SEGURO GUIDES

Simple (and free) CEO Impersonation Prevention in M365

SEGURO
Cyber Security Consulting

info@seguro.ltd • seguro.ltd • +44 (0) 191 637 5030

Simple CEO Impersonation Prevention in M365

SEGURO

Introduction

A common email phishing scam that still catches many organisations out is one that doesn't contain any links or attempt to steal credentials but rather relies on simple email communication – purporting to me from an executive or CEO - tricking employees in to making a purchase, often of vouchers or credit.

Strictly speaking, adding a generic "external email banner" to emails should make it obvious that these emails aren't legitimate but users can become blind to them so it can be worth adding an additional alert with a more striking warning for emails appearing to be from senior management.

1 How does it work?

Simply put, we setup a rule in Microsoft 365 (the platform formerly known as Office 365) that examines all inbound email where the sender's name includes the name of an exec or senior manager *but* it is not an internal email. In other words, someone has sent an email made to look like it's from someone senior.

The flaw in the plan? If your exec has a common name, you're going to get a lot of false positives (though you can easily add domains to an exception list).

While not sophisticated, I've seen this simple measure be effective in preventing fraud.

There is functionality in Microsoft 365 for impersonation prevention but it requires additional licenses so we like this free option!

2 How to setup the alert

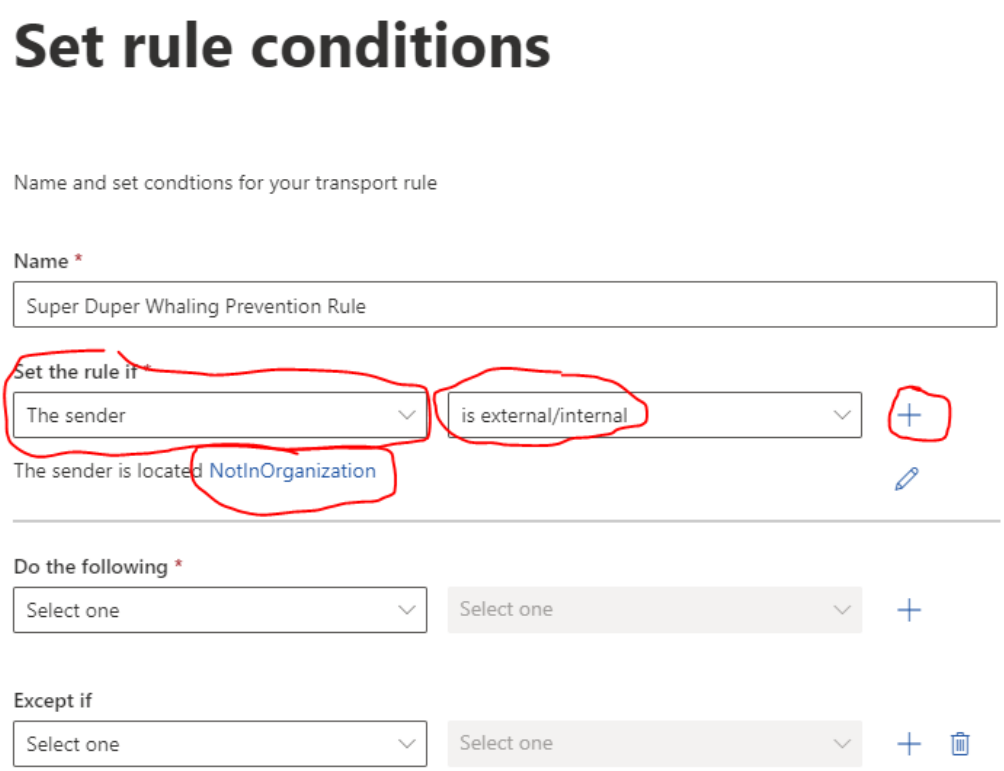
- Login to Microsoft 365 with an account with administrative privileges.
- Click **Admin** on the left-hand menu to enter the Microsoft 365 Admin Centre
- Click **Show all** to expand the side menu to show all options
- Under **Admin centers**, click **Exchange**
- In the **Exchange admin center** expand the **Mail flow** option
- Click **Rules**

NOTE: this tutorial is based on the **new** (Sept 2022) version of the rules manager, if you are not seeing it by default, you should be able to switch to it by clicking **Try it now** on this message:

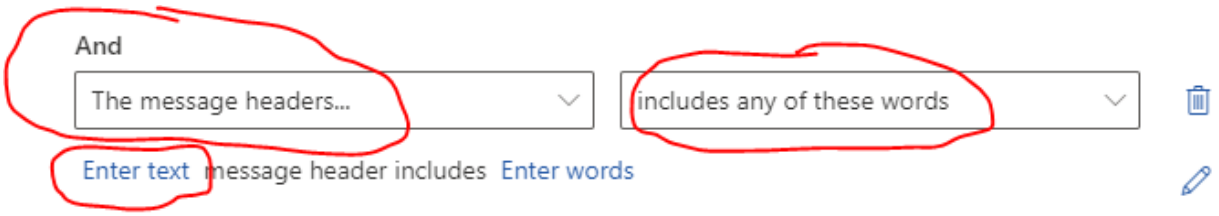
The Rules page will be updated to the new modernized version soon. This update will be rolling out and completed in September. Try it now

