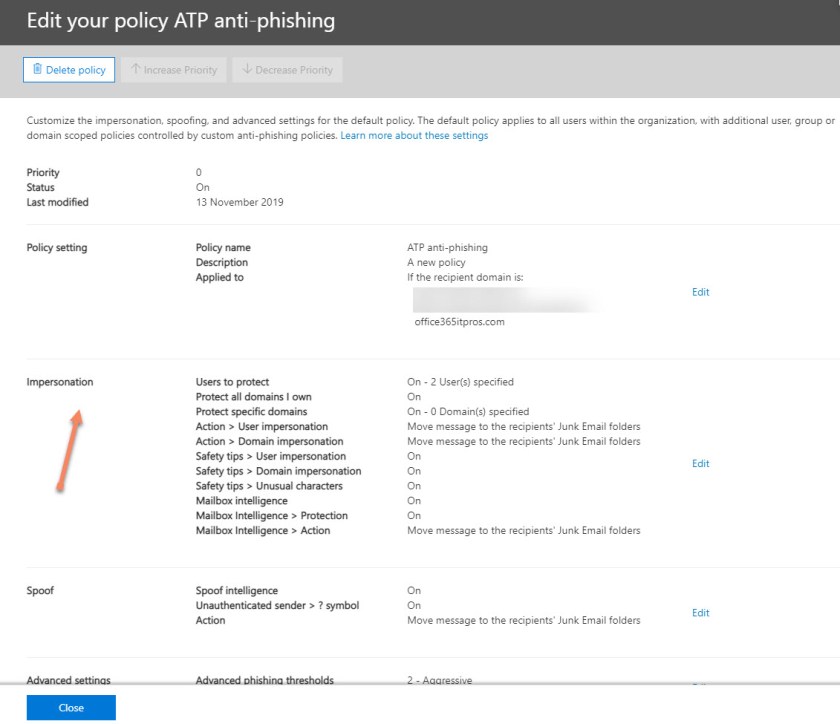
How to Enable the First Contact Safety Tip for Exchange Online Protection

Posted on [**November 26, 2020**](https://office365itpros.com/2020/11/26/enable-first-contact-safety-tip/) by [**Tony Redmond**](https://office365itpros.com/author/thoughtsofanidlemind/)

Anti-Phishing, Defender, and Impersonation

Microsoft Defender for Office 365 is the new name for what used to be called Advanced Threat Protection (ATP). While Exchange Online Protection includes anti-phishing policies to stop phishing attempts like [**this recent example**](https://office365itpros.com/2020/10/29/phishing-voip-voicemail/), Defender extends the anti-phishing policy with [**impersonation settings**](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#impersonation-settings-in-anti-phishing-policies-in-microsoft-defender-for-office-365) (Figure 1).

Figure 1: Impersonation settings in an anti-phishing policy

Impersonation is where an inbound email appears to come from a sender or domain that is known but is slightly different, such as email from Micriosoft.com. It’s done to lure the recipient into a false sense of security that the email they receive originated from a trusted sender or domain whereas it’s an attempt to hoodwink them into doing something bad, like revealing confidential information.

The impersonation settings in anti-phishing policies allow tenants to define up to 60 protected email addresses (per policy) which are then subject to checks to pick up attempts at impersonation. The checks only work if the sender has never communicated with the recipient before. If an attempt is detected, policy settings determine what happens next, such as moving the message to Junk Email.

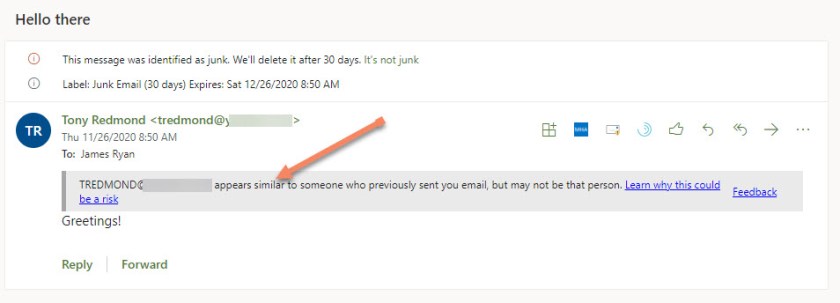
Safety Tips Highlight Potential Problems

Exchange Online Protection uses safety tips to [**highlight potentially problematic messages**](https://support.microsoft.com/en-ie/office/identify-suspicious-messages-in-outlook-com-and-outlook-on-the-web-3d44102b-6ce3-4f7c-a359-b623bec82206?ui=en-us&rs=en-ie&ad=ie) to users. For example, Figure 2 shows a safety tip for a message where the sender’s address could not be verified because the message failed both DKIM and DMARC tests upon arrival into Office 365

