Software Dynamics
Microsoft Solutions Partner

CUSTOMER ADVISORY

Microsoft 365, Entra ID and Dynamics 365

Outage phishing

A service-health notice that asks you to restore mail.

On 13 November 2026 Microsoft Threat Intelligence saw a high-volume phishing campaign across many industries. The messages pretend to be a Microsoft 365 outage notice and say held mail will be deleted within 24 hours. The likely aim is a password.

Search the mail. Name who clicked. Reset any account that may have typed a password.

17 NOVEMBER 2026

Read this against every mailbox that signs into Dynamics 365.

01 Observed

13 November 2026. High volume. Many industries. Worldwide. Built around a fake Microsoft 365 outage.

02 Assessment

Likely credential phishing. Link only. Microsoft found no malware in the samples, and named no threat actor.

03 The lure

Subject Outage, then a random token. A 24-hour deletion deadline. A button that leaves Microsoft.

01 Search

Sender domains, the Outage subject, and the destination reallifeaccounting[.]com. From 12 November.

02 Contain

Quarantine matches. List who clicked. Reset any account that may have typed a password on that page.

03 Verify

Service health is read in the Microsoft 365 admin centre. An unsolicited restore link is the phish.

13 NOVEMBER 2026

What arrived.

Microsoft analysed the lures sent that day and published the findings on 16 November. Software Dynamics has not examined the samples. The description below is Microsoft's.

FIELD	WHAT MICROSOFT OBSERVED
Subject	Outage – then six random letters or digits. Example: Outage – aF7vG6. An external-mail tag may sit in front. Two further patterns use the same trick: Strengthen – Security, and Restore — 4 messages, each with a random token.
Display name	Three characters in the style of an organisation code, then Outage Notification or Service Health. Examples: MSF Outage Notification, AMZ Service Health.
Sender	moments-notice[.]com, planetmaison[.]com and newbooker[.]com, plus bounce subdomains em4493.moments-notice[.]com and em.newbooker[.]com.
The claim	A purported Exchange Online incident on 12 November. Four messages held. They will be deleted within 24 hours unless the recipient acts.
The button	RESTORE MESSAGES or TAKE ACTION. The link is unique to the recipient and records the click.
The landing	reallifeaccounting[.]com, including /themelist0.html in multiple samples. Some messages continue to outagefixed[.]sbs or outagerestored[.]sbs.
Names used	The body names Exchange Online, Outlook, Teams, SharePoint and Copilot, and uses Microsoft copyright language. A fake hidden conversation sits in the message, assessed as an attempt to slip past filters.
Absent	QR codes, attachments other than the message itself, and any executable, archive or document payload in the samples Microsoft reviewed.

How far the evidence goes

Microsoft's assessment is credential phishing. The samples stop before the final page. They do not show a password field, a submitted password, malware, or activity after a compromise. The campaign is not tied to a named threat actor. Where Microsoft Defender for Office 365 is on, Microsoft is blocking and quarantining these messages, and reports no indicator of compromise from this attack. Mail that landed before the block, and mail in a tenant without that product, still needs a search.

Administrator

Search from 12 November, quarantine the matches, and block the three destination domains. The names are on page 5. The order of work is on page 6.

Finance

A click by payments, vendor master or payroll is a finance event. Read bank-account and journal changes before the next payment run. Page 7.

Every user

Send the staff note on page 4 this morning. People report the message when they know the sentence they are looking for.

AFTER THE CLICK

Six steps, then the ledger.

Microsoft mapped the chain through the redirect. Credential capture is the assessment, and it was not witnessed in the evidence. The ledger below is what a captured Microsoft 365 identity can reach on an estate we implement.

01 **Delivery**
The message comes from the moments-notice, planetmaison or newbooker sender cluster.

02 **Impersonation**
It poses as Microsoft 365 service health, with a display name built for the recipient's organisation.

03 **Urgency**
Held mail will be deleted in 24 hours. The message depends on the fear of lost business email.

04 **The click**
RESTORE MESSAGES or TAKE ACTION opens a tracking link that is unique to that person.

05 **The redirect**
The observed chain lands on reallifeaccounting[.]com, or on an outage-themed .sbs host.

06 **The aim**
A password. Microsoft did not see one submitted, and did not see the account used afterwards.

MITRE ATT&CK, as mapped by Microsoft: T1566.002 spearphishing link, T1036 masquerading, T1204.001 user execution of a malicious link. Microsoft did not map credential capture, malware, command and control, or theft of data.

If that password is later used

THE ACCOUNT REACHES	WHAT CHANGES IN THE BUSINESS
The mailbox	A reply to a supplier, a forged invoice, or a second wave of the same lure sent internally.
Inbox rules	Forwarding, or a rule that hides bank-detail and payment conversations from the real owner.
OAuth consent	An application that keeps access after the password is changed.
Files	Contracts, bank letters and payroll files in SharePoint, OneDrive and Teams.
Dynamics 365	A vendor bank account, a payment journal, a security role, or an approval that looks routine.

