Email issue. Many of our clients are getting Phishing emails that looks like it is from their own email. How can we stop this? Microsoft 365

You need to tighten email authentication (SPF/DKIM/DMARC) and enable/raise anti-spoofing/anti-phishing protection in Microsoft 365, plus add a couple of targeted mail flow rules for "mail from myself" scenarios.[1] [2] [3]

Below is a concrete, admin-level checklist you can roll out tenant-wide.

1. Fix the root cause: authentication (SPF/DKIM/DMARC)

Attackers are spoofing your domain because receiving systems can't reliably tell "real you" from "fake you." Microsoft explicitly calls out misconfigured SPF/DMARC as the primary cause of internal-looking spoofed mail.[4] [1]

1. SPF for Microsoft 365

- In public DNS for each accepted domain, make sure you have a single SPF TXT record similar to:
  `v=spf1 include:spf.protection.outlook.com -all`
- If you have other legitimate senders (Mailchimp, ticketing systems, etc.), include them in that one record.
- Use `-all` (hard fail), not `~all`, so spoofed mail is much more likely to be rejected.[5] [3] [1]

2. DKIM in Microsoft 365

- Go to Microsoft 365 Defender portal → Email & collaboration → Policies & rules → Threat policies → DKIM.
- For each custom domain, generate DKIM keys if not already present, publish the two CNAMEs in DNS, then flip status to "Enable." [2] [3] [5]

3. DMARC with enforcement

- In DNS for each domain, add a DMARC TXT record at `_dmarc.yourdomain.com`.
- Start at p=none to gather data, then move to quarantine/reject once stable. Example progression:
  - Phase 1 (monitoring):
    `v=DMARC1; p=none; rua=mailto:dmarc-reports@yourdomain.com; aspf=s; adkim=s`
  - Phase 2 (enforce):
    `v=DMARC1; p=quarantine; pct=50; rua=...; aspf=s; adkim=s`

- Phase 3 (full):
  `v=DMARC1; p=reject; rua=...; aspf=s; adkim=s`

- Microsoft and others specifically recommend strict DMARC + SPF hard fail to stop phishing that spoofs your own domain.[3] [1] [4] [5]

If you're routing mail through a third-party gateway or hybrid, you'll need to ensure those hops are reflected correctly in SPF/DMARC or they'll fail once you enforce.[1] [4]

2. Turn on and harden Microsoft 365 anti-spoofing / anti-phishing

Microsoft 365 has built-in spoof intelligence and domain impersonation protection, but a lot of tenants still run near-default settings.[6] [7] [2]

1. Use preset security policies where possible

- In Defender portal → Email & collaboration → Policies & rules → Threat policies → Preset security policies.
- Apply "Standard" at minimum to all users; "Strict" to high-risk accounts (execs, finance, IT). These presets include anti-spoofing and domain impersonation protections.[6] [2]

2. Verify anti-phishing / anti-spoofing settings

- Defender portal → Email & collaboration → Policies & rules → Threat policies → Anti-phishing.
- In your default/custom policies:
  - Ensure **spoof intelligence** is On.[2]
  - Turn on **unauthenticated sender indicators** so Outlook flags suspicious mail (question mark avatar, "via" tag).[6] [2]
  - In **Domain impersonation**, add your accepted domains so messages that pretend to be from them get higher scrutiny.[6]
  - Choose strong actions for detected spoof/impersonation: "Quarantine" rather than just "Move to Junk."

3. Use spoof intelligence reports

- In Defender, review the **Spoofing / Spoof intelligence** insights; approve known good third-party senders, block clearly malicious ones.[2]

3. Add a targeted mail flow rule for "email from myself"

To specifically nail the "I got a phishing email from my own address" complaint, a simple transport rule helps, especially while you're tightening DMARC.

Classic pattern:

- Exchange admin center → Mail flow → Rules → New rule.
- Example logic:

- Condition:
  - Sender domain is yourdomain.com
  - Sender is *outside* the organization (or message is not authenticated / fails DMARC/SPF depending on what's available in your build).
- Optional extra: SCL ≥ 1 or message is identified as spam/phish. (This keeps real internal mail safe.) [8]
- Action:
  - Quarantine the message or delete it, and optionally add an audit or notification.

