Phishing Reporter

This section describes in detail how to customize the add-in on the platform and deploy the Phishing Reporter add-in to users in Microsoft 365, Exchange, or Google Workspace platforms.

This page also contains how to customize the Diagnostic Tool service and deploy it to the users to monitor the users' Phishing Reporter Outlook Add-in.

Shortcuts

- Phishing Reporter Customization
- Phishing Reporter Deployment
- Diagnostic Tool Customization and Deployment

FAQ

How does the Phishing Reporter button work?

The Keepnet Phishing Reporter offers two methods for reporting a suspicious email:

1. It calls Keepnet's APIs to report the emails in a fully encrypted and secure manner.
2. It sends a copy of the reported suspicious email to the SOC team. The "Email Settings" section provides customization options.

How does the Phishing Reporter work with SOC Tools?

The Phishing Reporter from Keepnet works seamlessly with SOC tools to streamline and automate phishing analysis and incident response within organizations.

Keepnet offers native integration with several major SOC platforms, including IBM Resilient, IBM QRadar, Splunk Phantom, ArcSight, and SOAR tools. For further details, please contact us directly.

Keepnet also provides robust APIs that allow integration with any SOC tools or services. You can access the API documentation here to learn how to utilize the Incident Responder APIs.

How does the Phishing Reporter label or identify reporting of duplicates?

Keepnet's "cluster view" feature effectively manages duplicates by organizing reported suspicious emails into clusters. This feature works in two primary ways:

1. **Clustering similar reported suspicious emails**: This method groups together emails that are alike in content or characteristics, helping to identify and manage duplicate reports.
2. **Clustering reporters with different reported suspicious emails**: This approach groups reporters based on the types of suspicious emails they report, even if the emails themselves are not identical. This helps in recognizing patterns or trends in the reporting behavior across different users or departments.

Is there a feedback loop to the users on the result of the investigation?

Yes, Keepnet offers a feedback mechanism to inform users about the outcomes of their reported suspicious emails.

1. This is facilitated through the use of playbooks, which allow you to define the process for providing feedback to employees, the SOC team, or service providers. For instance, you can set up a playbook to send an email to your employees detailing the analysis results of a reported email or alert the SOC team about phishing or malicious activities flagged by your staff.
2. Additionally, Keepnet provides customizable notification templates to streamline the feedback process. These templates can be tailored to meet your organization's

specific needs, ensuring employees are appropriately informed about the status of suspicious emails they report.

3. Security admins can also manage feedback directly from the Incident Response dashboard. Admins can effectively update users on the reported incidents by selecting a notification template and adding a custom message.

How can we seamlessly integrate with investigative tools to ensure efficient handling/management?

To seamlessly integrate with investigative tools for efficient handling and management of reported incidents, Keepnet offers several approaches:

1. Native Integrations:

Contact Keepnet: Begin by contacting us to learn about the native integrations we offer with various SOC tools and solutions. This will provide direct, built-in connections that facilitate smooth data flow and interactions.

2. Using Email Formats:

Send Copies of Emails: One of the simplest methods to integrate third-party solutions is to send a copy of the reported suspicious email in either .eml or .msg format. This can be configured in the "Email Settings" section, as detailed in our documentation here.

3. API Integration:

Incident Responder APIs: Utilize Keepnet's Incident Responder APIs to fetch reported email data. This data can then be processed or analyzed using other incident management systems. Our APIs provide flexibility to adapt and integrate with any external system, enhancing the overall response capability.

These methods ensure that you can tailor the integration process to meet your organization's specific needs and existing infrastructure, enabling efficient management of phishing incidents.

Phishing Reporter Customization

This document provides a detailed description of the **Phishing Reporter** product. You can understand the basic functions of the **Phishing Reporter** page and use the suspicious email reporter add-in by following this document.

You can access the **Phishing Reporter** and the menu of related options from the left sidebar of the platform dashboard.

What is the Phishing Reporter?

Phishing Reporter is an add-in that allows users to easily report a suspicious email to cyber security teams. Quick, comprehensive analysis and response can be provided when used in conjunction with the Incident Responder. Further details about the capabilities and requirements are available in this document.

This add-on is compatible with Outlook, Outlook Web Access, Outlook Desktop, Outlook Mobile, Office 365, and Google Workspace environments.

You can download and customize the reporter add-in from the platform interface, as well as see which users currently have the add-in installed.

> When the add-in is distributed over Office 365 or Google Workspace, it is automatically installed and active for all users. Add-in user information is only available for those using Outlook Desktop (with the MSI extension)

How to Configure the Phishing Reporter?

Go to the **Phishing Reporter** page from the left sidebar menu of the dashboard and select **Users > Settings**.

Customization is available to four features:

1. Add-in Settings
2. Email Settings
3. Other Settings
4. Diagnostic Tool

Add-in Settings

You can easily customize any of the fields in the phishing reporter add-in's appearance and dialog settings. It also supports multiple languages, so you can tailor the add-in to various languages and deploy it to employees in their preferred language. To add a new language, simply click on the "**+ Add New Language**" button in the **"Dialog Box Settings."**

Add-in Name	Name of the add-in.
Brand Name	Company name used for the add-in.
Add-in Logo	For best results, the logo should be 60px (w) :60px (h). The maximum disk image size is 2 MB; .png and .jpg formats are acceptable.
Dialog Box Heading	Header information used in pop-up messages.
Confirm Button Label	**Yes** button text used in confirmation messages.
No Button Label	**No** button text used in confirmation messages.
Okay Button Label	**Okay** button text used in confirmation messages.
Instant Report Message	Text that will appear after a user reports a suspicious email.
Connection Error Message	Text that will appear if the server cannot be accessed when a report is attempted.
Sending Error Message	Text that will appear if the reported email is not delivered to the platform.
No Email Selected Message	Text that will appear if the user tries to report an email without selecting an email.
Bad Format Email Message	Text that will appear if the user tries to report an email that is not eligible for reporting.

Show Confirmation Message When Reporting Email	You must check this box if you wish to include a confirmation message window for a reported email.
Show Confirmation Message When Deleting Email	This option opens a dialog box that allows you to remove the associated email after a report. If you select the "Automatically" option, the reported email will be deleted from the inbox.
Turn off email forwarding for reported Phishing Simulation Emails	This option has **two features**: 1. When an employee reports a **phishing simulation email**, a dialog box will appear confirming the report, and employees will receive a **congratulatory message** for recognizing the simulation email. 2. Reported **phishing simulation emails** will **not** be forwarded to the SOC team's email address specified in the **Email Settings** menu. This ensures that SOC teams can **focus on real suspicious emails** instead of simulated ones.
Warning Label	You have the option to add a message as a tag to the reported

Click the **Next** button to go to the next page and save your changes in the first time customization. When the first customization is done, you can use the **Save Changes** button to save your changes or use **Save and Download** button to save your settings and download the add-in immediately.

Email Settings

You can configure the add-in to send a reported email to the SOC or IT team as an attachment in **.eml** format using the "**Send Information Email for Reported Incidents**" option. You can customize the following settings:

> ⚠ To use this feature, please enable the "**Send Information Email for Reported Incidents**" option.

Recipient Email Address	Email address that will receive the reported e-mail
CC	Optional additional recipient

BCC	Optional additional blind copy recipient
Email Subject	Subject line for the email used when reporting a suspicious email. Use {SUB merge tag as a variable for reported emails' original subject.
Email Message	Message template for the email used when reporting a suspicious email

Click the **Next** button to go to the next page and save your changes in the first time customization. When the first customization is done, you can use the **Save Changes** button to save your changes or use **Save and Download** button to save your settings and download the add-in immediately.

Other Settings

You can also customize additional settings.

Proxy Settings	If users are accessing the internet through a proxy, you can enable the plugir proxy configuration of the computer where it will be installed.
Site URL	API address that will be used when reporting an email via the add-in. **Please contact the support team if a change is needed.**
API Key	The API key is to be used in the add-in to communicate with the platform. **Please contact the support team if a change is needed.**
Company ID	The Company ID is to be used in the add-in to communicate with the platfor **Please contact the support team if a change is needed.**
Enterprise Vault	The suspicious email can be searched in the user's backup emails during the investigation.

Click the **Next** button to go to the next page and save your changes in the first time customization. When the first customization is done, you can use the **Save Changes** button to save your changes or use **Save and Download** button to save your settings and download the add-in immediately.

Diagnostic Tool

The **Diagnostic Tool** provides information about the status of the add-in by sending the statistics of the add-in to the platform regularly. The advanced level of awareness presented makes distribution and regulation of the add-in easier for system admins. For example, if the add-in has been disabled by a user or for any reason, the tool can be used to ensure automatic activation or report the situation to the platform for system admins to be aware of this case.

> The Diagnostic Tool is designed only for use on Outlook Desktop add-in with the MSI extension. When the add-in is distributed over Office 365 or Google Workspace, it is automatically installed and active for all users.

Check and Enable All Disabled Add-ins Automatically	The reporter add-in can be enabled automatically if it is not enabled for a rea
Proxy Settings	If users are accessing the internet through a proxy, you can enable the plugir use the defined proxy configuration of the computer where it will be installec

After completing the configuration steps and customizations, you can click the **Save and Download** button to download the add-in for your environment.

How to View Which Users Have the Phishing Reporter Add-In Installed?

The Phishing Reporter menu offers the option to view a list of users who have the add-in installed and its activation status.

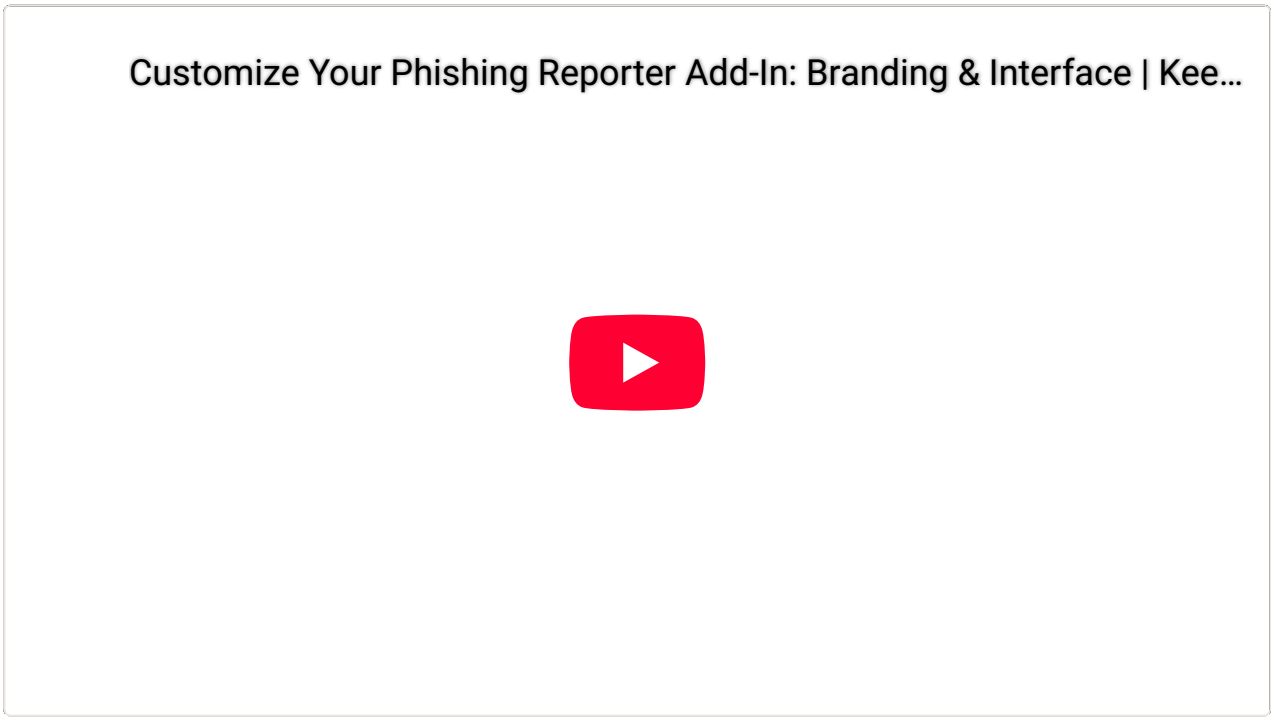
> When the add-in is distributed over Office 365 or Google Workspace, it is automatically installed and active for all users. add-in user information is only available for those using Outlook Desktop (with the MSI extension)

First name	First name of the target user. This field may be left blank if there is no target information for the related user on the platform.

Last name	Last name of the target user. This field may be left blank if there is no inform provided by the diagnostic tool.
E-mail	Email address of the add-in user. This field may be left blank if there is no ta information for the related user on the platform.
Add-in Status	Status of the add-in. If the Diagnostic Tool has not been enabled, the only vis will be **Online** or **Offline**. The Diagnostic Tool will indicate **Disabled, Not Insta** information about the add-in/user.
Last Seen	Date and time the add-in was last active.
Diagnostic Tool	Status of the Diagnostic Tool service. The tool can be Installed, Not Installed
Device	Name of the computer used.

Video Tutorial

This tutorial provides a detailed description of the Phishing Reporter product. You can understand the basic functions of the Phishing Reporter page and use the suspicious email reporter add-in by following this tutorial.



FAQ

Q: Is the Diagnostic Tool only available for the Outlook Desktop version of the add-on? Can it be used with Office 365 or Google workspace?

A: The Diagnostic Tool is designed specifically for the Outlook Desktop version. There is no need for the Diagnostic Tool for O365 and Google Workspace add-ins.

Q: I performed an update to the add-in. Do I need to uninstall the old version?

A: No. The new version of the add-in will update the old version.

Q: Do I need to update my existing Outlook, Office 365 or Google Workspace add-in if I change the content of the add-on on the platform?

A: You need to redistribute the current version of the add-in in order for any changes to be activated.

Q: When a user reports a suspicious email, can a backup of the reported email be forwarded to the SOC team?

A: Yes. please see more information on the ‘Email Settings’ page.

Q: Can I have a warning pop-up appear before the notification to prevent unintentional emails from being reported after clicking the add-in button?

A: Yes, you can enable the ‘Show confirmation message when reporting email’ option under the Add-in Settings page.

Q: Can I transfer the Phishing Reporter information to my own cybersecurity solutions or monitoring tools?

A: Yes. You can export all information related to Phishing Reporter via REST API using the API document.

Q: Does the add-in will prompt a "Delete" message after reports the phishing/training emails sent by the platform?

