Outlook-Mails retten? Vorsicht vor dieser Falle.

Leitfaden für private Postfächer und Arbeitskonten
Stand: 17. November 2026

Die dokumentierte Masche

Nach der Microsoft-365-Störung vom 12. November nutzt eine Phishing-Kampagne die echte Fallnummer EX1550543. Die falsche Mail verlangt einen Klick zum Retten angeblich zurückgehaltener Nachrichten und droht mit Löschung nach 24 Stunden. Logo und Fallnummer sind kein Echtheitsbeleg.

1 Die Mail erhalten, noch nichts angeklickt

Button und Anhänge in Ruhe lassen. Outlook über die gewohnte App oder ein gespeichertes Lesezeichen öffnen. Im Betrieb die IT über den bekannten Kontaktweg fragen. Administratoren prüfen Störungen direkt im Microsoft 365 Admin Center.

2 Verdächtige Nachricht melden

In vielen Outlook-Versionen: Nachricht auswählen, dann „Melden“ → „Phishing melden“. Die Bezeichnung kann abweichen. Bei Firmenkonten den internen Meldeweg nutzen. Außerhalb betrieblicher Vorgaben die Mail nach dem Melden löschen.

3 Geklickt, aber nichts eingegeben

Seite schließen. Festhalten, wann du geklickt hast und was angezeigt wurde. Keine Dateien öffnen und keine weiteren Freigaben erteilen. Ein Klick allein beweist keinen Kontodiebstahl. Beim Arbeitskonto die IT umgehend informieren.

4 Passwort eingegeben oder etwas freigegeben

Betroffenes Passwort über den offiziellen Zugang von einem vertrauenswürdigen Gerät ändern. Dasselbe Passwort auch bei anderen betroffenen Konten ersetzen. Zusätzlichen Anmeldeschutz mit zweitem Faktor prüfen. Der IT auch eingegebene Codes oder bestätigte Freigaben nennen.

5 Datei heruntergeladen oder geöffnet

Heruntergeladene Datei nicht öffnen. Falls schon geöffnet: Gerät auf Schadsoftware prüfen lassen; bei Firmenrechnern sofort die IT einschalten. Sage genau, was du getan hast, damit gezielt geprüft werden kann.

Was noch ungeklärt ist: Microsoft hat für diese Kampagne weder das tatsächliche Sammeln von Zugangsdaten noch die Auslieferung von Schadsoftware bestätigt. Die Schritte oben sind allgemeine Soforthilfe bei Phishingverdacht.

Quellen: Microsoft Threat Intelligence, Warnthread vom 14.11.2026; Verbraucherzentrale, Warnung vom 16.11.2026; Microsoft Support zu Phishing und kompromittierten Konten.

Microsoft-Originalwarnung · Verbraucherzentrale · Microsoft-Soforthilfe