Lab 07: Encrypted phishing with Unified Labeling

Table of Contents

| Lab 07: Encrypted phishing with Unified Labeling | 1 |
|---|---|
| Goals | 1 |
| Requirements | 1 |
| 1. Enable Unified Labeling in Azure and Microsoft 365 | 1 |
| 2. Send an encrypted email with Unified Labeling | 3 |
| 3. Observe the encrypted email from the recipient's point of view | 7 |

Goals

- Enable Unified Labeling on your domain.
- Send an encrypted email message and observe the email from the recipient's point of view.

Requirements

- Microsoft 365 Business Premium trial account.
- Microsoft Azure trial account.
- Optional: A work/personal email account to be used as a recipient.

1. Enable Unified Labeling in Azure and Microsoft 365

1. Log in to portal.azure.com with your organization administrator account.

https://portal.azure.com

2. Use the search box at the top of the Azure Portal to search for "Azure Information Protection". Press Enter or click on the "Azure Information Protection" item that appears under "Services".



Searching for Azure Information Protection

3. Unified Labeling is activated by default on new Microsoft 365 Business Premium accounts. You should see a message confirming that Unified Labeling is Activated on the page.

| Home > Azure Information Protection | | | | | | |
|-------------------------------------|------|---|--|--|--|--|
| Azure Information | n Pi | rotection Unified labeling | | | | |
| Y | | | | | | |
| ₽ Search (Ctrl+/) | ~ | 🕞 Activate 🖷 Publish 🗋 Copy policies | | | | |
| General | ^ | A This page is read-only, and current values cannot be modified. | | | | |
| 🗔 Quick start | | Azure Information Protection labeling and policy management | | | | |
| Analytics | | policies will continue to function as configured; however, no fu versions will no longer be released for the classic client. | | | | |
| IL Usage report (Preview) | | To make changes to your labels and labeling policies, you must | | | | |
| & Activity logs (Preview) | | unified labeling client. | | | | |
| 🖳 Data discovery (Preview) | ١. | Unified labeling status | | | | |
| 📒 Recommendations (Preview) | | | | | | |
| Classifications | | Unified labeling: Activated . | | | | |

Confirmation that Unified Labeling is Activated in Azure

4. Although the Unified Labeling status is "Activated", you still need to turn on content processing to enable sending encrypted emails. To do this, click on the link to the Microsoft 365 Compliance center on the right side of the page.



Link to Microsoft 365 Compliance Center

5. Scroll down the main page of the Microsoft 365 Compliance center until you see a button that says "Turn on now" beneath a message about turning on content processing for your environment. Then click the "Turn on now" button. This will enable your users to send emails encrypted by Unified Labeling.

| | Microsoft 365 compliance | \$ | ? |
|---|--------------------------|---|------------|
| = | | (i) Your organization has not turned on the ability to process content in Office online files that h encrypted sensitivity labels applied and are stored in OneDrive and SharePoint. You can turn of | ave on |
| ŵ | Home | here, but note that additional configuration is required for Multi-Geo environments. Learn m | <u>ore</u> |
| ₽ | Compliance Manager | | DW |
| Ø | Data classification | () You can now create sensitivity labels with privacy and access control settings for Teams, Shar | ePoint |
| 뮏 | Data connectors | feature. | - |
| Δ | Alerts | 🕂 Create a label 🗔 Publish labels 💍 Refresh | |
| Ł | Reports | Name Order Scope Crea | ated by |

Clicking "Turn on Now"

2. Send an encrypted email with Unified Labeling

1. Log in to outlook.office.com with either your Alice or Bob user account, and create a new email message.

| ttps://outlook.offic | e.com | | |
|----------------------|-------|--|--|
| | | | |

| | Outlook | , | | |
|--------|-------------|---------|-------|----------|
| ≡ | New message | | | |
| \sim | Favorites | Focused | Other | Filter ∨ |
| | Inbox | | | |
| ⊳ | Sent Items | | | |
| 0 | Drafts | | | |

Creating a New Email Message

2. Next, click the three dots in the menu bar at the top of the new message interface. You should now see a menu item labeled "Set Permissions". Click on "Set Permissions" in the menu, and in the sub-menu that appears, you

can assign permissions to the email message, such as "Encrypt" or "Do Not Forward". For this example, click "Encrypt" to enable encryption on your email.

| | Send | 0 Attach 🗸 | Discard | ··· 1 | |
|---|--------|--------------------|---------|----------------------|--|
| | | | | Save draft | |
| | То | | | Insert signature | |
| | Cc | | | Show From | |
| - | Confic | lential \ All Empl | oyees | Set Permissions 2 > | |
| | Do No | ot Forward | | Set importance | |
| | Encryp | ^{ot} J | | Show message options | |

"Encrypt" Button Shown in the "Set Permissions" Sub-Menu

In some instances, the Encrypt button may appear directly in the toolbar, as shown below. Either way, the effect will be the same.

| ▷ Send | 🛚 Attach 🗸 🕲 Encrypt 🛍 Discard \cdots | ď |
|----------|---------------------------------------|-----|
| То | | Всс |
| Cc | | |
| Add a su | bject | |

Alternate Location of the Encrypt Button

3. After clicking Encrypt, you should notice a message appear at the top of the new email interface, stating that the message is encrypted.





4. To see what an encrypted email message looks like when delivered to a user at another organization or email provider, fill in the recipient email address (To) with your work or personal email address. Fill in the Subject, and Message Body fields with sample text.

| ۵ | Encrypt Remove | This me encrypti | ssage is <mark>on</mark> | encryp | ted. Re | cipient | ts can't | remov | e encry | ption. | Chang | je pern | nission | s | | |
|-----------|-------------------|---------------------|-----------------------------|---------|-----------|----------|----------|----------------|---------|--------|-------|---------|---------|-------|---------|----|
| То | | | | | × | | | | | | | | | | | |
| Cc | | | | | | | | | | | | | | | | |
| This is t | the subje | ect of my | y encr | /pted (| email |] | | | | | | | | | | |
| This is | the bod | y of the | encry | /pted | email | mess | age. | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| S | A A | В | Ι | U | \square | <u>A</u> | Q | © _≯ | | 1 | € | →≣ | 33 | | | |
| Send | 4 V | Disca | ard | 0 ~ | | : | | Ą | | | | | Draft | saved | at 2:51 | PM |

Sample Encrypted Email Creation

5. You can also use the "Change permissions" link in the message that appeared to add additional restrictions to the message.

| ۵ | Encrypt: This message is encrypted. Recipients can't remove encryption Change permissions Remove encryption |
|----|---|
| То | |
| Cc | |

Change Permissions Link

6. Changing the permissions from "Encrypt" to "Do Not Forward" will prevent the recipient from forwarding the email message to other users **in addition** to encrypting the message. This can be useful for preventing end users from forwarding phishing messages to their security team.



"Do Not Forward" Feature

7. Once you have finished creating your email message, click the "Send" button to deliver the message to the recipient.

| Do Not Forward: Recipients can't forward, print, or copy content. Change permissions Remove encryption | | | | | | |
|--|--|--|--|--|--|--|
| То | | | | | | |
| Сс | | | | | | |
| This is the subject of my encrypted email external | | | | | | |
| This is the body of the encrypted email message. | | | | | | |
| \checkmark A A° B I \bigcup \swarrow A \sim \sim \approx \equiv $=$ $+=$ $*=$ " \equiv \cdots | | | | | | |
| Send V Discard U V N C C C V Draft saved at 4:22 PM | | | | | | |
| Send Button | | | | | | |

3. Observe the encrypted email from the recipient's point of view

1. Login to the recipient email account where your encrypted email was delivered to view the email from the recipient's point of view. Regardless of email client, the sender's name and email subject are not encrypted and should appear as normal when listed in the recipient's inbox.

| Q Search r | nail | r | ? | () | * * * * * * * * * * | | e |
|-------------------|--|---------|---|------------|---------------------------|-------|----------|
| □· C | : | | | 1-5 | of 5 | < | > |
| B | bb This is the subject of my encrypted email | message | | | e | 10:46 | 5 AM |

Sender Name and Subject are not Encrypted

2. Examples of opening the encrypted message in various email clients are included below.

Opening the Message in Outlook

 If the recipient uses the Outlook desktop application, the message may not be shown in the preview pane until the user double-clicks on the message to open it. The user may also see a pop-up message stating that Information Rights Management is being configured the first time they open a message that has a Unified Labeling policy applied.



Encrypted Email Shown in the Outlook Desktop Inbox

| Microsoft Outlook | ? | × |
|---|-------|-------|
| Configuring your computer for Information R Management | ights | |
| | C | ancel |

A Pop-Up May Appear on First Use

2. After opening the message, it behaves as any normal email message - except that if the Do Not Forward permission was applied, Outlook prevents the user from forwarding the message or from taking screenshots of

the message. (This screenshot had to be taken by running the Outlook application in a VM and taking a screenshot in the host OS.)



Encrypted Email Message Opened in the Outlook Desktop App

Opening the Message in the Outlook Web Interface

1. If the recipient opens the email from the Office 365 Outlook web interface, the message is displayed as normal in both the preview pane and when opened in new windows - again with the ability to forward the message disabled.



Encrypted Email Message After Opening in the Outlook Web Interface

Opening the Message Outside of Outlook

1. If the recipient uses a non-Outlook client or service to open the encrypted message, the user is prompted to read the message by clicking a button in the message body.

| is is the subject of my encrypted email | |
|--|---------------|
| J @n | 🔒 🗠 2:51 PM ☆ |
| To: <u>Show details</u> | Ø |
| $\varnothing \square \lor \qquad \bigtriangledown \lor \square \lor \oslash \lor$ | ☆ ☆ ⇒ |
| (@@@@@@@@.onmicrosoft.com) has sent you a protected n | nessage. |
| â | |
| Read the message | |
| Learn about messages protected by Office 365 Message Enc | ryption. |
| Privacy Statement | |
| Email encryption powered by Office 365. <u>Learn More</u> Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 | |
| | |
| 17.63 KB 🖉 1 file attached | Download all |
| | |

Encrypted Email Message as Shown in the Proton Mail Web Interface

2. After clicking "Read the message", the user is prompted to verify their identity by logging in or by receiving a one-time code sent to their email.

| Encrypted Message |
|---|
| @ .onmicrosoft.com has sent you a protected message |
| |
| Sign in to view the message |
| |
| Sign in with a work or school account |
| Sign in with a One-time passcode |

Sign-in Page Shown After Clicking "Read the message"

3. Once the user's identity has been verified, the message is displayed in the web browser via Outlook.com.

| @pm | i.me | Sign Out | ? |
|---|------|---------------|---|
| This is the subject of my encrypted email | | | ^ |
| J Today, 2:51 PM @pm.me > | \$ | Reply all 🗸 | |
| Encrypt: This message is encrypted. Recipients can't remove encryption. | | | |
| This is the body of the encrypted email message. | | | |

Encrypted Message Opened After Sign in