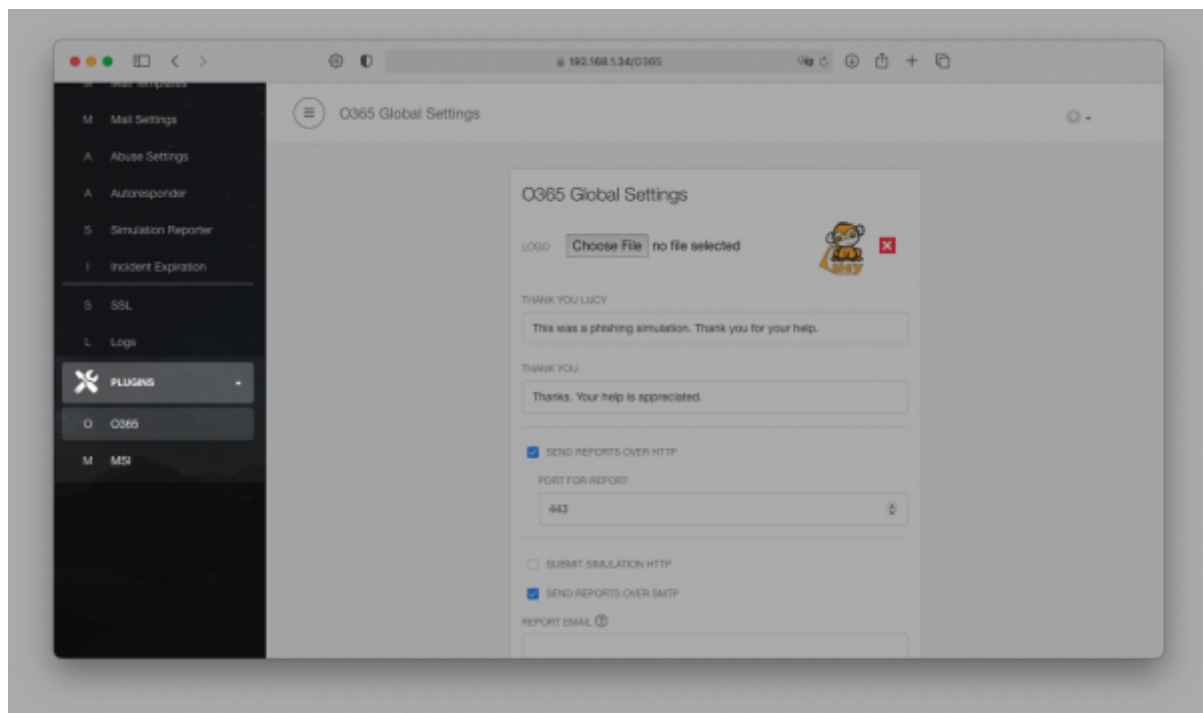


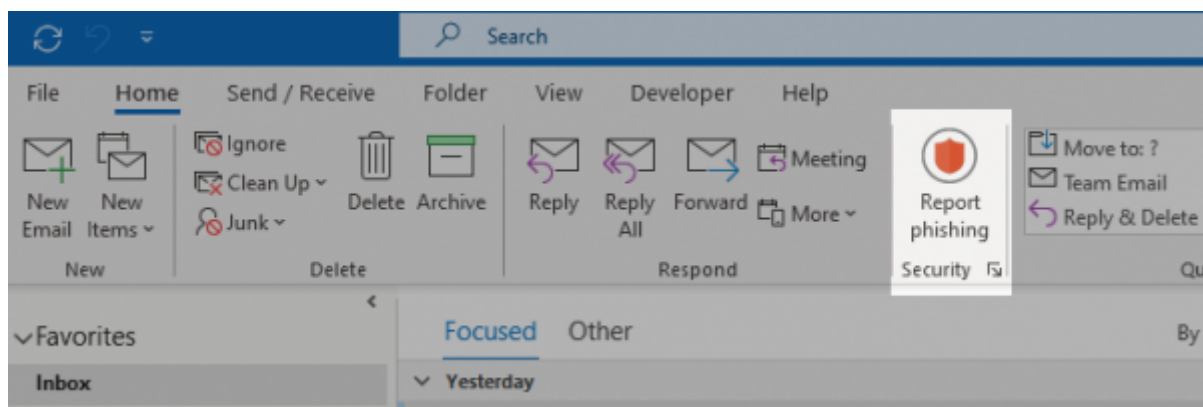
Screener O365 Plugin

Screener comes with the Report Plugin supporting mail clients or browsers.



