

Ticket ID	Alert Message	Severity	Details	Ticket status
A-2703	SERVER-MAIL Phishing attempt possible download of malware	Medium	The user may have opened a malicious email and opened attachments or clicked links.	Escalated ▾

Ticket comments
The alert came because of a phishing attack, and the employee got successfully tricked into downloading a suspicious file, which caused the problem. Looking at the alert message makes me believe the ticket should be escalated. Seeing the severity and details of the alert is a cause for alarm. Lastly, when looking at the poorly constructed email, it is clear that this ticket should be escalated.

## Additional information

### Known malicious file hash:

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

### Email:

From: Def Communications <76tguyhh6tgfrt7tg.su> <114.114.114.114>

Sent: Wednesday, July 20, 2022 09:30:14 AM

To: <hr@inergy.com> <176.157.125.93>

Subject: Re: Infrastructure Egnieer role

Dear HR at Inergy,

I am writing for to express my interest in the engineer role posted from the website.

There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.

Thank you,

Clyde West

Attachment: filename="bfsvc.exe"