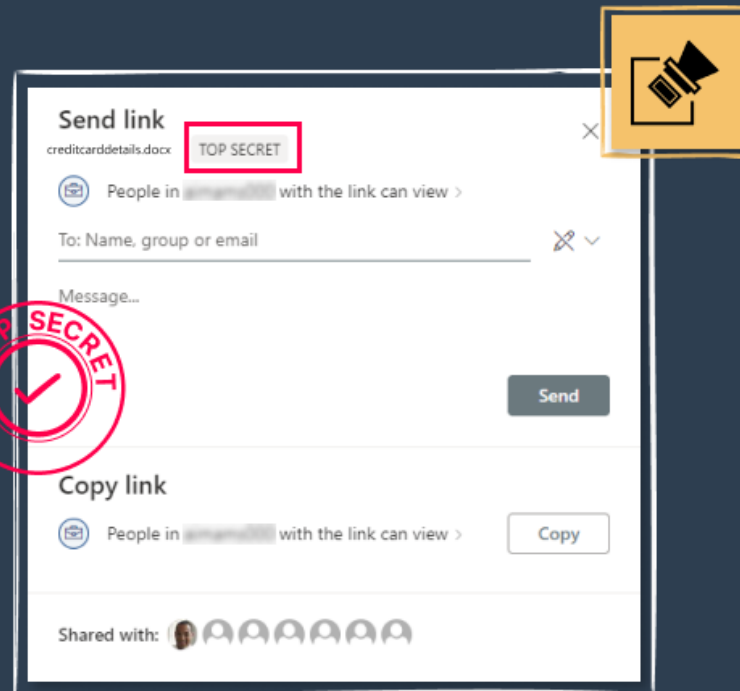


# Sharing Experience with **Sensitivity labels** in Microsoft 365



admindroid.com

ad  
AdminDroid

## Microsoft 365 Sensitivity Labels in the Sharing Dialog

December 28, 2022 [AIMA Office 365 Community](#) [Leave a Reply](#)

Protecting data within an organization is a complicated process to deal with. Classifying & protecting the data is something that eases this attempt. The **Microsoft 365 Sensitivity labels** protects data by classifying and enforcing them with labels. Most of us may be familiar with this concept. But Microsoft added a new experience to the Microsoft 365 app's sharing dialog box recently. In order to draw the picture perfectly, we will start from the basics.

## What are Microsoft 365 Sensitivity Labels?

Sensitivity labels are used to label sensitive documents that roam within or outside your organization. It classifies documents based on the pre-configured protection settings and extends security by using encryption and content markings. After applying sensitivity labels to documents, they are always protected no matter wherever they are!

With sensitivity labels, you can decide which users and groups can use the labels, and can be applied either manually or automatically. By default, a global administrator can create and manage sensitivity labels. Admins need to give compliance officers delegated access or add them to role groups that support sensitivity labels to manage labels. Once created, users can apply the labels manually or get them applied automatically.

## License Requirements for Sensitivity Labels

Users with the following licenses are eligible to benefit from the features of sensitivity labels in Microsoft 365.

- Microsoft 365 E5/A5/G5/E3/A3/G3/F1/F3/Business Premium
- Enterprise Mobility + Security E3/E5
- Office 365 E5/A5/E3/A3
- AIP Plan 1
- AIP Plan 2

## Why Sensitivity Labels for Office Files?

SharePoint and OneDrive are collaborative Office 365 services where people work with important documents that sometimes are sensitive to handle. In order to protect these documents from being compromised, security practices are followed. By labeling a document in Microsoft 365, it can be kept out of serious exploits. A sensitivity label protects a document's privacy and security when deployed properly.

Sensitivity labels can be applied to a specific file and it is completely customizable. You can configure a sensitivity label to encrypt a document or mark the content with watermarks, headers, and footers.

## Supported File Types for Microsoft 365 Sensitivity Labels

The following file types are supported for applying sensitivity labels in SharePoint and OneDrive.

