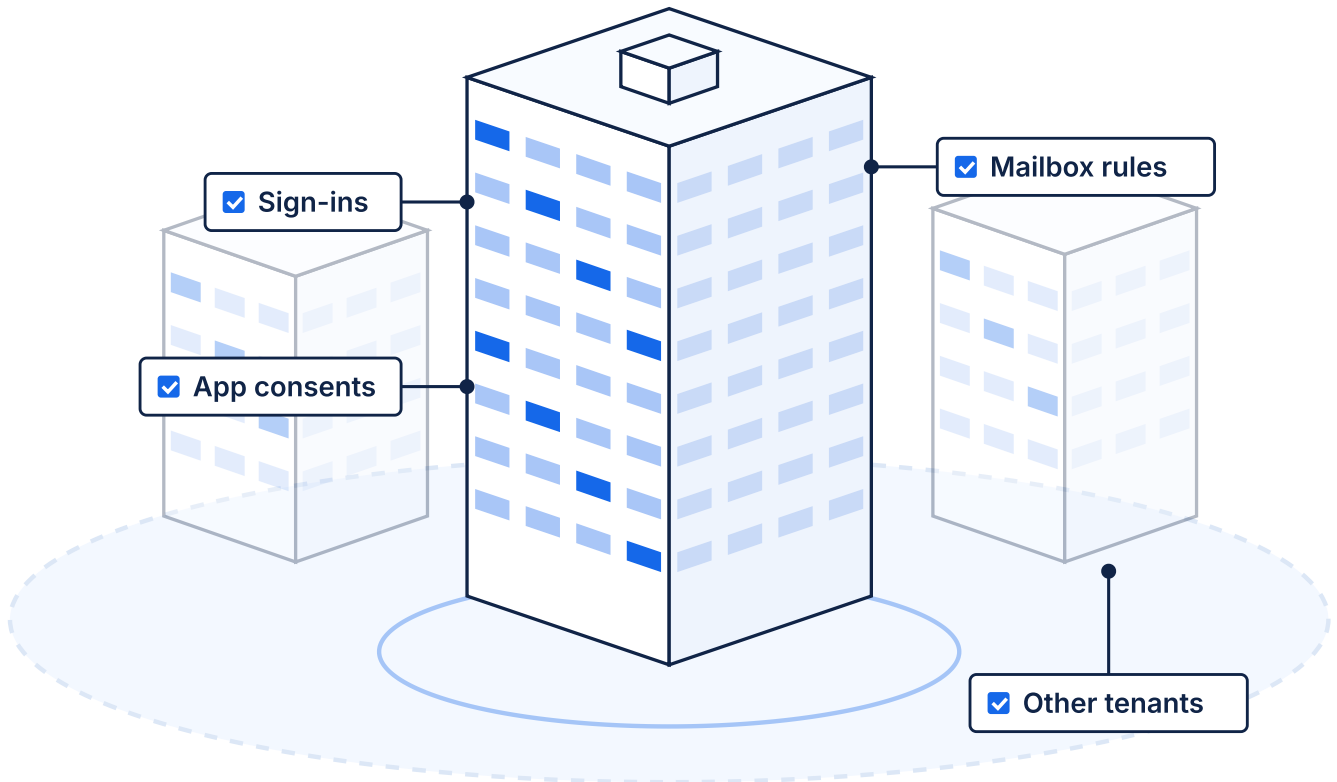




FREE RUNBOOK FOR MSPS AND MSSPS

The First-Hour Runbook

One customer shows a suspicious Microsoft 365 sign-in, a strange mailbox rule or a phishing email. What to check in the first hour, at that customer and at every other customer you look after.

- 1 Confirm
- 2 Check the mailbox
- 3 Contain
- 4 Check every other customer
- 5 Close the door
- 6 See it next time
- 7 Tell the customer

Customer		Ticket / incident	
Opened by		Date and time	

Before you start

Use this runbook the moment one of these lands on your desk. It's built for a technician working alone, so every step says where to click, what to run and what "good" looks like. Fill it in as you go and attach it to the ticket.

Open it when

A strange sign-in

A sign-in from an unusual country or provider, an MFA prompt the user didn't start, or a risky sign-in alert.

A mailbox rule nobody made

Mail disappearing, replies not arriving, or an alert about a new forwarding or redirect rule.

A phishing email

A user reports one, or clicked a link, entered a password or approved a prompt.

The first hour

0–15 min	15–30 min	30–45 min	45–60 min
Step 1–2. Confirm what happened at the first customer and check the mailbox.	Step 3. Contain: block sign-in, rules and forwarding, password, MFA, mailbox permissions, apps, sender.	Step 4. Check every other customer for the same sender, subject or sign-in source.	Step 5–7. Close the door it came through, make sure you'll see it next time, tell the customer.

What you need ready

Delegated admin access (GDAP) to the customer. Most steps need `Exchange Administrator` `Security Administrator` `Authentication Administrator` `User Administrator`; an admin account needs `Privileged Authentication Administrator`; a rogue app needs `Cloud Application Administrator`. Global Reader isn't enough: `Get-InboxRule` fails with it. Purging email (step 3) needs Search And Purge, which through GDAP only `Global Administrator` has. User consent settings (step 5) need `Privileged Role Administrator` in Graph PowerShell, or Global Administrator in the portal. Global Administrator through GDAP isn't recommended: ask the customer's own admin instead.

PowerShell modules: `ExchangeOnlineManagement` 3.9.0 or later (3.7.0 is the minimum for `Get-MessageTraceV2`, 3.9.0 for the purge in step 3) and `Microsoft.Graph`. Windows PowerShell 5.1 works; in PowerShell 7, module 3.10 or later needs PowerShell 7.6.

Graph PowerShell consent, set up before you need it. Through GDAP, Graph PowerShell only works in a customer tenant that has already consented to the Microsoft Graph Command Line Tools app for the scopes on page 04. An admin at the customer grants it once. Error AADSTS90099 means it hasn't been done: use the Entra admin centre instead.

A list of every customer tenant you manage (each tenant ID or primary `.onmicrosoft.com` domain), saved as `customers.csv` with one column called `Domain`. You'll need it in step 4.

The customer's contact for incidents, and who at your MSP signs off on contacting them.

How to read the tags

Any tenant

Works in every Microsoft 365 tenant with Exchange Online.

Entra ID P1

Needs Entra ID P1, included in Microsoft 365 Business Premium, E3 and E5. Office 365 E3 and E5 don't include it.

Entra ID P2

Needs Entra ID P2 (Microsoft 365 E5, or an add-on). Office 365 E5 doesn't include it.

Defender for Office 365 P2

Needs Defender for Office 365 Plan 2 (Microsoft 365 E5, Office 365 E5, or an add-on). Where there's a way without it, we give it.

Portal menus move. Microsoft renames admin-centre menus often. Each step names the setting, so search for that name if a path has changed.

1

0-10 MINUTES

Confirm it at the first customer

Find out whether someone else signed in as the user, and what they changed. If the attacker looks active right now (a sign-in in the last hour, mail going out, a payment request in progress), do step 3, items 1 and 2 first: block sign-in, then remove the rules and forwarding. Write each rule down before you remove it, and don't delete apps or messages until you've written them down.

Affected user

Read the user's sign-in log Any tenant

Look for sign-ins from a country, IP address or provider the user doesn't use, at odd hours, or a successful sign-in right after many failures. Check both the interactive and the non-interactive tabs.

Entra admin centre > Entra ID > Users > the user > Sign-in logs. Free tenants keep 7 days, P1 and P2 keep 30.

Check risky sign-ins and risky users Entra ID P2

Note any "at risk" or "confirmed compromised" state and the risk detections listed.

Entra admin centre > ID Protection > Risky users / Risky sign-ins. Without P2 you see limited detail; rely on the sign-in log.

Look for new MFA methods Any tenant

An attacker often registers their own phone or authenticator app to keep access. Compare the list with what the user really owns.

Entra admin centre > Entra ID > Users > the user > Authentication methods. Also Audit logs, service "Authentication Methods", activity "User registered security info".

Check the user's recent account activity Any tenant

In the Entra audit log, filter on the user for password changes, new app consents and role changes in the last 7 days.

Entra admin centre > Entra ID > Monitoring & health > Audit logs.

Write down what you found

You'll search for these at every other customer in step 4.

Suspicious IP(s)		Country / provider	
First bad sign-in		App used to sign in	
Phishing sender		Subject	
Link domain		Message ID	

Get the sender, subject and message ID from the reported email's headers, or run a message trace on the user's mailbox for the last 10 days. The sender and subject are the most useful things to search for at other customers; a message ID only finds that exact email.