A: No, the add-in will first ask if you wish to report it and then will show a message that the admin is customized under the **"Turn off email forwarding for reported Phishing Simulation emails"** field. There won't be other prompts such as **"Do you wish to delete the original email"** after report emails sent by the platform.

Q: After the deployment of Phishing Reporter, how can I access it and use it on my OWA account?

A: Log in to your OWA email account and **open an email**. After that, on the right-hand side, click on the **Apps** button and click on the **Phishing Reporter** button to report the suspicious email.

Phishing Reporter Deployment

This section describes in detail how to deploy the Phishing Reporter add-in to users in Microsoft 365, Exchange, or Google Workspace platforms.

For instructions on the required initial installation of the add-in, please refer to the explanation provided here: Phishing Reporter Customization.

Shortcuts

- How to Deploy the Add-in in Microsoft 365
- How to Deploy the Add-in in Exchange Admin Center
- How to Deploy the Add-in in Google Workspace
- Phishing Reporter Announcement Email Template

FAQ

Q: The add-in was deployed to one of the listed email servers more than 12 hours ago but is still not visible on users' email applications. What can I do?

A: You can try to re-deploy the add-in. If it still does not appear, you should contact the support team of the email service provider.

Q: Can an Attacker hijack Outlook Add-in?

A: The platform uses “Code Signing with Microsoft Authenticode” to protect tools against hacking attempt. For more information, please click here.

Q: Is it possible to centralise the distribution of add-in?

A: Yes, it is. Many institutions manage the add-in (install, uninstall, enable, disable) with central administration tools, such as Microsoft SCCM, IBM Bigfix.

Q: Does the Phishing Reporter Add-In work with the Outlook application on iOS?

A: Yes, if you distribute the Phishing Reporter Add-In as an XML package (Microsoft 365), it will be available in both OWA/Outlook applications and will also function within the Outlook application on iOS.

Q: Does the Phishing Reporter Add-In work in shared mailboxes in O365?

A: The add-in works in shared mailboxes in the Outlook Desktop Application. However, it is not supported in shared mailboxes in OWA (Outlook Web Access).

Q: Does the new Outlook application on Windows 11 support MSI-based add-ins?

A: No, the new Outlook application on Windows 11 does not support MSI-based add-ins. It is designed to work primarily with web-based add-ins such as XML add-in of Keepnet Phishing Reporter. If you need MSI-based add-ins, we recommend using the classic Outlook for Windows desktop application. For more information, please find information under the "Extensibility" section in this document.

Q: Can I use the O365 XML Add-In on OWA in a mobile browser?

A: No, you can't use the add-in if you open OWA in a mobile browser. Microsoft 365 does not support third-party add-ins in mobile browsers for OWA. Please use the Outlook app instead.

How to Deploy the Add-in in Microsoft 365

Deploy the Add-in

- Log in to Microsoft 365 Admin Center and go to Add-ins.
- Click **+Deploy Add-in** and click **Next**. Under **Deploy a custom add-in**, click **Download custom apps**.
- Select **I have the manifesto.xml file**.
- Click **Upload**.

Now proceed to **Configure Add-in**.

Configure Add-In

Assign the users who will have access to the add-in. Choose one of the following:

- **Everyone:** The add-in will be installed on every user under the Microsoft 365 tenant (recommended).
- **Specific Users/Groups:** The add-in will be installed on the selected group or user.
- **Just me:** The add-in will be installed only on your mail account.

Now proceed to the **Deployment Method**.

Deployment Method

Select a **Deployment Method**.

- Fixed (Default, Recommended)
- Available
- Optional

Click **Deploy**.

> You will receive an email notification confirming your successful deployment. It may take up to 24 hours for the add-in to be displayed on the users' email applications. Users may need to relaunch email applications.

Once you have received notification that the deployment was successful, click on **Next**, and then **Finish** to complete the process.

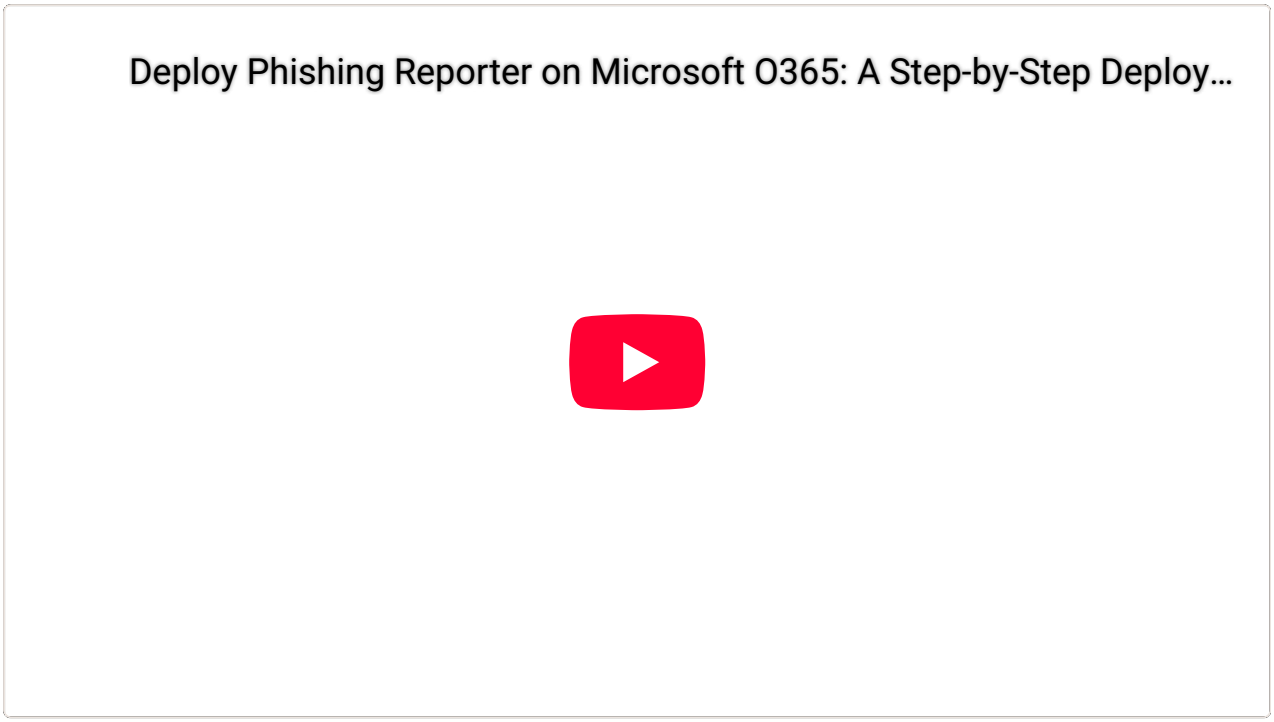
Uninstall the Add-in

To uninstall the Phishing Reporter add-in from Microsoft 365 user accounts, follow these steps:

- Log in to Microsoft 365 Admin Center and go to Add-ins.
- Select the add-in you want to uninstall.
- Click **Remove add-in** and then **Remove** to complete the process.

> It may take up to 24 hours for the add-in to be uninstalled. Users may need to relaunch email applications.

Video Tutorial


Deploy Phishing Reporter on Microsoft O365: A Step-by-Step Deploy...

Microsoft Ribbon Phishing Reporter

The **Microsoft Ribbon Phishing Reporter** allows your users to easily report suspicious emails and help protect your organization from cyberattacks. When you integrate the Phishing Reporter with Microsoft's integrated spam-reporting feature, the Phishing Reporter will appear in the Outlook ribbon.

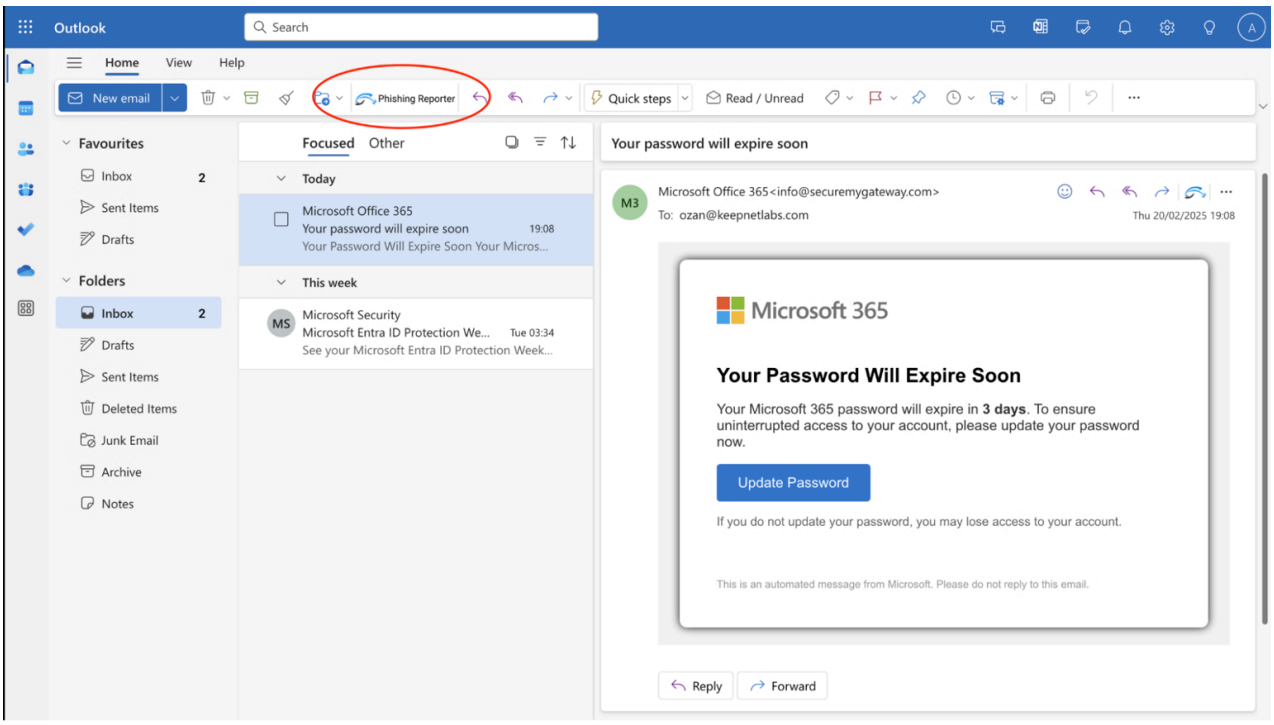
When your users click the Phishing Reporter to report an email, they can provide your IT team with an early warning about potential threats. You can receive reported emails in the Microsoft 365 Defender platform and the Keepnet Incident Responder page.

To learn how to install the Microsoft Ribbon Phishing Reporter and how your users can use the Phishing Reporter in their mail clients, see the sections below.

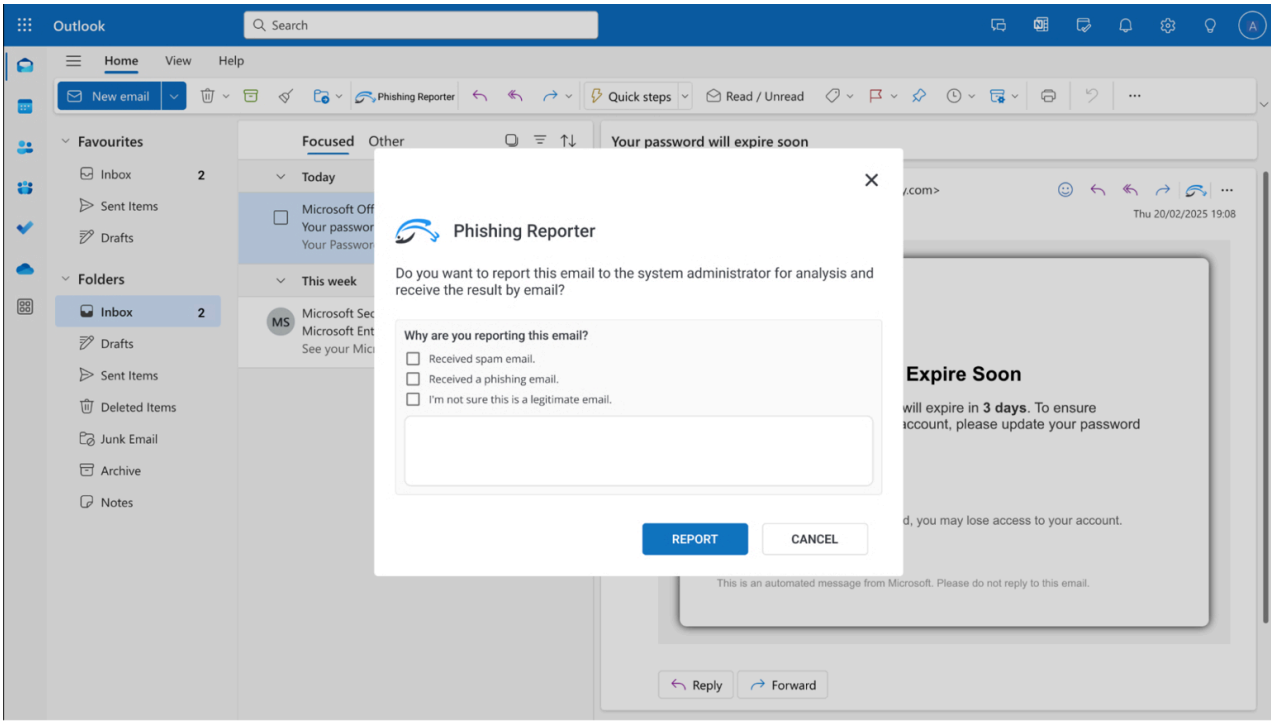
If you use the phishing feature in the Keepnet Incident Responder menu, the Microsoft Ribbon Phishing Reporter will also track if your users report our simulated phishing emails. You can use this feature to see which users successfully identify potential threats.

Microsoft Ribbon Phishing Reporter User Experience

Here is an example view of the ribbon phishing reporter on Outlook.



- When using the new Outlook Ribbon, clicking the Phishing Report button opens a pop-up window instead of a side panel.



- The pop-up provides the same reporting options but appears as a temporary dialog in the center of the screen.
- This is the default experience for some Outlook versions, including Outlook on Windows with the new Ribbon UI.

Supported clients

The following table identifies which Outlook clients support the integrated spam-reporting feature. See the full list here from Microsoft official documentation.