The O365 plugin is supporting the web-based Outlook Office365.

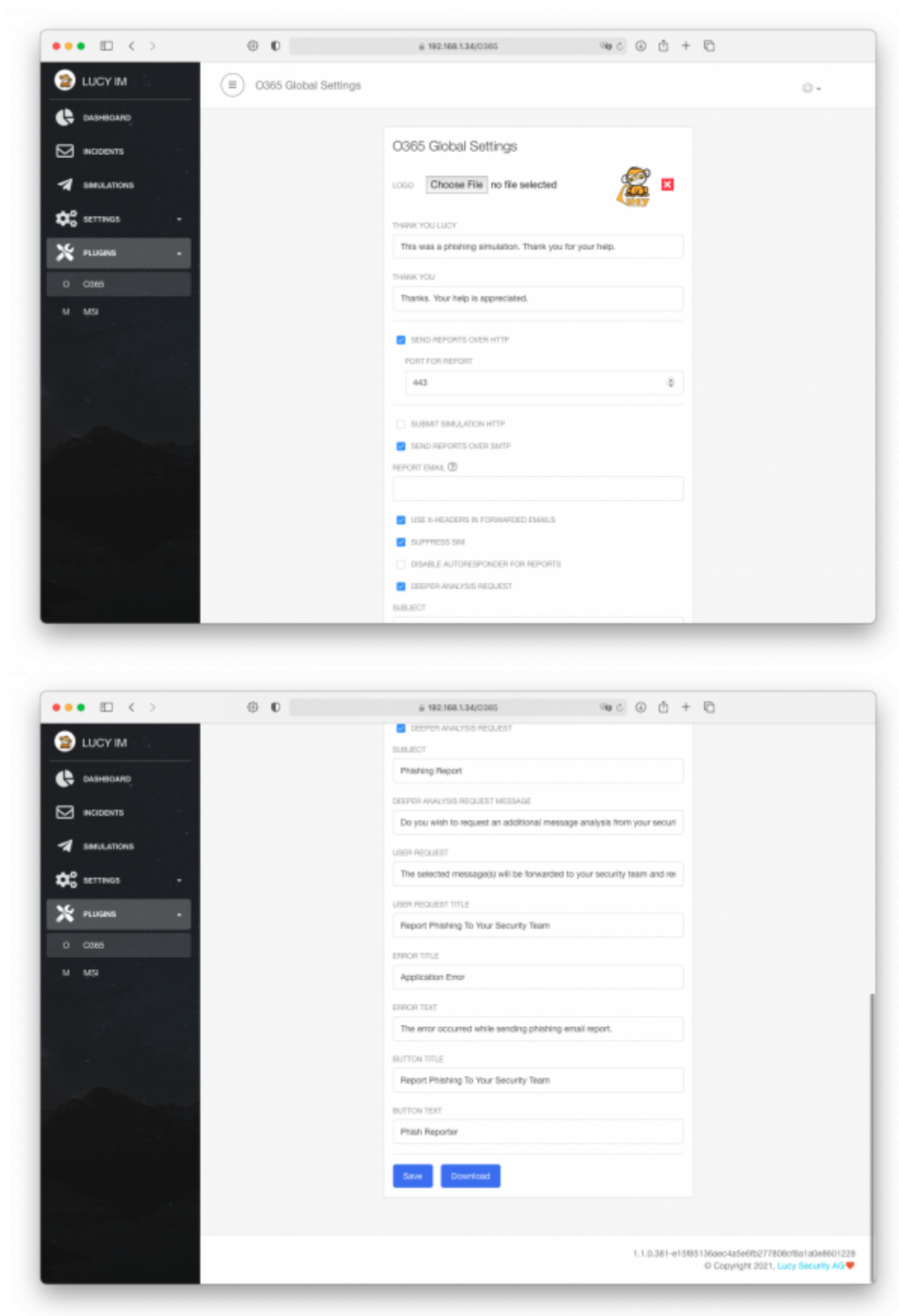
This add-in gives your users a safe way to forward suspected Emails with only one click and have them analyzed automatically by Screener. The tool empowers users to proactively participate in an organization's security program and makes it easy for your employees to report any suspicious email they receive. It has two main features