- **Word:** .docx, .docm
- **Excel:** .xlsx, .xlsm, .xlsb
- **PowerPoint:** .pptx, .ppsx

## How to Apply Microsoft 365 Sensitivity Labels for Files?

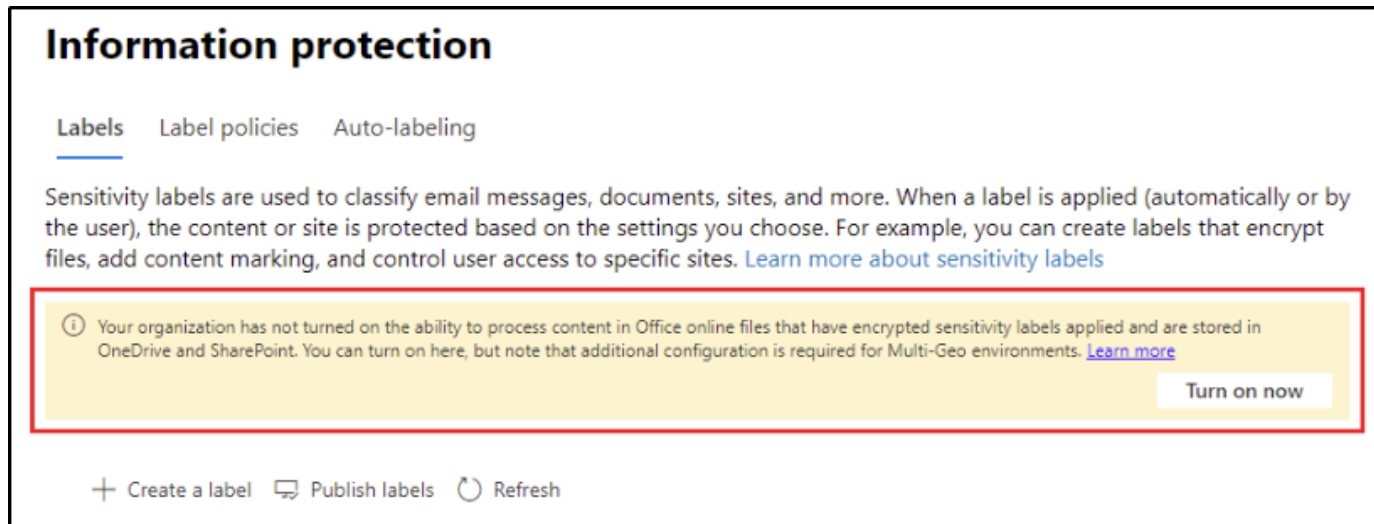
Create and apply sensitivity labels to files by following the steps given below.

## Creating the label

Step 1: Sign in to the [Microsoft Purview compliance portal](#) as a global administrator.

Step 2: Reach out to 'Information Protection' under 'Solutions'.

**Note: If you have not enabled this feature for your organization, a message will be displayed as shown in the screenshot below. You can turn it on right away there!**



The screenshot shows the 'Information protection' page in the Microsoft 365 compliance portal. The page has a header 'Information protection' and three tabs: 'Labels', 'Label policies', and 'Auto-labeling'. The 'Labels' tab is selected. Below the tabs, there is a paragraph explaining that sensitivity labels are used to classify email messages, documents, sites, and more. A yellow warning box is highlighted with a red border, containing a message: 'Your organization has not turned on the ability to process content in Office online files that have encrypted sensitivity labels applied and are stored in OneDrive and SharePoint. You can turn on here, but note that additional configuration is required for Multi-Geo environments. [Learn more](#)'. A 'Turn on now' button is located at the bottom right of the warning box. At the bottom of the page, there are three buttons: '+ Create a label', 'Publish labels', and 'Refresh'.

*Turn on Information Protection Sensitivity Labels*

Step 3: From the 'labels' tab, create a label and configure protection settings for it.

Step 4: Give name and description for your label and then give 'Next'.