Client	Status
Outlook on the web	**Supported***
New Outlook on Windows	**Supported***
Classic Outlook on Windows Version 2404 (Build 17530.15000)	**Supported**
Outlook on Mac Version 16.81 (23121700) or later	**Only in Preview, Not Fully Functional** (see Preview the integrated spam-reporting feature in Outlook on Mac)
Outlook on Android	**Not available**
Outlook on iOS	**Not available**

⚠ * In Outlook on the web and the new Outlook on Windows, the integrated spam-reporting feature isn't supported for Microsoft 365 consumer accounts. Microsoft 365 Consumer accounts (Outlook.com, Hotmail, Live.com) are for personal use and don't support the integrated spam-reporting feature in Outlook on the web or the new Outlook on Windows.

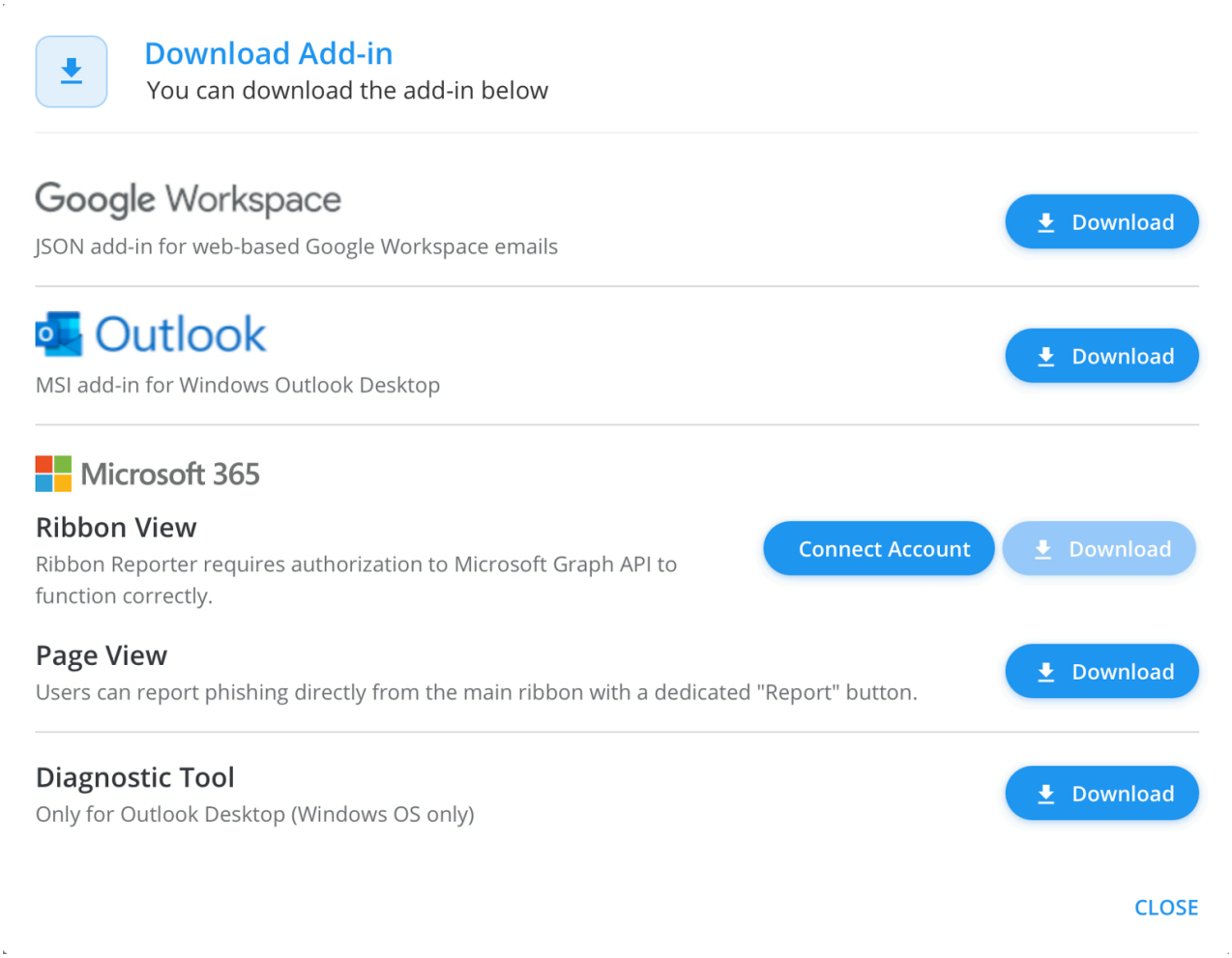
Prerequisites

Before you can install the Microsoft Ribbon Phishing Reporter for your organization, your organization will need to have a Microsoft 365 mail server and license. The Phishing Reporter is compatible with the following email clients and requirements.

⚠ The Microsoft Ribbon Phishing Reporter supports installation for shared mailboxes. This feature requires that Graph API and Nested App Authentication single sign-on (NAA-SSO) permissions are authorized in your Microsoft 365 tenant. See installation steps 5 through 9 below for how to authorize these permissions.

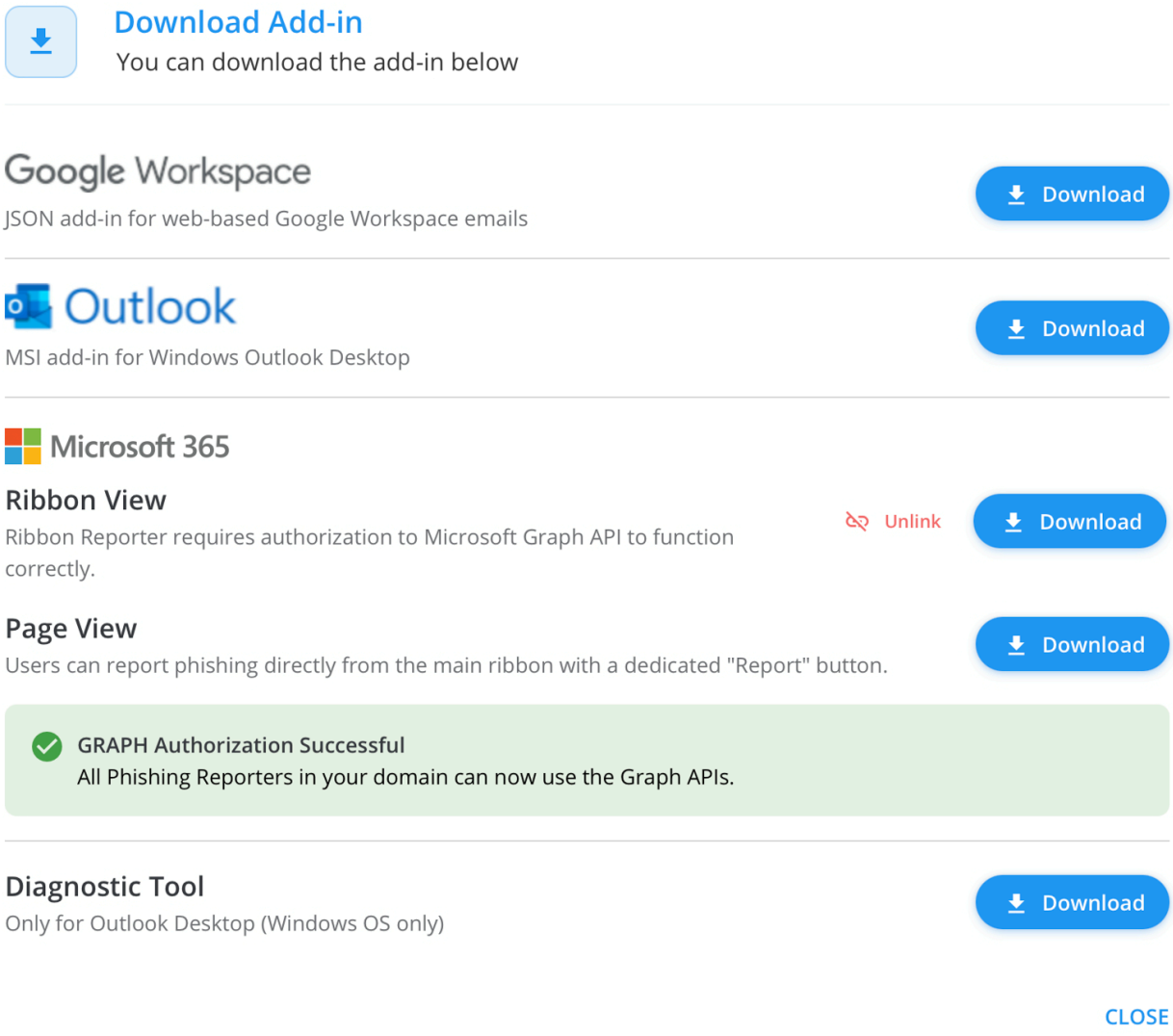
How to Install the Microsoft Ribbon Phishing Reporter

1. Customize Phishing Reporter for your organization's needs
2. Go to **Phishing Reporter > Manage and Download** section and click **“Connect Account”**

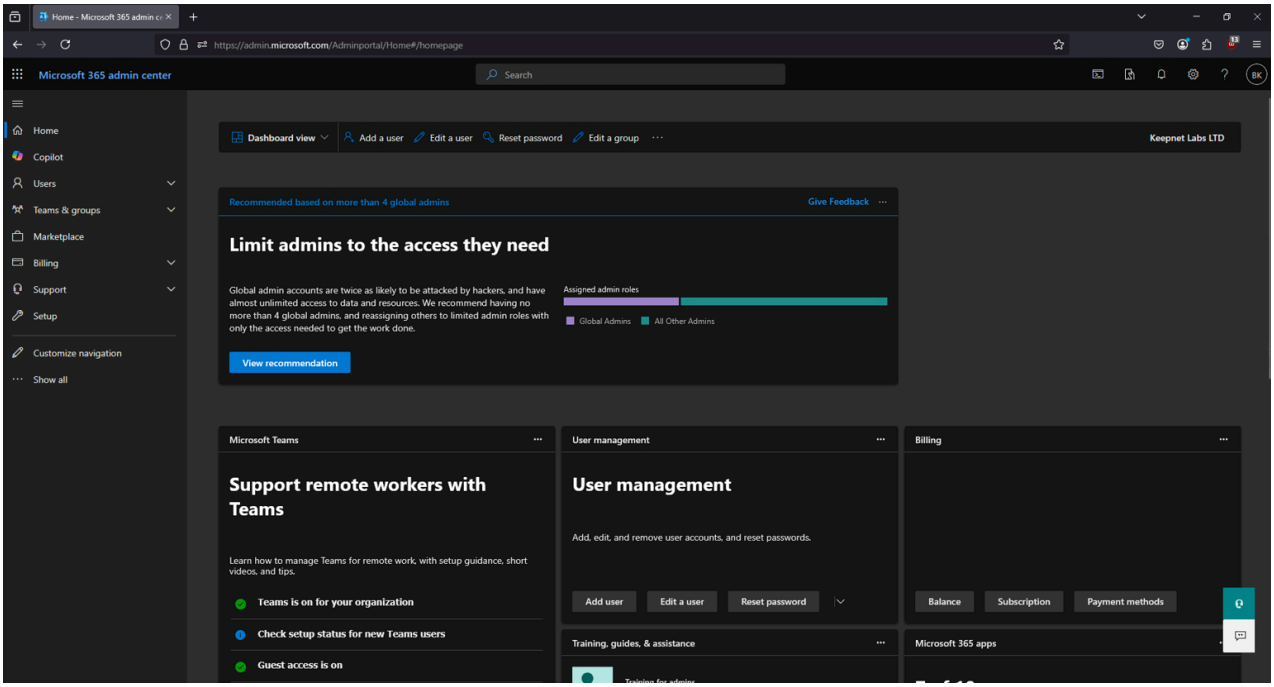


3. Log in to your Microsoft 365 account using your admin credentials.
4. Once you log in, the **Permissions requested** pop-up window will display. Read the permissions, then click **Accept**.

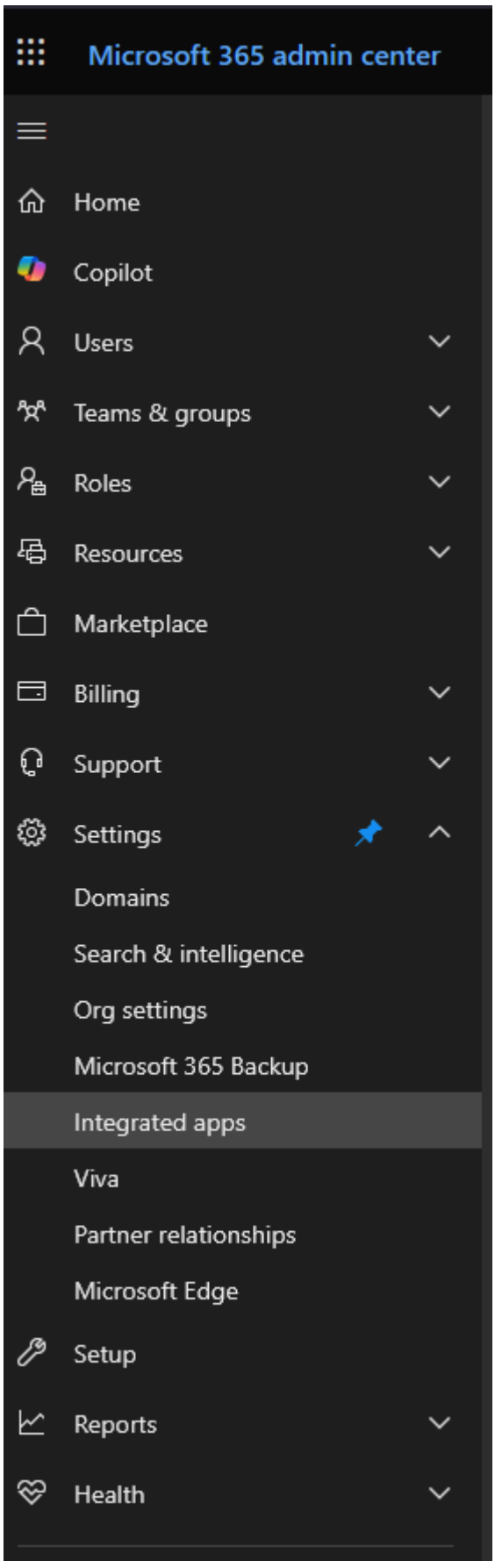
5. Once you accept the permissions, the GRAPH Authorization Successful window will display.



