Phishing Email Analysis Report – Microsoft 365 Password Expiring

Scope

* Analyze one suspicious email purporting to be a Microsoft 365 password‑expiration notice, including full header review, authentication results, relay path, content red flags, and risk verdict.

Email Summary

* From: "Microsoft Account Security" [no-reply@m1crosoft-security.com](mailto:no-reply@m1crosoft-security.com)
* To: [user@example.com](mailto:user@example.com)
* Subject: Action Required: Microsoft 365 Password Expiring in 24 Hours
* Date: Mon, 03 Feb 2025 06:18:03 +0000
* Body theme: 24‑hour password expiry; urges immediate reset through a link to a look‑alike domain; requests current password and MFA code.

Header Authentication Findings

* SPF: Authentication failed for the sending IP 185.203.110.24, while a separate SPF record exists; analyzer shows “SPF Authentication: fail” with “SPF Alignment: OK,” meaning the domain used for SPF matches the RFC5322.From, but the connecting IP is not authorized. This is consistent with phishing using a deceptive but aligned domain.
* DKIM: No DKIM‑Signature present; analyzer flags “No DKIM‑Signature header found” and “DKIM not authenticated/aligned.”
* DMARC: No DMARC record published for m1crosoft‑[security.com](http://security.com); analyzer reports “DMARC Compliant (No DMARC Record Found)” with failure status for policy evaluation.
* Verdict on auth: Absence of DKIM and DMARC, plus SPF auth failure, are strong technical indicators of spoofing/abuse.

Relay Path (Received Chain)

* Hop 1: [mail.m1crosoft-security.com](http://mail.m1crosoft-security.com) by [mx.example.com](http://mx.example.com) with ESMTPS at 06:18:07 UTC.
* Hop 2: [smtp-out.unrelatedsmtp.net](http://smtp-out.unrelatedsmtp.net) by [mail.m1crosoft-security.com](http://mail.m1crosoft-security.com) with ESMTPS at 06:18:05 UTC.
* Hop 3: localhost by [smtp-out.unrelatedsmtp.net](http://smtp-out.unrelatedsmtp.net) with ESMTPSA at 06:18:03 UTC.
* Notes: All hops reference non‑Microsoft infrastructure and the same suspicious IP range, indicating the message didn’t traverse Microsoft‑owned MTAs.

Domain and Alignment Observations

* Visible From domain: m1crosoft‑[security.com](http://security.com) (look‑alike of [microsoft.com](http://microsoft.com) with numeral “1”).
* Return‑Path/Envelope-From: [bounce-no-reply@m1crosoft-security.com](mailto:bounce-no-reply@m1crosoft-security.com) (same deceptive domain).
* Alignment: Analyzer shows SPF alignment OK (domain match), but that does not imply brand legitimacy; it only proves the domains match each other, not that they are Microsoft’s.

Link and Attachment Review

* Primary CTA: hxxps://m1crosoft‑security[.]com/account/reset?session=8f2a1c (defanged).
* “Report suspicious activity” link displays a Microsoft URL but the “actual” link is a shortened redirect (defanged), a common tactic to hide final destinations.
* No attachment in this sample, but the pattern often includes HTML disguised as PDF in similar campaigns.

Content and Social Engineering Indicators

* Urgency: 24‑hour deadline to prevent service disruption.
* Authority impersonation: Uses “Microsoft Account Security” branding and references Outlook/OneDrive/Teams.
* Data harvesting: Requests current password and MFA code, which legitimate providers never ask by email.
* Generic greeting and tone: “Dear User” instead of personalized salutation.
* Language: Professional tone but manipulative, emphasizing loss of access.

Risk Assessment

* Technical risk: High – SPF authentication failed for the connecting IP; DKIM missing; DMARC absent; relay path on non‑brand infrastructure.
* Behavioral risk: High – Urgent deadline, credential/MFA harvesting, look‑alike domain, link mismatch/shortener.

Conclusion

* Classification: Phishing – credential harvesting.
* Justification: Failed SPF authentication for the sending IP, no DKIM, no DMARC, look‑alike domain aligned only with itself, non‑brand relay infrastructure, urgent social‑engineering language, and requests for sensitive information.

Recommended Actions

* Do not click links or provide credentials.
* Navigate directly to [account.microsoft.com](http://account.microsoft.com) in a browser to verify any real account notices.
* Report the email to the organization’s security team and mark as phishing.
* If any interaction occurred, reset the Microsoft 365 password, revoke sessions, and re-enroll MFA; monitor for lateral movement.

Indicators of Compromise (IoCs)

* Domains: m1crosoft‑[security.com](http://security.com) (look‑alike)
* Envelope/From: [no-reply@m1crosoft-security.com](mailto:no-reply@m1crosoft-security.com); [bounce-no-reply@m1crosoft-security.com](mailto:bounce-no-reply@m1crosoft-security.com)
* Sending IP: 185.203.110.24 (non‑Microsoft)
* URLs (defanged):
  + hxxps://m1crosoft‑security[.]com/account/reset?session=8f2a1c
  + hxxps://tinyurl[.]com/2y-secure-alert (displayed as Microsoft link)

Appendix: Notes on Analyzer Results

* “SPF Alignment OK” only means RFC5321.MailFrom and RFC5322.From domains match; since the domain itself is deceptive, alignment does not confer trust.
* DMARC “No Record Found” means receivers can’t enforce policy; this increases deliverability of spoofed messages.
* Received timestamps and “With” values (ESMTPS/ESMTPSA) are present and parseable; non‑brand “By” hosts confirm off‑brand routing.