zensec

SECURITY BRIEFING NOTE

Microsoft 365 Service Outage: Update

Active phishing campaign exploiting the outage confirmed by Microsoft



Date of note	16 Nov 2026
Previous briefing	Security Briefing Note: Microsoft 365 Service Outage, 13 November 2026, 07:50 UTC (this update adds to it; the original guidance still applies)
Audience	Business leaders, IT and security teams, and all staff
Incident status	Service restored. Microsoft's final service health updates, posted at around 04:15 to 04:17 UTC on 14 November 2026, record the incident as "Service restored", with an end time of 16:10 UTC on 13 November 2026. Microsoft has confirmed the outage was a technical issue, not related to cyber activity.
Microsoft incident references	EX1550543 and MO1550821 (Microsoft 365 admin center)

Key messages

In Friday's briefing we warned that cybercriminals were likely to exploit the Microsoft 365 outage, and that organisations should expect fake notifications about held or quarantined messages that invite users to release them through a link. Microsoft has now confirmed that this is happening. Microsoft Threat Intelligence has reported an active phishing campaign, first detected on 13 November 2026, that poses as a Microsoft 365 service health notice and tells recipients that messages held during the outage will be deleted within 24 hours unless they click to restore them.

The campaign is convincing because it cites the real Exchange Online incident number, EX1550543, and arrives at a time when staff are genuinely waiting for delayed email. Microsoft describes the activity as consistent with credential phishing, which means its likely aim is to steal Microsoft 365 passwords.

Although Microsoft has now restored service, the risk has not passed. Outage-themed lures will continue while organisations work through delayed mail and wait for Microsoft's post-incident report. IT and security teams should search for this campaign in their own environments now, and every organisation should remind staff that a message quoting a genuine incident number is not proof that it is genuine.

Outage status

Microsoft's service health records for EX1550543 and MO1550821 now show the incident as resolved. Microsoft has given a preliminary cause of an issue during an earlier network capacity upgrade that surfaced following a recent network change, and has confirmed this was a technical issue rather than a cyber attack. It has said a preliminary post-incident report will follow within two business days and a final report within five business days.

Service restoration does not mean that security controls are confirmed as working. The post-restoration checks set out in Friday's briefing remain the priority, and the phishing campaign described below makes the email and identity checks more urgent.

The phishing campaign Microsoft has observed

According to Microsoft Threat Intelligence, the emails imitate Microsoft 365 service health notifications and refer to the legitimate incident EX1550543. Some of the messages detected on 13 November falsely claim that email was held during the outage and will be deleted within 24 hours unless the recipient clicks a link to restore it. The deadline is designed to rush users who are already worried about missing customer messages, payments or other urgent communications.

The emails are tailored to look like internal workplace notices. Subject lines follow the pattern "Outage - [six-character code]", and sender display names begin with an organisation-specific prefix followed by "Outage Notification" or "Service Health". Links in the messages pass through recipient-specific SendGrid click-tracking before redirecting the user to an attacker-controlled site. Microsoft reports that similar messages have targeted organisations across multiple sectors in the United States. UK organisations should assume they may receive the same or similar lures.

Indicators reported by Microsoft

The indicators below are shown in a "defanged" format, with square brackets around the final full stop, so they cannot be clicked by accident. Remove the brackets when entering them into security tools.

Indicator type	Value
Email subject pattern	Outage - [six-character code]
Sender display name pattern	[Organisation-specific prefix] Outage Notification, or [Organisation-specific prefix] Service Health
Sender domain	moments-notice[.]com
Sender domain	planetmaison[.]com
Sender domain	newbooker[.]com

Indicator type	Value
Link behaviour	Recipient-specific SendGrid click-tracking links that redirect to the domain below
Redirect domain	reallifeaccounting[.]com, including the path /themelist0.html
Lure content	References genuine incident EX1550543; claims held messages will be deleted within 24 hours unless the user clicks to restore them

What has and has not been confirmed

Microsoft has assessed the activity as consistent with credential phishing. It has not yet confirmed that credentials have been collected or that malware has been delivered, and it has not named the group behind the campaign. Microsoft states that Microsoft Defender blocks the malicious domains used in this campaign and that Microsoft Defender for Office 365 blocks and quarantines the phishing emails. Microsoft has said it will continue to monitor the campaign and share further findings.

Organisations should not treat this as reassurance that no harm has been done. As Friday's briefing set out, Defender for Office 365 protections such as Safe Links, Safe Attachments and quarantine were themselves degraded during the outage, so some messages may have reached inboxes before protections were fully restored. A message that was delivered, or a link that was clicked, still needs to be investigated.

Recommended actions

For IT and security teams now

- Block the three sender domains and the redirect domain listed above at the email gateway, web proxy and DNS filtering layers, and add them to the Tenant Allow/Block List if they are not already blocked.
- Search mail received since 12 November for the subject pattern, sender display names, sender domains and redirect domain, using Microsoft Defender for Office 365 Threat Explorer and Microsoft Defender XDR advanced hunting. Microsoft points to the EmailEvents, EmailUrlInfo and UrlClickEvents tables to identify the messages, examine embedded links and see which users clicked.
- Remove any matching messages that were delivered, including those that may have arrived while email remediation was degraded.
- Investigate every recorded click rather than relying on whether a message was delivered or blocked. For any user who clicked, review sign-in activity for the period, reset the password, revoke active sessions, and check for new multi-factor authentication methods, inbox rules, forwarding to external addresses and newly granted application permissions.

- Confirm that Safe Links policies are switched on and configured correctly. Microsoft notes that Safe Links provides time-of-click protection against malicious URLs when properly configured.
- Look beyond this single campaign. Other outage-themed lures from the list in Friday's briefing, such as fake helpdesk calls, multi-factor authentication prompts and payment detail changes, may be running in parallel using different domains.
- Continue working through the post-restoration checks in Friday's briefing, and review Microsoft's post-incident report when it is published.

Recommended actions

For all staff

- Be wary of any email about the outage, held or deleted messages, or mailbox recovery, even if it quotes a real Microsoft incident number or appears to come from your own organisation.
- Treat any deadline such as "your messages will be deleted within 24 hours" as a warning sign. Pressure to act quickly is a common phishing tactic.
- Do not click links in these messages. Open Outlook and other Microsoft services through your usual app or bookmark instead.
- If you have already clicked a link or entered your password after receiving one of these emails, report it to your IT or security team straight away. Reporting quickly limits the damage, and nobody will be blamed for raising it.
- Never share your password or one-time codes, and reject any sign-in approval prompt you did not start.

Updated staff advisory

The following text can be adapted and circulated to staff:

Microsoft has warned that criminals are sending fake emails about last week's Microsoft 365 outage. The emails look like official service notices, mention a genuine Microsoft incident number and claim that emails held during the outage will be deleted within 24 hours unless you click a link to restore them. These messages are designed to steal your password. Do not click links in any email about the outage, held messages or mailbox recovery, even if it looks official or appears to come from inside the organisation. If you receive one, report it to the IT or security team. If you have already clicked a link or entered your password, tell the IT or security team immediately so they can secure your account.

Need help?

If you believe someone in your organisation has interacted with this campaign, or you are unsure whether your Microsoft 365 security controls have fully recovered, contact Zensec immediately on 0333 091 7040 or at hello@zensec.co.uk.