Attack Simulation Training Report

Matthew Hazelwood

Contents

Objective

Investigate Microsoft Defenders Phishing Simulation and look into ways we can implement it: Attack simulation training - Microsoft Defender

Learning Recourses

Simulate a phishing attack with Attack simulation training

Simulate a phishing attack with Attack simulation training - Microsoft Defender for Office 365 | Microsoft Learn

YouTube Tutorial Guide

Attack Simulation Training with Microsoft:

Attack Simulation Training with Microsoft

Quick Access

In the Microsoft Defender portal at https://security.microsoft.com, go to:

Email & collaboration > Attack simulation training > Simulations

Or, use https://security.microsoft.com/attacksimulator?viewid=simulations

Guide for Microsoft Defender Attack Simulation Training

Select Technique

Select the social engineering technique you want to use with this simulation. We've curated these from the MITRE Attack framework. Depending on your selection, you will be able to use certain types of payloads.

Select Technique	Credential Harvest

Name Simulation

Name and describe the simulation

Simulation Name	Insert Name
Description	Insert Description *(this is optional)*

Select payload and login page

Select payload for this simulation technique. You can create or collect your own payloads to add this list. Note that if you create a new payload, you will be redirected to a payload creation wizard. You can also map a login page for Credential Harvest or Link in Attachment technique to a payload from the preview tab.

Type	Global payloads
Select the payload	Select the type/types of simulated phishing emails you were wanting to deploy
View and edit payload	• Clicking anywhere in the desired payload will allow you to preview it. From here you can see what the attack will look like, get a description of it, view its predicted compromise rate, etc. • Furthermore you can see previous attempts/simulations by selecting; Simulations launched

Additional Notes	• *You can select multiple different phishing emails you were hoping to deploy* • *You can send test email to the current logged in user for formatting and validation. This test email will not include any training, notifications or end simulation scenarios.*

Target users

Add existing users and groups or import a list of email addresses.

Include all users in my organization	Selecting this option will send the simulated attack to all users in the organisation.
Include only specific users and groups	• Selecting this option you will be able to add filters for specific users and groups. • This can be done either by using the search bar and typing in the user or groups name • By clicking Add Filters this will provide a wide variety of options to filter the users/groups

Exclude Users

Choose users or groups to be excluded from this campaign.

Exclude Users	This sub category will allow you to exclude selected users form receiving the simulated attack
Add users to exclude	• Selecting this option you will be able to add filter for specific users and groups. • This can be done either by using the search bar and typing in the user or groups name • Of clicking Add Filters will provide a wide variety of options to filter the users/groups
Additional Notes	• *This uses the same layout as Target Users section* • *You can leave this option blank if desired*

Assign Training

Select training preferences, assignment, and customize a landing page for this simulation.

Select training content preference	From here you can choose to assign: • Microsoft training modules • Assign no training • Redirect to a custom URL for training
Assign training for me	Let's Microsoft assign training courses and modules based on a user's previous simulation and training results using learning pathways.
Select training courses and models myself	Will add an additional sub category where you can assign training desired modules.
Due Date	Set a due date for the training to be completed by

Phish Landing Page

Select landing page that provides a learning moment to the user after getting phished.

Use landing pages from library	• Will allow you to select from an number of templates of landing pages users will be directed to if they click on the simulated phishing attack. • These templates can be previewed by clicking anywhere in their description. Furthermore in this preview menu you can change the language and view the results from previous simulations. • You can customise these template with your own logo on the home page.
Use a custom URL	Allows you to enter a custom landing page URL to direct users to the training material if they click on the simulated phishing attack.

Select end user notification

Select end user notification preferences for this campaign.

Do not deliver notifications	• Will not deliver notifications to the end user • This includes Positive Reinforcement, Training Assignments and Training Reminder, will not be delivered to the users • You will receive a popup to check if you are sure with this option and want to proceed

Microsoft default notification	• Allows you to customise the notifications sent to users regarding training and positive reinforcement
	• You will need to select Delivery Preferences for
	  ○ "Microsoft default positive reinforcement notification"
	  • Options include to deliver the notifications for positive reinforcement after the simulation is complete, during the simulation or not deliver notifications at all
	  ○ "Microsoft default training reminder notification"
	  • Options include deliver reminders weekly or twice weekly

Customised end user notifications	Will add an additional subcategories where you can edit desired end user notifications

Launch Details

Configure when you want this simulation to launch, and if you'd like to remove the payloads from user inboxes.

Launch the simulation as soon as I'm done	Will launch the simulation immediately
Schedule this simulation to be launched later	Can set a specific date, time, hour and minute you would like the simulated attack to be launched

Configure number of days to the end simulation after	• Can configure the number of days the simulation will remain active • This need to be at least 2 days and at most 30 days

Review Simulation

Review your Simulation information below before you launch it. You currently have it scheduled to be launched on ##/##/#### at ##:##:##. It will end on ##/##/#### at ##:##:##.

Additional Notes	• *You can send test email to the current logged in user to ensure the email will look as intended* • *You can go back and review/edit setting* ○ *Please note by selecting edit you will be directed back to that section and will need to progress through the rest of the sections again*
To finalise	Click Submit

Test Attack simulation training V.1

Select Technique

Select Technique	Credential Harvest

Name Simulation

Simulation Name	Test Attack simulation training V.1
Description	Test Credential Harvest Attack simulation training V.1

Select payload and login page

Type	Global payloads
Select the payload	Keep Office 365 Password

Target users

Include only specific users and groups	Selected only: matthew.hazelwood@eso.sa.gov.au

Exclude Users

Exclude Users	No users excluded

Assign Training

Select training content preference	Microsoft training experience (Recommended)
Assign training for me	Selected

Due Date	30 Days after Simulation ends

Phish Landing Page

Use landing pages from library	• No edit to the layout • Using Template 1

Select end user notification

Microsoft default notification	• "Microsoft default positive reinforcement notification"
	  ○ Deliver after simulation
	• "Microsoft default training reminder notification"
	  ○ Weekly

Launch Details

Launch the simulation as soon as I'm done	Will launch the simulation as soon as I'm done
Configure number of days to the end simulation after	2

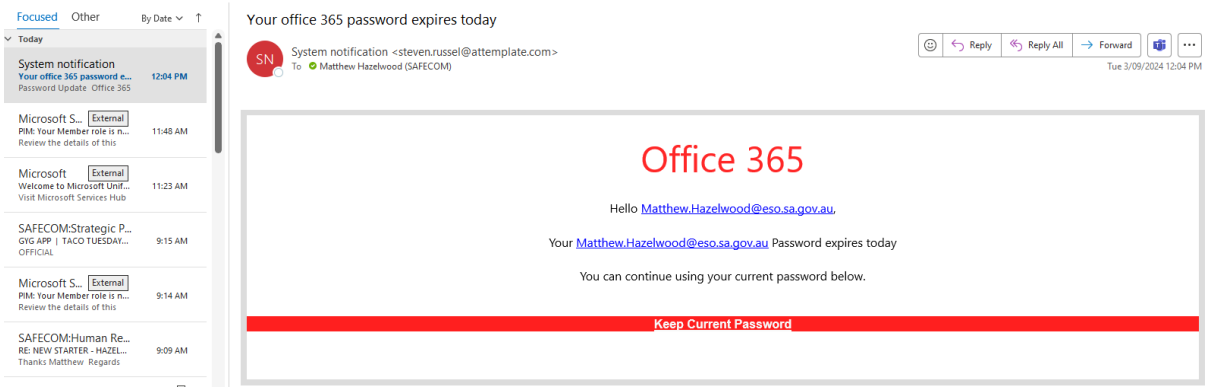
Review Simulation

To finalise	Submit

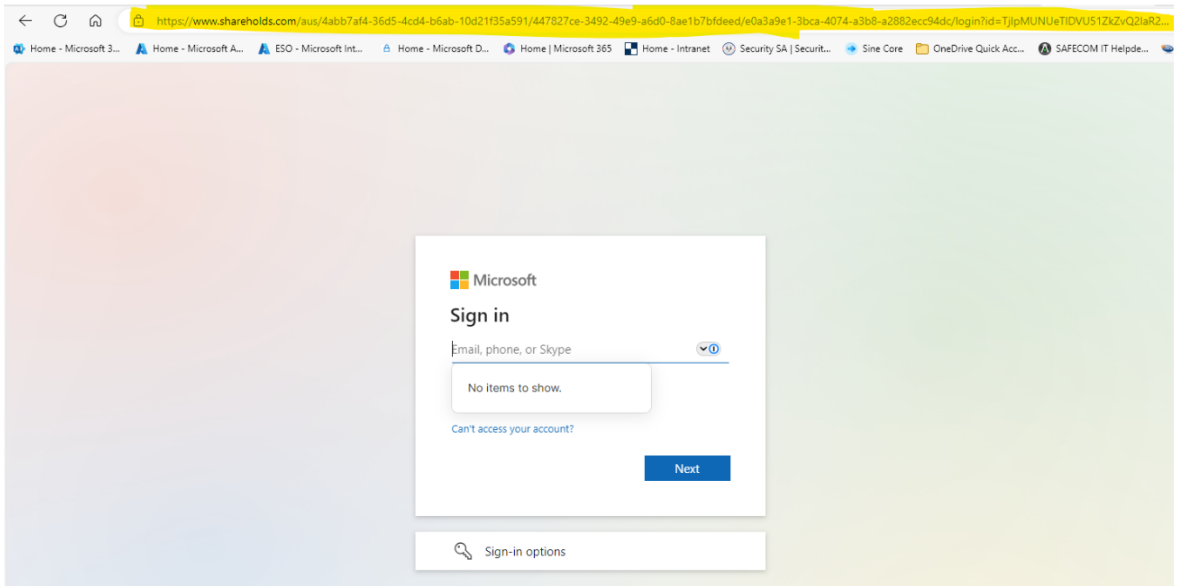
Results of Test Attack simulation training V.1

Simulated phishing attack was lunched at 12:03:20 PM on 03/09/2024 with