Anti-spoofing protection - Microsoft Defender for Office 365

By chrisda

Archived: 2026-04-06 00:18:26 UTC

All organizations with cloud mailboxes include features to help protect against spoofed (forged) senders Spoofing is a common technique used by attackers. **Spoofed messages appear to originate from someone or somewhere other than the actual source**. This technique is often used in phishing campaigns designed to get user credentials.

Anti-spoofing technology in Microsoft 365 specifically examines forgery of the From header in the message body (also known as the `5322.From` address, From address or P2 sender), because email clients show the From header value as the message sender. When Microsoft 365 has high confidence the From header is forged, the message is identified as spoofed.

The following anti-spoofing technologies are available in the built-in security features for all cloud mailboxes:

- **Email authentication**: An integral part of any anti-spoofing effort is the use of email authentication (also known as email validation) by SPF, DKIM, and DMARC records in DNS. You can configure these records for your domains so destination email systems can check the validity of messages that claim to be from senders in your domains. For inbound messages, Microsoft 365 requires email authentication of sender domains. For more information, see Email authentication.

  Microsoft 365 analyzes and blocks messages based on the combination of standard email authentication methods and sender reputation techniques.

  Diagram showing Microsoft 365 anti-spoofing checks.

- **Spoof intelligence insight**: Review detected spoofed messages from senders in internal and external domains during the last seven days. For more information, see Spoof intelligence insight.

- **Allow or block spoofed senders in the Tenant Allow/Block List**: When you override the verdict in the spoof intelligence insight, the spoofed sender becomes a manual allow or block entry that only appears on the **Spoofed senders** tab on the **Tenant Allow/Block Lists** page at https://security.microsoft.com/tenantAllowBlockList?viewid=SpoofItem. You can also manually create allow or block entries for spoof senders before spoof intelligence detects them. For more information, see Spoofed senders in the Tenant Allow/Block List.

- **Anti-phishing policies**: In the built-in security features for all cloud mailboxes and in Microsoft Defender for Office 365, anti-phishing policies contain the following anti-spoofing settings:

  - Turn spoof intelligence on or off.
  - Turn unauthenticated sender indicators in Outlook on or off.
  - Specify the action for blocked spoofed senders.

For more information, see Spoof settings in anti-phishing policies.

Anti-phishing policies in Defender for Office 365 contain addition protections, including *impersonation* protection. For more information, see Exclusive settings in anti-phishing policies in Microsoft Defender for Office 365.

- **Spoof detections report**: For more information, see Spoof Detections report.

  Microsoft 365 organizations with Defender for Office 365 (included or in add-on subscriptions) have Real-time detections (Plan 1) or Threat Explorer (Plan 2) to view information about phishing attempts. For more information, see Microsoft 365 threat investigation and response.

Tip

It's important to understand that a composite authentication failure doesn't directly result in blocking a message. Microsoft 365 using a holistic evaluation strategy that considers the overall suspicious nature of a message along with composite authentication results. This method is designed to mitigate the risk of incorrectly blocking legitimate email from domains that might not strictly adhere to email authentication protocols. This balanced approach helps distinguish genuinely malicious email from message senders that simply fail to conform to standard email authentication practices.

Spoofed senders in messages have the following negative implications for users:

- **Deception**: Messages from spoofed senders might trick the recipient into giving up their credentials, downloading malware, or replying to a message with sensitive content (known as business email compromise or BEC).

  The following message is an example of phishing that uses the spoofed sender `msoutlook94@service.outlook.com`:

  
  Phishing message impersonating service.outlook.com.

  This message didn't come from service.outlook.com, but the attacker spoofed the **From** header field to make it look like it did. The sender attempted to trick the recipient into selecting the **change your password** link and providing their credentials.

  The following message is an example of BEC that uses the spoofed email domain contoso.com:

  
  Phishing message - business email compromise.

  The message looks legitimate, but the sender is spoofed.

- **Confusion**: Even users who know about phishing might have difficulty seeing the differences between real messages and messages from spoofed senders.

  The following message is an example of a real password reset message from the Microsoft Security account:


Microsoft legitimate password reset.

The message really did come from Microsoft, but users are conditioned to be suspicious. Because it's difficult to the difference between a real password reset message and a fake one, users might ignore the message, report it as spam, or unnecessarily report the message to Microsoft as phishing.

