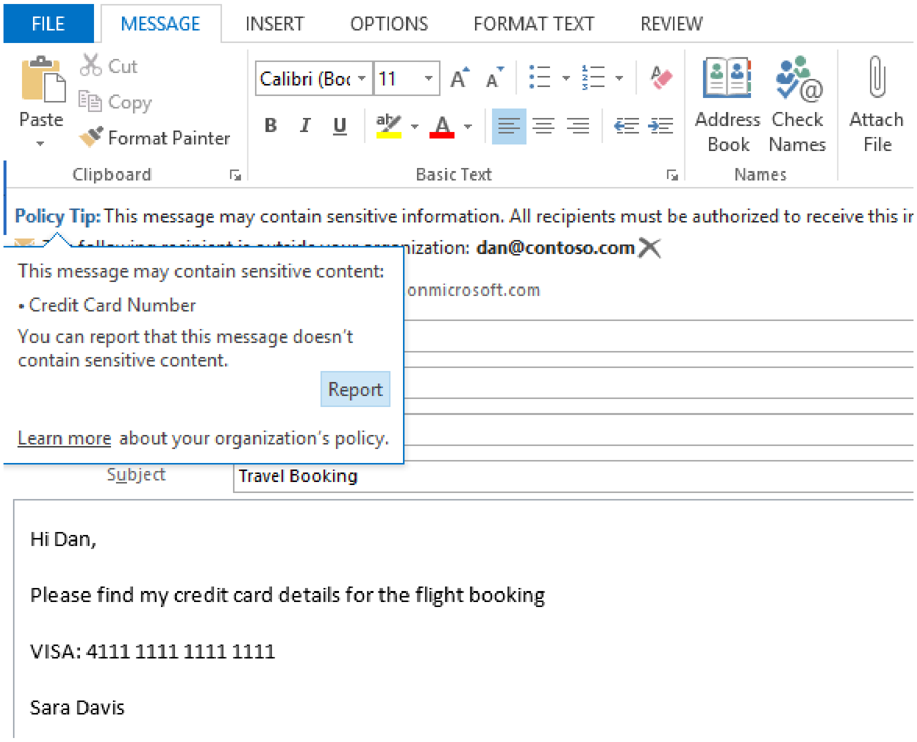
Office 365 compliance controls: Data Loss Prevention

DLP Policy Tips inform your workers in real time

With the new DLP Policy Tips in Office 365, admins can inform email senders that they may be about to pass along sensitive information that is detected by the company's policies-before they click Send. This helps your organization stay compliant and it educates your employees about custom scenarios based on your organization's requirements. It accomplishes this by emphasizing in-context policy evaluation. Policy Tips not only analyzes email messages for sensitive content but also determines whether information is sensitive in the context of communication. That means you can target specific scenarios that you associate with risk, external communication for example, and configure custom policy tips for those scenarios. Reading those custom policy tips in email messages keeps your workers aware of your organization's compliance policies and empowers them to act on them, without interrupting their work.

How do Policy Tips work? Consider a real-life scenario. Contossoplay is a company that has an internal policy to warn its employees any time they include sensitive information like a credit card number in email communications. Sara Davis is a Contossoplay employee composing an email to Dan, who works outside her organization. She includes credit card information in the mail, and immediately a DLP policy tip shows up in the message in Outlook.



Policy Tip: This message may contain sensitive information. All recipients must be authorized to receive this ir

following recipient is outside your organization: **dan@contoso.com**

onmicrosoft.com

This message may contain sensitive content:

- Credit Card Number

You can report that this message doesn't contain sensitive content.

Report

Learn more about your organization's policy.

