Why is it suspicious?

- The sender's IP address varied
    - Legit bulk emails from vendors usually come from consistent known IP ranges and don't randomly switch sending servers
    - Multiple sending IPs can indicate:
        - Compromised email accounts sending the same message
        - Botnet-based phishing distribution
        - A spoofed domain sent through multiple mail relays
- File detonation
    - Taking the suspicious link or file and executing it inside an isolated sandbox environment to observe its behavior safely
    - If the file detonation was triggered by that means, there was a harmful link or file that is looking to harm the environment
- File reputation
    - Checks if a file is known to be safe or risky based on cloud intelligence and worldwide telemetry
    - File reputation is exactly as it says, checking the reputation of the file to see if it comes from a trusted source, whether trusted publishers signed it, how new it is, and how many people have seen this file
- File Fingerprint Matching
    - Fingerprint matching is analyzing a file by its unique characteristics or hashes and comparing it to malicious or safe files

    - If a file matches the hash of a known malware sample, it should be blocked immediately without having to execute it
    - For example, if a file has a hash that matches a known ransomware strain it is instantly blocked.
- ZAP-Success for some messages
    - Rescans emails for up to 48 hours
    - When Microsoft updates its threat intelligence, ZAP can identify that a previously delivered message is malicious and can remove it retroactively
    - Once ZAP realizes an already delivered email is malicious it removes it from the inbox and into quarantine

What to do if an employee has already interacted with this phishing attempt?

- The employee should immediately stop interacting with the link or file
- See what the employee clicked on, if they entered credentials, approved of any MFA, or downloaded anything
- Reset the user's password, revoke all sessions and refresh tokens, and check MFA settings for any tampering

Why would only 1/10 emails be blocked if it is the same email being sent out?

- The one that was blocked was sent last at 7:23pm compared to all the others that were sent from 1pm – 2pm
- The email was reported between the times of 2pm and 7:23pm and was able to learn that the email was fake automatically quarantining it

- Looking at the defender page, all the fake emails are now ZAP-succeeded since it was learned that it was a fake email and a threat to the environment
- The defender page also lets me look at the actual email and it looks anything but legit, shows employees are hesitant to report possible fake emails or they are just ignoring them

Final Thoughts:

One employee interacted with the suspicious link in the email, and she stated that she did not submit any personal information to the website that she was taken to. We have instructed her that she needs to change her password as soon as possible just in case the link was malicious and has infected her computer, stealing her information. I have also run an antivirus scan on her device to check if there was anything hiding in there, thankfully there wasn't.