Microsoft differentiates between two different types of spoofed senders in messages:

- **Intra-org spoofing**: Also known as *self-to-self* spoofing. For example:
  - The sender and recipient are in the same domain:

    ```
    From: chris@contoso.com
    To: michelle@contoso.com
    ```

  - The sender and the recipient are in subdomains of the same domain:

    ```
    From: laura@marketing.fabrikam.com
    To: julia@engineering.fabrikam.com
    ```

  - The sender and recipient are in different domains that belong to the same organization (that is, both domains are configured as accepted domains in the same organization):

    ```
    From: cindy@tailspintoys.com
    To: steve@wingtiptoys.com
    ```

  Messages that fail composite authentication due to intra-org spoofing contain the following header values:

  `Authentication-Results: ... compauth=fail reason=6xx`

  `X-Forefront-Antispam-Report: ...CAT:SPOOF;...SFTY:9.11`

  - `reason=6xx` indicates intra-org spoofing.
  - `SFTY` is the safety level of the message.
    - `9` indicates phishing.
    - `.11` indicates intra-org spoofing.

- **Cross-domain spoofing**: The sender and recipient domains are different, and have no relationship to each other (also known as external domains). For example:

  ```
  From: chris@contoso.com
  To: michelle@tailspintoys.com
  ```

  Messages that fail composite authentication due to cross-domain spoofing contain the following headers values:

`Authentication-Results: ... compauth=fail reason=000/001`

`X-Forefront-Antispam-Report: ...CAT:SPOOF;...SFTY:9.22`

- `reason=000` indicates the message failed explicit email authentication. `reason=001` indicates the message failed implicit email authentication.
- `SFTY` is the safety level of the message.
  - `9` indicates phishing.
  - `.22` indicates cross-domain spoofing.

For more information about **Authentication-Results** and `compauth` values, see Authentication-results message header fields.

Mailing lists (also known as discussion lists) are known to have problems with anti-spoofing protection because of how they forward and modify messages.

For example, Gabriela Laureano (`glaureano@contoso.com`) is interested in bird watching, so she joins the mailing list `birdwatchers@fabrikam.com` , and sends the following message to the list:

```
 From: "Gabriela Laureano" <glaureano@contoso.com>
To: Birdwatcher's Discussion List <birdwatchers@fabrikam.com>
Subject: Great viewing of blue jays at the top of Mt. Rainier this week

Anyone want to check out the viewing this week from Mt. Rainier?
```

The mailing list server receives the message, modifies its content, and replays it to the members of list. The replayed message has the same From address (`glaureano@contoso.com`), but a tag is added to the subject line, and a footer is added to the bottom of the message. This type of modification is common in mailing lists, and might result in false positives for spoofing.

```
 From: "Gabriela Laureano" <glaureano@contoso.com>
To: Birdwatcher's Discussion List <birdwatchers@fabrikam.com>
Subject: [BIRDWATCHERS] Great viewing of blue jays at the top of Mt. Rainier this week

Anyone want to check out the viewing this week from Mt. Rainier?

This message was sent to the Birdwatchers Discussion List. You can unsubscribe at any time.
```

To help mailing list messages pass anti-spoofing checks, do the following steps based on your circumstance:

- **Your organization owns the mailing list**:
  - Check the FAQ at DMARC.org: I operate a mailing list and I want to interoperate with DMARC, what should I do?.

    - Read the instructions at this blog post: A tip for mailing list operators to interoperate with DMARC to avoid failures.
    - Consider updating your mailing list server so it supports ARC. For more information, see http://arc-spec.org.

- **Your organization doesn't own the mailing list**:

    - Ask the maintainer of the mailing list to configure email authentication for the domain that the mailing list is relaying email from. The owners are more likely to act if enough members ask them to set up email authentication. While Microsoft also works with domain owners to publish the required records, it helps even more when individual users request it.
    - Create Inbox rules in your email client that move messages to the Inbox.
    - Use the Tenant Allow/Block List to create an allow entry for the mailing list to treat it as legitimate. For more information, see Create allow entries for spoofed senders.

If all else fails, you can report the message as a false positive to Microsoft. For more information, see Report messages and files to Microsoft.

Admins of organizations that regularly send email to Microsoft 365 need to ensure the email is properly authenticated. Otherwise, it might be marked as spam or phishing. For more information, see How to avoid email authentication failures when sending mail to Microsoft 365.

In Microsoft 365, senders in user allowlists bypass parts of the filtering stack, including spoof protection. For more information, see Outlook Safe Senders.

If possible, admins should avoid using allowed sender lists or allowed domain lists in anti-spam policies. These senders bypass most of the filtering stack (high confidence phishing and malware messages are always quarantined). For more information, see Use allowed sender lists or allowed domain lists.
