Indicators

Technical indicators

* From/Envelope domain: [m1crosoft-security.com](http://m1crosoft-security.com) (look‑alike of [microsoft.com](http://microsoft.com); numeral “1” used).
* Return-Path: [bounce-no-reply@m1crosoft-security.com](mailto:bounce-no-reply@m1crosoft-security.com) (matches deceptive domain).
* Sending IP: 185.203.110.24 (non‑Microsoft infrastructure).
* Received chain: localhost → [smtp-out.unrelatedsmtp.net](http://smtp-out.unrelatedsmtp.net) → [mail.m1crosoft-security.com](http://mail.m1crosoft-security.com) → [mx.example.com](http://mx.example.com) (off‑brand MTAs).
* SPF authentication: Fail for connecting IP 185.203.110.24; SPF alignment may appear OK only because From and MailFrom share the same deceptive domain.
* DKIM: None present; not authenticated/aligned.
* DMARC: No record published for [m1crosoft-security.com](http://m1crosoft-security.com) (policy absent).
* Message-ID domain: [smtp-out.unrelatedsmtp.net](http://smtp-out.unrelatedsmtp.net) (mismatch with claimed brand).
* X-Originating-IP: 185.203.110.24 (matches off‑brand host).

Link and attachment indicators

* Primary CTA URL: hxxps://m1crosoft‑security[.]com/account/reset?session=8f2a1c (defanged; look‑alike host, not Microsoft).
* “Report suspicious activity” displays a Microsoft URL but actual link is a shortened redirect: hxxps://tinyurl[.]com/2y-secure-alert (defanged; mismatch between displayed and actual).
* No attachment in this sample; note that similar campaigns often use .htm disguised as .pdf.

Content and social‑engineering indicators

* Urgency: 24‑hour deadline to avoid account/service disruption.
* Authority impersonation: “Microsoft Account Security” and references to Outlook/OneDrive/Teams.
* Sensitive data request: Asks for current password and MFA code (never requested by legitimate providers via email).
* Generic greeting: “Dear User,” not personalized.
* Psychological levers: Fear of loss, time pressure, single-click convenience CTA.

Branding and quality indicators

* Look‑alike domain: m1crosoft‑[security.com](http://security.com) vs [microsoft.com](http://microsoft.com).
* Inconsistent infrastructure: Non‑Microsoft sending hosts and IPs.
* Footer/formatting: Generic, non‑standard verbiage; lacks legitimate Microsoft compliance details.

Verdict tags you can include

* Category: Phishing – credential harvesting.
* Confidence: High (multiple strong technical and behavioral indicators).
* Recommended action: Do not click; report as phishing; verify account directly at [account.microsoft.com](http://account.microsoft.com); if interacted, reset password, revoke sessions, and re‑enroll MFA.