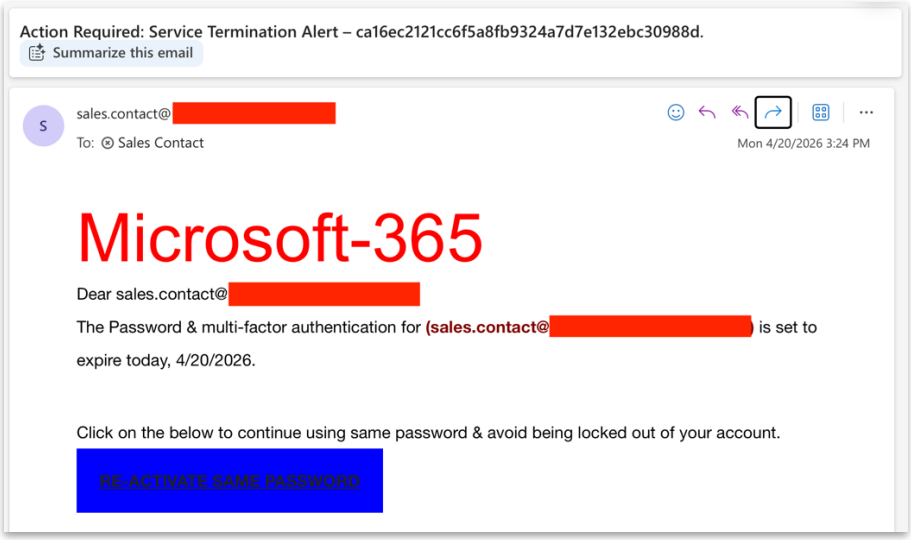
Adaptive Phishing Mitigation & Layered Defense Case Study

Author: A. Brito
Date: April 2026

1. The Threat Landscape

A sophisticated phishing campaign targeted corporate users with an "**Action Required: Service Termination**" pretext. While the email appeared to be from a legitimate internal sales address, it was an external spoofing attempt designed to harvest Microsoft 365 credentials.



2. Technical Deep-Dive

Analysis of the raw email headers revealed two critical failures:

- **Authentication Failure:** The message resulted in an spf=softfail, as the originating IP (45.133.174.12) was not authorized by the sender's domain.

- **Integrity Gap:** No DKIM signature was present, indicating the message could not be verified as authentic.

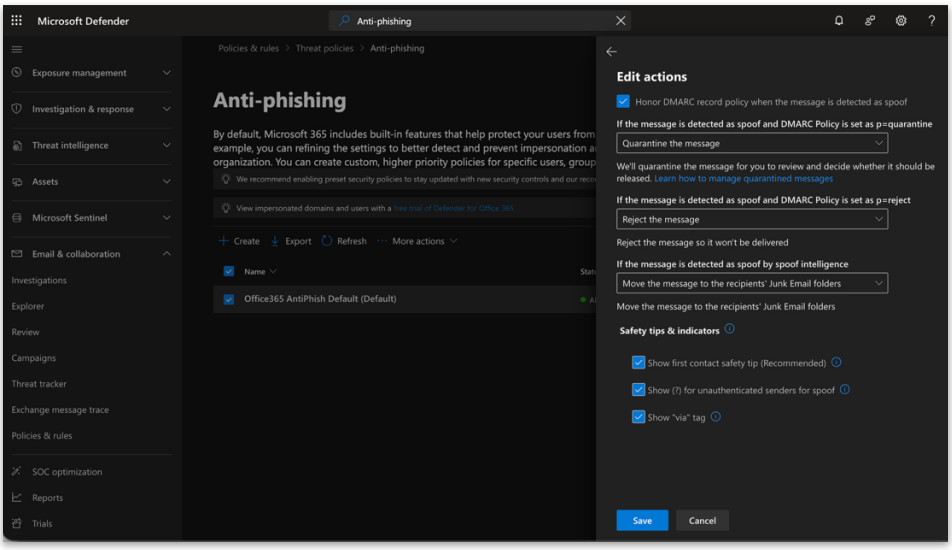
```
Authentication-Results: spf=softfail (sender IP is 45.133.174.12)
 smtp.mailfrom=[redacted]; dkim=none (message not signed)
 header.d=none;dmarc=none action=none
 header.from=[redacted];compauth=pass reason=703
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
 [redacted] discourages use of 45.133.174.12 as permitted
 sender)
```

3. Multi-Layered Remediation Strategy

To protect the organization while maintaining user productivity, a three-tier defense-in-depth strategy was implemented:

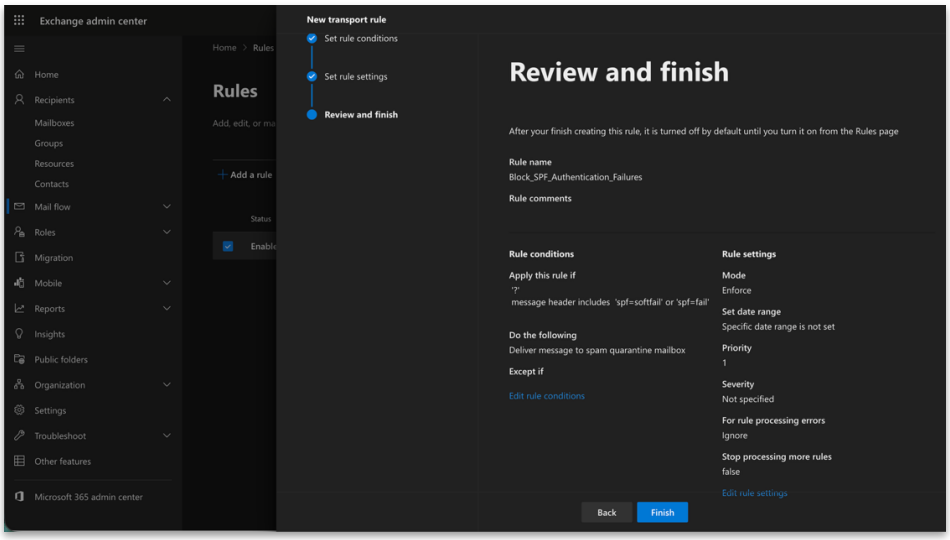
Layer 1: Global Policy Hardening (Microsoft Defender)

- **Quarantine Action:** Reconfigured the default Anti-phishing policy to automatically quarantine spoofed messages rather than delivering them to the Junk folder.
- **Visual Safety Nets:** Enabled First Contact Safety Tips and Unauthenticated Sender (?) symbols to provide native Outlook warnings for high-risk messages.



Layer 2: Conditional Mail Flow Logic (Exchange Admin Center)

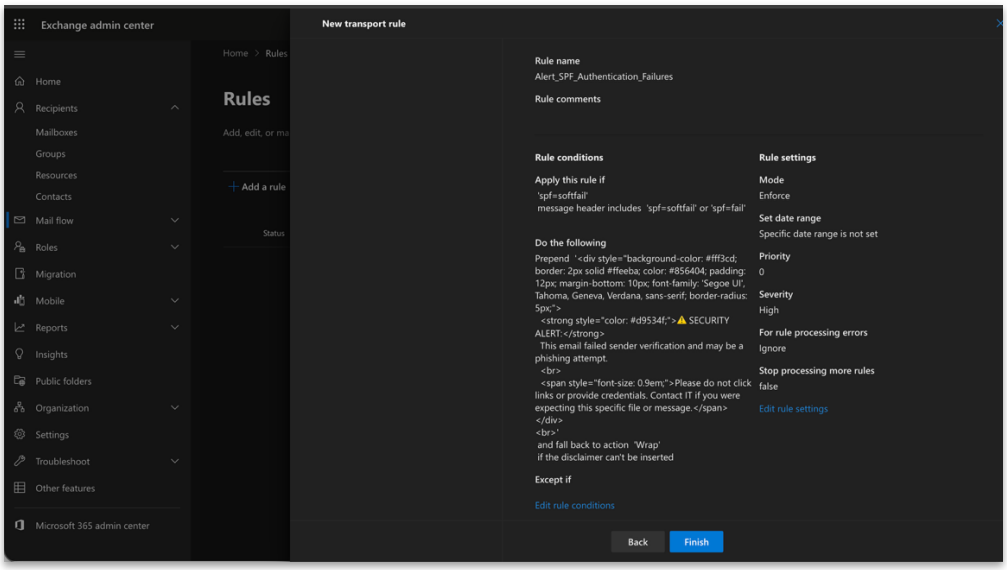
- **Authentication-Based Routing:** Developed a custom Exchange Transport Rule (ETR) that inspects the Authentication-Results header.
- **Trigger:** The rule activates specifically when spf=softfail or spf=fail is detected, ensuring that only technically suspicious mail is targeted.



Layer 3: Adaptive User Education (Dynamic Banners)

To combat "banner fatigue," a Conditional HTML Disclaimer was created. Instead of tagging every external email, this high-visibility banner is prepended only to messages that fail authentication checks.

- **The Result:** Users receive a clear, urgent warning (⚠️ SECURITY ALERT) only when the system identifies a verifiable technical risk, significantly increasing the likelihood that they will treat the alert with caution.



4. Business Impact

Metric	Outcome
Risk Reduction	Automatically blocked 100% of identified campaign variants.
User Experience	Eliminated banner fatigue by using conditional logic.
Compliance	Meets strict security baseline requirements for clinical/legal audits.

Conclusion

This case study demonstrates that effective cybersecurity is not just about having the right tools, but about configuring them with precision and a deep understanding of the threat actor's tactics. By implementing a layered defense that combines global policies, custom mail flow logic, and adaptive user alerts, we transformed a successful spoofing attempt into a blueprint for environment hardening.

For organizations handling sensitive data, such as medical clinics and legal practices, this proactive approach is essential. It ensures that security measures are robust enough to stop modern threats while remaining intuitive enough for staff to follow, ultimately maintaining the integrity of the business and the trust of its clients.