2 10–15 MINUTES

Check the mailbox

After a mailbox takeover, attackers hide what they do. A password reset alone doesn't undo any of it, so record what you find before you contain.

Connect first. These two connections cover steps 2 and 3.

```
Connect-ExchangeOnline -UserPrincipalName you@yourmsp.com -DelegatedOrganization customer.onmicrosoft.com
Connect-MgGraph -TenantId customer.onmicrosoft.com -Scopes "User.Read.All","Application.Read.All", `
"DelegatedPermissionGrant.ReadWrite.All","User.RevokeSessions.All","User.EnableDisableAccount.All","AuditLog.Read.All"
```

Graph through GDAP only works if the customer has already consented to Microsoft Graph Command Line Tools for these scopes (page 02). If it fails, use the Entra admin centre paths.

Inbox rules, including hidden ones Any tenant

Rules that forward or redirect mail, delete it, mark it as read, or move it to RSS Feeds, Archive or Conversation History, often matching words like invoice, payment or bank. Hidden rules don't show in Outlook. The Description line sums up every condition and action; note each rule's Identity for step 3.

```
Get-InboxRule -Mailbox user@customer.com -IncludeHidden |
Format-List Name,Identity,Enabled,Description,ForwardTo,ForwardAsAttachmentTo,RedirectTo
```

Forwarding on the mailbox Any tenant

```
Get-Mailbox user@customer.com | Format-List ForwardingSmtpAddress,ForwardingAddress,DeliverToMailboxAndForward
```

Who else can read, send as or send on behalf of this mailbox Any tenant

```
Get-MailboxPermission user@customer.com | Where-Object { $_.User -notlike 'NT AUTHORITY*' }
Get-RecipientPermission user@customer.com | Where-Object { $_.Trustee -notlike 'NT AUTHORITY*' }
Get-Mailbox user@customer.com | Format-List GrantSendOnBehalfTo
```

Apps the user consented to Any tenant

Consent phishing gives an app lasting access to mail or files, and MFA doesn't stop it. Look for apps you don't recognise with mail, file or offline-access permissions. Note each GrantId: step 3 needs it.

Entra admin centre > Entra ID > Users > the user > Applications, or in Graph PowerShell:

```
Get-MgUserOAuth2PermissionGrant -UserId user@customer.com | ForEach-Object {
$app = Get-MgServicePrincipal -ServicePrincipalId $_.ClientId
[pscustomobject]@{ App = $app.DisplayName; AppId = $app.AppId; Scope = $_.Scope; GrantId = $_.Id } } | Format-List
```

This lists only consents the user gave. Apps an admin approved for everyone are under Enterprise apps > the app > Permissions > Admin consent.

2 CONTINUED

Did the account send phishing onwards? Any tenant

Attackers often use the hijacked mailbox to phish the customer's own contacts. Check outbound mail from the user.

```
Get-MessageTraceV2 -SenderAddress user@customer.com -StartDate (Get-Date).AddDays(-7) -EndDate (Get-Date) |
Format-Table Received,RecipientAddress,Subject,Status
```

What did the attacker do or read? Any tenant

Search the audit log from the first bad sign-in for New-InboxRule, Set-Mailbox, MailItemsAccessed, FileDownloaded and AnonymousLinkCreated. MailItemsAccessed is on by default only for E3 and E5 users. If `Get-AdminAuditLogConfig` shows False (step 6), there's no history to search: write that down, it matters for step 7.

```
Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-10) -EndDate (Get-Date) -UserIds user@customer.com `
-ResultSize 5000 |
Sort-Object CreationDate | Format-Table CreationDate,Operations,RecordType
```

Found

Incident timeline

Times from the logs and from your own actions, in one place. You'll need them for step 7. Message trace and audit times are in UTC.

TIME (UTC)	WHAT YOU SAW OR DID

3

15-30 MINUTES

Contain

Work in this order. Block sign-in first: revoking sessions alone doesn't stop an attacker who has the password, or their own MFA method, from signing straight back in. Then remove the forwarding: it keeps sending mail to the attacker even while sign-in is blocked.

1. Block sign-in, then revoke all sessions Any tenant

Entra admin centre > Entra ID > Users > the user > Account status > Edit > clear Account enabled, then Overview > Revoke sessions, or:

```
Update-MgUser -UserId user@customer.com -AccountEnabled:$false
Revoke-MgUserSignInSession -UserId user@customer.com
```

Revoking can take a few minutes, and apps keep any access token they already hold until it expires (usually an hour). If the user is synced from on-premises Active Directory, disable the account in AD instead.

2. Remove the malicious rules and forwarding Any tenant

Use the Identity from step 2: attacker rules often have blank or duplicate names. If you came straight from step 1, list and note the rules first with the step 2 command. Changing rules in PowerShell also removes the user's client-side Outlook rules, so tell them.

```
Remove-InboxRule -Mailbox user@customer.com -Identity "Identity from step 2"
Set-Mailbox user@customer.com -ForwardingSmtpAddress $null -ForwardingAddress $null
```

3. Reset the password and tell the user out of band (phone, not email). If the user is synced from Active Directory, reset it in AD. If the account is an admin, also check what it changed.

4. Remove MFA methods the user doesn't own, or select Require re-register MFA. Any tenant

Require re-register MFA only removes phone numbers, Authenticator apps and OATH tokens, so delete any passkey or other method you don't recognise by hand.

Entra admin centre > Entra ID > Users > the user > Authentication methods.

5. Remove the extra mailbox permissions found in step 2: anyone who shouldn't read, send as or send on behalf of the mailbox Any tenant

```
Remove-MailboxPermission user@customer.com -User "account from step 2" `
-AccessRights FullAccess -InheritanceType All
Remove-RecipientPermission user@customer.com -Trustee "account from step 2" `
-AccessRights SendAs
Set-Mailbox user@customer.com -GrantSendOnBehalfTo @{Remove="account from step 2"}
```

6. Remove consent for apps you don't trust Any tenant

A grant the user made can't be removed in the portal. Remove each grant with its GrantId from step 2, and switch a malicious app off at once: Enterprise apps > the app > Properties > Enabled for users to sign-in? > No (needs Cloud Application Administrator). Tokens the app already holds keep working until they expire.

```
Remove-MgOAuth2PermissionGrant -OAuth2PermissionGrantId "GrantId from step 2"
```

3

CONTINUED

7. Block the sender and the link in this tenant [Any tenant](#)

A sender block also stops users here mailing that address, so check first whether it's a real supplier's hijacked mailbox. If the link sits on a shared service (SharePoint, OneDrive, Dropbox), block the path, for example `contoso.sharepoint.com/sites/x/*`, not the whole domain.

```
New-TenantAllowBlockListItems -ListType Sender -Block -Entries "phisher@example.com" -NoExpiration
New-TenantAllowBlockListItems -ListType Url -Block -Entries "badsite.example" -NoExpiration
```

8. Remove the phishing email from other mailboxes in this tenant

Both routes need the Search And Purge role; through GDAP only Global Administrator includes it. Without it, ask the customer's admin, or in Explorer choose Propose remediation for someone with the role to approve.

With [Defender for Office 365 P2](#): Defender portal > Email & collaboration > Explorer > select the messages > Take action > Move or delete > Soft deleted items.

Without it: in Security & Compliance PowerShell (module 3.9.0 or later), search for the sender and subject, never the message ID, check the count, then purge:

```
Connect-IPPSSession -UserPrincipalName you@yourmsp.com -DelegatedOrganization customer.onmicrosoft.com `
-AzureADAuthorizationEndpointUri https://login.microsoftonline.com/customer.onmicrosoft.com -EnableSearchOnlySession
New-ComplianceSearch -Name "Phish purge" -ExchangeLocation All `
-ContentMatchQuery '(From:phisher@example.com) AND (Subject:"Invoice overdue")'
Start-ComplianceSearch -Identity "Phish purge"
Get-ComplianceSearch -Identity "Phish purge" | Format-List Status,Items
New-ComplianceSearchAction -SearchName "Phish purge" -Purge -PurgeType SoftDelete
```

A purge removes at most 10 items per mailbox per run, and doesn't work on mailboxes on litigation hold.

9. Turn sign-in back on, then give the user a Temporary Access Pass so they can set up MFA safely, once items 2 to 7 are done. A user whose sign-in is blocked can't set up MFA. [Any tenant](#)

Entra admin centre > Entra ID > Users > the user > Account status > Edit > Account enabled, then Authentication methods > Add authentication method > Temporary Access Pass.

The user signs in with the pass at `mysignins.microsoft.com/security-info` and sets up MFA. Creating a pass needs Authentication Administrator, or Privileged Authentication Administrator for an admin account. If the option is missing, enable Temporary Access Pass under Entra ID > Authentication methods > Policies first.