Subject: Travel Booking

Hi Dan,

Please find my credit card details for the flight booking

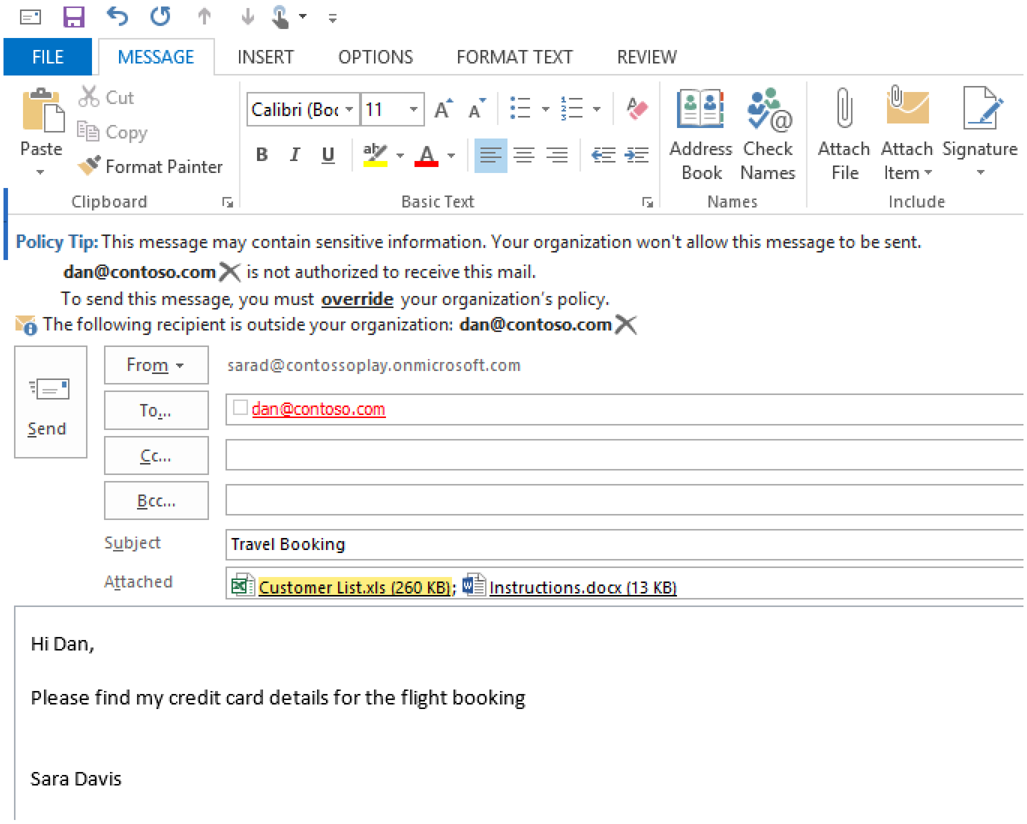
VISA: 4111 1111 1111 1111

Sara Davis

When you include sensitive information in an email message, a DLP policy tip alerts you before you send the message.

At this point Sarah can decide to: send the email message with the credit card information, send the message with the credit card information and click **Report** to report a false positive, or delete the credit card information before sending the message. If she's unsure what to do, she can click **Learn more** to understand her company's policy, which her admin may have customized.

Let's look at another scenario. Contossoplay has recently set up a policy that blocks emails containing multiple credit cards or that need to be overridden with a business justification. Sara starts an email message to book the travel for multiple employees in the company and attaches a document that includes the personal credit card information of the employees. A different policy tip shows up, highlighting the new compliance requirement.



Policy Tip: This message may contain sensitive information. Your organization won't allow this message to be sent.

dan@contoso.com is not authorized to receive this mail.

To send this message, you must **override** your organization's policy.

The following recipient is outside your organization: **dan@contoso.com**

From: sarad@contossoplay.onmicrosoft.com

To...: dan@contoso.com

Subject: Travel Booking

Attached: Customer List.xls (260 KB); Instructions.docx (13 KB)

Hi Dan,

Please find my credit card details for the flight booking

Sara Davis

A custom DLP policy tip alerts you about an attachment that may contain high-count sensitive information.

As these two scenarios show, data loss prevention empowers end users, making them part of the organization's compliance process and ensuring that the business flow is not interrupted or delayed, because achieving compliance does not get in users' way.