Microsoft Purview

## New sensitivity label

- Name & description**
- Scope
- Items
- Groups & sites
- Schematized data assets (preview)
- Finish

### Name and create a tooltip for your label

The protection settings you choose for this label will be immediately enforced on the items or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

**Name \*** ⓘ


**Display name \*** ⓘ

**Description for users \*** ⓘ

**Description for admins** ⓘ

**Label color**

The color selected below is currently applied to the parent label. As a result, all sublabels of the parent label will inherit the same color. If you want to use a different color, edit the parent label. [Learn more about label color](#)



**Next**

*Creating a new Sensitivity label*

Step 5: Define where you want to apply the label by defining the scope. Additional steps need to be done to enable this feature for groups and sites.

## Define the scope for this label

Labels can be applied directly to items (such as files, emails, meetings), containers like SharePoint sites and Teams, Power BI items, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. [Learn more about label scopes](#)

**Items**

Configure protection settings for labeled emails, Office files, and Power BI items. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

Include meetings

**Groups & sites**

Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

**Schematized data assets (preview)**

Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

*Defining scope of the label*

Step 6: Under '**Items**' category, configure protection settings for the labeled items. There are two protection configurations – Encryption and content marking. In the 'Encryption' section, you can assign permissions to specific users and groups so that only they can use the content that has this label applied. '**Teams Premium**' users can utilize the option to configure protection settings for Teams meetings and chats.

## Encryption

Control who can access items that have this label applied. Items include emails, Office files, Power BI files, and meeting invites (if you chose to configure meeting settings for this label). [Learn more about encryption settings](#)

Remove encryption if the file or email is encrypted

Configure encryption settings

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. [Learn more](#)

**Assign permissions now or let users decide?**

Assign permissions now ▾

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

**User access to content expires** ⓘ

Never ▾

**Allow offline access** ⓘ

Always ▾

**Assign permissions to specific users and groups** \* ⓘ

[Assign permissions](#)

---

1 item

Users and groups	Permissions
------------------	-------------

*Encryption Configuration for the label*

For content marking, select the option you want to use and add customized text for the watermark, header, or footer.

## Content marking

Add custom headers, footers, and watermarks to content that has this label applied. [Learn more about content marking](#)

① All content marking will be applied to documents but only the header and footer will be applied to email messages. If you chose to configure meeting settings for this label, the header and footer will also be applied to meeting invites.

### Content marking



Add a watermark

Customize text

Protected

Add a header

Customize text

This content is protected for some reasons

Add a footer

Customize text


This content is protected for some reasons




*Adding custom headers, footers, and watermarks*






Step 7: In the next step, you can choose to apply the label automatically to content that matches the conditions of your label settings. In this case, I have enabled it and selected the condition to automatically label the content if it has a **credit card number** in it.


^ Detect content that matches these conditions

^ Content contains 


Group name \*  Group operator  

**Sensitive info types**


Credit Card Number	<input data-bbox="963 435 1215 475" type="text" value="High confidence"/> 	Instance count <input data-bbox="1474 435 1555 475" type="text" value="1"/> to <input data-bbox="1591 435 1672 475" type="text" value="Any"/> 	
Add 			
 Create group			

+ Add condition 


---

 Recommended labeling and displaying a message to users is supported only for Office apps. This label will be automatically applied to files in Microsoft Purview Data Map, but no message will be displayed.

**When content matches these conditions**



Automatic and recommended labeling works differently for items in Office 365 vs. files stored on Windows devices. [Learn more](#)

Display this message to users when the label is applied 

*Defining conditions using sensitive info types*

Step 8: You can define protection settings for groups and sites as the next step and finish creating the label. Before publishing the label, editing it can also be done.

**'Auto-labelling for schematized data assets'** is another option you can configure to apply labels to data assets in Microsoft Purview data map. It allows you to automatically label database columns in SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and various other data sources governed by Microsoft Purview data map.

After reviewing your settings, create the label and enhance protection for your confidential office files.

## Publishing the Label

Step 9: After creating a label, you will have to publish it to be available for the users. To do so, select the label you just created from the list of labels -> A flyout page appears -> Review your policy settings -> Publish label. You can also publish it from the final page of the label creation step by selecting the label from the "Sensitivity labels to publish" option.

When you publish a label, you can choose users and groups to whom the label should be applied and configure default settings for documents, emails, meetings, sites and groups, and Power BI separately.

