

GUIDE · TOMORIS TOOLBOX

Exchange Online: Protection Against Spam, Phishing, and Malware

Built-in protection, preset policies, Defender for Office 365 Plan 1 and 2, quarantine, and sender authentication, based on Microsoft Learn and RFCs

UPDATED

Oct 25, 2026

LENGTH

PDF, 11 pages

ONLINE

tomoris.com/en/downloads/exchange-online-schutz-leitfaden

AT A GLANCE

3 levels

Protection ladder: built-in, Plan 1, Plan 2

48 h

ZAP retroactively checks delivered emails

30 days

Retention in quarantine with Standard and Strict

350

People per policy in impersonation protection

WHO IT IS FOR

- Microsoft 365 and Exchange Online administrators in small and medium-sized companies
- IT service providers that set up and manage their customers' tenants
- IT management that defines licenses and the level of email protection

WHAT THIS COVERS

Every mailbox in Exchange Online is scanned for spam, malware, and phishing, but only the right settings turn this into effective protection. This guide explains the layers of protection, separates the built-in features from those that require Microsoft Defender for Office 365 Plan 1 or Plan 2, and shows the values Microsoft recommends: the Standard and Strict preset policies, anti-phishing with spoofing and impersonation protection, Safe Links, Safe Attachments, ZAP, quarantine, reporting, and sender authentication for your own domain. A checklist and the most common mistakes round it off.

This guide and checklist are a TOMORIS recommendation and must be adapted to your own environment; they do not replace legal advice. Microsoft constantly changes features, names, menus, default values, and license scopes: the linked Microsoft Learn pages in their current version are authoritative, and for NIS2 obligations, the statutory text of the NISG 2026 in its current version. The DNS records are examples using reserved example domains.

CONTENTS

01	Layers of protection at a glance	2
02	What built-in protection always does	3
03	Preset policies as a starting point	4
04	Settings in detail	5
05	Sender authentication for your own domain	6
06	Quarantine and reporting	7
07	Allowing, blocking, and common mistakes	8
08	Checklist to tick off	9
09	Sources	10

01 —

Layers of protection at a glance

What every mailbox in Exchange Online comes with and what Defender for Office 365 Plan 1 and Plan 2 add.

Every organization with mailboxes in Exchange Online receives protection against spam, malware, and phishing without an additional license. What many know as Exchange Online Protection (EOP) is now called "built-in security features for all cloud mailboxes" on Microsoft Learn; the preset policies wizard and the PowerShell cmdlets still use the name EOP. Incoming messages pass through connection filtering (sender reputation, where most spam stops), anti-malware, mail flow rules, and finally anti-spam and anti-phishing. Defender for Office 365 adds to this layer but does not replace it.

The protection ladder according to Microsoft Learn (as of October 25, 2026)

LEVEL	INCLUDED IN	WHAT IS ADDED
Built-in (EOP)	All subscriptions with cloud mailboxes	Anti-malware, anti-spam, anti-phishing with spoofing protection, ZAP for email, quarantine, reporting, Tenant Allow/Block List, preset policies, configuration analyzer
Defender for Office 365 Plan 1	For example, Microsoft 365 Business Premium, since July 2026 also Microsoft 365 E3; otherwise as an add-on	Impersonation protection, phishing thresholds, Safe Attachments, Safe Links, Built-in protection, real-time detections, ZAP for Teams
Defender for Office 365 Plan 2	For example, Microsoft 365 E5, A5, and G5	Everything from Plan 1, plus attack simulation training, Threat Explorer, automated investigation and response (AIR), advanced hunting

The Microsoft 365 admin center shows your licenses under "Your products"; in the Defender portal, under Email & collaboration, the menu item Real-time detections appears with Plan 1, and Explorer with Plan 2.

Changes in 2025 and 2026



02

What built-in protection always does

Default policies for all recipients and "Secure by Default" for malware and high confidence phishing.

There are default policies for anti-malware, anti-spam, and anti-phishing. They apply to all recipients, cannot be turned off, and always take effect last; preset and custom policies take precedence over them.

Malware

A detection in an attachment leads to quarantine. By default, only administrators may view it; users can never release it themselves, at most request a release. The common attachments filter rejects the file types on its list with a non-delivery report; in the default policy, it is turned on out of the box in tenants created after December 1, 2023; in older tenants, check the switch.