- Forward the mail (.msg or .eml) to a predefined mail address (e.g. your security team). Within the plugin, you have the ability to define a custom message that appears to the user after the mail gets reported. Once the message gets forwarded to your team, it will automatically be deleted from the user's inbox to prevent future exposure.
- Report back to Screener: the plugin may forward suspected phishing emails as well Screener generated emails back to the Screener server via HTTPS or SMTP. If the mail was generated by LUCY, the reports will be automatically identified as phishing simulation. All other emails can be analyzed in Screener automatically at first, then by a Screener [user](https://wiki.lucysecurity.com/).

Configuration

The configuration of the O365 plugin and phishing events is done within Plugin → O365 Menu.



Settings

Setting Name	Description
Logo (ico)	Choose an icon for visual representation of plugin's button in the Outlook MSI interface. Once it has been picked up there is a preview and an option to delete icon.
Thank you Lucy	The message that will be displayed for all emails, that are created by Lucy within a simulated phishing campaign.
Thank you	The message that will be displayed after the user marks a suspected phishing email and pushed the plugin button.
Send Reports Over HTTP	Enable this option if you want the Outlook Plugin to send a copy of the reported phishing mail to Screener (does not include emails from phishing simulations). You may specify the Port for Report (default value is 443).
Submit simulation HTTP	If the option is enabled, the plugin will send reports regarding phishing simulations to Screener via HTTP.
Send Reports over SMTP	Enable this option if you want to forward the mail to the predefined mail address via SMTP. If enabled, the plugin will send the report to the email you provided on the same page. That is supposed to be your own email or the email of your security team. Please do not use this method at the same time with HTTP to send reports to Screener, if you do not want to have duplicated reports. Only pick one delivery method.
Use X-Headers in forwarded emails	If true, the plugin will make the following changes in the email forwarded over SMTP: * Add a new header X-CI-Report: True * Add an HTML code <p>X-CI-Report: True</p> after the body tag within the email body.
Supress Sim	No reports will be sent over HTTP if a user reports a simulation email generated by Screener. So the plugin will send only "real phishing" emails over HTTP.
Disable Autoresponder For Reports	If true, Screener will not send an automatic email to a user as a reaction to report.
Deeper Analysis Request	If true, the plugin will ask the user whether to request a deeper analysis of the reported phishing mail.
Subject	The subject of the forwarded email message when sending a report over SMTP. You may use %subject% variable to insert the subject of the phishing email. Example: Phish Alert %subject%.
Deeper Analysis Request Message	Deeper analysis request confirmation text. This message box is shown after user clicks on the report button.
User Request	The message that will be displayed after the user marks a suspected phishing email and clicks the plugin button.
User Request Title	Title of the message that will be displayed after the user marks a suspected phishing email and clicks the plugin button.
Error Title	Title of the message that will be displayed when an issue with sending the report occurs.
Error Text	The message that will be displayed when an issue with sending the report occurs.
Button Title	Title of the name of the area in which the button is located.
Button Text	The name of the area in which the button is located.

Download Office365 Plugin & Deployment

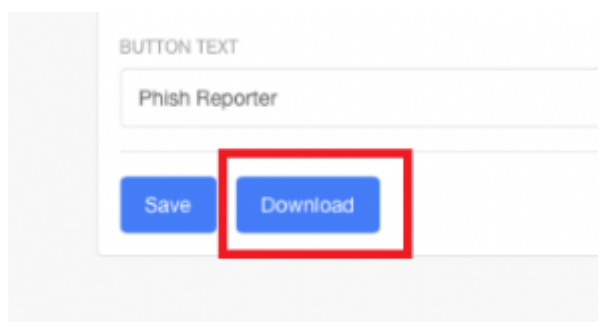
The Outlook 365 button works the same as the Outlook client – just for the web-based Outlook access 365. For its work, it is necessary to have a network connection between Screener and O365 server in case if you use a web browser as a client, and a network connection between Screener and user's workstation in case if a desktop client is used. The XML is the file that needs to be installed for O365:

Outlook 365 sequence:

- **Individual installation**

Step 1

Go Plugins/O365, scroll down the settings and press "Download", your browser will download an XML file

