proofpoint.

SOLUTION BRIEF

Proofpoint Email Warning Tags with Report Suspicious

Strengthen security with an easy way for users to report malicious emails

Products

- Proofpoint Email Protection
- Proofpoint Threat Response Auto-Pull

Key Benefits

- Enhance overall email security
- Reduce IT overhead and downstream impacts
- Improve email and reporting experience for users
- Device and application agnostic
- Included with Proofpoint Email Protection v8.18 and above

Attack sophistication and a people-centric threat landscape have made email-based threats more pervasive and widespread, so it's important to have layered, integrated defenses. This includes how your users engage with email. Every day users sift through hundreds of email messages. And every time, they must determine how to engage with each one. Proofpoint makes all of this easier.

Proofpoint Email Warning Tags with Report Suspicious strengthens email security with a new, easier way for users to engage with and report potentially malicious messages. And it reduces IT burden in the process.

Proofpoint Email Warning Tags with Report Suspicious displays different types of tags or banners that warn users about possible email threats. Each of these tags gives the user an option to report suspicious messages.

These tags are HTML-based banners. They can appear for users regardless of device or application but they don't involve typical overhead associated with email

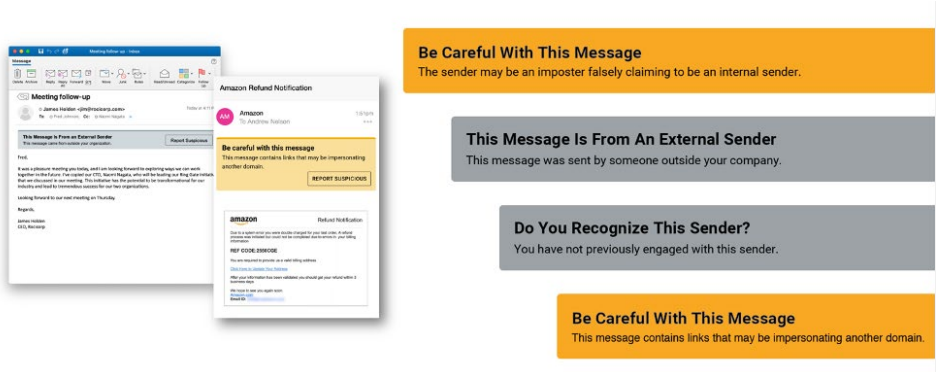

Figure 1: Proofpoint Email Warning Tags with Report Suspicious example.

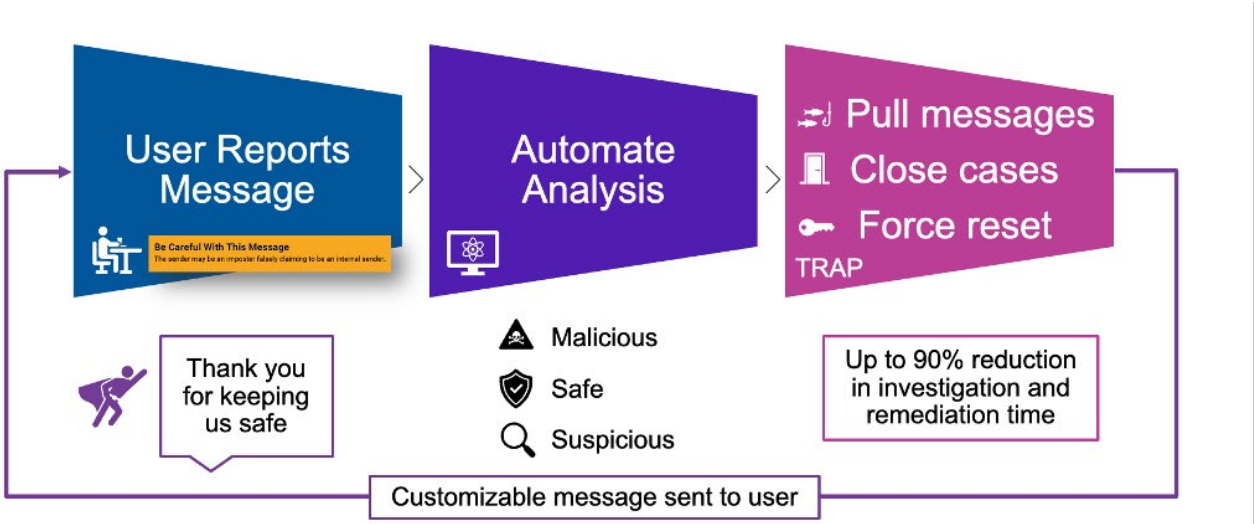

Figure 2: Proofpoint Email Warning Tags with Report Suspicious seamlessly integrates into an existing Proofpoint TRAP workflow.

reporting add-ins. Customers have the option of enabling specific tags, such as:

- **External Sender.** This tag could appear when a received message originated from outside the organization.
- **Unknown Sender.** This tag could appear when a received message is from an address that a user has not communicated with previously.
- **Unsafe Email.** This tag could appear when a received message has been generally designated unsafe based on Proofpoint analysis**.**
- **Newly Registered Domain.** This tag could appear when an email sender's domain is less than 90 days old. Attackers commonly use new domains to launch their email attacks.
- **Mixed Script Domain.** This tag could appear when a received message might contain links to a fake website.
- **Impersonating Sender.** This tag could appear when a received message may be trying to impersonate another sender.
- **DMARC Authentication Failure.** This tag could appear when the sender's identity could not be verified and may be impersonating the sender.

Customers can customize each tag, tailoring their colors and specific verbiage in 38 languages. They can also choose to have the tags appear in plain text.

Proofpoint Email Protection customers can now add Report Suspicious capabilities directly in the Email Warning Tags themselves. This helps their users report suspicious messages with an email add-in and works alongside our PhishAlarm reporting button. It also makes it easier for users to report potentially malicious messages in fewer steps, on any device, with any application.

Organizations can provide an enhanced and more impactful user experience that is fully customizable. With Email Warning Tags being front-end-device and application agnostic, users can more easily report suspicious messages with one click. And because the tags provide context and guidance, user reports can be more accurate. Organizations can decide when to implement and customize each tag. This provides a user-facing experience that suits their culture and immediate needs.

You need an integrated approach for effective email security. Using Email Warning Tags with Report Suspicious, organizations can spend less time managing different point email warning, reporting and remediation solutions. This means they can focus more on being proactive with activities like educating users and understanding trends in user-reported threats.

Organizations don't need to rely entirely on email add-ins for their users to report suspicious messages. Add-ins should still be deployed alongside the tags. But if new deployments or updates for traditional add-ins are needed, they are not as urgent. This is because Email Warning Tags with Report Suspicious can cover most situations when users need to be cautious with emails.

Organizations enjoy the same automation, time savings and user experience of the Closed-Loop Email Analysis and Response (CLEAR) solution using Proofpoint Threat Response Auto-Pull (TRAP). The CLEAR workflow reduces remediation time by up to 90%. After users report a message, they receive the same customized feedback. Administrative reporting will remain the same and remediation workflows will not be impacted. In the future, users will be able to "Learn More" directly from the tags. And they'll receive dynamic educational content to help improve their email hygiene further.

To configure Email Warning Tags with Report Suspicious, reach out to your Account Teams or visit the Proofpoint Community.

LEARN MORE

For more information, visit **proofpoint.com**.