**Information protection**

Overview **Labels** Label policies Auto-labeling

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label Publish label Refresh

Name	Order	Scope	Created by
<input type="checkbox"/> TOP SECRET	1	File, Email, Site, UnifiedGroup, Schematized data assets	...
<input type="checkbox"/> Secret500	2	File, Email, Site, UnifiedGroup, Schematized data assets	...
<input type="checkbox"/> EXTSHARING	3	File, Email, Site, UnifiedGroup, Schematized data assets	...
<input type="checkbox"/> INTERNAL	4	File, Email, Site, UnifiedGroup, Schematized data assets	...
<input type="checkbox"/> LabelTest	5	File, Email, Site, UnifiedGroup, Schematized data assets	...
<input type="checkbox"/> OneD	6	File, Email, Site, UnifiedGroup, Schematized data assets	...
<input type="checkbox"/> Bank Details	7	File, Email, Meetings, Site, UnifiedGroup, Schematized data assets	...

**Bank Details**

Edit label Publish label Delete label

**Name**  
Bank Details

**Display name**  
Bank Details

**Description for users**  
This label is applied for documents that expose bank details in and outside the organization.

**Scope**  
File, Email, Meetings, Site, UnifiedGroup, Schematized data assets

**Encryption**  
Encryption

**Content marking**  
Watermark: Protected  
Header: This content is protected for some reasons  
Footer: This content is protected for some reasons

**Auto-labeling for files and emails**  
 Automatically apply the label

Close

*Publishing the label*

Step 10: From the **'Users and groups'** section, select the users to whom you want the label to be applied. In the next section **'Policy Settings'**, select **'Users must provide a justification to remove a label or lower its classification'**, so that users will be asked to provide justification for any label removals.

**Justification Required** ×

Your organization requires justification to change this label.

Previous label no longer applies

Previous label was incorrect

Other (explain)

Explain why you're changing this label.