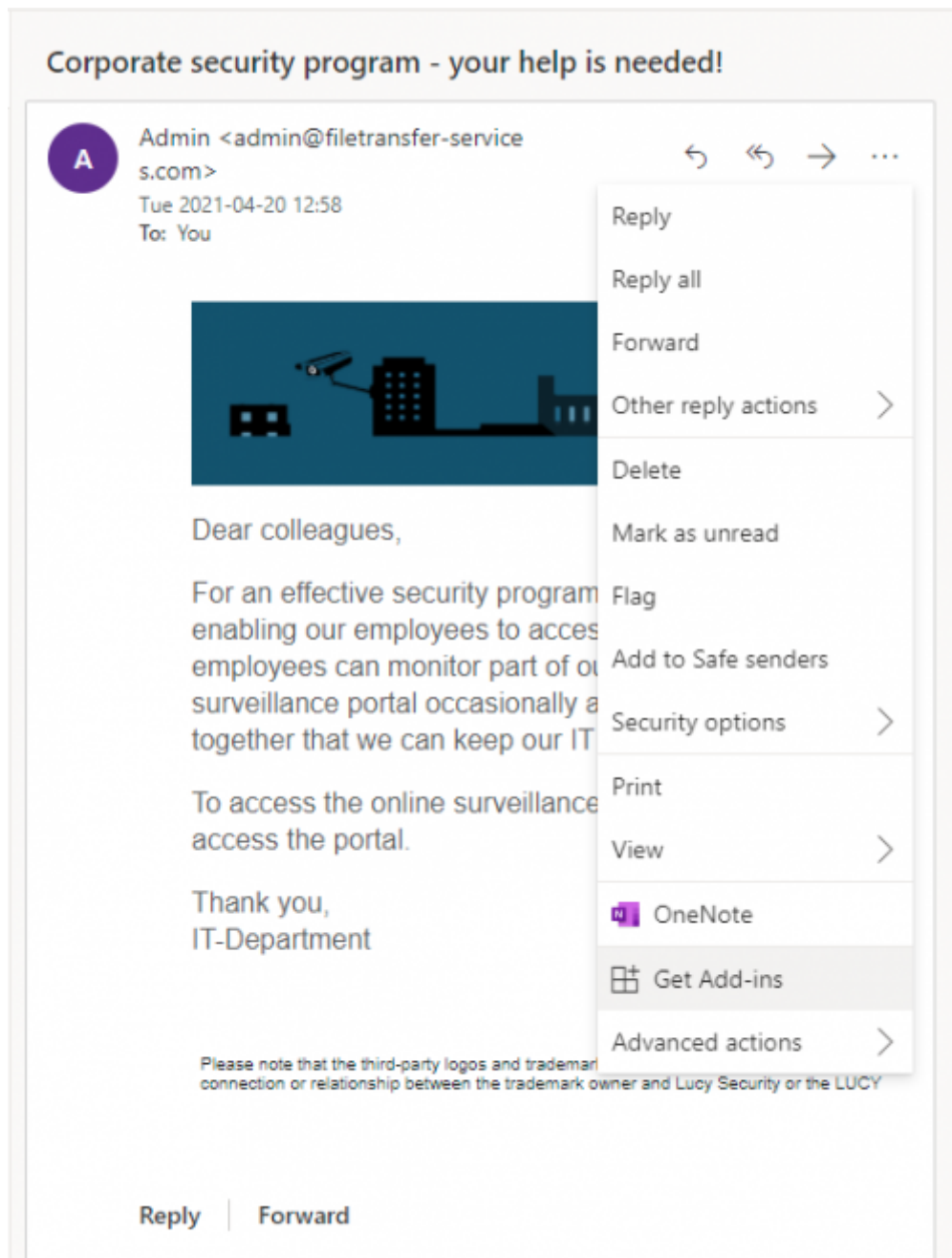


Step 2

Go to MS Outlook - <https://outlook.live.com/owa/>

Step 3

Open any email and press "Get Add-ins" as it described on the screenshot below



Step 4

Go to "My add-ins" and upload the Plugin's XML file

Add-Ins for Outlook

Add-ins may access personal information. By turning an add-in on, you agree to its License Terms and Privacy Policy.



All

My add-ins

My add-ins


Store add-ins



Add-ins that you added from the Office store.


No add-ins found.



Added by Microsoft

Microsoft has provided these add-ins so you can try them out.

**My Templates**

 Added 

**Bing Maps**
Map addresses found in your email.
This add-in will send addresses to Bing but will not share your data with any...

 Added 

Custom add-ins

You can install add-ins from a file or from a URL. [+ Add a custom add-in](#) ▾

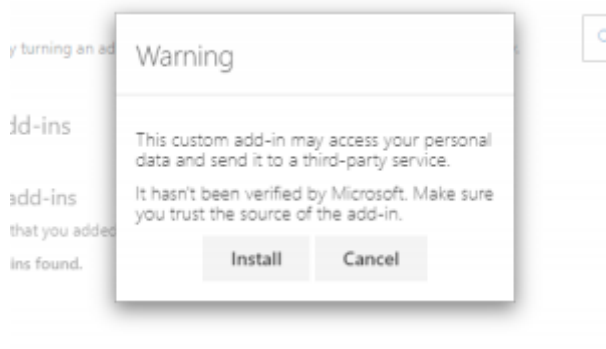
No add-ins found.

Add from URL...

Add from file...

Step 5

The Warning message would appear, press Install

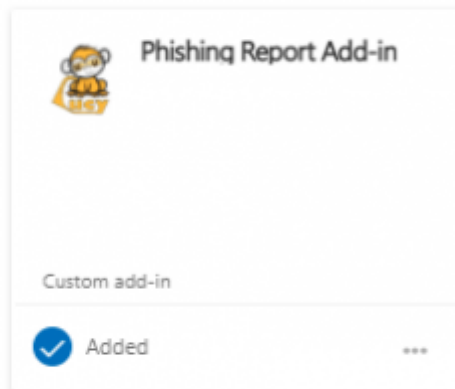


Step 6

Once installed, the Plugin will appear in the custom add-ins section

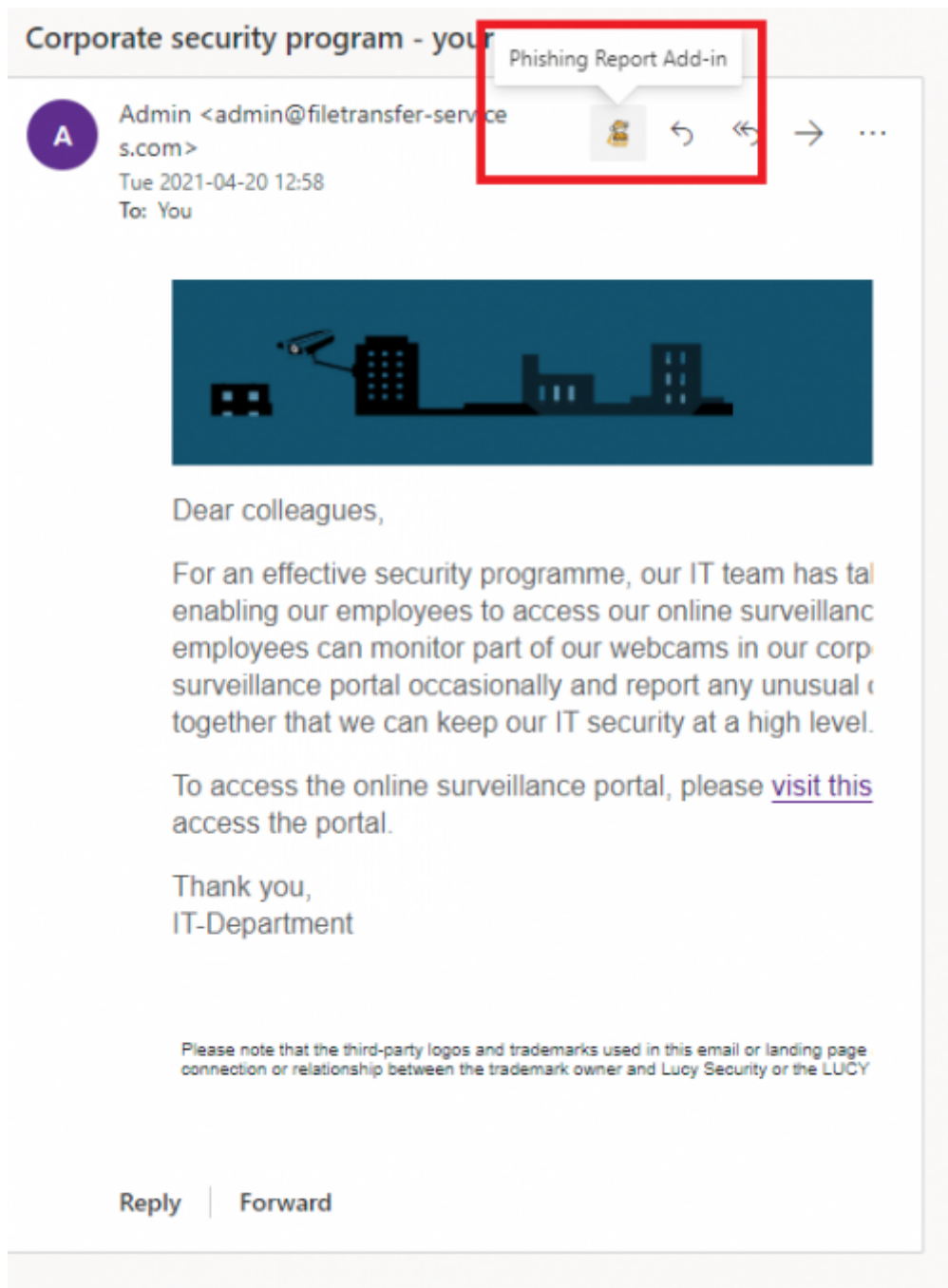
Custom add-ins

You can install add-ins from a file or from a URL. [+ Add a custom add-in](#) 

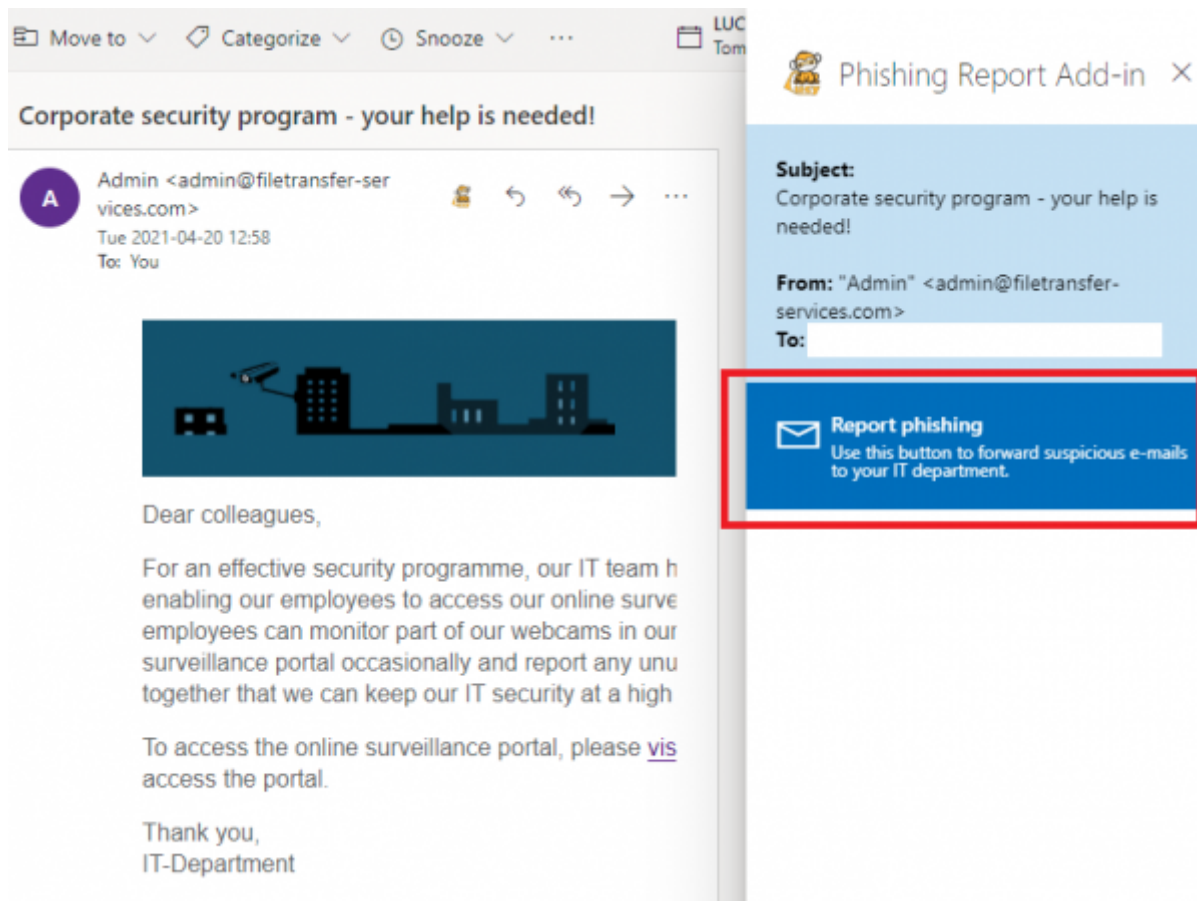


Step 7

Now in email panel, you will see the Plugin's icon, which is the Report Plugin

**Step 8**

To perform a report press the Button and hit "Send Report" on the right



- **Centralized O365 plugin installation for multiple users**

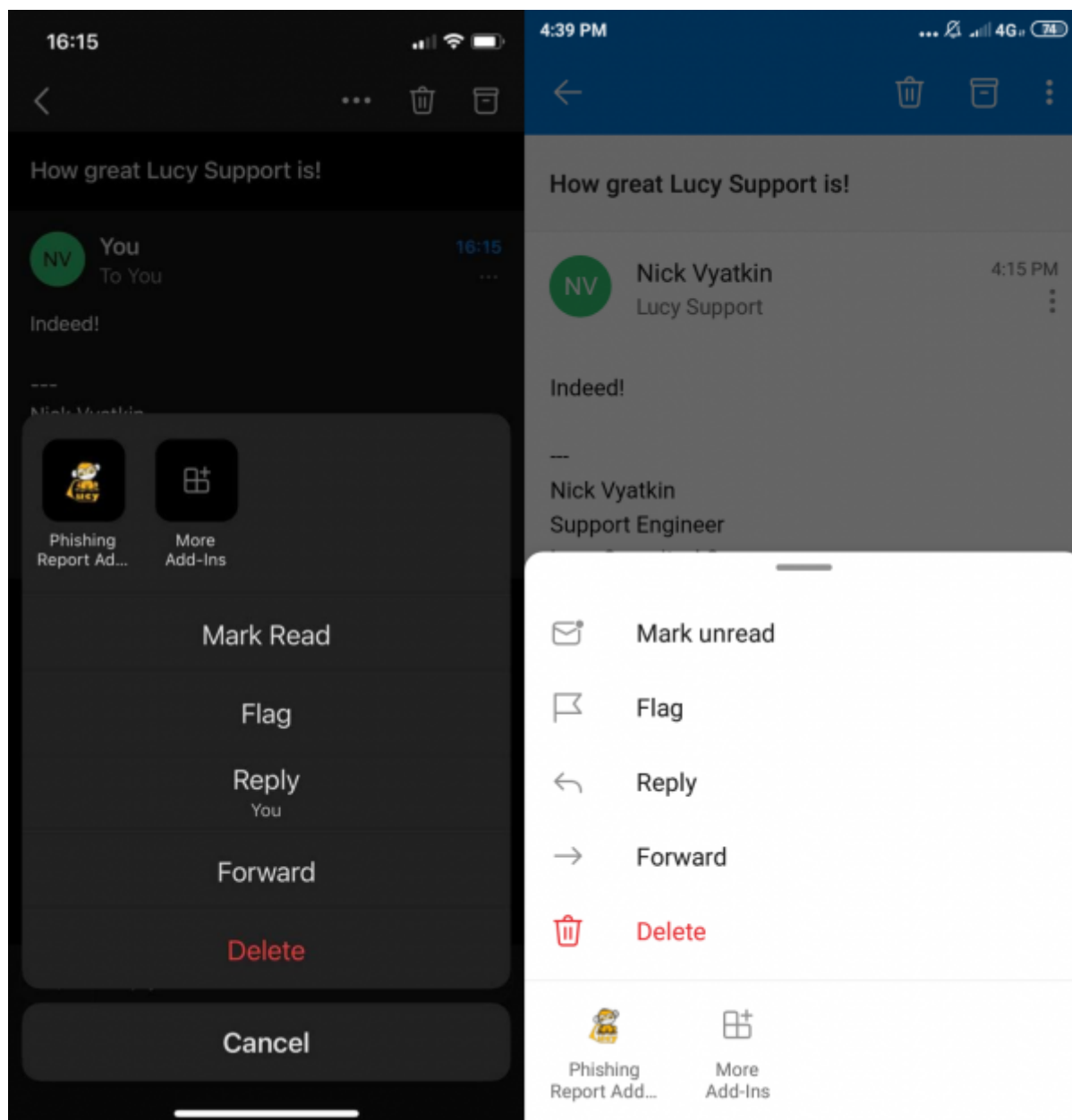
You can install the O365 plugin for multiple users in the Microsoft 365 admin center. Detailed instruction on how to do it is available on the Microsoft website:

<https://docs.microsoft.com/en-us/office365/admin/manage/manage-deployment-of-add-ins?view=o365-worldwide>

O365 Mobile plugin

The phishing plugin can be utilized in the O365 Mobile version both on Android and iOS platforms. In order to make the plugin available for mobile applications simply install the XML plugin as described in the according to the section above. After the plugin is deployed for the web version it will automatically appear in the Outlook mobile application. Feel free to contact the support team if any issues occur.

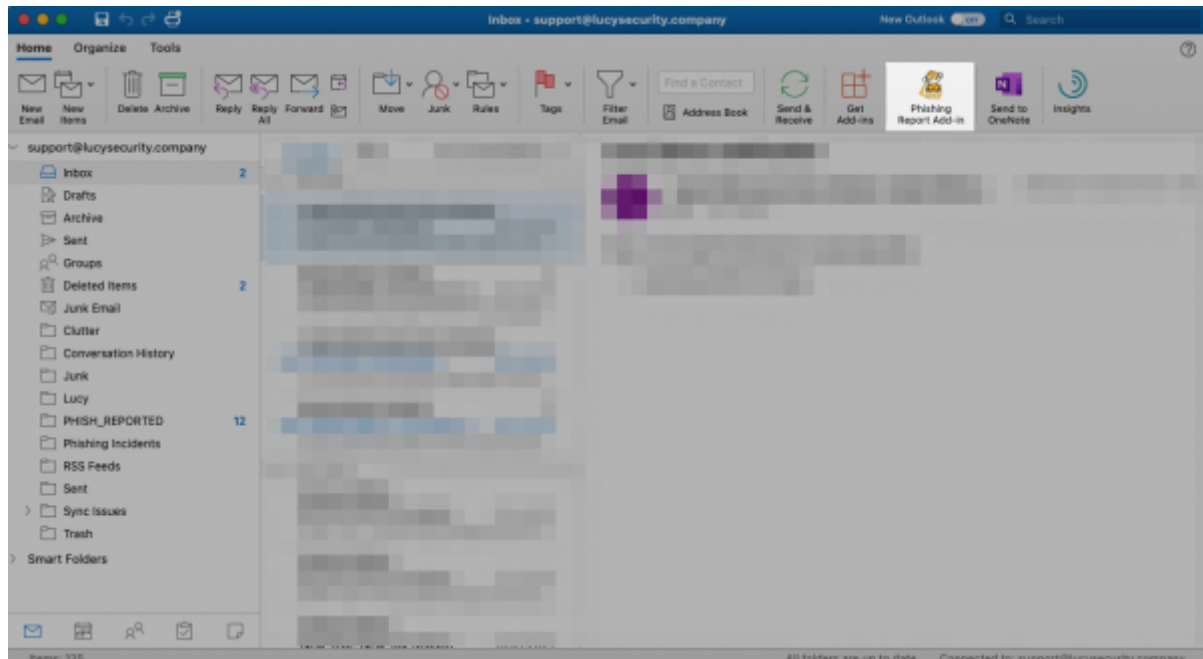
It is also possible to deploy O365 XML into Exchange with compatibility mode, the report button will be available for Android & iOS as well.



Deployment on Apple Computer

Microsoft has "Office for Mac" product, which requires the O365 account to run. When you open Outlook application on Mac, it fetches all plugins from the corresponding O365 account and shows them in the interface, so the plugin is available both in the web interface and on Mac. Therefore, you first need to install the plugin in O365 before you set it up on a MAC.

The installation procedure is the same as for O365 and described above.



From:

<https://wiki.lucysecurity.com/> - LUCY

Permanent link:

https://wiki.lucysecurity.com/doku.php?id=screener_o365_plugin

Last update: **2021/09/03 15:16**