Secure by Default

Malware and high confidence phishing are quarantined even if allowed senders or domains, safe senders in Outlook, the IP Allow List, or mail flow rules would allow them; for high confidence phishing, only the action "Redirect message to email address" is not affected. This is not a switch and applies only as long as the MX record points to Microsoft 365. Intended exceptions: advanced delivery for SecOps mailboxes and phishing simulations, submissions for false positives.

Spoofing protection

Spoof intelligence is turned on and detects senders whose address in the "From" field does not match the source. Microsoft combines SPF, DKIM, and DMARC into composite authentication (**compauth**); a single failure does not block on its own, the message is assessed as a whole.

Zero-hour auto purge (ZAP)

Moves already delivered messages that later turn out to be malware, phishing, or, as long as unread, spam to quarantine or the Junk Email folder, depending on the verdict and the policy action; the last 48 hours are searched. Users are not notified. For email without an additional license, for Teams from Plan 1.

03 —

Preset policies as a starting point

Standard for everyone, Strict for particularly at-risk people, Built-in protection as a safety net for Safe Links and Safe Attachments.

Preset security policies set the values recommended by Microsoft, which can hardly be changed. Microsoft advises assigning Standard and/or Strict to all recipients; until then, they apply to no one. Strict is intended for particularly at-risk people ("high value targets or priority users"). All recipients without another policy for Safe Links and Safe Attachments automatically receive Built-in protection as soon as the tenant has at least one license for Defender for Office 365; Microsoft recommends licenses for all users.

1

Open the page

Microsoft Defender portal > Email & collaboration > Policies & rules > Threat policies > Preset security policies (security.microsoft.com/presetSecurityPolicies).

2

Assign Standard protection

Turn the switch "On", then select "Manage protection settings" and, under "Apply Exchange Online Protection", choose "All recipients". If not all users have a license, assign the Defender for Office 365 protection only to licensed users.

3

Fill in impersonation protection (Plan 1)

Up to 350 people whom attackers could imitate, such as executive management and the head of finance, and up to 50 external domains you frequently correspond with. Your own domains and mailbox intelligence are protected automatically.

4

Add Strict and test

Additionally assign Strict to at-risk people. Test: with Standard, spam lands in the Junk Email folder; with Strict, in quarantine. Do not change the profile policies with PowerShell; Microsoft does not support this.

If a recipient is included in several policies, only the first one in this order takes effect: Strict, Standard, Defender for Office 365 evaluation policies, custom policies by priority, and finally Built-in protection and default policies. Outbound spam and Teams protection are not part of the profiles.

04

Settings in detail

The values of the default policy and the Standard and Strict profiles, plus the features that require Defender for Office 365.

Anti-spam and anti-phishing (Default = default policy without profile, Junk = Junk Email folder)

SETTING	DEFAULT	STANDARD	STRICT
Bulk email: threshold (BCL), action	7, Junk	6, Junk	5, Quarantine
Spam	Junk	Junk	Quarantine
High confidence spam	Junk	Quarantine	Quarantine
Phishing	Junk	Quarantine	Quarantine
Retention in quarantine	15 days	30 days	30 days
Spoof according to spoof intelligence	Junk	Junk	Quarantine
Sender DMARC: p=quarantine / p=reject	Quarantine / reject	Quarantine / reject	Quarantine / reject
First contact safety tip	Off	On	On
Phishing threshold (Plan 1)	1	3	4
User and domain impersonation (Plan 1)	No action	Quarantine	Quarantine
Impersonation according to mailbox intelligence (Plan 1)	No action	Junk	Quarantine

For phishing, Junk applies to the default policy and to policies created with PowerShell; policies newly created in the portal quarantine phishing. Anti-malware, Safe Attachments, and Safe Links are configured identically in Standard and Strict.

Safe Links (Plan 1)

Checks URLs before delivery, rewrites them, and checks again on click, including in Teams and Office apps. Standard and Strict: internal messages included, delivery only after the check, no click-through to the original URL. Built-in protection allows click-through, does not rewrite, and excludes internal messages; likewise, custom policies newly created in the portal do not rewrite by default (section 07).

