zensec

SECURITY BRIEFING NOTE

Microsoft 365 Service Outage

Microsoft 365 outage of 12–13 November 2026



Date of note	13 November 2026, 07:50 UTC
Audience	Business leaders, IT and security teams, and all staff
Incident status	Ongoing. Microsoft's public status page reports "Service degradation" for Microsoft 365 (Business or Enterprise) and Microsoft consumer products. Microsoft Azure shows no issues.
Microsoft incident references	EX1550543 and MO1550821 (Microsoft 365 admin center)

Key messages

A global Microsoft 365 outage that began at around 18:00 UTC on 12 November 2026 has disrupted Exchange Online and the many Microsoft 365 features that depend on it, including Outlook, Teams calendar functions, Copilot, Planner, To Do and parts of SharePoint. Microsoft has stated that it is not aware of any malicious activity causing the incident. Its investigation points to a large number of servers becoming unexpectedly unavailable, with recent configuration changes identified as a potential cause.

Although the outage is not believed to be a cyber attack, it has a direct security consequence. Several of the tools organisations rely on to filter malicious email, prevent data loss, monitor threats and manage devices are themselves listed as degraded. For the duration of the outage, and until those controls are confirmed as fully restored, organisations should treat their Microsoft 365 environment as operating with reduced security assurance.

The risk does not end when service returns. Cybercriminals routinely exploit high-profile disruptions, and businesses and their staff should expect outage-themed phishing, fraud and impersonation attempts over the coming weeks.

How the outage weakens security controls

Microsoft's status page lists the services affected. Not all of them carry security consequences, but the following directly reduce an organisation's ability to prevent, detect and respond to threats.

Service	Impact reported by Microsoft	Security implication
Microsoft Defender for Office 365	Safe Links, Safe Attachments and protection and submission policies may fail. Quarantine, Threat Explorer and email remediation may be unavailable. Tenant Allow/Block list changes, message traces and outbound protection may be delayed. Links rewritten by Safe Links fail to open.	Reduced ability to block, investigate and remove malicious email. Security teams cannot reliably block a sender or URL at short notice. Staff frustrated by broken links may look for ways around the protection.
Microsoft Defender XDR	Defender portal pages and solution tabs may not load.	Reduced visibility for security operations and slower incident response across the estate.
Microsoft Purview	Data Loss Prevention, Information Protection labelling and auto-labelling, Communication Compliance, access control and Data Classification are impacted. Audit searches and eDiscovery may be impacted.	Data leakage controls may not enforce as expected, and audit evidence for the period may be delayed or incomplete.
Microsoft Fabric and Power BI	Failures with items carrying sensitivity labels. Microsoft's suggested workaround is to remove the label, where policy allows.	Labels removed as a workaround may never be reapplied, leaving sensitive content unprotected.
Microsoft Intune	Device enrolment, check-in and compliance policies intermittently impacted.	Device compliance status may be out of date, which can affect access decisions that rely on it.
Microsoft 365 admin center	Admins may be unable to load some pages.	Reduced visibility of service health and configuration; Microsoft is posting updates publicly for this reason.
Microsoft Graph	API requests that access Exchange data (mail, calendar, contacts) may time out.	Security monitoring, backup and automation tools that rely on Graph may silently miss data during the outage.
SharePoint Online	Issues sharing files with people outside the organisation.	Staff may turn to unsanctioned file-sharing services to meet deadlines.
Exchange Online	Mailbox access lost on multiple clients; delivery delayed.	A large backlog of delayed mail may arrive at once on recovery, and staff may move work to personal email.

Behavioural and operational exposure

Prolonged outages create pressure to keep business moving, and that pressure produces workarounds. The most common risks are staff sending work documents or customer data through personal email or consumer messaging apps, automatic forwarding rules set up to external accounts, temporary changes to mail routing or security policy, and the use of unapproved file-sharing sites.

Organisations should record each approved workaround and exception made during the outage, and should review and close each once normal service resumes.

Heightened phishing and fraud risk in the coming weeks

Whilst there is no indication that the outage was caused by a cyber incident, as advised by Microsoft, cybercriminals often seek to take advantage of the uncertainty around disruptions of this nature, targeting potentially affected customers with phishing attacks. Businesses should remain vigilant in the coming weeks, not only while the outage continues.

Organisations should expect lures such as:

- Emails or text messages appearing to come from Microsoft or internal IT, asking users to "verify", "reactivate" or "restore" their mailbox, or to sign in to recover lost or undelivered messages.
- Fake notifications about quarantined, held or failed messages that invite the user to release or view them through a link.
- Phone calls, text messages or Teams chats from people posing as the IT helpdesk or Microsoft support, offering help to reconnect and asking for passwords, one-time codes, or for remote access software to be installed.
- Unexpected multi-factor authentication prompts, timed to coincide with "service restoration" messages.
- Lookalike status pages, fake "fix" or "patch" downloads, and counterfeit copies of Microsoft's post-incident report.
- Invoice and payment fraud that uses the outage as cover, for example "our email was down, please use this new address" or "the payment failed, here are our updated bank details".
- Offers of refunds, service credits or compensation for the outage that require a sign-in or payment details.
- Search engine adverts and social media posts that point to fake Microsoft support phone numbers.

Microsoft's genuine public status page is located at status.cloud.microsoft

Recommended actions

For IT and security teams while the outage continues

- Track Microsoft's public status page and, where available, the Microsoft 365 admin center under incident references EX1550543 and MO1550821.
- Communicate with staff through channels that do not depend on email. Microsoft reports that core Teams chat, calls and meetings are largely unaffected; intranet, SMS and phone trees are alternatives.
- Issue an early advisory on outage-themed phishing and fraud (suggested text is below).
- Keep a log of every workaround, temporary exception and configuration change made during the outage.
- Give closer attention to sign-in and identity alerts where those tools remain available, particularly unusual sign-ins and repeated authentication prompts.
- Discourage the use of personal email accounts and unapproved file-sharing services, and remind staff of approved alternatives.

For IT and security teams once services are restored

- Confirm that Safe Links, Safe Attachments, anti-phishing and Data Loss Prevention policies are operating, and that any Tenant Allow/Block list changes made during the outage have taken effect.
- Treat the outage window as a period of reduced assurance: hunt for threats across email and identity activity for the period, scrutinise the backlog of delayed mail as it is delivered, and review quarantine.
- Check for new inbox rules, forwarding to external addresses, changes to mail flow and newly granted application permissions.
- Reapply any sensitivity labels removed as a workaround, and confirm device compliance status in Intune is current.
- Confirm that security monitoring, backup and automation tools connected through Microsoft Graph have caught up, and fill any data gaps.
- Once audit search is available, confirm audit records for the period are complete and document any gaps for compliance purposes.
- Reverse the workarounds and exceptions recorded in the log.
- Review Microsoft's post-incident report when it is published and update business continuity and resilience plans, including alternative communication channels.

Recommended actions

For all staff

- Be suspicious of any message about the outage, passwords, mailbox recovery, quarantined mail or account verification, even if it appears to come from Microsoft or your own IT team.
- Do not click links or open attachments in unexpected messages. Open Microsoft services through your usual bookmarks or apps.
- Never share your password or one-time codes with anyone. Reject any sign-in approval prompt you did not start, and report it.
- Do not move work to personal email or personal cloud storage, and do not install software that claims to fix the problem.
- Report anything suspicious to your IT or security team through your usual route.

Suggested staff advisory

The following text can be adapted and circulated to staff:

You may be aware that Microsoft 365 services, including Outlook and Teams, have been disrupted by a global outage. Microsoft has said it is not aware of any malicious activity causing the problem. However, criminals often take advantage of events like this to send fake emails, text messages and calls. Over the coming weeks, please be especially careful with any message about the outage, your mailbox, passwords, held or undelivered emails, or changes to payment details. Do not click links or share passwords or codes. If something seems unusual, check it with the sender using contact details you already have, and report it to the IT or security team.