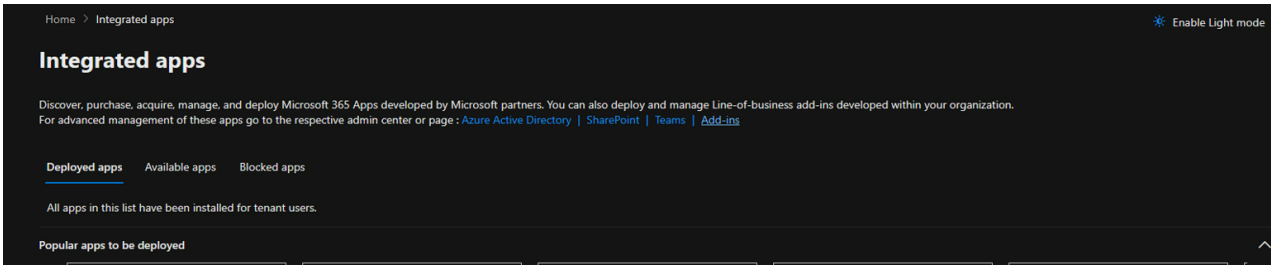
6. Click the **Download** icon below the **Microsoft Ribbon Phishing Reporter** option to download the **PhishingReporterRibbon.xml** file.
7. In a new tab of your browser, log in to your **Microsoft 365 admin center**.



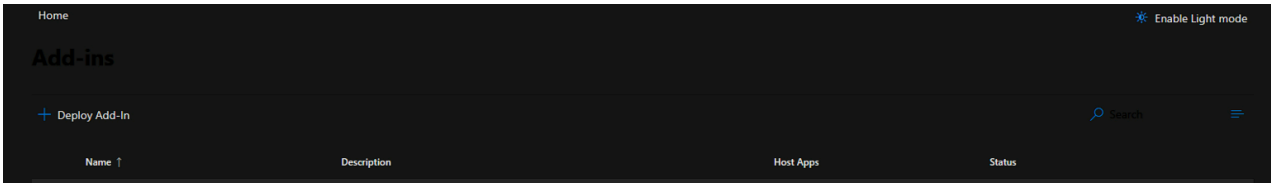
8. From the menu on the left side of the page, click **Settings**.
9. From the **Settings** drop-down menu, select **Integrated apps**.



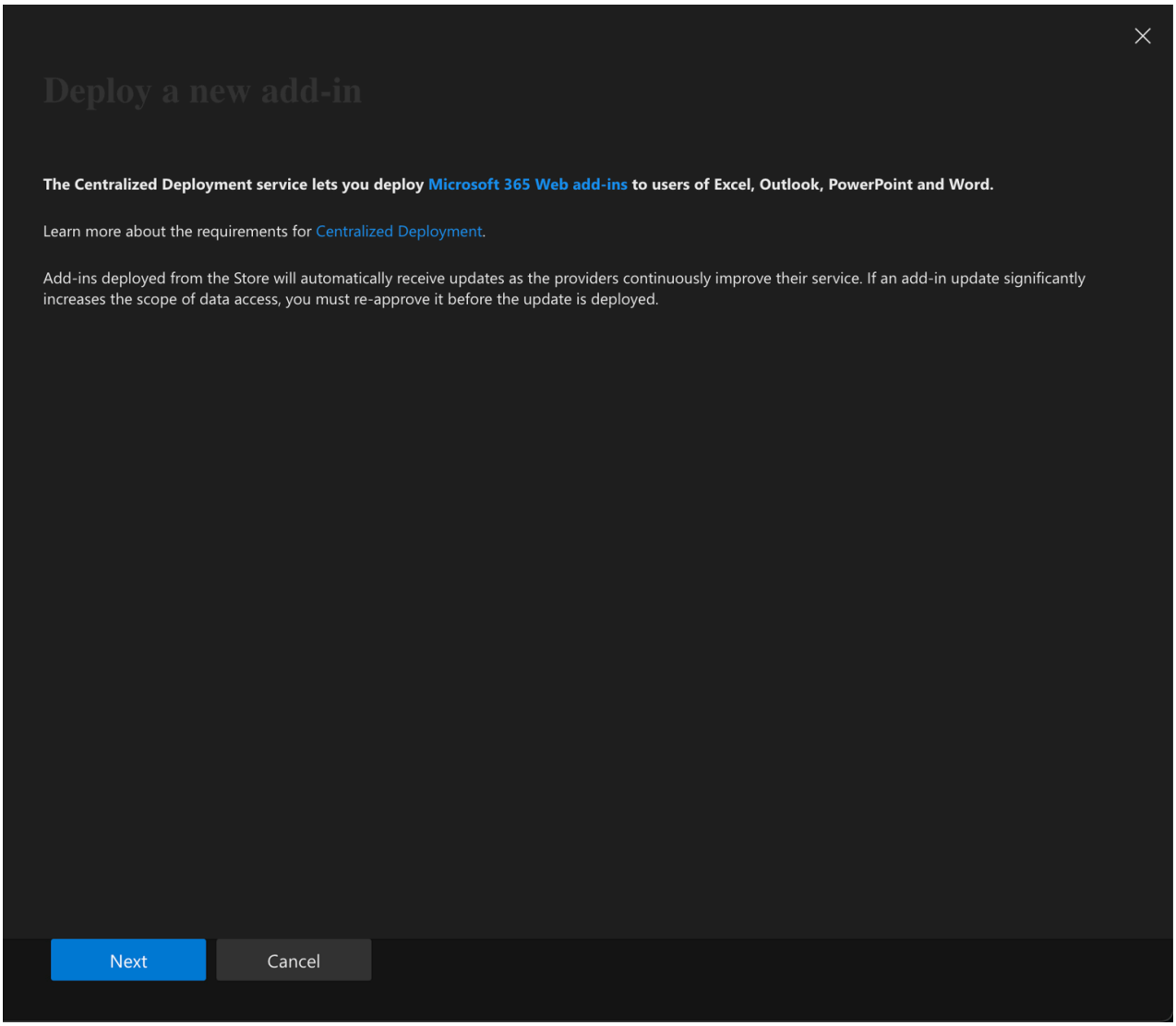
10. Click Add-ins at the top-right corner of the page. The Add-ins page will open



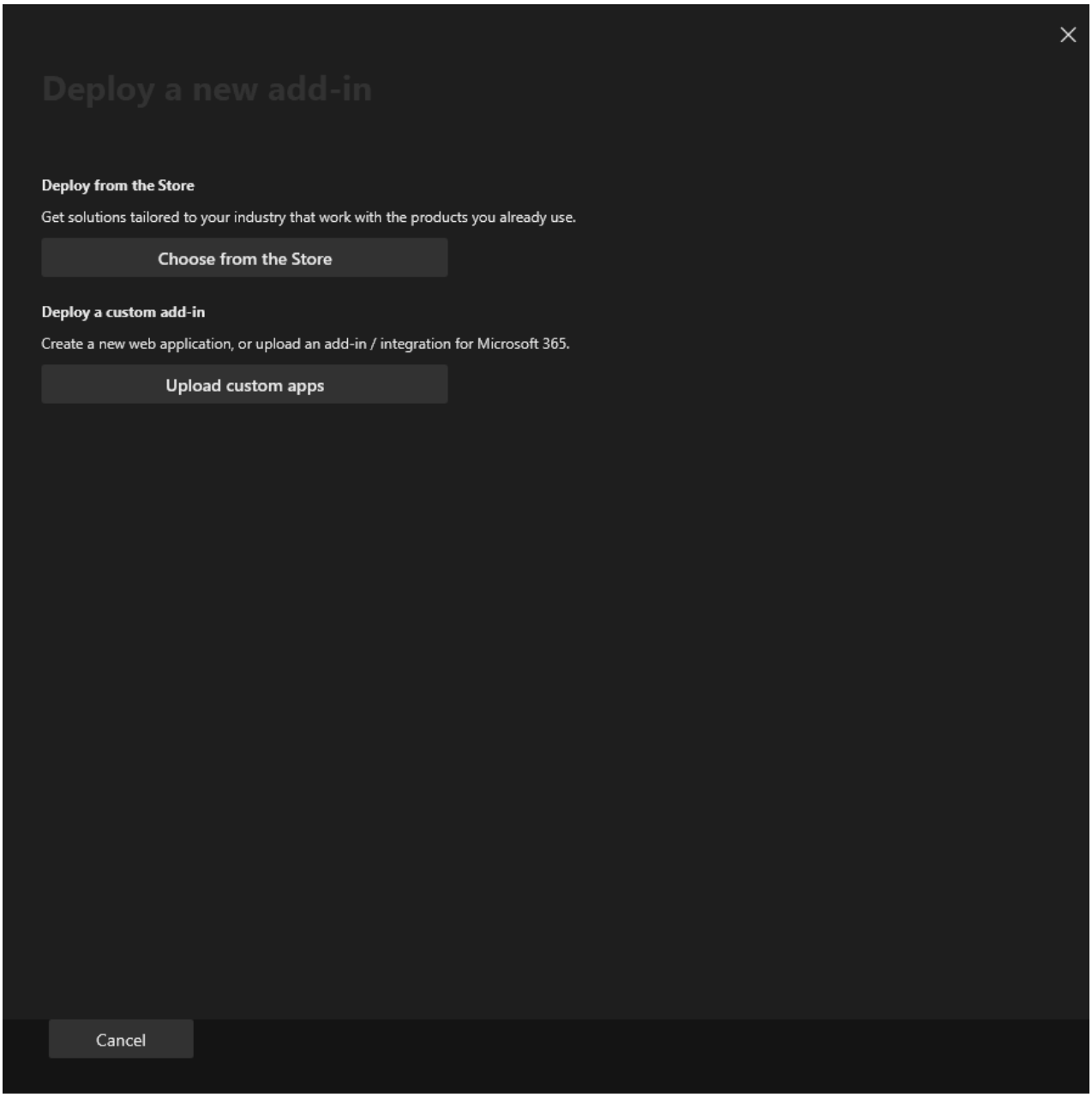
11. On the Add-ins page, click Deploy Add-In. The Deploy a new add-in pop-up window will open.



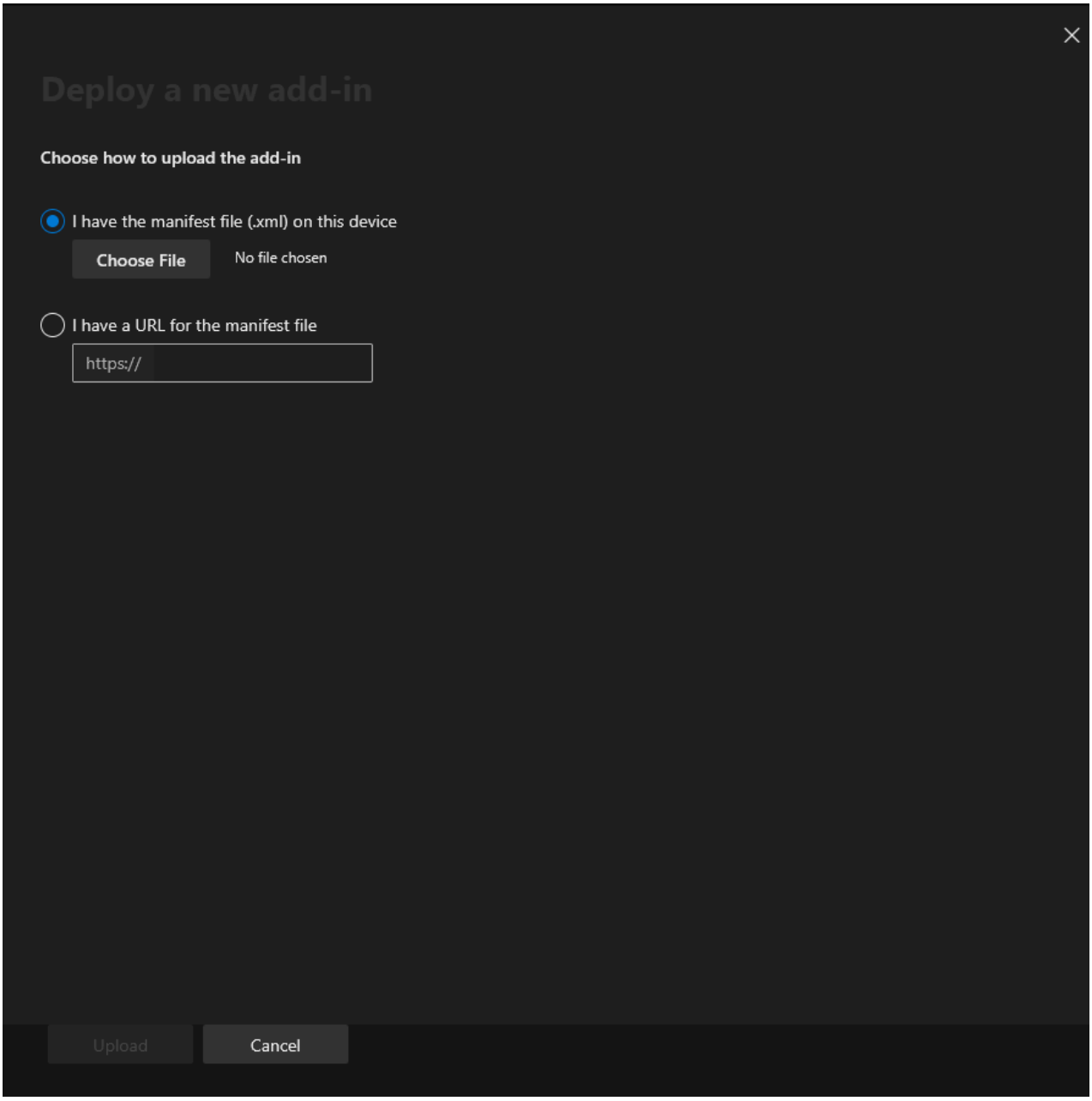
12. In the pop-up window, click Next.