- Click **+ Add a rule** then **Create a new rule**

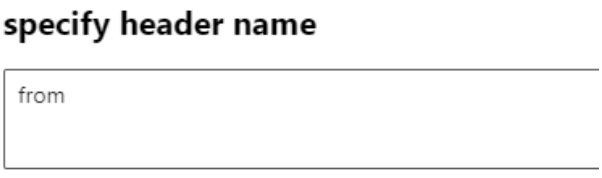
- In the form, give your rule a name (e.g. “Super Duper Whaling Prevention Rule”.
- In first dropdown under **Set the rule if…** select the option **The sender** and then select **is external/internal** from the second dropdown menu, finally select **Outside the organisation** from the **select sender location** options:
- Next click the plus symbol to add another condition:



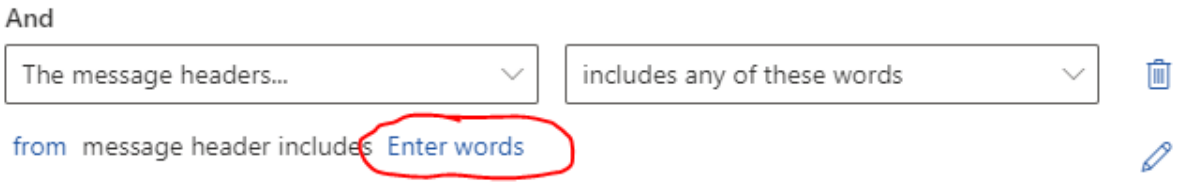
- On the new condition (under the **And** heading), from the first dropdown select **The message headers…** and from the second dropdown, select **includes any of these words**
- Next click **Enter text**:



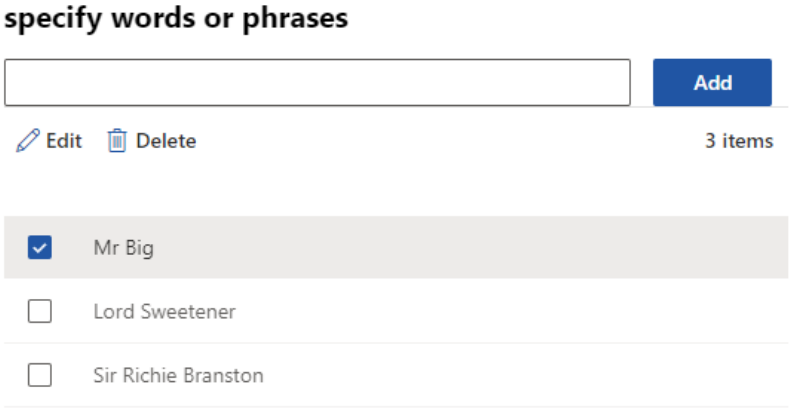
- In the **specify header name** form that appears, enter the word **from** and click **Save:**



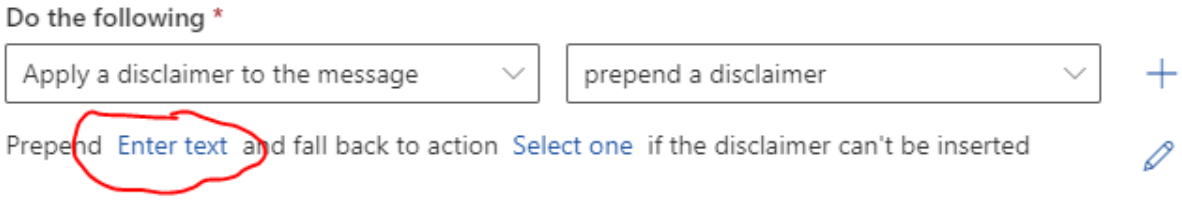
- Next click Enter words:



- In the **specify words or phrases** form, enter the names of the employees (typically senior ones) you want to prevent impersonation of:



- Now click **Save**
- From the **Do the following**... drop down select **Apply a disclaimer to the message** and select the **prepend a disclaimer** option.
- Click the **Enter text** hyperlink:



- Enter some text or HTML for a banner, for example:

```
<p style="font-family:'Arial Black', sans-serif; font-
size:18px;color:#FFFFFF;background-color:#CC0000;
padding:10px">WARNING: It looks like this message might be a CEO
fraud scam - check the sender email address and be wary of any
urgent call to actions.</p>
```

- Click the ***Select one...** text and in the **specify fallback action,** select **Wrap** from the options.
- Click **Next**
- Leave the rest of the options (unless you need to tweak them) and click **Next** again
- Click **Finish**

3 Result

You can see a (fairly dramatic) example of what the recipient of an intended personation attack could receive below. However you device to format that HTML, it needs to be markedly different from your standard "External email" banner if you have one: