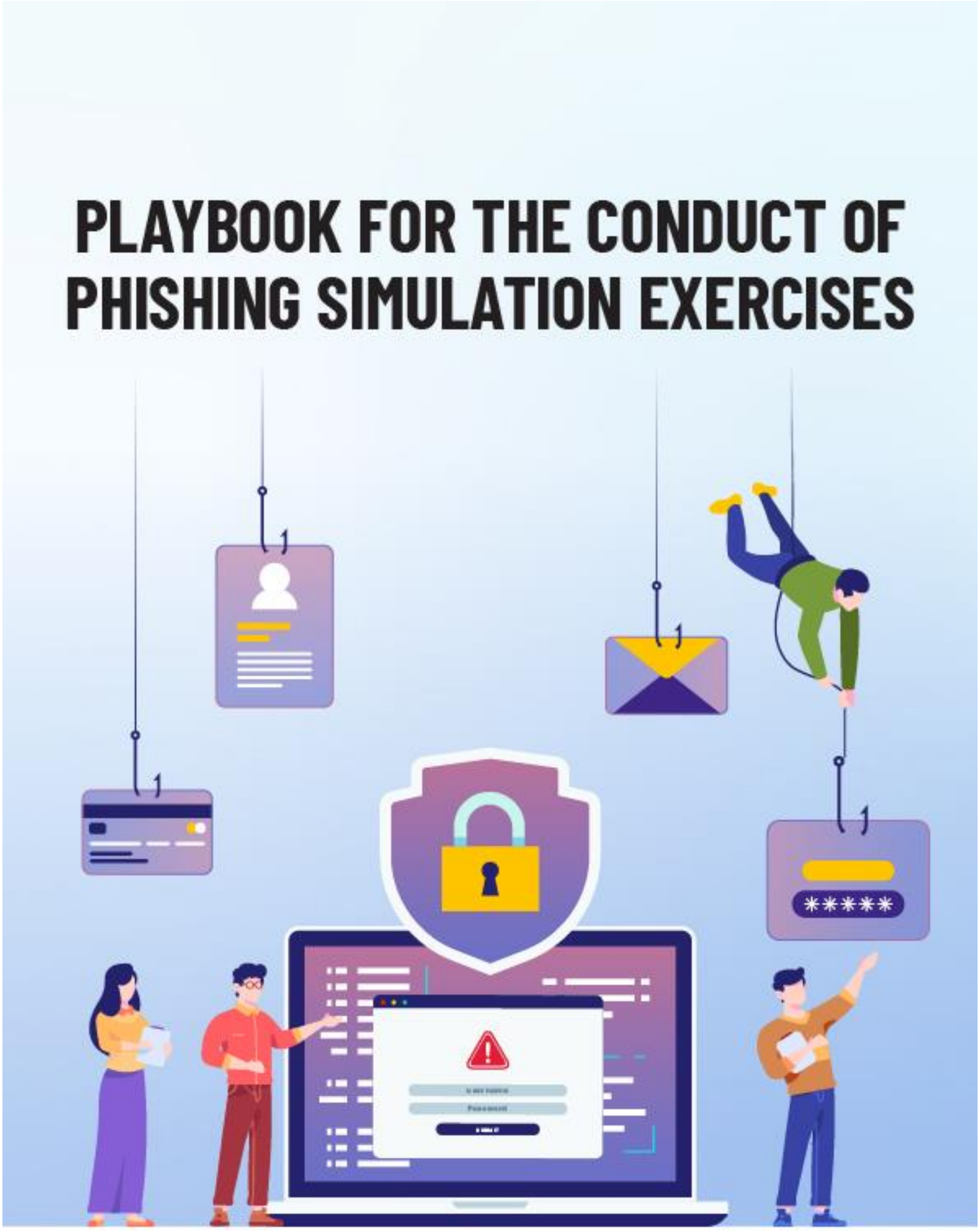
PLAYBOOK FOR THE CONDUCT OF PHISHING SIMULATION EXERCISES



A collaboration between

CSA SINGAPORE
Cyber Security Agency of Singapore

Microsoft

Document History

Version No.	Effective Date	Description
1.0	January 2024	First Release

Contents Page

Playbook for the Conduct of Phishing Simulation Exercises

This playbook provides guidance to IT administrators of corporate networks in organisations on how to conduct phishing simulation exercises using Microsoft 365 Defender. The goal of conducting phishing simulation exercises is to test and improve the cybersecurity awareness and readiness of employees and to help organisations identify potential gaps to better defend against real phishing attacks. By continually educating employees on the dangers of phishing attacks, organisations can enhance their overall cybersecurity posture. Organisations are strongly encouraged to improve on the cybersecurity awareness of employees in the organisation by referencing CSA's Cybersecurity Toolkits for Employees.