One Entra account, two front doors

The person who reads finance mail usually signs into Finance and Operations or Business Central with the same Entra ID account. A captured Microsoft 365 password is a path to the mailbox and, where multifactor authentication is weak or already satisfied, a path into the ledger. Treat a click by a payments, vendor-master or administrator account as a finance event.

Read these accounts first: accounts payable, vendor master, treasury, payroll, and anyone who can assign a security role in Finance and Operations or Business Central.

SERVICE HEALTH LIVES IN THE ADMIN CENTRE

Refuse the link.

A genuine Microsoft 365 service-health notice is confirmed in the Microsoft 365 admin centre. Recovery of held mail is not sent through a website outside Microsoft.

01 **Leave the button alone**

RESTORE MESSAGES and TAKE ACTION in this lure leave Microsoft. The tracking link records the click and leads to reallifeaccounting[.]com or a related host.

02 **Read service health where it is published**

The administrator opens Service health in the Microsoft 365 admin centre. A real Exchange Online incident is published there. Confirm the incident in that centre when mail claims an outage is underway.

03 **Report it, and say so if you already clicked**

Use the Report button in Outlook, or the path your security team has set. If you clicked, or if you typed a password, tell the service desk the same day and include the time.

WORDS YOU CAN SEND TO STAFF

Microsoft has warned of phishing email that pretends to be a Microsoft 365 outage notice. It says messages were held during a disruption and will be deleted within 24 hours, and it asks you to click Restore messages. Microsoft publishes service health in the admin centre. An email that sends you elsewhere to recover mail is not that notice. Do not click the button. Do not type your password. Report the message in Outlook. If you already clicked or typed a password, tell IT today and include the time.

From-address

The domain is moments-notice, planetmaison, newbooker, or another name that is not Microsoft.

Subject

Outage – and a random token, or Strengthen – Security, or Restore — 4 messages.

Deadline

Twenty-four hours, and the loss of mail if you do nothing.

Destination

The address you would open is not a Microsoft domain. Hover before any click, on any mail.

If you already clicked

01 **The page, and nothing typed**

Report the message and the time. Keep using the mailbox. IT will watch the account.

02 **A password typed**

Tell IT before you send more mail, change a vendor, or approve a payment. The account is reset the same day.

03 **Then an MFA prompt**

You approved a sign-in prompt you were not expecting. Say so. That prompt is part of the incident.

DEFANGED FOR CIRCULATION

What to search.

Microsoft published these indicators on 16 November 2026. Brackets keep the names from becoming links. Remove the brackets before you search or block. Confirm a hit in your own logs before you treat it as this campaign.

INDICATOR	TYPE	USE
moments-notice[.]com	Sender	Search
em4493.moments-notice[.]com	Sender	Bounce or mail-from
planetmaison[.]com	Sender	Search
newbooker[.]com	Sender	Search
em.newbooker[.]com	Sender	Bounce or mail-from
url.newbooker[.]com	Tracking	Click and open host
url7489.newbooker[.]com	Tracking	Click and open host
reallifeaccounting[.]com	Destination	Block
reallifeaccounting[.]com/themelist0.html	URL	Block the path
outagefixed[.]sbs	Destination	Block
outagerestored[.]sbs	Destination	Block
outagerestored[.]sbs/topics_pxyk/themelist0.html	URL	Block the path
162.120.17[.]69 port 8080	IP	Tracking images, /t/v3
Outage – <six characters>	Subject	Random token
Strengthen – Security <token>	Subject	Random token
Restore — 4 messages <token>	Subject	Random token

Leave SendGrid in place

Three tracking hosts appeared under ct.sendgrid[.]net: u113727626, u118254266 and u118250677. Search for them beside the sender, the subject and the destination. A block on sendgrid[.]net will break legitimate mail. Microsoft’s guidance is to combine sender, content, URL and behaviour, and to block the destination domains above.

In Microsoft Defender XDR, Microsoft published three advanced hunting queries: messages by sender domain or subject, messages that contain the campaign URLs, and clicks on those URLs. Tenants without Defender for Office 365 can search for the same sender domains, subjects and URLs in Exchange message trace and the URL click report, from 12 November 2026.

SEARCH, THEN DECIDE

This week.

Defender for Office 365 is already blocking this mail where it is switched on. The search still matters for anything delivered earlier, and for tenants that do not have that product.

01 **Search from 12 November**

Sender domains and subject patterns on the previous page, plus any URL containing reallifeaccounting, outagefixed or outagerestored. Use Explorer or quarantine if you have Defender for Office 365. Otherwise use message trace in the Exchange admin centre.

02 **Remove what was delivered**

Quarantine matches and delete delivered copies under your usual process. Record the recipients before you purge, so the click review has a list.

03 **Name who clicked**

Use the click log in Microsoft Defender, the URL click report, proxy logs, and the browser on the endpoint. Record whether the click was allowed and whether the destination opened.

04 **Split the response**

A click with no password typed: watch the account and coach the person. A password that may have been typed: go to the next page the same day. Payments, vendor-master and administrator accounts take the stronger path on any doubt.

05 **Block the destinations**

Block reallifeaccounting[.]com, outagefixed[.]sbs and outagerestored[.]sbs at the mail gateway and the web proxy. Keep the block tied to this campaign. Revisit it when Microsoft updates the indicator list.

06 **Tell people where service health lives**

Send the staff note on the previous page. Say, in one line, who receives a report and how fast a typed password is reset.

Name an owner for each action

The Microsoft 365 administrator runs the search and the quarantine. The identity administrator resets passwords and revokes sessions. The finance controller watches vendor bank accounts and payment journals for the people on the click list. The service desk sends the staff note and takes the reports. One name on each, today.

Done when

The week is complete when four things are true. The search runs from 12 November through today, and the recipient list is kept. Every click is marked as a password typed, or as no password typed. reallifeaccounting[.]com, outagefixed[.]sbs and outagerestored[.]sbs are blocked at mail and at the web proxy. The staff note has gone out, and each of the four owners above has a name.

SAME DAY

If a password was typed.

Microsoft did not observe this follow-on activity in the samples. These checks are the ones to run when a person may have submitted credentials to the landing page.

01 **Reset and revoke**

Reset the password. Revoke active sessions and refresh tokens in Entra ID. Sign the user out of Outlook, Teams and Dynamics 365.

02 **Check the second factor**

Look for an MFA method added or changed after 12 November. Remove anything the user does not recognise. Prefer a phishing-resistant method when you re-register them.

03 **Read the sign-ins**

New IP addresses, new devices, unfamiliar user agents, and sign-ins outside the person's normal hours. Include the Dynamics 365 and Business Central applications, not only Exchange.

04 **Read consent and rules**

New OAuth grants. Inbox rules, forwarding, and delegate access. Sweep rules and mailbox permissions. Remove anything the user did not create.

05 **Read the files they can open**

Unusual access to Exchange, SharePoint, OneDrive and Teams from that account after the click time.

Then read Finance and Operations, or Business Central.

LOOK AT	FROM THE CLICK TIME, FOR THAT USER
Vendor bank account	Any change by that user, or by someone they emailed in the days after the click.
Payment journal	Lines created, edited or posted by that user.
Security roles	A new role, a new approver, or a change to an integration account they administer.
Workflow	Approvals completed from a new location or a new device.
Power Automate	A flow that moves mail, payment files or vendor records, created by that user.

Pause that user. The payment run continues.

Until the five identity checks and the ledger checks are clean, pause vendor-bank edits and payment posting for that user. A finance manager reviews the held items before they are released. Bring six facts to the ticket: the user, the click time, whether a password was typed, whether an unexpected MFA prompt was approved, sign-ins since the click, and any vendor-bank or payment-journal change since the click.

AFTER THIS CAMPAIGN

Make the next lure expensive.

The pretext will change. The next one will borrow a different outage, a tax deadline, or a payment hold. The controls below still apply.

01 **Phishing-resistant sign-in**
Passkeys or FIDO2 security keys for finance, vendor-master and administrator roles first. App-based MFA everywhere else. Retire SMS for those roles.

02 **Defender for Office 365**
Safe Links, Safe Attachments, and Zero-hour auto purge, so a message delivered before the intelligence lands can still be removed.

03 **Conditional Access**
Block legacy authentication. Require MFA for Exchange, SharePoint, and the Dynamics 365 and Business Central applications.

04 **Two people on a bank account**
A vendor-bank change needs a second person. Alert when the bank account on a vendor changes, and when a payment journal is posted by a new device.

05 **Practice this exact lure**
Attack simulation training with an outage, a 24-hour deadline, and a Restore messages button. Include the finance team.

06 **A report path that is used**
The Outlook report button, routed to people who can search the tenant the same day. Publish that path in the staff note.

Source. Microsoft Threat Intelligence, 16 November 2026. High volume phishing campaign, Microsoft Security Blog

THREE REGISTERED COMPANIES

Johannesburg
South Africa
Software Dynamics SA (Pty) Ltd
Reg. No. 2026/211288/07
37 Willow Avenue, Craigavon, Sandton 2191
+27 72 972 3135
sales@softwaredynamics.co.za

Nairobi
Kenya
Software Dynamics Limited
CPR/2011/62397
Mezzanine Floor, Titan Complex, Chaka Road, Nairobi
+254 768 341 410
sales@softwaredynamics.co.ke

Melbourne
Australia
Software Dynamics Group Pty Ltd
ACN 696 184 666
5A Springs Road, Donnybrook, VIC 3064
+61 423 605 291
sales@softwaredynamics.com.au

Send the click list sales@softwaredynamicsgroup.com