Notes

Contained at

By

4

30-45 MINUTES

Check every other customer

Every Microsoft 365 tenant is separate. The block you just made protects this customer only. Phishing waves often hit several customers of the same MSP: shared suppliers, the same region, the same sector. So search each tenant for what you wrote down in step 1.

A. The same email, in every tenant

This script reads `customers.csv`, connects to each customer through your delegated access, runs the same message trace and saves two files: the hits, and one summary line per customer. You may be asked to sign in for each customer. Message trace covers the last 90 days, at most 10 days and 5,000 results per search. Times are in UTC. [Any tenant](#)

```
# Fill in what you found in step 1
$sender = "phisher@example.com"
$end = Get-Date
$start = $end.AddDays(-10)
$me = "you@yourmsp.com"
$conn = @{ UserPrincipalName = $me; CommandName = 'Get-MessageTraceV2'
          ShowBanner = $false; ErrorAction = 'Stop' }
$summary = @()

$hits = foreach ($c in Import-Csv .\customers.csv) {
    try {
        Connect-ExchangeOnline @conn -DelegatedOrganization $c.Domain
        $found = @(Get-MessageTraceV2 -SenderAddress $sender -StartDate $start -EndDate $end `
            -ResultSize 5000 -ErrorAction Stop)
        $found | Select-Object @{n='Customer';e={$c.Domain}}, Received, RecipientAddress, Subject, Status
        $summary += [pscustomobject]@{ Customer = $c.Domain; Result = "$($found.Count) found" }
    }
    catch {
        $summary += [pscustomobject]@{ Customer = $c.Domain; Result = "NOT CHECKED: $($_.Exception.Message)" }
    }
    finally { Disconnect-ExchangeOnline -Confirm:$false -ErrorAction SilentlyContinue }
}
$hits | Export-Csv .\phish-sweep.csv -NoTypeInformation
$summary | Export-Csv .\phish-sweep-summary.csv -NoTypeInformation
$summary | Format-Table -AutoSize
```

No sender to search? Replace `-SenderAddress $sender` with `-Subject "..." -SubjectFilterType Contains`, or with `-MessageId "<id@host>"` using the full ID including the angle brackets. A message ID only finds that same email, not a new send of it. Message trace can't search inside the body for a link; that needs Explorer [Defender for Office 365 P2](#) in each tenant.

B. The same sign-in source

In each customer's Entra admin centre, go to Entra ID > Monitoring & health > Sign-in logs, filter on the IP address from step 1 and check both the interactive and the non-interactive tabs. [Any tenant](#) To script it, connect with the scope `AuditLog.Read.All` and run `Get-MgAuditLogSignIn -Filter "ipAddress eq '203.0.113.7'" -Top 50` [Entra ID P1](#). That only returns interactive sign-ins, so still check the non-interactive tab in the portal.

On a hit

Treat that customer as a new incident: repeat steps 1 to 3 there, and note it in the table on the next page. Every "NOT CHECKED" line in the summary is a gap to fix, not a clean result.

Every customer checked

Tenants I could not check	
---------------------------	--

5

45-55 MINUTES

Close the door it came through

Five settings explain most account takeovers in Microsoft 365. Check them at the affected customer now, and plan the same check for the others.

MFA exclusions nobody owns Entra ID P1

Open every Conditional Access policy that requires MFA and read who is excluded. Only break-glass accounts and documented service accounts belong there, through a named group with an owner.

Entra admin centre > Entra ID > Conditional Access > Policies > the policy > Users or workload identities > Exclude.

Old sign-in methods still allowed Any tenant

Legacy protocols can't do MFA, so a stolen password works straight away. In the sign-in log, filter Client app on the legacy protocols, on both the interactive and non-interactive tabs. Block them with a Conditional Access policy (P1) or security defaults (free). Check SMTP AUTH, the one most often left on. Microsoft plans to turn basic authentication for it off by default at the end of December 2026, but admins can turn it back on, so don't rely on that date. With security defaults on, it's already off. Otherwise check the organisation setting and any mailbox that overrides it:

```
Get-TransportConfig | Format-List SmtplibAuthenticationDisabled
Get-CASMailbox -ResultSize Unlimited |
  Where-Object { $_.SmtplibAuthenticationDisabled -eq $false } | Format-Table Identity
```

True on the first line means it's off for the organisation; the second line lists mailboxes set to allow it anyway.

Too many Global Administrators Any tenant

Microsoft recommends giving Global Administrator to fewer than five people, and keeping two cloud-only break-glass accounts with the role. Admins should use phishing-resistant MFA (passkeys, FIDO2 keys, Windows Hello for Business).

Entra admin centre > Entra ID > Roles & admins > Global Administrator > Assignments.

Users can approve any app Any tenant

"Allow user consent for apps" is the setting that makes consent phishing work. Choose a stricter option ("Do not allow user consent", or consent only for apps from verified publishers) and turn on the admin consent workflow. User consent settings need Privileged Role Administrator in Graph PowerShell, or Global Administrator in the portal; the admin consent workflow needs Global Administrator. Changing them doesn't remove consents users already gave; that's step 3.

Entra admin centre > Entra ID > Enterprise apps > Consent and permissions > User consent settings, then Admin consent settings.

Device-code sign-in allowed for everyone Entra ID P1

Device-code phishing tricks users into signing an attacker in. First look for the Microsoft-managed policy "Block device code flow" and check it's On. Otherwise block the device code flow for users who don't need it with a Conditional Access policy (Conditions > Authentication flows > Device code flow), in report-only first if Teams Rooms or shared devices sign in this way. Without P1, security defaults block device code flow.

Changed today

To plan for all customers

6

55-60 MINUTES

Make sure you'll see it next time

Audit logging is on [Any tenant](#)

Microsoft states that auditing isn't turned on by default for Business Basic, Business Standard and Business Premium, or for unmanaged tenants on free enterprise trials. Without it you can't see what an attacker did, and turning it on doesn't recover past activity.

```
# Exchange Online PowerShell only: in Security & Compliance PowerShell the value always shows False
Connect-ExchangeOnline -UserPrincipalName you@yourmsp.com -DelegatedOrganization customer.onmicrosoft.com
Get-AdminAuditLogConfig | Format-List UnifiedAuditLogIngestionEnabled
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
# If told to run Enable-OrganizationCustomization, run it once, then repeat the Set command. Allow up to 60 minutes.
```

Microsoft's alerts reach someone

Built-in alert policies are on by default and email the customer's Global Administrators, not your GDAP technicians. Add your MSP's monitored mailbox as a recipient on "User restricted from sending email" (all plans, including Business) and, on E1, E3 and E5, "Creation of forwarding/redirect rule", which only catches rules made in Outlook on the web or PowerShell. Changes can take up to 24 hours.

Microsoft Defender portal > Email & collaboration > Policies & rules > Alert policy.

7

BEFORE YOU CLOSE THE TICKET

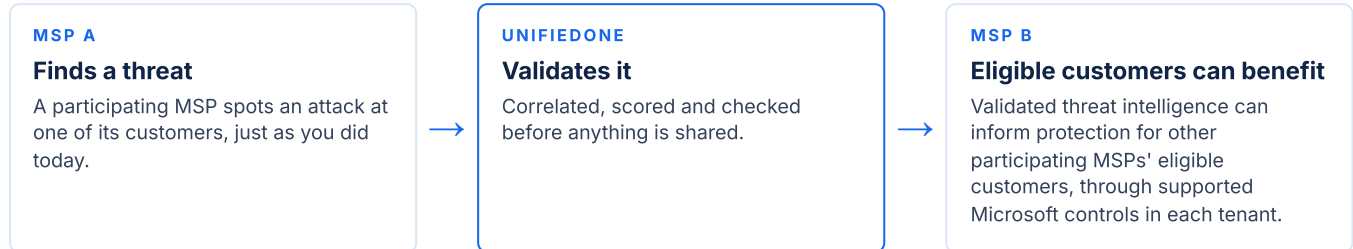
Tell the customer

Short and plain. Send it from your ticket system, and phone your contact first if money or bank details could be involved. If personal data may have been read or sent on, tell the customer today and note the time. Under GDPR they decide whether to report it to their data protection authority, within 72 hours of becoming aware where that's required. If they fall under NIS2, a significant incident needs an early warning within 24 hours.

What happened	
When we found it	
What we did	
What you need to do	
For example: tell staff to ignore and delete the email; finance to confirm any change of bank details by phone; the user to sign in again and set up MFA.	
Your contact	

What if one MSP has already spotted it?

Step 4 is the slow one: one tenant at a time, and only your own customers. One MSP may have spotted the same phishing wave yesterday. That's the problem UnifiedONE is built for.



What travels

Privacy-safe, validated threat intelligence, under the platform's participation and data-handling controls. Customer identities and raw tenant data are not shared between participants.

Who decides

Each customer's policy and permissions decide what happens in its tenant. Community sharing is optional.

What it protects today

Each eligible customer's Microsoft 365 tenant: supported protection for identities, sign-ins and email, plus devices where Microsoft Defender for Endpoint is in place.

What it needs

A Microsoft 365 tenant with Microsoft Entra ID P1 or higher, and consent from a Global Administrator. No UnifiedONE agents to install.

Keep your existing security tools. Strengthen your Microsoft protection. We replace nothing.

Microsoft Defender for Endpoint is integrated with UnifiedONE today. Customers who use CrowdStrike, Bitdefender, ESET, SentinelOne, Sophos or another endpoint product keep it, and UnifiedONE can still add supported Microsoft identity and email protection.

Free protection check. Connect one customer tenant in the 30-day free trial and see what UnifiedONE can protect, and where the gaps are. Start at unifiedone.com/free-trial. After 30 days, your subscription starts automatically unless you cancel.



UnifiedONE

Connected Intelligence. Collective Protection.

unifiedone.com

Where each step comes from

Every step follows Microsoft's own documentation, checked on 22 October 2026. Microsoft changes portal menus and cmdlets regularly; if something doesn't match, the page below has the current version.

STEP	MICROSOFT LEARN PAGE
1 Sign-in logs	Sign-in logs in Microsoft Entra ID https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-sign-ins
1 Risky users	Investigate risk with Microsoft Entra ID Protection https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-investigate-risk
1, 3 MFA methods	Manage user authentication methods https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-userdevicesettings
2–3 Compromised mailbox	Respond to a compromised email account https://learn.microsoft.com/en-us/defender-office-365/responding-to-a-compromised-email-account
2 Inbox rules	Detect and remediate Outlook rules and custom forms injections attacks https://learn.microsoft.com/en-us/defender-office-365/detect-and-remediate-outlook-rules-forms-attack
2 App consents	Detect and remediate illicit consent grants https://learn.microsoft.com/en-us/defender-office-365/detect-and-remediate-illicit-consent-grants
2 What the attacker read	Use MailItemsAccessed to investigate compromised accounts https://learn.microsoft.com/en-us/purview/audit-log-investigate-accounts
2, 4 Message trace	Get-MessageTraceV2 https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/get-messagetracev2
3 Block and revoke	Revoke user access in an emergency in Microsoft Entra ID https://learn.microsoft.com/en-us/entra/identity/users/users-revoke-access
3 Switch off an app	Disable user sign-in for an application https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/disable-user-sign-in-portal
3 Mailbox permissions	Remove-MailboxPermission https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/remove-mailboxpermission
3 Temporary Access Pass	Configure a Temporary Access Pass in Microsoft Entra ID https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-temporary-access-pass
3 Block sender and URL	Manage the Tenant Allow/Block List https://learn.microsoft.com/en-us/defender-office-365/tenant-allow-block-list-about
3 Remove the email (P2)	Remediate malicious email delivered in Office 365 https://learn.microsoft.com/en-us/defender-office-365/remediate-malicious-email-delivered-office-365
3 Remove the email	Find and delete email messages in eDiscovery https://learn.microsoft.com/en-us/purview/edisc-search-mailbox-data
3 Security & Compliance	Connect to Security & Compliance PowerShell https://learn.microsoft.com/en-us/powershell/exchange/connect-to-scc-powershell
4 Delegated access	Connect to Exchange Online PowerShell https://learn.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell
5 Legacy sign-in	Block legacy authentication with Conditional Access https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-legacy-authentication
5 SMTP AUTH	Enable or disable SMTP AUTH in Exchange Online https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission
5 Admins	Best practices for Microsoft Entra roles https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices
5 User consent	Configure how users consent to applications https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent
5 Device code flow	Block authentication flows with Conditional Access https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows
6 Audit logging	Turn auditing on or off https://learn.microsoft.com/en-us/purview/audit-log-enable-disable
6 Alerts	Alert policies in the Microsoft Defender portal https://learn.microsoft.com/en-us/defender-xdr/alert-policies

About this runbook. Free from UnifiedONE for MSPs and MSSPs. It is general guidance and doesn't replace your incident process, your contract with the customer or legal advice on notification duties. Share it freely inside your team.