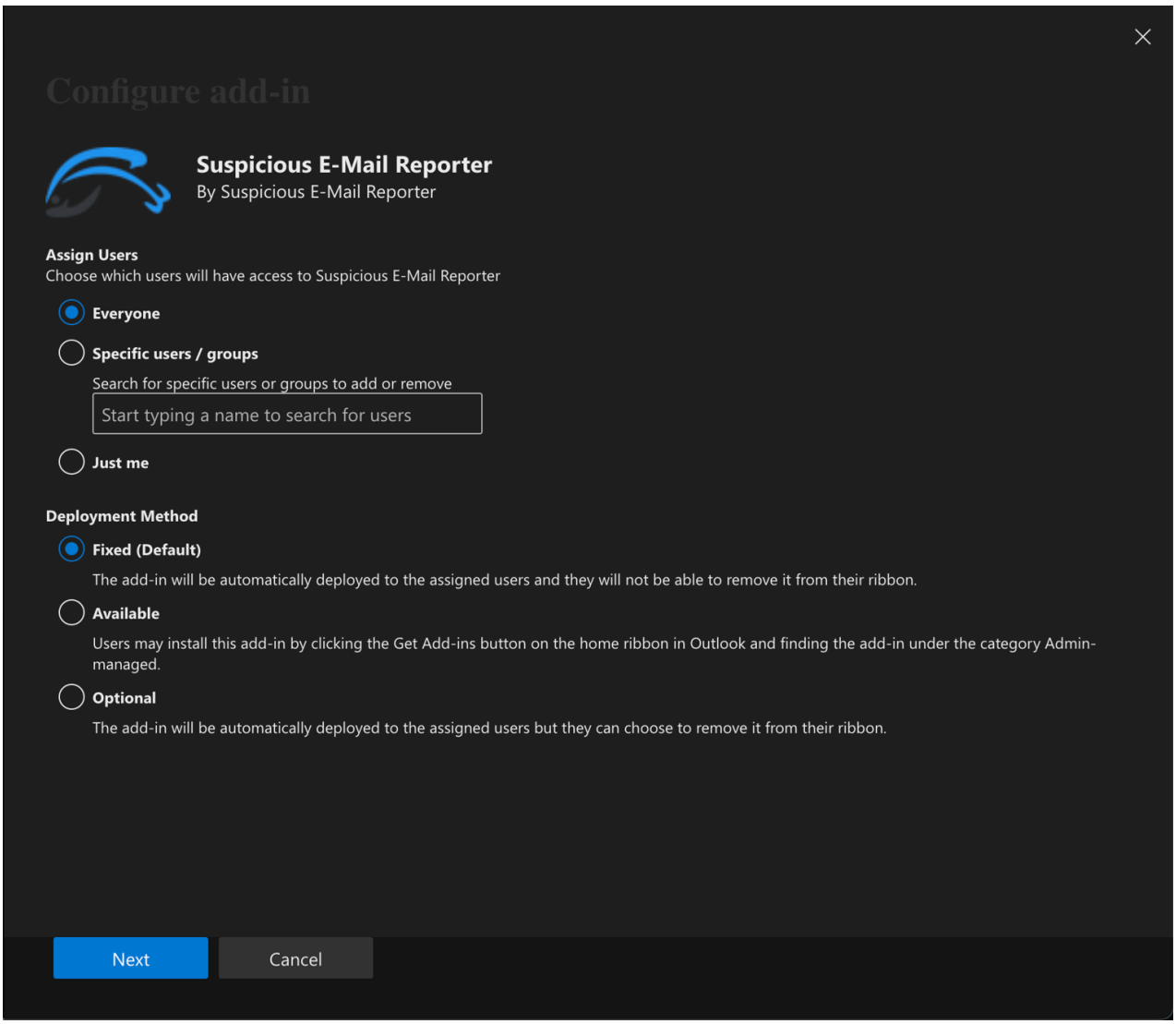
13. Click Upload custom apps.



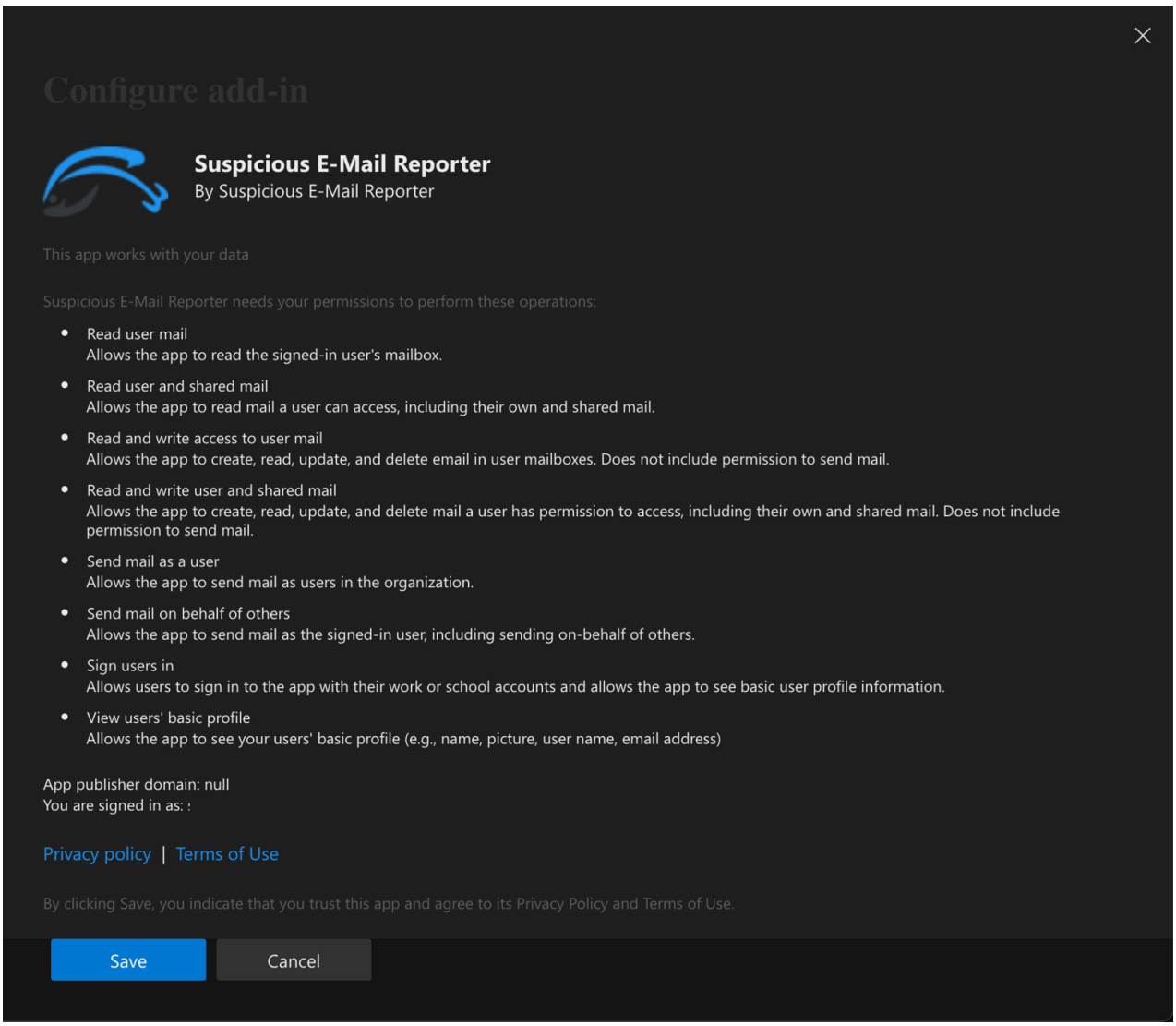
14. Select the **I have the manifest file (.xml) on this device** option. Then, click **Choose File** and select the **PhishingReporterRibbon.xml** file that you downloaded in step 6.



15. Click **Upload** to install the Phishing Reporter. The **Configure add-in** pop-up window will open.

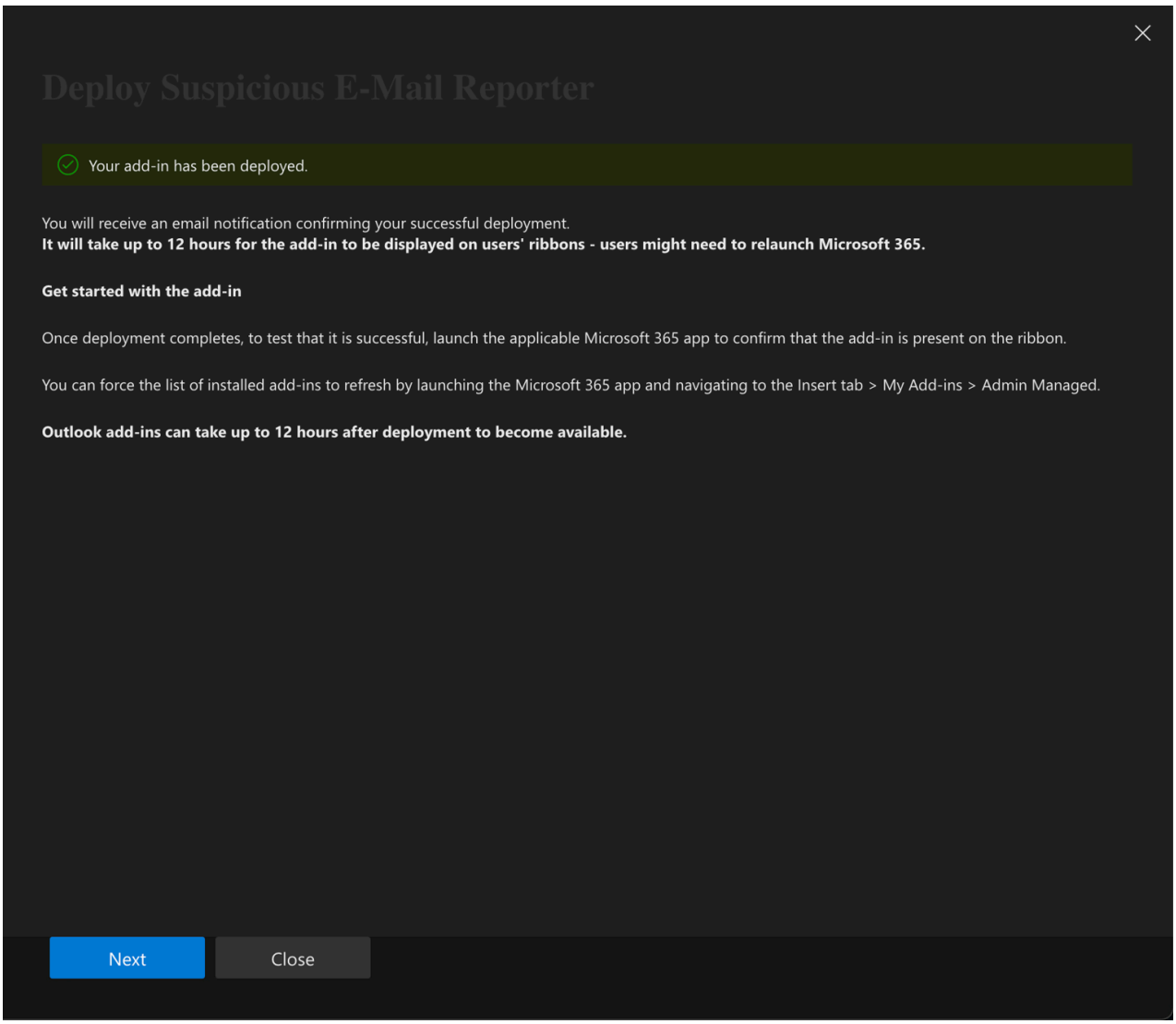


16. From the pop-up window, select which users will have access to the Phishing Reporter and which method you would like to use to deploy the Phishing Reporter.



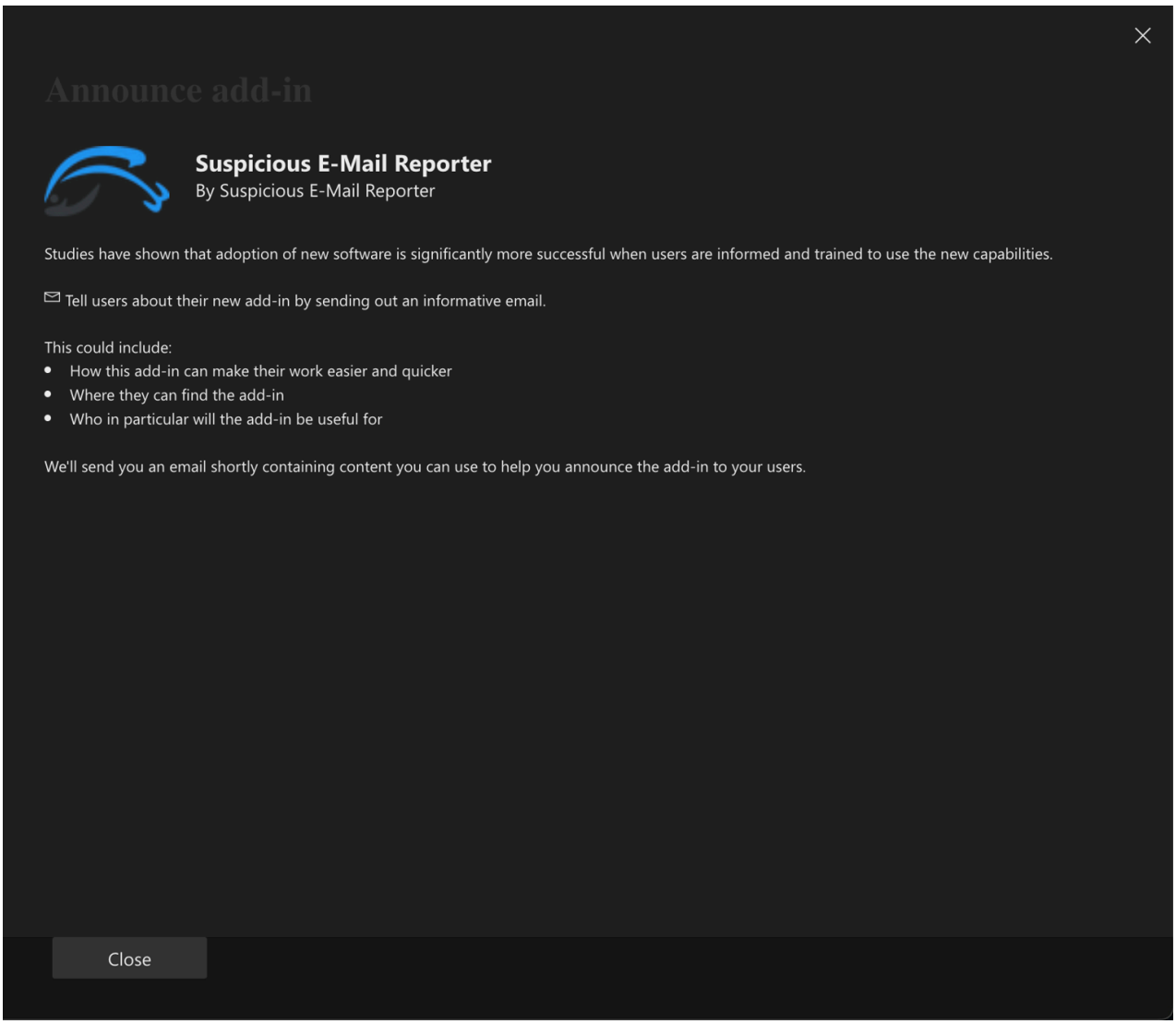
We recommend that you allow all users to access the Phishing Reporter. We also recommend that you use the Fixed deployment method.

17. Click **Next**, and additional app permissions will display.
18. Once you have read the permissions, click **Save**. The **Deploy** Phishing Reporter pop-up window will open.



The expected timeframe for the Phishing Reporter to deploy is 24 hours, but timeframes can vary. For more information about deploying add-ins, see Microsoft's Deploy add-ins in the Microsoft 365 admin center article.

19. Once the pop-up window displays a confirmation that the add-in successfully deployed, click **Next**. The **Announce add-in** pop-up window will open and display a message about announcement recommendations from Microsoft.



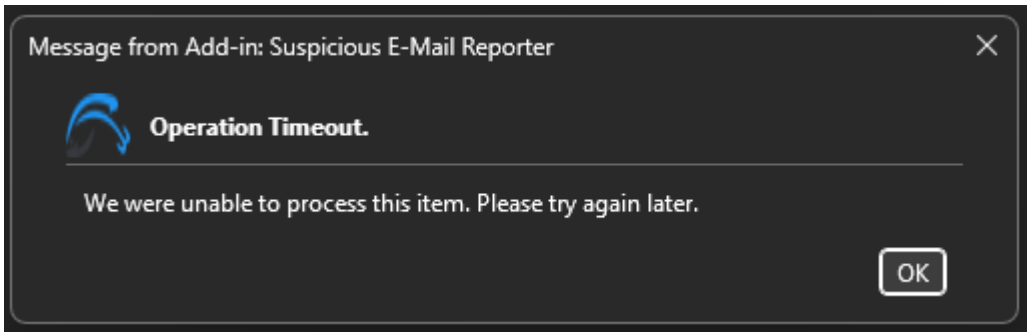
After you install and deploy the Phishing Reporter, you might receive an email from your mail service provider that contains information you can use to help you announce the Phishing Reporter add-in to your users. Keepnet does not send the email about the Phishing Reporter's intended usage and benefits.

20. Click Close to close the pop-up window.

Troubleshooting Microsoft Ribbon Phishing Reporter

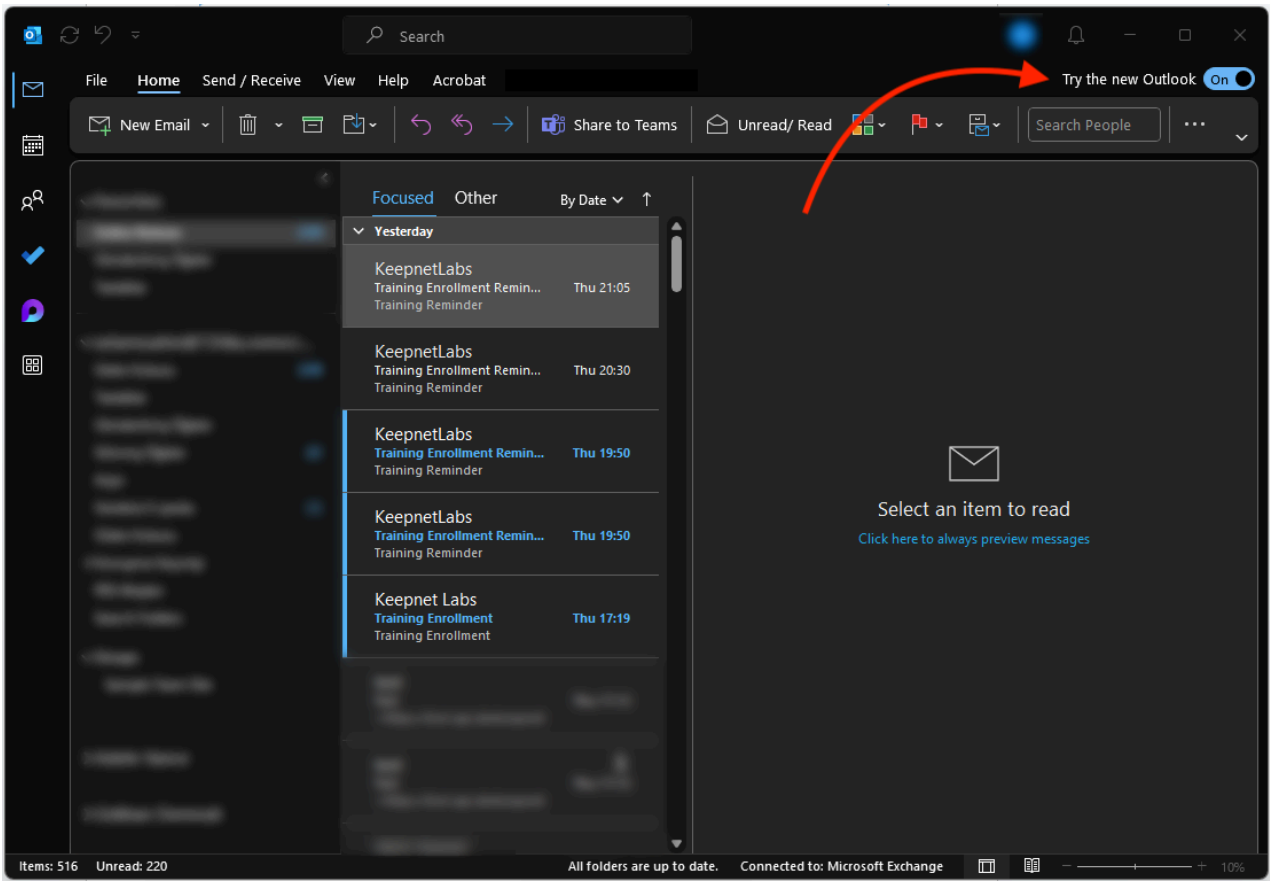
We were unable to process this item. Please try again later.

"We were unable to process this item. Please try again later." message in the Ribbon Phishing Reporter in Outlook.



We were unable to process this item issue on Microsoft Ribbon Phishing Reporter

The suggested solution is to "Toggling on New Outlook"



Toggling on New Outlook

It is recommended because:

1. **Compatibility Issues with Classic Outlook**

- The Microsoft Ribbon Phishing Reporter add-in might not be fully supported or optimized in the classic (legacy) Outlook for Windows **except Version 2404 (Build 17530.15000).** See Supported Clients
- Microsoft is shifting support toward New Outlook, which has improved integration with cloud-based services and add-ins.

2. **Performance & Connectivity Fixes in New Outlook**

- New Outlook is built on a web-based architecture, offering better compatibility with Microsoft 365 cloud services, including phishing reporting.
- It resolves time-out errors caused by outdated local add-in frameworks.

3. **Bug Fixes & Updates**

- Microsoft frequently updates the New Outlook, while the classic version may have outdated code that affects add-in performance.

4. **Cloud Integration & Service Connectivity**

- The Phishing Reporter add-in relies on Microsoft 365 cloud APIs to submit reports.
- If the classic Outlook version struggles with these connections, switching to the New Outlook can ensure a more stable connection.

Try Enabling "New Outlook" as suggested.

Frequently Asked Questions (FAQs)

Q: Can I show a confirmation prompt before deleting a reported email?

A: No, Microsoft Ribbon Phishing Reporter automatically deletes the reported email and does not provide an option to prompt employees for confirmation before deletion.

Q: Does the Ribbon work on Outlook Mobile for iPhone or Android?

A: As of March 2025, Microsoft does not support Outlook Mobile. Please refer to the supported clients list for updates: Supported Clients

Q: Can I change the window size of the Ribbon message (e.g., set a fixed width and height)?

A: No, Microsoft does not allow modifications to the pop-up box. Its size is automatically adjusted.

Q: Can I provide a language selection option for users to choose their preferred language for pop-up messages?

A: No, Microsoft does not support adding a language selection option within the pop-up. The language is automatically set based on the user's Outlook language settings.

Q: I see the Microsoft Ribbon Phishing Reporter in Outlook Desktop on my MacBook, but it doesn't work. Why?

A: Microsoft currently provides the Ribbon Phishing Reporter for preview purposes only on Outlook Desktop for Mac. While it may be visible, it is not fully functional. Please refer to the supported clients list for details: Supported Clients

Q: If Microsoft automatically deletes the reported email, can it be recovered?

A: Yes, after an email is reported, Microsoft displays a message confirming its deletion. This message includes an "Undo" option, allowing employees to recover the reported email if needed.

Q: Can I use the Ribbon Add-in and Page View Add-in together?

A: Yes, you can deploy both of them, and your employees can use either the Ribbon Add-in or the Page View Add-in based on their preference.

Q: Why can't I report multiple emails at the same time in Classic Outlook on Windows?

A: In **classic Outlook on Windows**, the **Phishing Reporter** processes one reported message at a time. If you attempt to report another email while the first one is still being processed, a **notification dialog** will appear, informing you that the previous report is still in progress.

To report multiple emails, please wait for the current report to complete before submitting the next one. This limitation ensures that each report is properly processed without conflicts.

Q: What Permissions are Required for Microsoft Graph API

A: The **Microsoft Ribbon Phishing Reporter** requires specific Microsoft Graph API permissions to function effectively within an organization's Microsoft 365 environment. These permissions allow the application to interact with users' emails, retrieve necessary details for reporting phishing attempts, and ensure smooth integration with the email infrastructure.

Below is a breakdown of the permissions required and their purpose:

1. Mail Permissions

- **Mail.Read**: Allows the Phishing Reporter to read the user's email to retrieve necessary email details such as headers, attachments, and content.
- **Mail.Read.Shared**: Extends read access to shared mailboxes, ensuring that the application can retrieve phishing emails reported from shared accounts.

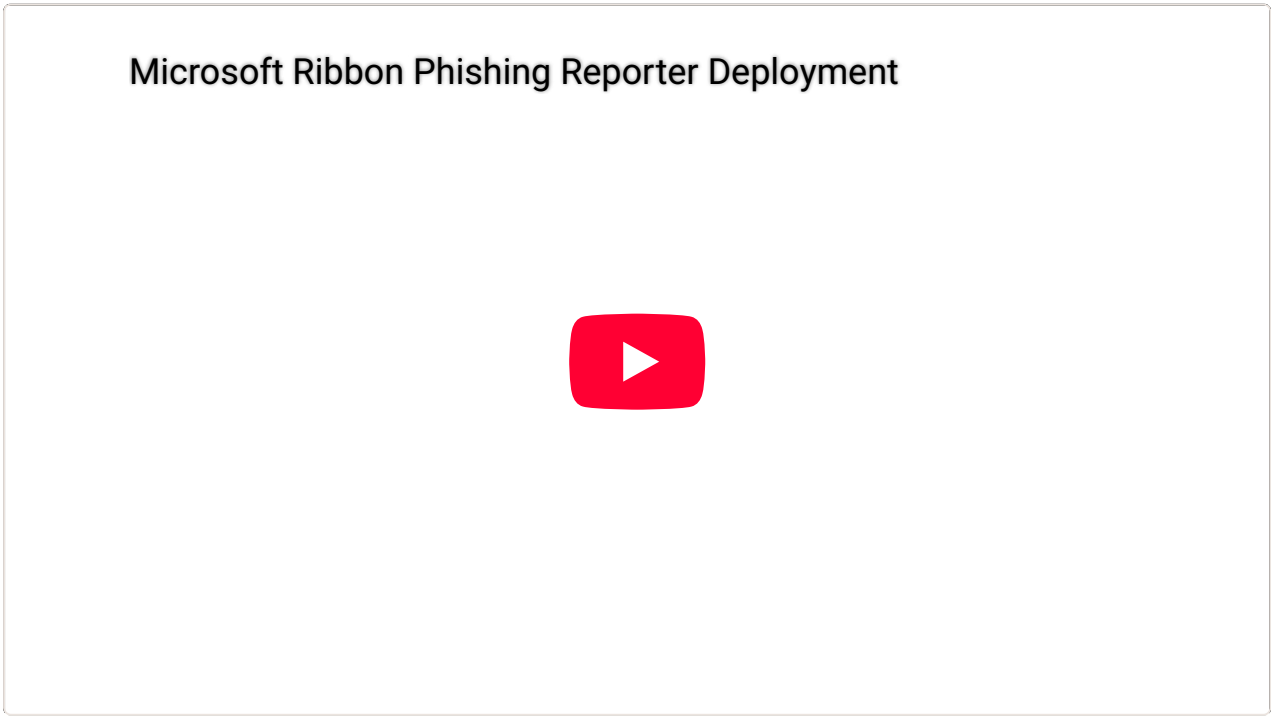
- **Mail.ReadWrite**: Provides both read and write access to the user's mailbox, enabling modifications or tagging of emails as needed.
- **Mail.ReadWrite.Shared**: Extends read and write permissions to shared mailboxes for better handling of phishing reports.
- **Mail.Send**: Enables the application to send emails, which may be necessary when forwarding reported phishing emails.
- **Mail.Send.Shared**: Allows the application to send emails from shared mailboxes when the user has the appropriate permissions.

2. User Profile Permissions

- **openid**: Grants access to the user's unique ID, helping in authentication and identity verification.
- **profile**: Allows the Microsoft Ribbon Phishing Reporter to retrieve basic user profile information, ensuring accurate reporting and tracking.

Tutorial Video

This video tutorial shows the documentation steps for deploying Microsoft Ribbon Phishing Reporter add-in on M365.



How to Deploy the Add-in in Exchange Admin Center

Requirements

In order to use the Phishing Reporter add-in in the Exchange environment, your platform must meet the following requirements.