Users should note the importance of communicating the objective and intent of the phishing simulations (both before and after the simulations), and to ensure that phishing simulations are carried out in a controlled and carefully managed manner. This is to minimise confusion and avoid causing unnecessary alarm among employees.

1. What is Phishing?

Phishing is a social engineering technique used by cybercriminals to fraudulently obtain sensitive information such as account credentials, personal information, or financial details by impersonating a legitimate individual or reputable organisation online. Phishing can come in the form of emails, messages, and websites.

Phishing attacks often utilise malicious attachments and deceptive links disguised as legitimate documents, invoices, or account login portals. When a user clicks on these attachments and links, they might have malware installed on their devices or get redirected to a fraudulent website mimicking a legitimate website.

2. Importance of Remaining Vigilant Against Phishing Attacks

It is important for individuals and organisations to remain vigilant against phishing attacks due to the high damage potential that successful phishing attacks may cause. Phishing attacks can lead to identity theft and financial loss when attackers gain access to personal information, potentially resulting in unauthorised transactions, credit card fraud, or fraudulent loans taken out on behalf of the victim. For businesses, the repercussions of a successful phishing attack can be equally severe, as attackers may disrupt business operations, access sensitive company data, and even gain control of entire IT systems.

Furthermore, phishing attacks often result in data breaches, posing significant risks to organisations. Such breaches can lead to reputational damage, legal penalties, and substantial financial costs. Phishing emails often contain malicious attachments or links that can install malware on a user's computer, allowing attackers to steal sensitive information, compromise systems, or serve as a launch pad for additional attacks.

3. Common Types of Email Phishing Attacks

There are several variations of phishing, each with its own techniques and objectives. Email phishing is one of the common types of phishing attacks targeting organisations and involves sending fraudulent emails that appears to be sent from a legitimate source to deceive recipients. Email phishing attacks are widespread as it is relatively easy to execute and targets large number of individuals simultaneously. Here are some common types of email phishing.

3.1 Spear Phishing

Spear phishing is a targeted form of phishing where attackers customise their messages for specific individuals or organisations, with the intent of stealing sensitive information, gaining unauthorised access to accounts, or delivering malware to the target. Attackers often gather personal information about the target to make the phishing attempt more convincing.

3.2 Whaling

Whaling targets high-profile individuals, often senior executives, or key decision-makers in organisations, to deceive these high-value targets into divulging sensitive information or performing unauthorised actions. Attackers might also impersonate these individuals to manipulate employees into taking actions such as authorising financial transactions, revealing sensitive information, or gaining access to critical systems.

3.3 Business Email Compromise

Business Email Compromise (BEC) is a type of phishing attack that specifically targets businesses. In a BEC attack, cybercriminals employ various tactics, including email spoofing, to impersonate a trusted party, typically someone within the organisation's leadership or a trusted business partner. By using deceptive emails that appear to come from a legitimate source, the attackers aim to manipulate employees into making fraudulent payments, transferring funds, or revealing sensitive data.

3.4 Credential Harvesting

Credential harvesting refers to cybercriminals attempting to steal credentials from individuals by employing deceptive techniques, including the creation of fake login websites that closely mimic legitimate ones, to lure victims into submitting their login credentials. Phishing attacks that focus on credential harvesting are designed to obtain login credentials for various online accounts, such as email accounts, social media profiles, banking websites, and business applications.

4. Possible Signs of Phishing

It is crucial for individuals and organisations to recognise potential signs of phishing to prevent themselves from falling victim to phishing. Here are some possible signs of phishing attempts to watch out for.

4.1 Misspelled or Suspicious Sender Email Addresses

Check the sender's email address carefully, as email spoofing is a common tactic used by attackers. They often manipulate email addresses to closely resemble those of legitimate organisations but may include slight misspellings or use free email hosting services.

4.2 Urgent or Threatening Language

Phishing emails often create a sense of urgency or fear pressuring recipients to take immediate action. These tactics include threats of account suspension or legal consequences, limited time offers, fake security alerts, emergency notifications, free prizes, and fake payment requests.

4.3 Suspicious Attachments or Links

Phishing emails might contain suspicious attachments or links which contain malware and employ social engineering tactics to deceive recipients into opening malicious files. These attachments often contain executable code which compromise the security of the recipient's device, leading to unauthorised system access or data theft.

4.4 Unexpected Emails

Phishing emails often impersonate legitimate entities, such as government agencies, financial institutions, or popular websites. If you receive an unexpected email claiming to be from an official source, it could be an attempt to trick you into providing sensitive information.

4.5 Promises of Attractive Rewards

Promises of attractive rewards in emails often indicate potential phishing attempts, as attackers use enticing offers to perform social engineering. Phishing schemes offering seemingly too good to be true rewards, such as lottery winnings or exclusive prizes, aim to trick individuals into providing sensitive information.

4.6 Requests for Personal or Financial Information

Legitimate organisations typically do not request for sensitive information like passwords, NRIC numbers, or credit card details via email.

5. Why Conduct Phishing Simulations?

Phishing simulation exercises serve as an essential tool for enhancing cybersecurity awareness and readiness among individuals and organisations. These exercises mimic real-world phishing threats and are conducted to educate individuals about the tactics and dangers of phishing attacks. Through the simulated phishing scenarios, individuals learn to recognise potential phishing attempts, minimise their risks of falling prey to cybercriminals, and respond to phishing emails appropriately. Taking part in the phishing simulation exercises provide employees with proper cyber hygiene skills required to scrutinise emails, verify sender authenticity, and refrain from clicking on suspicious links or downloading malicious attachments.

From an organisational level, phishing simulations enable organisations to test the effectiveness of their cybersecurity defences and employees' education. By tracking employee responses to simulated phishing emails, companies can identify weak links in their security posture, pinpoint vulnerable employees, and take targeted measures for improvement. These exercises also facilitate the cultivation of a security-conscious and collective responsibility culture within organisations. As employees become more adept in identifying potential phishing attempts and more proactive in reporting suspicious emails, these will contribute to raising the overall cybersecurity posture of the organisation.

6. Guidelines for Organisations Conducting Simulated Phishing Exercises

Establishing guidelines and parameters allow organisations to establish a framework for conducting phishing simulations in a responsible and productive manner. This contributes towards a positive learning environment, minimises misunderstandings and fosters a constructive atmosphere among exercise participants. Organisations conducting simulated phishing exercises must abide by the following guidelines to ensure that the simulated phishing exercises are conducted in an ethical and legal manner.

6.1 Scope and Boundaries of Phishing Exercise

Simulated phishing exercises should be conducted in a controlled manner, should not cause distress to participants, and should avoid contravening any laws or giving rise to any causes of legal action. Such instances may arise where, for example, participants are induced into providing information which may contravene the Personal Data Protection Act (for example, NRIC or other personal information) or which may result in offences under the Computer Misuse Act (for example, credentials to access accounts or computers). Organisations should also not design the phishing simulation to appear too similar to a real attack, such that it would cause distress and may lead to unexpected actions by participants (for example, by communicating to participants that their family members are in danger, which may lead to them making a police report).

6.2 Acceptable Use Policies

Organisations that plan to conduct simulated phishing exercises should have policies in place that inform their employees that they will be required to participate in cybersecurity awareness trainings and exercises. Organisations could consider leveraging IT acceptable use agreements (or relevant agreements in other forms) to include relevant clauses notifying employees that phishing simulations will be conducted periodically.

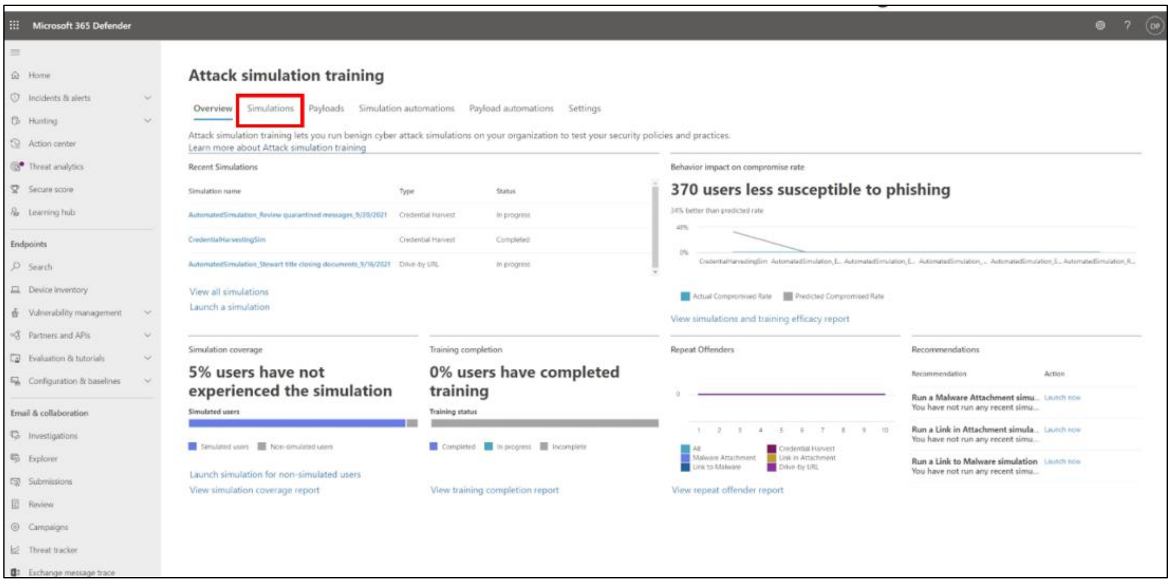
6.3 Clear Pre- and Post- Exercise Communications