Safe Attachments (Plan 1)

Opens attachments in a virtual environment before delivery, usually within 15 minutes. "Block" is recommended; detections go to quarantine. Built-in protection turns on protection for SharePoint, OneDrive, and Teams globally. Optionally, messages with password-protected attachments that cannot be scanned can be quarantined; this is off in all profiles.

Automatic external forwarding

`AutoForwardingMode Off`

Outbound spam policy, for all licenses. The default "Automatic – System-controlled" behaves differently depending on the organization; Microsoft recommends "Off – Forwarding is disabled".

Junk email filter in Outlook

Microsoft recommends "No automatic filtering" so that Outlook does not work against the verdicts of Microsoft 365.

05 —

Sender authentication for your own domain

SPF, DKIM, and DMARC for every sending domain, blocking records for every domain that does not send; you turn on DKIM for your own domains yourself.

According to Microsoft, threat policies work best when your domains are correctly authenticated. SPF checks the envelope sender (MAIL FROM, RFC 7208), DKIM the domain's signature in the d= field (RFC 6376), and DMARC whether one of these domains matches the visible sender domain (RFC 9989).

DNS: example with reserved example domains

```
; Zone example.com: only Microsoft 365 sends
@           TXT      "v=spf1 include:spf.protection.outlook.com -all"
selector1._domainkey CNAME <target 1 from the Defender portal>
selector2._domainkey CNAME <target 2 from the Defender portal>
_dmarc      TXT      "v=DMARC1; p=none; rua=mailto:dmarc@example.com"

; Zone example.net: does not send email
@           TXT      "v=spf1 -all"
_dmarc      TXT      "v=DMARC1; p=reject;"
```

- SPF: at most one `v=spf1` record per domain, several result in permerror (RFC 7208, section 4.5), and at most 10 terms that trigger DNS lookups (`include`, `a`, `mx`, `ptr`, `exists`, `redirect`), including nested ones (section 4.6.4). Microsoft recommends `-all` and advises against replacing Microsoft's `include` with IP addresses.

- DKIM: Microsoft automatically signs only emails from addresses of the *.onmicrosoft.com domain; emails from your own domains remain unsigned without setup. To set it up, create the two CNAME records shown under Threat policies > Email authentication settings > DKIM and turn on "Sign messages for this domain with DKIM signatures".
- DKIM keys created with PowerShell have 1024 bits; `Rotate-DkimSigningConfig -KeySize 2048` switches to 2048 bits during rotation.
- DMARC: create the record with your DNS provider and tighten it from `p=none` via `p=quarantine` to `p=reject`, subdomains with little traffic first, the main domain last. Microsoft's examples still mention `pct`, which RFC 9989 has removed.
- Unused domains receive `v=spf1 -all` and `v=DMARC1; p=reject;`, but no DKIM record. An unused *.onmicrosoft.com also needs `p=reject;`; you create the record in the Microsoft 365 admin center (Settings > Domains > DNS records).
- For third-party sending services such as newsletter platforms, Microsoft recommends a subdomain such as marketing.example.com, with its own SPF and DKIM.

For inbound mail, Microsoft 365 honors the DMARC policy of external senders ("Honor DMARC record policy", on by default): `p=reject` is rejected, `p=quarantine` goes to quarantine. The rollout plan is included in the download "SPF, DKIM, and DMARC in five steps".

06

Quarantine and reporting

Quarantine policies control what users may do and whether they are notified; reported messages belong in a dedicated mailbox.

A quarantine policy bundles permissions (No access, Limited access, Full access) and defines whether users are notified (every four hours, daily, or weekly). Default policies are read-only; you create your own under Threat policies > Quarantine policies. A changed assignment only applies to messages quarantined in the future.

Default quarantine policies (Microsoft Learn)

POLICY	USERS MAY	NOTIFICATION
AdminOnlyAccessPolicy	Nothing, only administrators manage (malware, high confidence phishing)	No
DefaultFullAccessPolicy	Release, delete, preview, allow sender	No
DefaultFullAccessWithNotificationPolicy	As above; used in Standard and Strict instead of the previous one	Yes
NotificationEnabledPolicy	As above; only in some older organizations	Yes

- Users can never release malware and high confidence phishing themselves; if the quarantine policy allows release, they can only request it. The alert policy "User requested to release a quarantined message" notifies the administrators of this.

- The retention of 1 to 30 days is set in the anti-spam policy ("Retain spam in quarantine for this many days"); it also applies to anti-phishing. After that, the message is deleted and cannot be recovered.
- Reporting: under Settings > Email & collaboration > User reported settings, select "Monitor reported messages in Outlook" with the built-in "Report" button and enter a dedicated Exchange Online mailbox; the default is the Global Administrator's mailbox.
- Register the reporting mailbox as a SecOps mailbox in advanced delivery and exclude it from DLP; otherwise, reported messages are filtered. Reply to the reporters on the Submissions page with "Mark as and notify".

07

Allowing, blocking, and common mistakes

The Tenant Allow/Block List first, allow entries only temporarily, and the typical mistakes that undermine protection.

Microsoft ranks the ways to allow senders, starting with the most recommended: Tenant Allow/Block List, mail flow rules, safe senders in Outlook, IP Allow List, allow lists in anti-spam policies. In the list, blocks take precedence; blocked domains, addresses, and URLs are treated as high confidence phishing. Direct allow entries only work against the verdicts bulk email, spam, high confidence spam, and phishing; against malware and high confidence phishing only via the Submissions page. Microsoft removes unnecessary allow entries itself.

Common mistakes according to Microsoft Learn

Transport rule based only on the sender domain	According to Microsoft, a mail flow rule that bypasses spam filtering (-SCL -1) based solely on the sender domain significantly increases the risk that spoofed senders arrive unfiltered. Microsoft additionally provides for <code>dmARC=pass</code> or <code>dmARC=bestguesspass</code> in the <code>Authentication-Results</code> header or a narrowly scoped IP allow entry, and advises against using your own or widely used domains as a condition.
Allowed domains in anti-spam	According to Microsoft "a bad idea": senders bypass almost all filters, including SPF, DKIM, and DMARC. At most temporarily for testing, never for widely used domains such as microsoft.com.
Simulations allowed by a rule	For third-party phishing simulations and SecOps mailboxes, the advanced delivery policy is intended, not a mail flow rule and not a URL allow entry.
Third-party filter in front of Microsoft 365	If the MX record points to another service, Secure by Default does not apply, and the sender's DMARC policy only takes effect with Enhanced Filtering for Connectors. Enable it instead of turning off spoofing protection.
Safe Links watered down	Custom policies newly created in the portal do not rewrite by default and allow click-through; deliberately set or clear both checkboxes. API-only scanning means that links weaponized later remain undetected in clients without this interface; overly broad entries in "Do not rewrite the following URLs": <code>*contoso.com*</code> also covers fraudulent domains such as <code>falsecontoso.com</code> , <code>*.contoso.com/*</code> does not.

08 —

Checklist to tick off

The items in the order TOMORIS recommends, with the configuration analyzer as a check.

The configuration analyzer (Threat policies > Configuration analyzer) compares your own policies with Standard and Strict, checks SPF and DKIM records in DNS, and shows changes from the last 90 days.

- ☐ Licenses clarified; Defender for Office 365 protection assigned only to licensed users.
- ☐ Every sending domain with SPF (-all), DKIM with your own domain, and DMARC with a reporting address; target p=reject.
- ☐ Domains that do not send blocked with v=spf1 -all and p=reject, including an unused *.onmicrosoft.com via DMARC.
- ☐ Standard profile for all recipients, Strict for particularly at-risk people.
- ☐ Impersonation protection filled with executives and important partner domains (Plan 1).
- ☐ Built-in protection without exceptions for licensed users (Plan 1); common attachments filter turned on.
- ☐ Automatic external forwarding off; justified exceptions in a separate policy.
- ☐ Junk email filter in Outlook set to "No automatic filtering".
- ☐ Quarantine with notification, release requests are processed; "Report" active, reporting mailbox registered as a SecOps mailbox.
- ☐ Allow entries only temporary in the Tenant Allow/Block List; allow lists in anti-spam empty.
- ☐ No mail flow rule bypasses spam filtering based only on the sender domain.
- ☐ Configuration analyzer without open recommendations.