This "if it says it's from us but is coming from outside, treat it as highly suspicious" pattern is widely recommended by admins and Microsoft community answers for this scenario. [9] [8]

If you have legitimate external systems sending as your domain (ERP, scanners, etc.), make sure they're properly authenticated (SPF/DKIM or trusted connector) so they don't trip this rule.

4. Check MX / routing and connectors

Microsoft has been flagging a very specific problem pattern: MX not pointing directly to Microsoft 365 plus complex routing or poorly configured connectors lets spoofed messages appear internal. [4] [1]

Review:

- MX: Ideally, point MX for your domains directly to `*.mail.protection.outlook.com` unless you intentionally front-end with a third-party gateway. [1] [4]
- Connectors:
  - For any inbound connectors (on-prem, third-party relay, security appliance), enable **Enhanced Filtering for Connectors** so anti-spoofing and spam filtering see the true source IP. [2] [6]
- If you keep a third-party gateway, ensure it respects DMARC and doesn't just pass spoofed mail through.

5. User training and incident response

Even with a hardened setup, some phishing will slip by, especially before DMARC is at p=reject. [10]

- Train users to distrust "from yourself" mail that asks for passwords, crypto, or urgent actions; this scenario is a known common scam. [11] [10]
- Make reporting easy (Report Message add-in, abuse@ mailbox).
- Use Defender's tools like Zero-Hour Auto Purge and threat explorer (if licensed) to pull similar messages once you identify a new campaign. [7] [12] [2]

6. Quick “minimum viable fix” you can do this week

If you want a prioritized action list:

1. Confirm SPF is `include:spf.protection.outlook.com -all` and clean.[5] [3]
2. Enable DKIM for all accepted domains.[5] [2]
3. Add DMARC at p=none, then move toward quarantine/reject once you’ve validated flows.[3] [4] [5]
4. Turn on Standard/Strict preset security policies and verify anti-phishing/anti-spoofing toggles.[7] [6] [2]
5. Add a mail flow rule: if sender domain = yourdomain.com AND it’s external/unauthenticated, quarantine.[8] [9]

Would it be possible for you to share whether your clients’ MX records point directly to Microsoft 365 or through a third-party spam gateway/hybrid server? That will change how aggressive you can be with DMARC and mail flow rules.

⁂

1. https://www.microsoft.com/en-us/security/blog/2026/01/06/phishing-actors-exploit-complex-routing-and-misconfigurations-to-spoof-domains/
2. https://learn.microsoft.com/en-us/defender-office-365/anti-phishing-protection-spoofing-about
3. https://learn.microsoft.com/en-us/answers/questions/5491704/receiving-weird-phishing-emails-from-myself
4. https://www.paubox.com/blog/microsoft-warns-of-rising-phishing-threats-using-domain-spoofing
5. https://www.mailsdaddy.com/blogs/office-365-email-authentication-setting-up-spf-dkim-dmarc/
6. https://learn.microsoft.com/en-us/defender-office-365/anti-phishing-policies-about
7. https://www.linkedin.com/pulse/stop-phishing-emails-microsoft-365-businessit365-fdlvc
8. https://www.reddit.com/r/sysadmin/comments/1sof2w7/office_365_phishing_emails_epidemic/
9. https://learn.microsoft.com/en-us/answers/questions/4660508/fraudulent-email-similar-to-my-domain
10. https://guardiandigital.com/resources/must-read-blog-posts/how-phishing-emails-bypass-microsoft-365-default-security
11. https://learn.microsoft.com/en-us/answers/questions/4691202/got-an-email-send-by-my-own-email-address-do-i-hav
12. https://www.youtube.com/watch?v=ABEGgrRXcL8
13. https://help.vtiger.com/faq/163601817-How-do-I-set-up-Anti-Spoofing-in-Office-365
14. https://support.microsoft.com/en-us/office/set-up-your-microsoft-365-sign-in-for-multi-factor-authentication-ace1d096-61e5-449b-a875-58eb3d74de14
15. https://support.microsoft.com/en-us/account-billing/set-up-an-email-address-as-your-verification-method-250b91e4-7627-4b60-b861-f2276a9c0e39