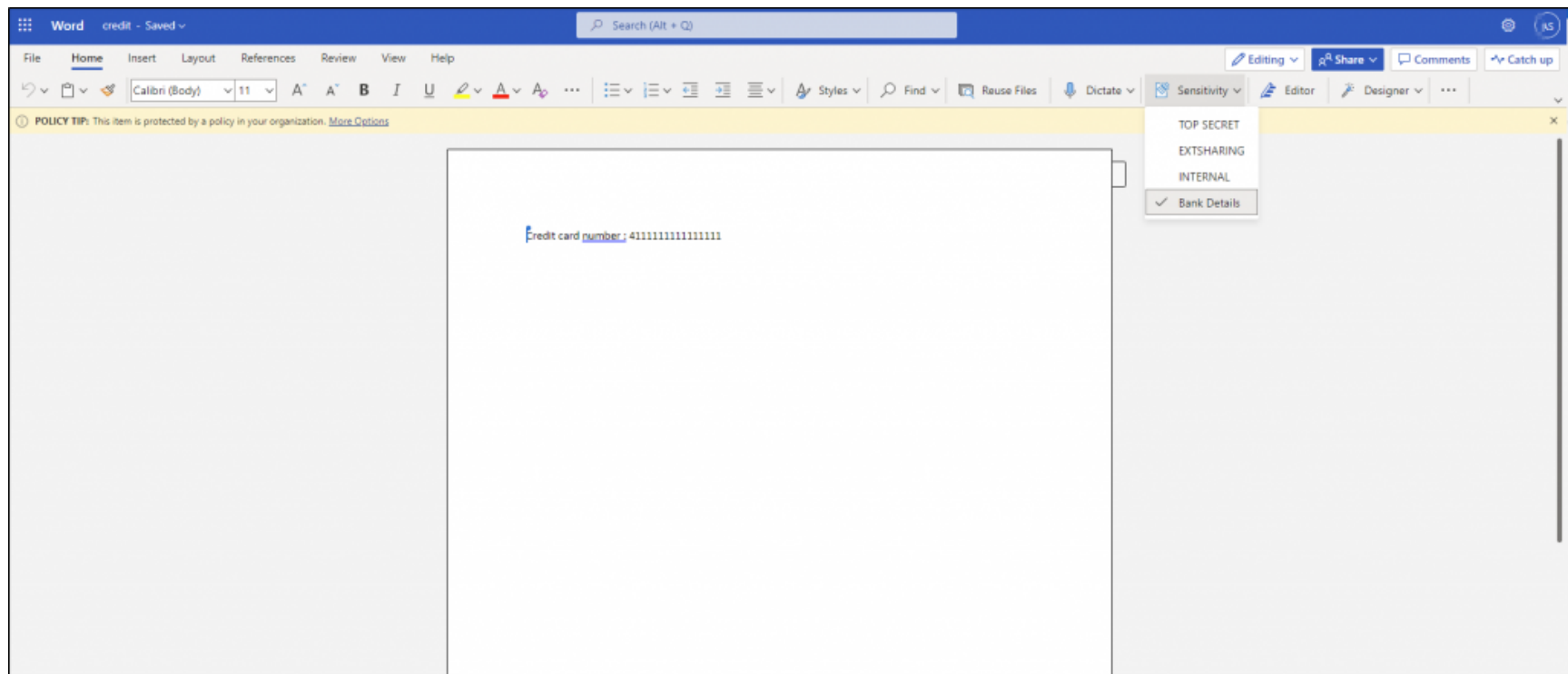
Change Cancel

*Justification for changing the label*

Step 11: After choosing the default label, name it and **'Submit'**.

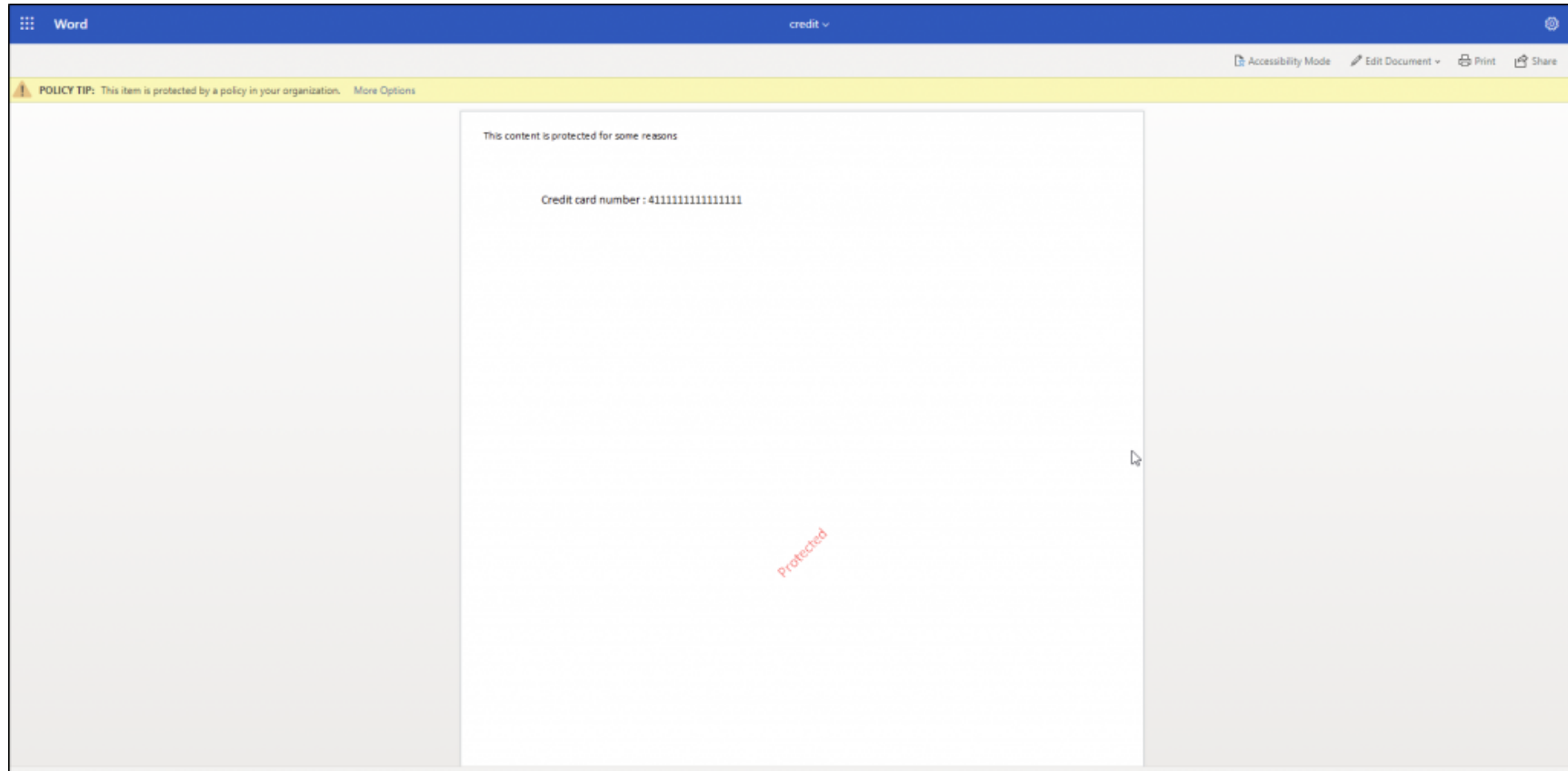
**Important: Note that it may take up to 24 hours for the sensitivity labels to be available for the users after creation.**

