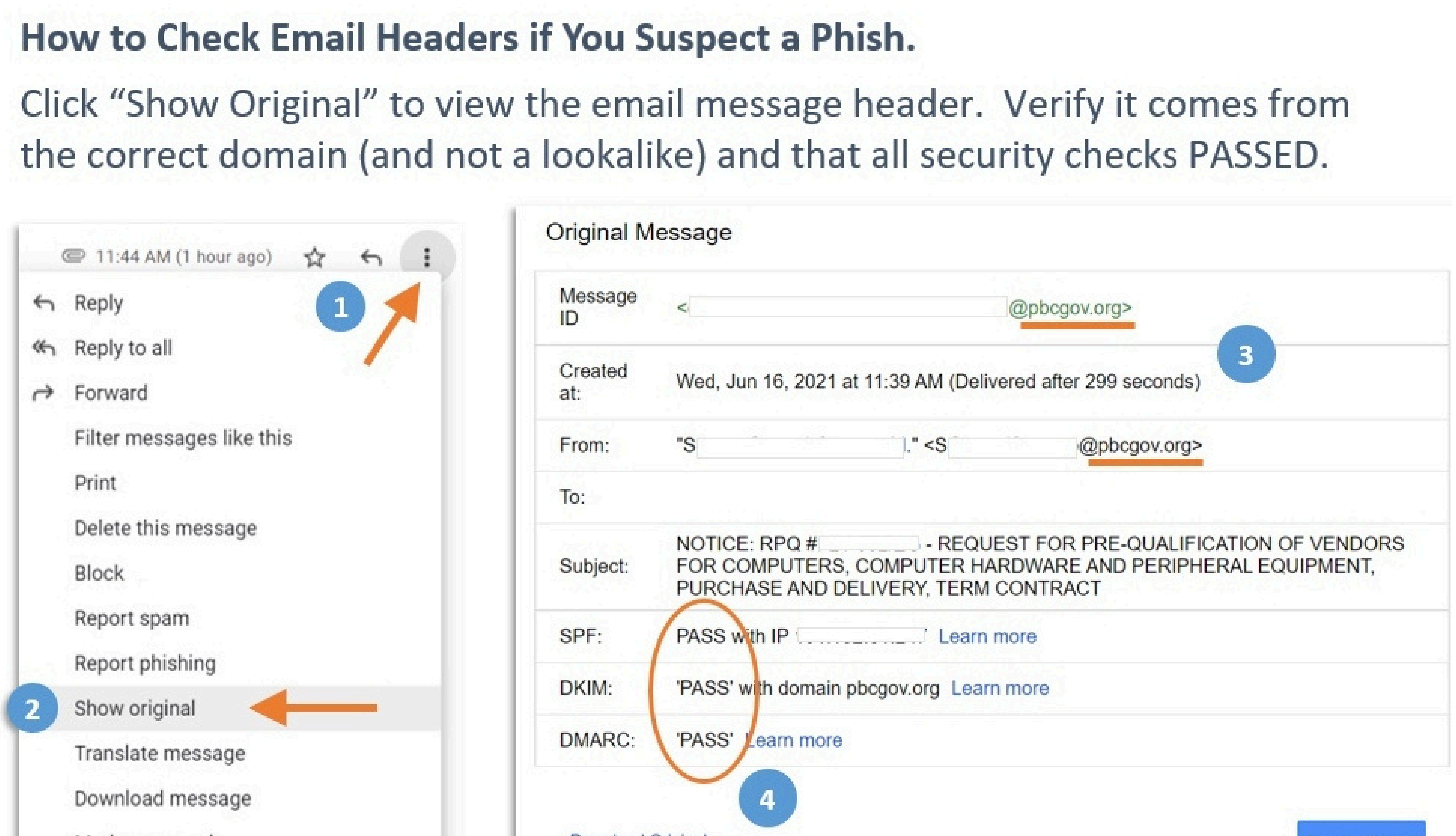
WHAT TO DO IF TARGETED

- **Do Not Respond: Avoid replying to phishing messages.**
- **Report the Email: Notify your IT team or email provider.**
- **Change Passwords: Update your passwords immediately.**
- **Monitor Accounts: Watch for unusual activity in your bank and email accounts.**

CODE ALPHA

EXAMPLES OF PHISHING EMAILS

- **Show Real Examples: Analyze suspected phishing emails.**
- **Identify Red Flags: Highlight key indicators of phishing.**



How to Check Email Headers if You Suspect a Phish.

Click "Show Original" to view the email message header. Verify it comes from the correct domain (and not a lookalike) and that all security checks PASSED.

Original Message

Message ID	<[redacted]@pbcgov.org>
Created at:	Wed, Jun 16, 2021 at 11:39 AM (Delivered after 299 seconds)
From:	"S[redacted]." <S[redacted]@pbcgov.org>
To:	
Subject:	NOTICE: RPQ #[redacted] - REQUEST FOR PRE-QUALIFICATION OF VENDORS FOR COMPUTERS, COMPUTER HARDWARE AND PERIPHERAL EQUIPMENT, PURCHASE AND DELIVERY, TERM CONTRACT
SPF:	PASS with IP [redacted] Learn more
DKIM:	'PASS' with domain pbcgov.org Learn more
DMARC:	'PASS' Learn more

CODE ALPHA

CONCLUSION

- **Summary: Emphasize the importance of phishing awareness and prevention.**
- **Questions: Open the floor for questions and discussions.**

CODE
ALPHA

RESOURCES AND REFERENCES

Phishing.org

wikipedia

CODE
ALPHA

AHMED SAEED AHME
ID CA/MY3/4222