Quote by Devroop Dhar, Co-Founder and Managing Director, Primus Partners

Published in Computer World
November 17th, 2026

Hackers exploit Microsoft 365 outage to launch credential phishing campaign

Using fake Microsoft service health notifications and malicious recovery links, attackers attempted to steal employee login credentials.

Authored by Nidhi Singal



Read on: Hackers exploit Microsoft 365 outage to launch credential phishing campaign | Keywords [with Link in hyperlink]

Article Content:

Cybercriminals are exploiting genuine cloud service disruptions to make phishing attacks more convincing. Just a day after a prolonged outage disrupted several Microsoft services, including Outlook, Exchange Online, Teams and Copilot, Microsoft Threat Intelligence identified a coordinated, high-volume phishing campaign targeting organisations across multiple industry sectors.

The attackers impersonated service notifications and sent emails disguised as legitimate Microsoft 365 service-health notifications. Claiming emails held during the outage would be permanently deleted within 24 hours unless recipients restored them, the threat

actors created a false sense of urgency, tricking recipients into clicking malicious links and potentially exposing their login credentials.

“We assess that the activity was likely credential phishing; however, the available evidence does not confirm credential capture, malware delivery, or post-compromise activity. Multiple threat actors may continue to look for ways to exploit notable global events in any social engineering pretext,” Jeremiah Jasmin, security researcher at Microsoft, said in a blog post.

Outages in cloud services bring about uncertainty and panic, an area where attackers always thrive, said Devroop Dhar, co-founder and MD at Primus Partners. “In cases where employees cannot access their emails and other applications, they will easily fall victim to any email promising to restore their service or help recover their account. This is especially dangerous for industries like finance, health care, government and educational institutions because employees in such organizations work with sensitive data and rely heavily on cloud services,” said Devroop Dhar, co-founder and MD at Primus Partners.

Carefully constructed phishing trap:

The attackers used several techniques to make the emails appear relevant to recipients while evading basic email security filters. These included using specific sender domains, randomised outage-related subject lines, recipient-specific tracking links and a common non-Microsoft destination domain. The combination made the messages harder to identify through conventional pattern matching.

The campaign began with emails sent from domains including moments-notice[.]com, planetmaison[.]com, and newbooker[.]com. Their subject lines followed the pattern “Outage” followed by a randomised string of characters. Microsoft also found a fake email conversation embedded in the message body, positioned to remain hidden from recipients. This appeared to be an attempt to evade email filtering mechanisms.

The messages impersonated Microsoft 365 service health notifications. They used recipient-specific display name prefixes and referenced Microsoft services, including Exchange Online, Outlook, Teams, SharePoint and Copilot.

To create a sense of urgency, the emails claimed that messages held during the November 12 Exchange Online disruption would be deleted within 24 hours. Recipients were prompted to click a prominent “RESTORE MESSAGES” button. The links contained recipient-specific tracking URLs that recorded or routed clicks before redirecting users to reallifeaccounting[.]com, including the path /themelist0.html.

One of the emails analysed by Microsoft had a subject line following the pattern “Outage – <random token>” and a display name comprising a three-character organisation-style prefix followed by “Outage Notification.” Its body referred to a purported Exchange Online incident on November 12, claimed that four messages had been held during the outage and warned that they would be deleted within 24 hours unless restored.

A successful credential theft attempt could expose more than an employee’s email account. Dhar explained that, depending on the permissions of the user, threat actors can gain access to sensitive emails, customer information, balance sheets, SharePoint, OneDrive Storage, and Microsoft Teams communication. Moreover, attackers can pretend to be representatives of the company and send believable emails to colleagues, clients, and contractors for the purposes of money fraud or theft of credentials.

From containment to preparedness:

Microsoft said it had not observed any evidence of account compromise linked to the campaign. Messages detected and protected by Microsoft Defender for Office 365 were being blocked or quarantined. However, the company has advised organisations to remain vigilant and take several precautionary steps.

CISOs should search email telemetry for the identified sender domains, display-name and subject-line patterns, lure phrases, tracking hosts, and destination domains. Matching messages should be quarantined, and copies already delivered to inboxes should be removed in accordance with the organisation’s incident response procedures.

Security teams should also identify users who clicked on campaign links and review click telemetry, proxy logs, and browser or endpoint evidence to establish whether they reached the malicious destination and potentially entered their credentials. If credentials were exposed, organisations should immediately reset the affected passwords, revoke active sessions and refresh tokens, and verify multifactor authentication registrations.

They should also check affected accounts for suspicious sign-ins, unauthorised OAuth consent, new inbox or forwarding rules, delegate permissions and unusual access to Exchange Online, SharePoint, OneDrive or Teams. Microsoft has also advised security teams to block or closely monitor reallifeaccounting[.]com and the observed /themelist0.html path while the activity is investigated. Employees should be reminded that legitimate Microsoft 365 service-health communications do not direct users to non-Microsoft domains to recover held emails.

Dhar added that organizations should make cybersecurity an integral part of their business continuity planning. Any technology disruption should trigger heightened security monitoring and clear internal communication to ensure employees know how to

verify service-related updates. He also recommended conducting phishing simulations during such disruptions to test how employees respond to suspicious communications. CIOs and CISOs should regularly conduct tabletop exercises to assess their preparedness for attacks that exploit technology outages.