## How Microsoft 365 Sensitivity Labels Work?



*Selecting a label from the list and applying*

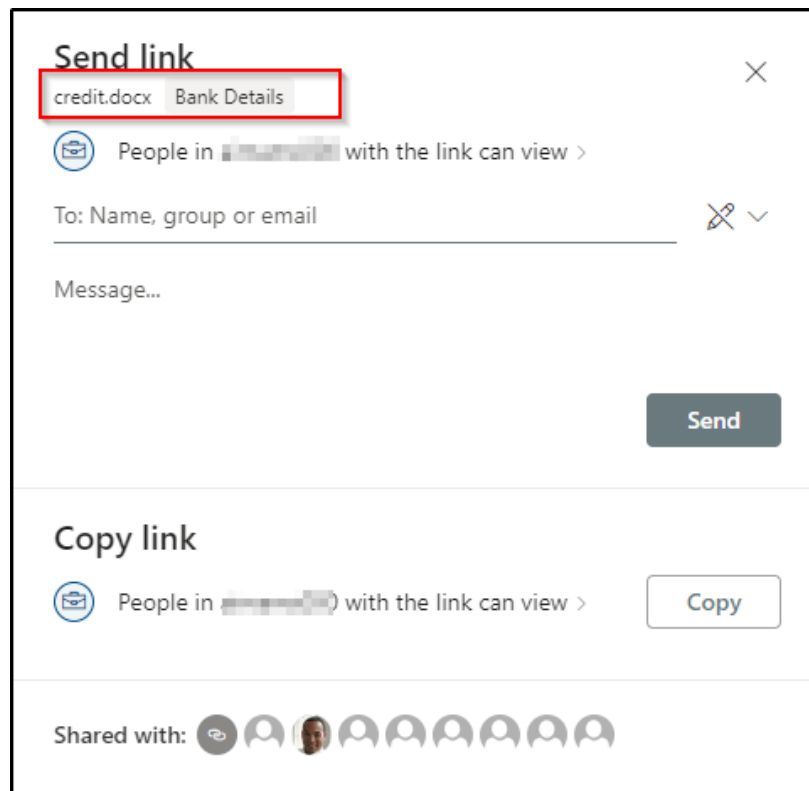
You can test it by applying the label manually from the **'Sensitivity'**  button from the ribbon and opening the document in the **'Viewing mode'**



*Document marked with watermarks, headers and footers*

## What's New? – Sensitivity label info in the Sharing Dialog!

After the rollout of Sensitivity labels, new features that support those labels are developed following it. One such feature is its addition to the shared dialog. That is, **when you try to share a labeled document in OneDrive or SharePoint, the sensitivity label's name and description (on hovering over the label) are displayed in the shared dialog**. As a result, people who are sharing can ensure what type of file they are attempting to share.



*Sensitivity label in the sharing dialog*

I hope this blog will help you understand the concepts of Sensitivity labels in Microsoft 365.