**You can ask copilot to filter the recommendations to Microsoft 365 solutions.** Then when you’re given recommendations, take them one at a time , & ask for specific steps to configure in Microsoft 365

With those specific steps, you can then configure in the environment id give you access to

**Solution:**

To address the fraudulent email issue effectively, here's a comprehensive plan for the security analyst:

1. Microsoft 365 Plan Recommendation

- Plan to Purchase: Microsoft 365 Enterprise E5 or Microsoft Defender for Office 365 Plan 2. These plans include advanced email security features such as anti-phishing, anti-malware, and Safe Links/Attachments.

- Key Features:

- Anti-Phishing Protection: Detects and mitigates phishing attempts, including impersonation attacks.

- Safe Links and Safe Attachments: Scans URLs and attachments in real-time to block malicious content.

- Threat Explorer: Provides insights into email threats and trends.

- Automated Investigation and Response (AIR): Automates threat detection and remediation.

2. Configuration Steps

- Anti-Phishing Policies:

- Navigate to the Microsoft Defender portal ([security.microsoft.com](https://security.microsoft.com)).

- Configure anti-phishing policies to include impersonation protection and advanced thresholds.

- Safe Links and Attachments:

- Enable Safe Links to rewrite and scan URLs in emails.

- Configure Safe Attachments to scan and block malicious files.

- Email Authentication:

- Set up SPF, DKIM, and DMARC protocols to prevent spoofing.

- Preset Security Policies:

- Apply "Strict" preset security policies for maximum protection.

3. Testing with a Group of Users

- Test Group:

- Apply the new policies to a small group of test users, including non-VIP and VIP users, to evaluate effectiveness and minimize disruptions.

- Simulation Mode:

- Use simulation mode for sensitivity labels or DLP policies to monitor impact without enforcing restrictions.

4. Documentation and GitHub Repository

- Screenshots:

- Use the Windows Steps Recorder or similar tools to capture configuration steps.

- GitHub Repository:

- Create a repository and upload screenshots with detailed explanations of each step, including the rationale and potential implications.

- Include a README file summarizing the policies and their expected outcomes.

5. Stakeholder Reports

- Mail Flow Reports:

- Use the Exchange Admin Center ([admin.exchange.microsoft.com](https://admin.exchange.microsoft.com)) to generate mail flow reports, such as inbound/outbound messages and non-delivery details.

- Stakeholder Communication:

- Share periodic reports with stakeholders to ensure transparency and build trust.