the end date being 12:03:20 PM on 05/09/2024.

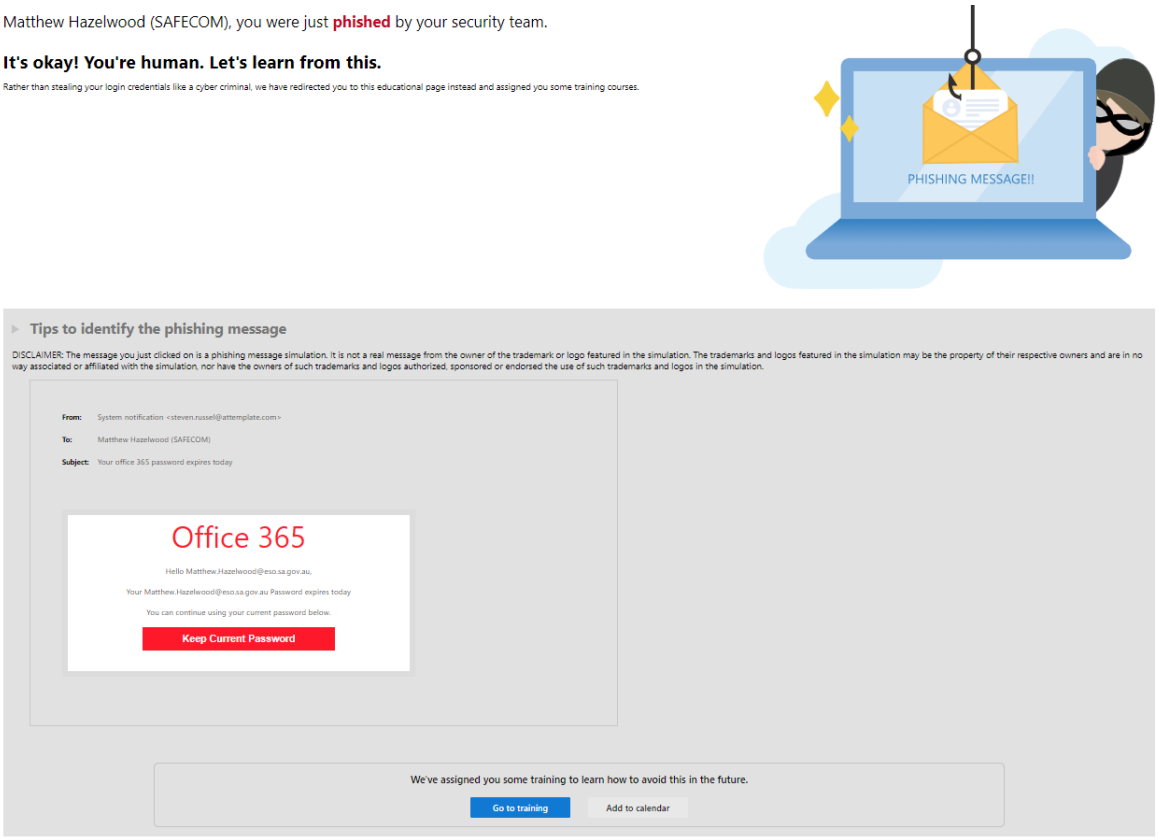
The test simulated phishing attack was only sent to the assigned recipient: matthew.hazelwood@eso.sa.gov.au which arrived in their inbox at 12:04 PM



To test the simulation, the hyperlink Keep Current Password was clicked which redirected to a Microsoft Login Page. The login page looked legitimate however the URL was suspicious and 1Password did not recognise the website:

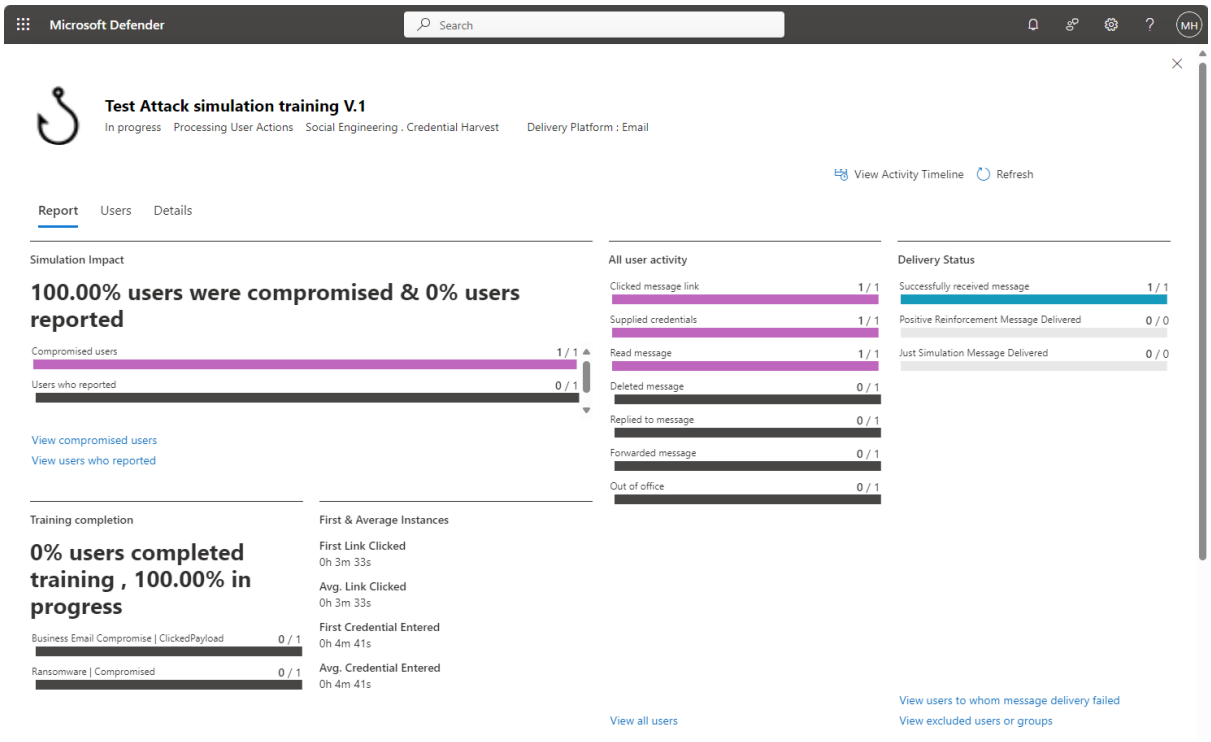


Logon details were entered manually which then redirected the user to a webpage informing them that they have just been victim of a phishing attack by the security team. The Page reassured them that this was not an actual malicious attack but a training exercise. It went on to give tips on identifying malicious emails and had a link to the training material:



Clicking the Go to training link redirect to an only module hosted in Microsoft Defender.

Returning Microsoft Defender as an Admin, under the simulation tab you could see an entry for the "Test Attack simulation training V.1". Clicking anywhere in the entry will allow you to see the results of the phishing attack:


Microsoft Defender
Search
MH
Test Attack simulation training V.1
In progress Processing User Actions Social Engineering . Credential Harvest Delivery Platform : Email
View Activity Timeline
Refresh
Report
Users
Details
Simulation Impact
100.00% users were compromised & 0% users reported
Compromised users 1 / 1
Users who reported 0 / 1
View compromised users
View users who reported
All user activity
Clicked message link 1 / 1
Supplied credentials 1 / 1
Read message 1 / 1
Deleted message 0 / 1
Replied to message 0 / 1
Forwarded message 0 / 1
Out of office 0 / 1
Delivery Status
Successfully received message 1 / 1
Positive Reinforcement Message Delivered 0 / 0
Just Simulation Message Delivered 0 / 0
Training completion
0% users completed training , 100.00% in progress
Business Email Compromise | ClickedPayload 0 / 1
Ransomware | Compromised 0 / 1
First & Average Instances
First Link Clicked
0h 3m 33s
Avg. Link Clicked
0h 3m 33s
First Credential Entered
0h 4m 41s
Avg. Credential Entered
0h 4m 41s
View all users
View users to whom message delivery failed
View excluded users or groups

Test Attack simulation training V.2

This second test attack simulation training was created nearly identically to the first attempt. The purpose of this second attempt was to:

- Test different layouts
- Ensure the Attack simulation is able to work repeatedly
- View the changes if the malicious email was deleted instead of being clicked on

Select Technique

Select Technique	Malware Attachment

Name Simulation

Simulation Name	Test Attack simulation training V.2
Description	Test Attack simulation training V.2 was created nearly identically to Test Attack simulation training V.1. The purpose of this second attempt was to: • Test different layouts • Ensure the Attack simulation is able to work repeatedly • View the changes if the malicious email was deleted instead of being clicked on

Select payload and login page

Type	Global payloads
Select the payload	DocuSign Shared Document

Target users

Include only specific users and groups	Selected only: matthew.hazelwood@eso.sa.gov.au

Exclude Users

Exclude Users	No users excluded

Assign Training

Select training content preference	Microsoft training experience (Recommended)
Assign training for me	Selected
Due Date	7 Days after Simulation ends

Phish Landing Page

Use landing pages from library	• Since simulated malware is being deployed via attachment using a custom URL is not an option • Using Template 5 • SAFECOM LOGO.PNG was uploaded

Select end user notification

Microsoft default notification	• "Microsoft default positive reinforcement notification"
	  ○ Deliver after simulation
	• "Microsoft default training reminder notification"
	  ○ Weekly

Launch Details

Launch the simulation as soon as I'm done	Will launch the simulation as soon as I'm done
Configure number of days to the end simulation after	2

Review Simulation

To finalise	Submit

Review your Simulation information below before you launch it. You currently have it scheduled to be launched on 03/09/2024 at 2:05:35 pm. It will end on 05/09/2024 at 2:05:35 pm.

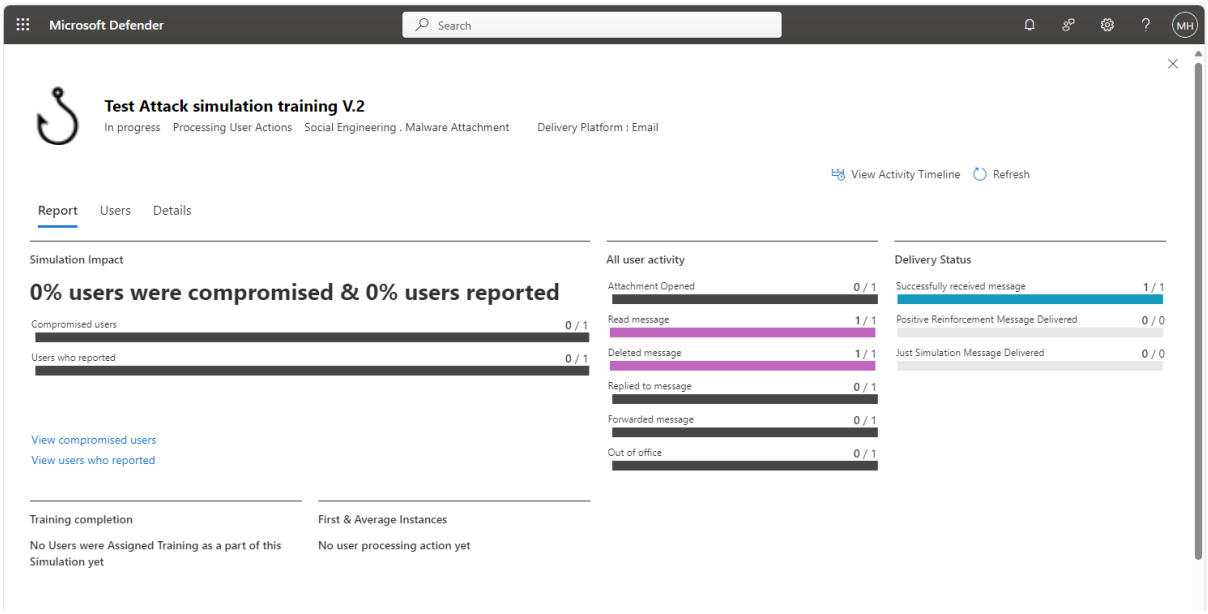
Results of Test Attack simulation training V.2

Simulated phishing attack was lunched at 03/09/2024 at 2:05:35 pm. It will end on 05/09/2024 at 2:05:35 pm.

The test simulated phishing attack was only sent to the assigned recipient: matthew.hazelwood@eso.sa.gov.au which arrived in their inbox at 2:07 PM

Email was immediately deleted, and no training information was forwarded and no other emails or notifications were sent.

Returning Microsoft Defender as an Admin, under the simulation tab you could see an entry for the "Test Attack simulation training V.2". Clicking anywhere in the entry will allow you to see the results of the phishing attack:


Microsoft Defender
Search
MH
Test Attack simulation training V.2
In progress
Processing User Actions
Social Engineering . Malware Attachment
Delivery Platform : Email
View Activity Timeline
Refresh
Report
Users
Details
Simulation Impact
0% users were compromised & 0% users reported
Compromised users
0 / 1
Users who reported
0 / 1
View compromised users
View users who reported
All user activity
Attachment Opened
0 / 1
Read message
1 / 1
Deleted message
1 / 1
Replied to message
0 / 1
Forwarded message
0 / 1
Out of office
0 / 1
Delivery Status
Successfully received message
1 / 1
Positive Reinforcement Message Delivered
0 / 0
Just Simulation Message Delivered
0 / 0
Training completion
No Users were Assigned Training as a part of this Simulation yet
First & Average Instances
No user processing action yet