This checklist is a TOMORIS recommendation based on Microsoft's recommendations. Since October 1, 2026, essential and important entities have had to implement appropriate and proportionate risk management measures that, taking into account the state of the art, ensure a level of cybersecurity appropriate to the risk (§ 32 paras. 1 and 2 NISG 2026, Austrian Network and Information Systems Security Act 2026). Under § 2 NISV 2026, the annex to IR (EU) 2024/2690 applies for this purpose, including an implementation plan for modern email communication standards (point 6.7.2(k)) and protection against malware (point 6.9); your own risk analysis determines which specific settings this requires.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

Email security check (German)

tomoris.com/tools/email-security-check

Microsoft 365 domain check (German)

tomoris.com/tools/microsoft-365-check

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

09

Sources

All statements are supported by sources. Legislation applies in its current version.

- 1 **Microsoft Learn: Built-in security features**
How it works, features; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/eop-about
- 2 **Microsoft Learn: Microsoft Defender for Office 365**
Protection ladder, Plan 1 and Plan 2; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/mdo-about
- 3 **Microsoft Learn: What's new in Defender for Office 365**
March 2025 to October 2026; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/defender-for-offi...
- 4 **Microsoft Learn: Preset security policies**
Assignment, profiles, order of precedence; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/preset-security-p...
- 5 **Microsoft Learn: Recommended security settings**
Default, Standard, Strict, Built-in protection; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/recommended-setti...
- 6 **Microsoft Learn: Secure by default**
Overrides, exceptions; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/secure-by-default
- 7 **Microsoft Learn: Anti-spam protection**
Verdicts, actions, retention; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/anti-spam-protect...
- 8 **Microsoft Learn: Anti-phishing policies**
Spoofing, DMARC, impersonation; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/anti-phishing-pol...
- 9 **Microsoft Learn: Safe Links**
Email, Teams, Office apps, exceptions; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/safe-links-about
- 10 **Microsoft Learn: Safe Attachments**
Actions, password-protected attachments; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/safe-attachments-...
- 11 **Microsoft Learn: Zero-hour auto purge**
Email, Teams, licenses; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/zero-hour-auto-pu...
- 12 **Microsoft Learn: Quarantine policies**
Default policies, permissions; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/quarantine-poli...
- 13 **Microsoft Learn: User reported settings**
Reporting mailbox, destinations; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/submissions-user-...
- 14 **Microsoft Learn: Tenant Allow/Block List**
Block and allow entries; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/tenant-allow-bloc...
- 15 **Microsoft Learn: Create allow lists**
Methods, mail flow rules; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/create-safe-sende...
- 16 **Microsoft Learn: Configuration analyzer**
Recommendations, drift analysis; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/configuration-ana...
- 17 **Microsoft Learn: Prompt injection protection**
Plan 2, verdict, detection; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/step-by-step-guid...
- 18 **Microsoft Learn: Set up SPF**
Syntax, parked domains, flattening; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/email-authenticat...
- 19 **Microsoft Learn: Set up DKIM**
CNAME, turning on, key length; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/email-authenticat...
- 20 **Microsoft Learn: Set up DMARC**
Stages, *.onmicrosoft.com, parking; October 25, 2026
learn.microsoft.com/de-de/defender-office-365/email-authenticat...
- 21 **RFC 7208: Sender Policy Framework (SPF)**
Sections 4.5 and 4.6.4
www.rfc-editor.org/rfc/rfc7208
- 22 **RFC 6376: DKIM Signatures**
Section 3.6.2.1
www.rfc-editor.org/rfc/rfc6376
- 23 **RFC 9989: DMARC (May 2026, Standards Track)**
Sections 4.1 and 4.7 (tag t), Appendix A.6
www.rfc-editor.org/rfc/rfc9989
- 24 **RFC 7489: DMARC (2015, Informational)**
Obsolete according to the RFC Editor, replaced by RFC 9989, 9990, and 9991
www.rfc-editor.org/rfc/rfc7489

25 NISG 2026, BGBl. I No. 94/2025 (RIS)

§ 32 paras. 1 and 2, § 51 para. 2; version as of October 25, 2026

www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...

26 NISV 2026, BGBl. II No. 290/2026 (RIS)

§ 2; promulgated on October 1, 2026

www.ris.bka.gv.at/eli/bgbl/II/2026/290

27 Implementing Regulation (EU) 2024/2690, annex

Points 6.7.2(k) and 6.9; applicable under § 2 NISV 2026

eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu