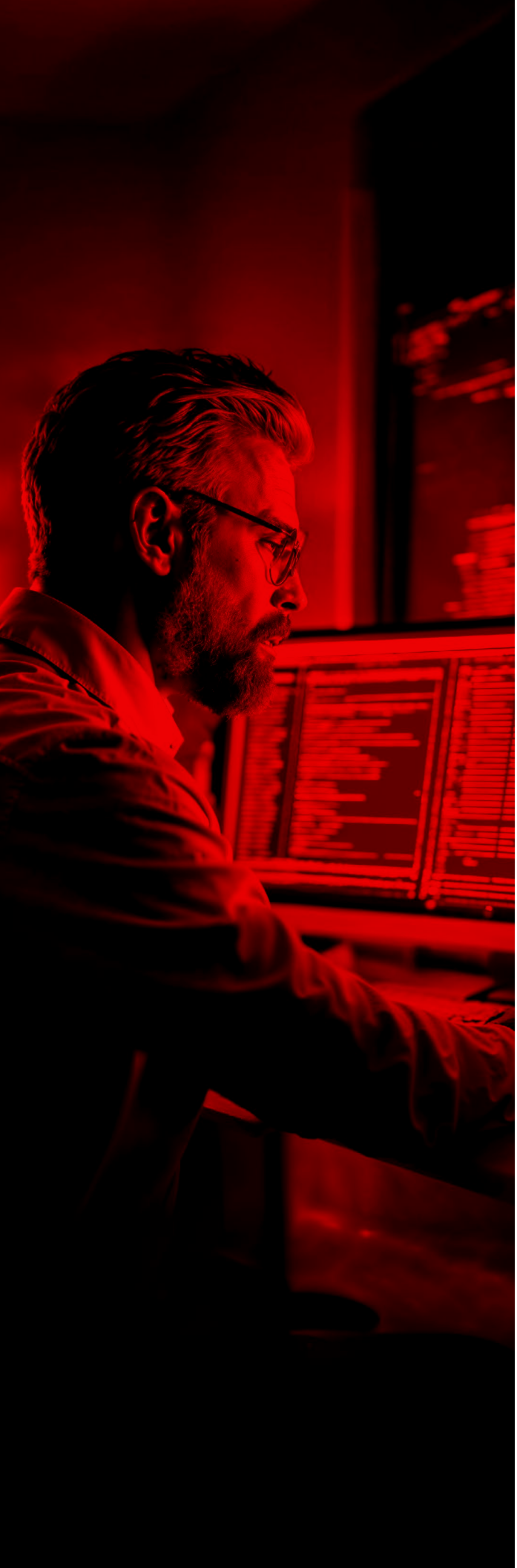


Acronis
Threat Research Unit

02

Best Practices Guide

Enhancing Microsoft Exchange Online security: Best practices

Securing Microsoft Exchange Online (EXO) is crucial for protecting organizational data from cyberthreats, phishing attempts and unauthorized access. Below is a prioritized list of security measures, starting with free or built-in features available with Exchange Online and moving towards advanced configurations requiring additional licenses. Each section provides details on implementation steps, PowerShell commands and references.

Essential free / built-in security measures (available with Exchange Online)

These features provide significant security improvements without additional licensing costs.

1. Enable external email warning

Enabling external email warnings in Outlook helps users identify emails originating from outside the organization, reducing the risk of phishing and spoofing attacks.

Implementation:

- Configure Exchange Online to tag external emails.
- **PowerShell command:**

```
Set-ExternalInOutlook -Enabled $true
```

- Enable external email tagging in Outlook Web Access (OWA).

License requirement:

- Included in all Microsoft 365 and Exchange Online plans.

References:

- Get-ExternalInOutlook Cmdlet
- Protect Office 365 from Phishing with External Email Tagging

2. Block email auto-forwarding to external domains

Automatic email forwarding to external domains can be exploited for data exfiltration. Organizations should disable this feature to prevent unauthorized email forwarding.

Implementation:

- Block auto-forwarding via outbound spam policies in Exchange Online.
- **PowerShell Command:**

```
Set-TransportConfig -AutoForwardEnabled $false
```

- Modify outbound spam filter policy in the Exchange admin center.

License requirement:

- Included in all Microsoft 365 and Exchange Online plans.

References:

- Blocking Auto-Forwarding to External Domains

Essential free / built-in security measures (available with Exchange Online)

3. Secure shared mailboxes

Shared mailboxes are commonly used for group communication but pose security risks if not properly managed.

Implementation:

- **Block sign-in for shared mailbox accounts:**

```
Set-MsolUser -UserPrincipalName <UPN of the shared mailbox>
-BlockCredential $true
```

- Reset auto-generated passwords to long, complex passphrases and avoid saving them.

License requirement:

- Available in all Microsoft 365 and Exchange Online plans.

References:

- lock Shared Mailbox Sign-in

4. Prevent Microsoft Exchange misconfiguration leading to spoofing attacks

Incorrect configuration of inbound connectors can expose an organization to spoofing attacks.

Implementation:

- Verify and configure inbound connectors correctly in Exchange Online.
- Ensure that Exchange Online is properly integrated with third-party security solutions.

License requirement:

- Available in all Microsoft 365 and Exchange Online plans.

References:

- Microsoft Exchange Misconfiguration and Spoofing Attacks

Intermediate security measures (requires Microsoft Defender for Office 365 Plan 1 or above)

These features offer enhanced protection and require additional licensing.

5. Enable first contact safety tip

This feature warns users when they receive an email from an unfamiliar sender, helping mitigate phishing risks.

Implementation:

- Enable the feature in the Microsoft Defender for Office 365 security policies.
- Apply the policy across all mailboxes.

License requirement:

- Microsoft Defender for Office 365 Plan 1 or Plan 2.

References:

- Enable First Contact Safety Tip

6. Enable Safe Links and Safe Attachments

Safe Links and Safe Attachments protect users from malicious URLs and attachments.

Implementation:

- **Enable Safe Links:**

```
Set-SafeLinksPolicy -Identity “Default Safe Links Policy”
-EnableSafeLinks $true
```

- **Enable Safe Attachments:**

```
Set-SafeAttachmentPolicy -Identity “Default Safe Attachments Policy”
-Enable $true
```

- Configure these policies in the **Microsoft Defender Portal** under **Threat Management.**

License requirement:

- Microsoft Defender for Office 365 Plan 1 or Plan 2.

References:

- Safe Links Protection
- Safe Attachments Protection

Advanced security measures (requires Microsoft 365 E3 / E5 or Defender for Office 365 Plan 2)

These measures provide the highest level of protection and require additional Microsoft licensing.

7. Implement multifactor authentication (MFA)

MFA significantly reduces the risk of account compromise.

Implementation:

- Configure MFA in Microsoft Entra Admin Center under Security Defaults.
- **Use PowerShell to enable MFA for users:**

```
Set-MsolUser -UserPrincipalName user@domain.com
-StrongAuthenticationRequirements @()
```

License requirement:

- Microsoft 365 Business Premium, E3, E5.

References:

- Set up multifactor authentication

Acronis
Threat Research Unit

Misconfiguring Microsoft Exchange Online is an invitation to a cyberattack. By following these best practices for advanced configurations, you can fortify Microsoft 365 against the most common attacks.

You can find more information here:

www.acronis.com/en-sg/cyber-protection-center/about/

About the author

Alexander Romanov

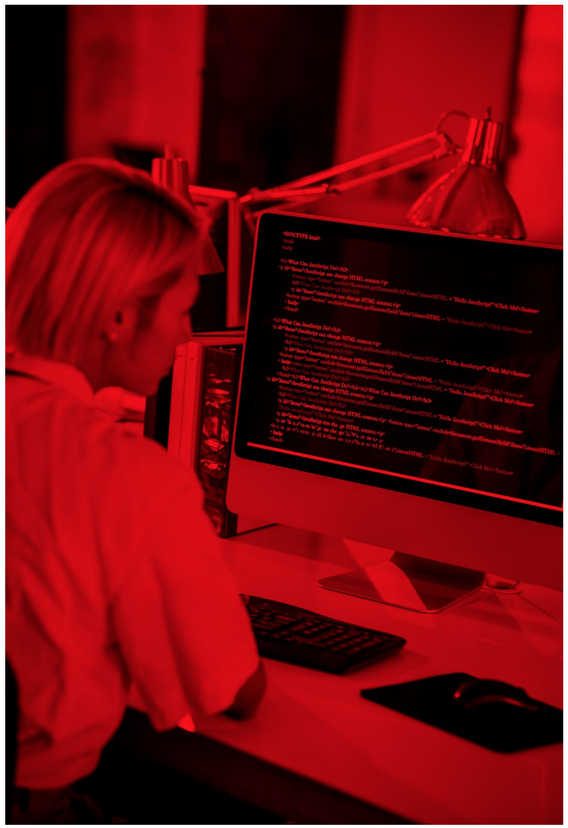
Alexander Romanov is a Cyber Defense Unit Manager at Acronis. Between 2017 and 2021, Alexander specialized in offensive security, focusing on penetration testing, red teaming, code analysis and mobile application security. Since 2021, he has taken on a leadership role in a Cyber Defense team, where he drives infrastructure hardening efforts, builds and operates Security Operations Centers (SOC), and leads threat hunting, threat intelligence, and incident response initiatives.

Alexander is passionate about continuous improvement, security architecture, and building resilient environments to defend against advanced cyber threats.

About TRU

Acronis Threat Research Unit (TRU) is a dedicated unit composed of experienced cybersecurity experts. Our team includes cross-functional experts in cybersecurity, AI, and threat intelligence.

TRU conducts deep research into emerging cyberthreats, focusing on malware, ransomware, phishing and APTs.



We help proactively manage cyber risks and respond to incidents effectively. Our team leverages threat intelligence to prevent future attacks and compiles guidelines and recommendations to assist IT teams in building robust security frameworks.

02

Best Practices Guide

Acronis
Threat Research Unit

2025