Graphical user interface, application, Teams

Description automatically generatedFigure 2: Safety tip for an unverifiable sender address

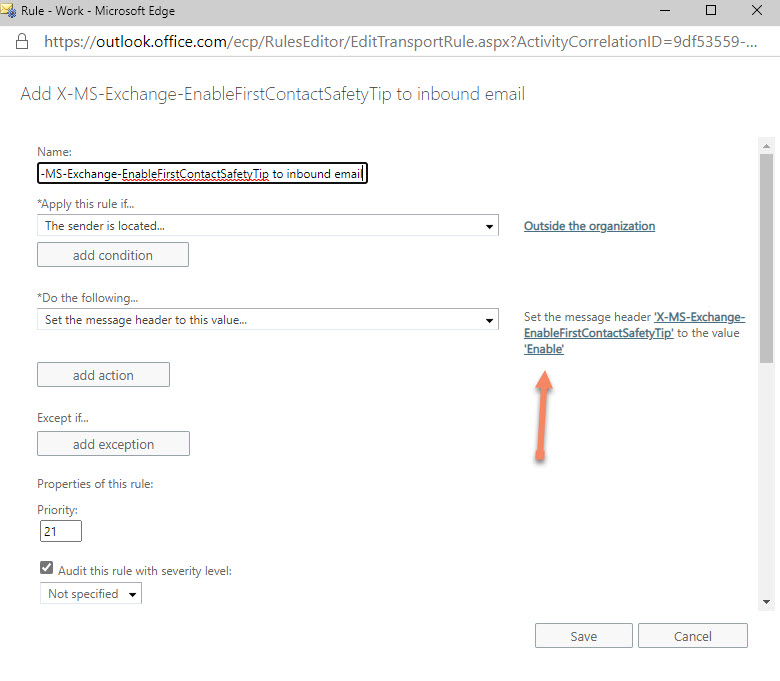
Figure 3 shows an example of an impersonation safety tips. Microsoft Defender has identified that the email address of an inbound message is similar to an address used by a regular correspondent, so the fact is highlighted.

Figure 3: An example of an impersonation safety tip

Enabling the First Contact Safety Tip

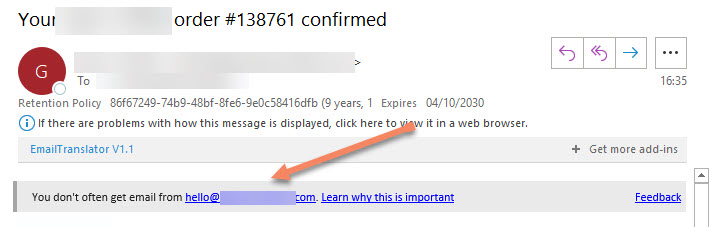
Although the safety tips to highlight impersonation attempts can be disabled in the anti-phishing policy, Microsoft recommends that tenants use a mail flow (transport) rule to insert the *X-MS-Exchange-EnableFirstContactSafetyTip* x-header into messages received from outside. The presence of the header causes Microsoft Defender to generate a safety tip if the sender has never sent email to the recipient before. This is a recent change introduced by Microsoft that isn’t well known.

The mail flow rule is very straightforward. It applies to all inbound email and applies the x-header to those messages (Figure 4).

Figure 4: Creating a mail flow rule to apply X-MS-Exchange-EnableFirstContactSafetyTip

*Note: An earlier version of this post used****True****as the value for the x-header. Exchange engineering have advised that the x-header should be set to****Enable****.*

The effect of the mail flow rule is shown in Figure 5. The [**documentation**](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#impersonation-settings-in-anti-phishing-policies-in-microsoft-defender-for-office-365) says “*Specific safety tips will be displayed notifying recipients that they often don’t get email from the sender or in cases when the recipient gets an email for the first time from the sender*.” This implies that different text is used when a message is received from someone for the first time. However, I have only ever seen safety tips saying that “*You don’t often get email from…*”

Figure 5: An inbound message is tagged with the “first contact” safety tip

Even though the first contact safety tip is connected to impersonation prevention, it’s not covered by the same licensing requirements. The safety tips appear on messages sent to mailboxes which don’t have Microsoft Defender for Office 365 licenses.

Warning Users is Goodness

If your tenant has Microsoft Defender for Office 365 it’s a good idea to create and use the mail flow rule recommended by Microsoft. There’s no downside and it could stop someone falling victim to an phishing attempt in an email received from someone who seems to be like a person that the recipient is used to receiving messages from. Warning people of potential problems is pure and simple goodness!