- Exchange 2013 - version (15.0.847.32) or above
- Exchange 2016 - version (15.1.225.42) or above
- Exchange 2019

Deploy Add-in

To deploy the Phishing Reporter add-in, follow the steps below.

- Log in to the Exchange Admin interface.
- Go to **Exchange Admin Center > Organization > Add-ins**.
  - If you have Exchange 2013 or a different Exchange Admin interface, you can try **Exchange Admin Center > Organization > Apps.**
- Click the **(+)** button and select **Add from file**. Install the Phishing Reporter .xml file that you previously downloaded and click **Next**.
- Make sure that these options are selected:
  - Make this add-in available to users in your organization
  - Mandatory is always enabled
  - Users can't disable this add-in.
- Click **Save** to complete the process.

> It may take up to 12 hours for the add-in to be displayed on users' email applications. Users may need to relaunch their email applications.

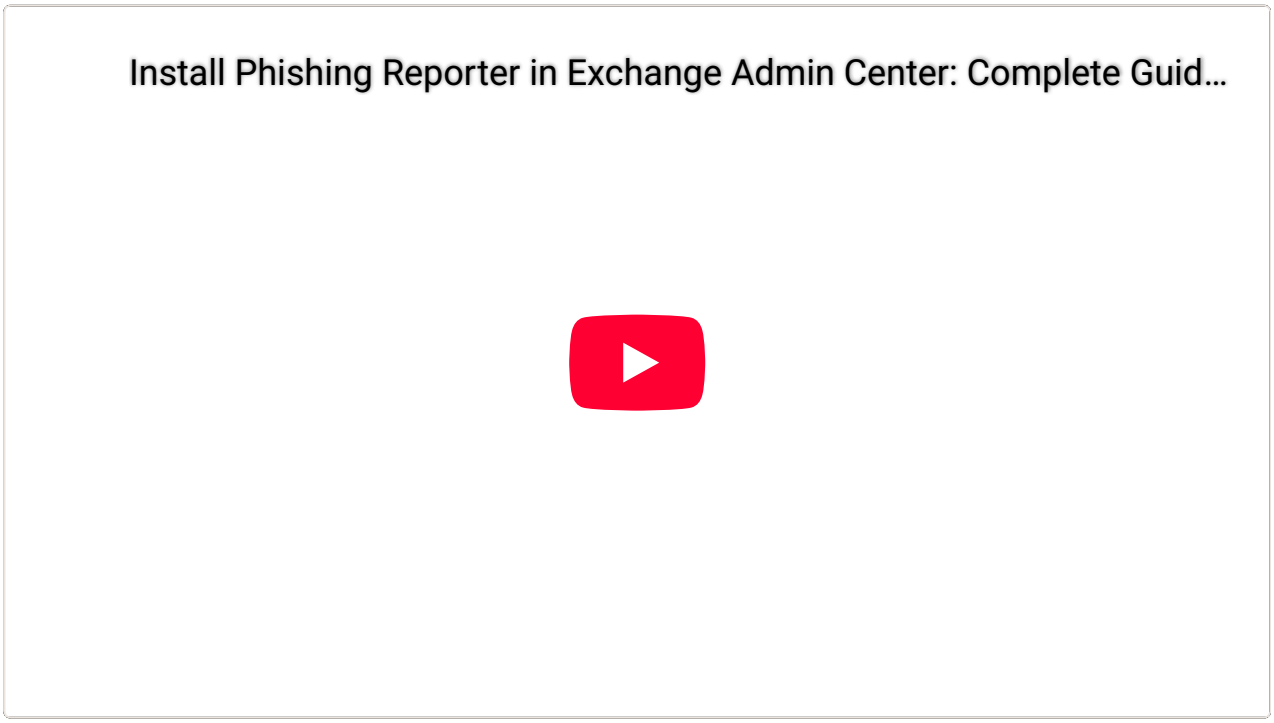
Uninstall the Add-in

To uninstall the Phishing Reporter add-in from Exchange Admin Center user accounts, follow these steps:

- Log in to Exchange Admin Center.
- Go to **Exchange Admin Center > Organization > Add-ins**.
  - If you have Exchange 2013 or a different Exchange Admin interface, you can try **Exchange Admin Center > Organization > Apps**.
- Click the add-in you want to uninstall.
- Click the **trash bin icon** and then click the **Yes** to complete the process.

> It may take up to 12 hours for the add-in to be uninstalled. Users may need to relaunch email applications.

Video Tutorial



How to Deploy the Add-in in Google Workspace

Deployment Steps

Create Script

To deploy the Phishing Reporter add-in to users in Google Workspace, follow these steps:

- Go to script.google.com and click on the **New Project** button.
- The new script file that is opened is saved with a project name.
- In the **Code.gs**, paste the script code provided by the platform and save it.
- Go to the settings icon and click **Project Settings**.
- In the **project settings**, click: **Show "appsscript.json" manifest file in editor.**
- Save the **appscript.json** file. Copy and save the manifest code.

Create Project

- Go to console.cloud.google.com and create **a new project**.
- Name your project and select the location. Then click on **Create** to start your project.
- Go to the **API & Services** page. Open the **OAuth content screen** page from the left menu and select your project.
- Please make sure the **User type** option selected is **Internal**.
- Click **Create**

OAuth Content Screen Configuration

- On the **OAuth content screen**, fill in the **App Name, User Support Email, App Logo** and **Developers Contact Email Address.** Then click **Save and Continue.**

- After that, click the **Save and Continue** button again on the **Scope** screen without making any changes. Then click **Back to Dashboard.**
- Go to **API & Services,** open the **Library** page to search **Gmail API,** and then **enable it**.
- Go to **Project Settings** and copy the **Project Number.**

Change the Project Number of Script

- Go to **Project Settings,** find the "**Cloud Platform Project**" title, and click on the **Change Project** button on script.google.com.
- Paste the **Project Number** in the designated field and click **Set Project**.
- Confirm the project change.

The change is enabled once the project change is confirmed.

Testing the Add-in

If you don't want to test the add-in in your Gmail account, please go to the "**Enable Google Workspace Marketplace SDK**" part to distribute the add-in to the organization.

If you want to test and see the add-in functionality, logos, add-in name, description, and more information, you can deploy the add-in to your Gmail account for test purposes and remove it anytime.

- Go to script.google.com
- Select the add-in project.
- Click on **Deploy >Test Deployments > Install** button.
- Click **Done**.

The add-in will appear on your Gmail account shortly.

Enable Google Workspace Marketplace SDK

- From the **Library** page, search for the **Google Workspace Marketplace SDK** and click on it.
- Click the **Enable** button and activate **Google Workspace Marketplace SDK**.
- Go back to script.google.com and click on the **Deploy > New Deployment** button.
- Enter information in the **Description** field, click the **Deploy** button, and copy the **Deployment ID**.
- Go back to the Console Cloud. Go to the **API & Services** page, find **“Google Workspace Marketplace SDK”** and click on it.
- Go to the **App Configuration** tab and enable the **Google Workspace add-on** option and check **Deploy using Apps Script Deployment ID**.
- Then paste the **Deployment ID** to the deployment field on the page and then fill in the following fields.
  - **Developer Name** with **Keepnet Labs**.
  - Fill in the **Developer Website URL** with **https://keepnetlabs.com**
  - Fill in the **Developer Email** with **support@keepnetlabs.com**.
- Before saving, do not forget to select the **Private** option and then click **Save**.
- Go to the **Google Workspace Marketplace SDK** page and click the **Manage** button to see the **Store Listing** menu.
  - Select the **Category** as **"Web Project".**
  - Select the **Language** as **"English".**
  - Upload your company logos. If you prefer, you can use the default logos below.
- Fill in the **Terms of Service URL**, **Private Policy URL**, and **Support URL** with **https://keepnetlabs.com** for the add-in.
- Under **Distribution**, select the **Region** that you will be deploying the add-in to and click **Publish**.

15KB | Add-In Logos.zip
archive

Default Phishing Reporter Add-In Logos

Deploy Add-in

Please follow up the following steps to deploy the add-in to your target users.

- To deploy the add-in, go to mail.google.com and click on the **Google Apps** icon in the top right-hand corner of the screen.
- Scroll down to **More from Google Workspace Marketplace** and click on it.
- Click **Internal Apps** and find the add-in
- Click the **Admin Install** button to start the deployment process.
- Click **Continue** to start the distribution of the extension.
- Accept the required permissions to complete the deployment.

> It may take up to 24 hours for this app to be installed for your entire Google Workspace domain or organizational unit.

Uninstall the Add-in

- Go to Google **Admin > Apps > Google Workspace Marketplace apps >** App list on the left menu.
- Click on the Phishing Reporter add-in you want to uninstall.
- Click the **Delete App** to complete the process.

> It may take up to 24 hours for this app to be uninstalled for your entire Google Workspace domain or organizational unit.

FAQ

Q: Does Google charge if we deploy the add-in?

A: No, there is no charge by Google.

Q: Can I use my phishing reporter add-in in the Gmail app on iOS or Android?

A: Yes, you can use the Phishing Reporter add-in in the Gmail App on Android or IOS.

Phishing Reporter Announcement Email Template

This text has been prepared for customers to use who want to inform their users about the Phishing Reporter add-in.

Email Template

Dear …. Team,

We are happy to announce to you a new email function: “Suspicious (Phishing) E-mail Reporter”.This add-in will help you to easily and instantly report suspicious emails to Information Security Team for analysis.

Please read the instructions below to understand how to use this add-in.

What is the Phishing Reporter add-in?

The Phishing Reporter add-on is a button placed on your email menu bar. This button will enable you to report suspicious emails to us. It will also give us the opportunity to timely identify email-born cyber threats and take action before any damage occurs.

What will the add-on bring?

- You can report email attacks with a single click.
- Timely notifications of "Phishing" attacks will help the information security team be more proactive and reinforce our company’s cybersecurity posture.
- The add-in will help you be more aware of cyber risks.

A Sample Usage

1. The user clicks on the “Report Phishing” button to report the suspicious email, then he/she is asked whether to delete the original email or not.

2. At the end of this process, the result of the analysis of the suspicious email you reported will be sent to you via email.
3. The user is then appreciated for his/her attentive action.

Diagnostic Tool

In standard Windows, the MS Outlook service does not support monitoring and reporting the functionality of the installed add-ins on it. This service has been developed in order to monitor and report whether Keepnet Outlook add-in functions properly or not.

Using this service, system administrators will be aware of the potential environment-based errors which could affect the Keepnet Outlook Phishing Reporter add-in not functioning properly and be able to take action.

Downloading Diagnostic tool

Go to **Phishing Reporter > Settings > Diagnostic Tool** to download the diagnostic tool.

Configure the following settings:

- **Proxy Settings:** Enable proxy settings for the Diagnostic Tool to go internet through a proxy.
- **Optional Settings:** Select if you want the Diagnostic Tool to check the Phishing Reporter add-in and enable it automatically if disabled.

Once you're happy with your settings, click **Download** under the diagnostic tool. Then follow the steps below to install the service.

Installation

There are two options to install the service, either install it on your computer or deploy the service to thousands of users' computers using centralized software distribution tools.

Normal installation

- Click on the **MSI package** to install it on your computer.
- Click the **Next** button and continue with the default settings.

- Click the **Yes** button to finish the installation.

Silent Installation

You can use the following commands for silent installation and removal.

Silent Installation	C:\Windows\System32\msiExec.exe -i "KeepnetPhishDiagInstaller.msi" /QN /norestart
Silent Removal	C:\Windows\System32\msiExec.exe -x "KeepnetPhishDiagInstaller.msi" /QN /norestart
Product Guid Detection	get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name, LocalPackage -AutoSize
Remove with Product Guid	C:\Windows\System32\msiExec.exe -x {product-guid} /QN /norestart

Once the installation is complete, you can confirm that the diagnostic tool has been installed by going to **Phishing Reporter > Users** and looking under the **Diagnostic tool** column.

This column will show one of the following in the table below.

Not Installed	The diagnostic tool has not been installed
Online	The diagnostic tool has been installed, and the user is online
Offline	The diagnostic tool is installed, but the user is offline
Error/Uninstalled	There is an error with the diagnostic tool installation or the tool has been removed

Understand Diagnostic Tool information

To view the **Diagnostic Tool** information, go to **Phishing Reporter > Users** and look under the **Add-in Status** column. When hovering the mouse over this column under the desired user, you will see the following information below.

Add-in is installed and	• User is online • User is offline
HKLM Number	List of possible values: 1: Active: Don't load automatically 2: Disabled: Load at startup 3: Active: Load at startup
Boot time	How long it takes for the add-in to start
Outlook version	Version information of Outlook application
Outlook Architecture	Either: • X32 • X64
OS version	User's operating system version information

The Diagnostic Tool has been successfully installed, operated and can communicate with the platform to help you obtain Phishing Reporter status information for all target users.

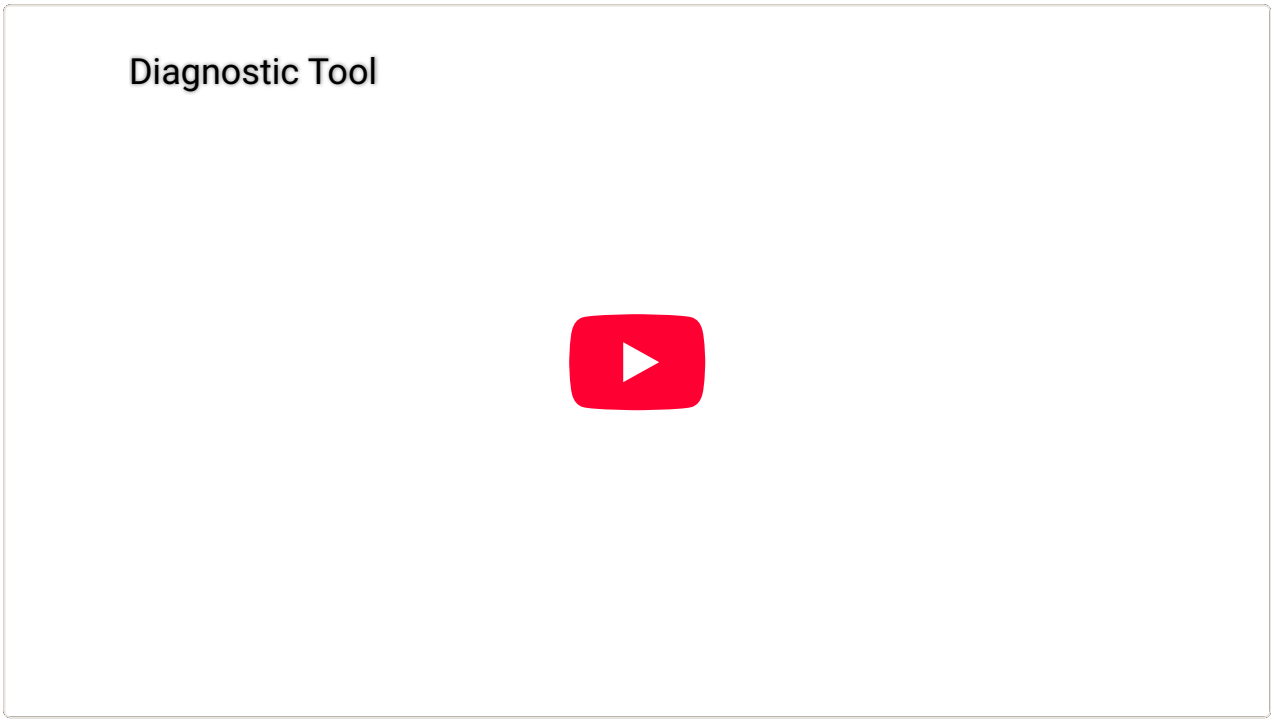
Troubleshooting

For troubleshooting purposes, you can provide the support team with the log and configuration files, which can be found in the following path on the user's computer.

- C:\Program Files (x86)\Keepnet Labs\KeepnetLabs Phishing Reporter Diagnostic Service

Tutorial Video

This video tutorial explains how to customize the Diagnostic Tool service and download it.



FAQ

Q: Some users have the add-in enabled, but they seem offline on the interface. Why?

A: If the add-in is installed and active, but seems Offline, then the Outlook application is closed. If Outlook is still running, but it is still Offline, it means that there is a communication problem between the add-in and the platform. You can easily detect this problem from the logs created by the add-in on the user's computer or get support from our support team.

Q: How do I know if the add-in is disabled by the user or by Outlook?

A: If you see the “Inactive" notification, then it is disabled by the user. If it says “Disabled", it means that it is disabled by Outlook. You can also verify this from the interface of user’s Outlook Desktop in the **File > Options > Add-Ins** window.

Q: Can I have different teams log into the Keepnet Portal and see only the Outlook detail report page?

A: With the user role feature, you can authorize your users with custom permissions.

Integrating Microsoft Phishing Reporting Button with Keepnet

This integration allows your employees to continue using **Microsoft's Phishing Reporting** button to report suspicious emails to your **SOC team** or **Microsoft Defender**. Along with that, this integration adds new benefits by forwarding reported emails to **Keepnet's Incident Responder**. This ensures deeper analysis and tracking capabilities while maintaining your existing reporting process.

Key Benefits:

- **Dual Reporting:** Emails reported via the Microsoft Phishing Reporting Button are sent to both Microsoft Defender and Keepnet's Incident Responder product for advanced analysis.
- **Simulation Tracking:** During phishing simulation campaigns, Keepnet tracks employees who report simulated phishing emails, helping administrators measure awareness and provide training.

Steps to Set Up the Integration

Step 1: Create a Shared Mailbox for Reports

If you don't already have a shared inbox for phishing reports:

1. Log into the Microsoft Exchange Admin Center.
2. Navigate to **Recipients > Mailboxes > Add a Shared Mailbox**.
3. Enter a **Display Name** and **Email Address** for the shared mailbox.
4. Click the **Create** button to create a shared mailbox.

Step 2: Set Up a Mail Flow Rule

Forward reported phishing emails to Keepnet using a mail flow rule:

1. Please contact the support team of Keepnet to get the **Keepnet email address for forwarding**.
2. Log into the Microsoft 365 Admin Center and open the Exchange Admin Center.
3. Go to **Mail Flow > Rules** and click **Create New Rule**.
4. Configure the rule:
   - **Name:** Enter a name such as "**Forward Reported Emails to Keepnet**".
   - **Set Apply this rule if:** Select the "**The recipient**" and then select the "**is this person**" option. Please enter the shared mailbox email address that you created in the previous section.
   - **Do the following:** Select the "**Add Recipients**" and then select the "**to the To box**" option. Please enter the email address that you got from the Keepnet Support Team.
5. Leave the "**Except if**" option as default and then click **Next**.
6. Leave the "**Set rule settings**" page settings as default and then click **Next**.
7. Click **Finish** to create the rule.

Step 3: Configure the Microsoft Phishing Reporting Add-In

1. Open User Submission Settings in your Microsoft 365 portal.
2. Ensure **“Monitor reported messages in Outlook”** is active.
3. Choose **“Use the built-in Report button in Outlook”**.
4. Set **“Reported message destinations”** to **“Microsoft and my reporting mailbox”** or **“My reporting mailbox only”.**
5. **Add your shared mailbox** that you created at the beginning of the document to the "**Add an exchange online mailbox to send reported messages to:**" field and save.

Step 4: Install the Microsoft Outlook 365 'Report Phishing' Add-In

If not already installed:

1. Visit **Microsoft AppSource** and search for **“Report Phishing”**.

2. Click **Get it now** and follow the installation instructions.
3. Wait up to 12 hours for the add-in to appear in Outlook.

Step 5: Test the Integration

1. Launch a phishing simulation campaign through Keepnet.
2. Report a simulation email using the **Microsoft Phishing Reporting** button. Then, go to your campaign report and click the **Reporters** menu to verify that you reported the simulation email.
3. Verify the email is also visible on Keepnet's **Incident Responder** page.

Possible Considerations

- **Reporting Delays:** When Microsoft forwards reported emails to the specified email destination, there may be a delay caused by Microsoft's internal processing. For example, some emails may appear immediately whilst other emails may take 10 minutes to get reported to Keepnet from Microsoft.
- **Blocked Emails:** Emails flagged as phishing might be quarantined by Microsoft or other security solutions, causing delays in forwarding.
- **Interference:** External security solutions, such as Data Loss Prevention (DLP) systems, may interfere with email forwarding from Microsoft to Keepnet. This can result in delays or prevent emails from being reported altogether.
- **Email Quarantine:** Emails flagged as phishing might be quarantined by Microsoft or other security solutions, causing delays in forwarding.
- **Policy Conflicts:** Custom email policies on the customer's Microsoft tenant could block or redirect reported emails, affecting Keepnet's tracking.
- **Server Downtime:** Temporary unavailability of Microsoft or Keepnet's email servers can result in reporting delays.

Troubleshooting Phishing Reporter on Outlook Desktop

If you've installed the Phishing Reporter on the Microsoft Outlook Desktop version successfully to report any suspucious phishing emails but are unable to see the Phishing Reporter button, here are some steps you can follow to troubleshoot the issue.

Step 1: Check your Outlook Version

First, confirm that you are using a version of Outlook that is compatible with Phishing Reporter. It might be possible that your current Outlook version is outdated and not supported by the add-in. Phishing Reporter usually supports the most recent versions of Outlook, but you can double-check the specific versions from here.

Step 2: Verify Installation

Make sure the Phishing Reporter Add-in was installed correctly. If the installation was interrupted or not completed, it could result in the button not appearing.

- Press the Win+S button combination on your keyboard, and find ‘Installed Apps’.
- Locate 'Phishing Reporter Outlook AddIn' in the list of installed programs.
- If you cannot find it, try reinstalling the software.

Step 3: Enable Add-in

Sometimes, the add-in might not be enabled, or it may have been disabled. Here's how to check:

- In Outlook, go to 'File' > 'Options' > 'Add-ins'.
- In the 'Manage' dropdown, select 'COM Add-ins', then select 'Go'.
- If 'Phishing Reporter' is listed but not checked, tick the checkbox to enable it.

- If 'Phishing Reporter' is not listed, it means the add-in is not installed correctly. Try reinstalling.

Step 4: Check the Ribbon

In some cases, the button may not be visible because it's not added to your Outlook ribbon, or it's located under a different tab.

- Right-click on the ribbon and select 'Customize the Ribbon'.
- Look for 'Phishing Reporter Add-in Name' in the list. If it's there, make sure it's ticked and placed under the Home tab.

Step 5: Check Windows Event Logs

Sometimes, Outlook or the add-in may be experiencing issues that could be found in the Windows Event Logs.

- Type 'Event Viewer' in the Start menu and open it.
- On the left side, navigate to 'Windows Logs' > 'Application'.
- Look for any recent warnings or errors related to Outlook or the Phishing Reporter Add-in around the time you last launched Outlook. Pay particular attention to Event ID 45 and 59, which might be related to this issue.

5.1 - AddIn Disabled

When examining your Windows Event Logs, you may encounter a log entry indicating that the Phishing Reporter add-in has been disabled by Outlook. This typically occurs when the add-in takes too long to load at startup. Once identified, the disabled add-in can be enabled again, as outlined in Step 3 of this guide. If the issue continues after this action, please refer to Step 8 for further troubleshooting assistance.

```
Event ID:59
Source:Outlook
Log:Application
Message:Outlook disabled the following add-in(s):

ProgID: PhishingReporter.Outlook.Addin
GUID: {D0F2562C-3BC1-42E3-B34E-8A735974A173}
Name: PhishingReporterAddIn
Description: AddinModule
Load Behavior: 2
HKLM: 1
Location: C:\Program Files (x86)\Phishing Reporter\Phishing Reporter Outl
Threshold Time (Milliseconds): 1000
Time Taken (Milliseconds): 1875
Disable Reason: This add-in caused Outlook to start slowly.
Policy Exception (Allow List): 0
```

5.2 - AddIn Load Times

Microsoft Outlook Desktop may occasionally deactivate add-ins to prevent the application from crashing. By leveraging the Windows Event Logs, you can acquire valuable insights about the loading times of all add-ins. This knowledge helps identify add-ins exceeding the optimal loading time of 1000 milliseconds.

Outlook loaded the following add-in(s):

```
Name: Microsoft Exchange Add-in
Description: Exchange support for Unified Messaging, e-mail permission ru
ProgID: UmOutlookAddin.FormRegionAddin
GUID: {F959DBBB-3867-41F2-8E5F-3B8BEFAA81B3}
Load Behavior: 3
HKLM: 1
Location: C:\Program Files\Microsoft Office\root\Office16\ADDINS\UmOutloo
Boot Time (Milliseconds): 0

Name: Skype Meeting Add-in for Microsoft Office
Description: Skype Meeting Add-in for Microsoft Office
ProgID: UCAddin.LyncAddin.1
GUID: {A6A2383F-AD50-4D52-8110-3508275E77F7}
Load Behavior: 3
HKLM: 1
Location: C:\Program Files\Microsoft Office\root\Office16\UCAddin.dll
Boot Time (Milliseconds): 15

Name: PhishingReporterAddIn
Description: AddinModule
ProgID: PhishingReporter.Outlook.Addin
GUID: {D0F2562C-3BC1-42E3-B34E-8A735974A173}
Load Behavior: 3
HKLM: 1
Location: C:\Program Files (x86)\Phishing Reporter\Phishing Reporter Outl
Boot Time (Milliseconds): 146
```

Step 6: Run the Maintenance Tool

Use the Maintenance Tool provided by Keepnet Labs to gather relevant diagnostic data.

- Go to the Maintenance Tool page and follow the instructions to run the tool.
- This tool will generate a report file. Send this report file to support@keepnetlabs.com for analysis.

Step 7: Check your error logs

7.1 - Phishing reporter add-in could not report

Error Message: “Phishing reporter add-in could not report. This email account is not a valid sender account. Please check the setting in Outlook and make sure you have a valid sender account or contact your network administrator.”

The error message you're encountering typically surfaces when users try to report an email, but encounter difficulties due to issues concerning their email accounts. This problem may arise if your email account isn't configured properly.

- If you're using Microsoft Outlook Desktop or Microsoft 365, you should verify your email account's setup. Ensure that it's properly configured to send emails. This involves confirming that the email address in use is valid and granted appropriate permissions.
- As a user, ensure that you have the necessary permissions to send emails. If you're a Microsoft 365 user and do not have the permission to send emails, you won't be able to report phishing attempts via the add-in.

7.2 - The remote name could not be resolved

This shows that the computer could not resolve this name to an IP address.

Most of the time, this is usually due to DNS resolution problems. Here, the problem has been that the computer could not resolve the domain name "https://addin-api.keepnetlabs.com/" to an IP address.

This error usually stems from the following situations:

- The DNS server is not working properly. In this case, the DNS server should be checked and, if necessary, restarted, or DNS settings should be reviewed.
- Network connection problems. In this case, the network connection should be checked, and it should be checked whether the computer has general access to the internet.

Error Log:

```
Request url: https://addin-api.keepnetlabs.com/api/heartbeat response con
System.Net.Http.HttpRequestException: An error occurred while sending the
```

7.3 - Unable to connect to the remote server

This log indicates a network connectivity error during an HTTP request.

This error usually stems from the following situations:

- The network connection dropped or there is a temporary problem in the network. In this case, the network connection should be checked and, if necessary, the network may need to be restarted or the network settings may need to be checked.
- The client side is using an incorrect IP address or port number. In this case, the target and parameters of the request should be checked.
- The connection is being blocked due to a firewall or other network security settings. In this case, the security settings should be checked.

Error Log:

```
Request url : https://addin-api.keepnetlabs.com/api/notify/email response
System.Net.Http.HttpRequestException: An error occurred while sending the
```

7.4 - The remote name could not be resolved

This log represents a network error situation.

This error usually stems from the following situations:

- Network connection problems. In this case, the network connection should be checked, and it should be ensured that the computer has general access to the internet.
- The DNS server is not functioning correctly. In this case, the DNS server should be checked, if necessary, restarted, or DNS settings should be reviewed.

Error Log:

```
Request url: https://addin-api.keepnetlabs.com/api/heartbeat response con
System.Net.Http.HttpRequestException: An error occurred while sending the
```

Step 8: Contact Support

If the above steps don't resolve your issue, it's suggested to ask for assistance from the Keepnet support team. There are two primary ways to get in touch with them:

1. **Email:** You can send an email to support@keepnetlabs.com. Make sure to include all relevant details about your problem, such as your Outlook version, OS version, and any other pertinent information about your system.
2. **Support Portal:** Alternatively, you can submit a ticket directly via the Keepnet Labs support portal at https://support.keepnetlabs.com/portal/en/home.

For additional information on how to contact support, please refer to our Help Desk documentation.