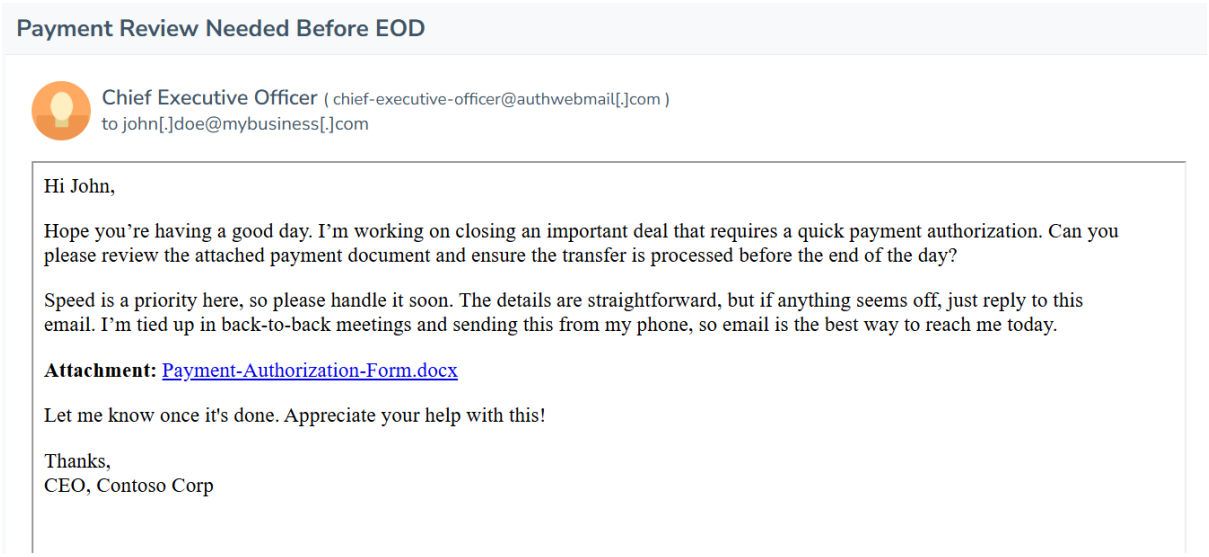
Phishing Email Analysis Report

Phishing mail example:


Payment Review Needed Before EOD

Chief Executive Officer (chief-executive-officer@authwebmail[.]com)
to john[.]doe@mybusiness[.]com

Hi John,

Hope you're having a good day. I'm working on closing an important deal that requires a quick payment authorization. Can you please review the attached payment document and ensure the transfer is processed before the end of the day?

Speed is a priority here, so please handle it soon. The details are straightforward, but if anything seems off, just reply to this email. I'm tied up in back-to-back meetings and sending this from my phone, so email is the best way to reach me today.

Attachment: Payment-Authorization-Form.docx

Let me know once it's done. Appreciate your help with this!

Thanks,
CEO, Contoso Corp

1. Sample Phishing Email
   A phishing email was obtained from the CanIPhish simulator with the subject:
   "Payment Review Needed Before EOD"

2. Sender's email address
   Here the was sent from chief-executive-officer@authwebmail[.]com to john[.]doe@mybusiness[.]com
   The sender email id doesn't match with the company domain(contoso.com)

3. Suspicious Links or Attachments Attachment:
   Payment-Authorization-Form.docx - May contain malware or data harvesting tools.
   This type of document is commonly used to deliver **malware** or **harvest credentials** when opened.

4. Urgent or Threatening Language Example: "Speed is a priority here, so please handle it soon.
   This Creates a **sense of urgency**, a common phishing tactic to pressure the recipient into acting quickly without verification.

5. Mismatched URLs - No explicit links found in this sample.

6. Spelling or Grammar Errors - No major spelling errors. - Formal, robotic tone used to deflect suspicion.

Summary:

This phishing email is crafted to appear as though it comes from a legitimate sender. Key red flags include:

- Mismatched email domain
- Suspicious attachment
- Urgency in tone
- Unusual sender address format
- Mentioning not to contact through the phone and asking to reply to the same email address.

These characteristics align with common phishing techniques aimed at tricking recipients into initiating unauthorized payments or opening malicious documents.