Simulated phishing exercises should be conducted within a context that would give participants a fair appreciation and learning opportunity that the messages sent are part of a phishing simulation. Organisations conducting simulated phishing exercises should have clear pre- and post-exercise communications about an ongoing effort to educate the participants about phishing attempts (e.g. within the context of an anti-scam campaign, or with follow up messaging to highlight that the messages sent previously were part of a simulated phishing exercise). In particular, post-exercise communications should be prompt so that participants can better appreciate the simulated phishing message in the context of raising their cybersecurity awareness. For instance, organisations may consider immediately sending an automated individualised reply to participants who click on phishing emails, which can be followed subsequently by an organisation-wide message summarising the simulated phishing exercise.

7. Step-by-step Instructions on Conducting Phishing Simulation Exercises in an M365 Environment Using Microsoft 365 Defender

Step 1: In Microsoft 365 Defender portal **, go to **Email & collaboration** under **Attack simulation training** and select **Simulations** tab.

NOTE: ** Available in Microsoft 365 E5 or A5, Microsoft Defender for Office 365 Plan 1 or 2, or included in add-on licenses. For more information about the availability of Attack simulation training across different Microsoft 365 subscriptions, see Microsoft Defender for Office 365 service description.



Attack simulation training

Attack simulation training lets you run benign cyber attack simulations on your organization to test your security policies and practices.
Learn more about Attack simulation training

Recent Simulations

Simulation name	Type	Status
AutomatedSimulation_Review quarantined messages_9/20/2021	Credential Harvest	In progress
CredentialHarvestingSim	Credential Harvest	Completed
AutomatedSimulation_Stewart title closing documents_9/16/2021	Drive-by URL	In progress

View all simulations
Launch a simulation

Behavior impact on compromise rate

370 users less susceptible to phishing

34% better than predicted rate

View simulations and training efficacy report

Simulation coverage

5% users have not experienced the simulation

Simulated users

Launch simulation for non-simulated users
View simulation coverage report

Training completion

0% users have completed training

Training status

View training completion report

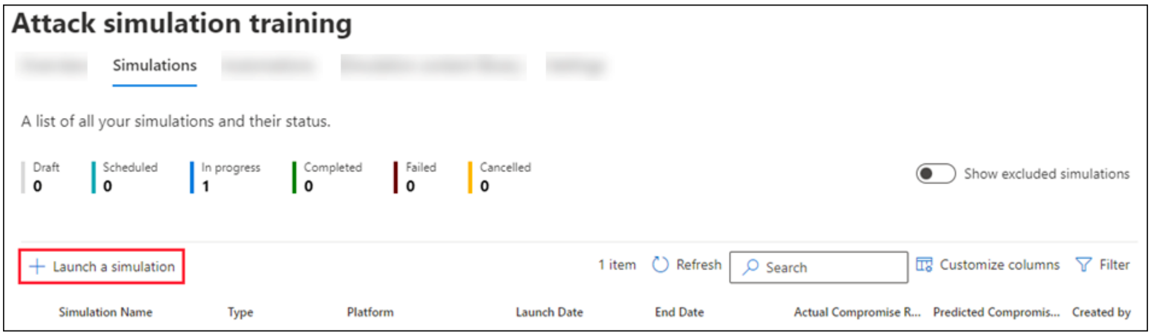
Repeat Offenders

View repeat offender report

Recommendations

Recommendation	Action
Run a Malware Attachment simu... You have not run any recent simu...	Launch now
Run a Link in Attachment simula... You have not run any recent simu...	Launch now
Run a Link to Malware simulation You have not run any recent simu...	Launch now

Step 2: On the **Simulations tab**, select **Launch a simulation** to start a new simulation wizard.



Attack simulation training

A list of all your simulations and their status.

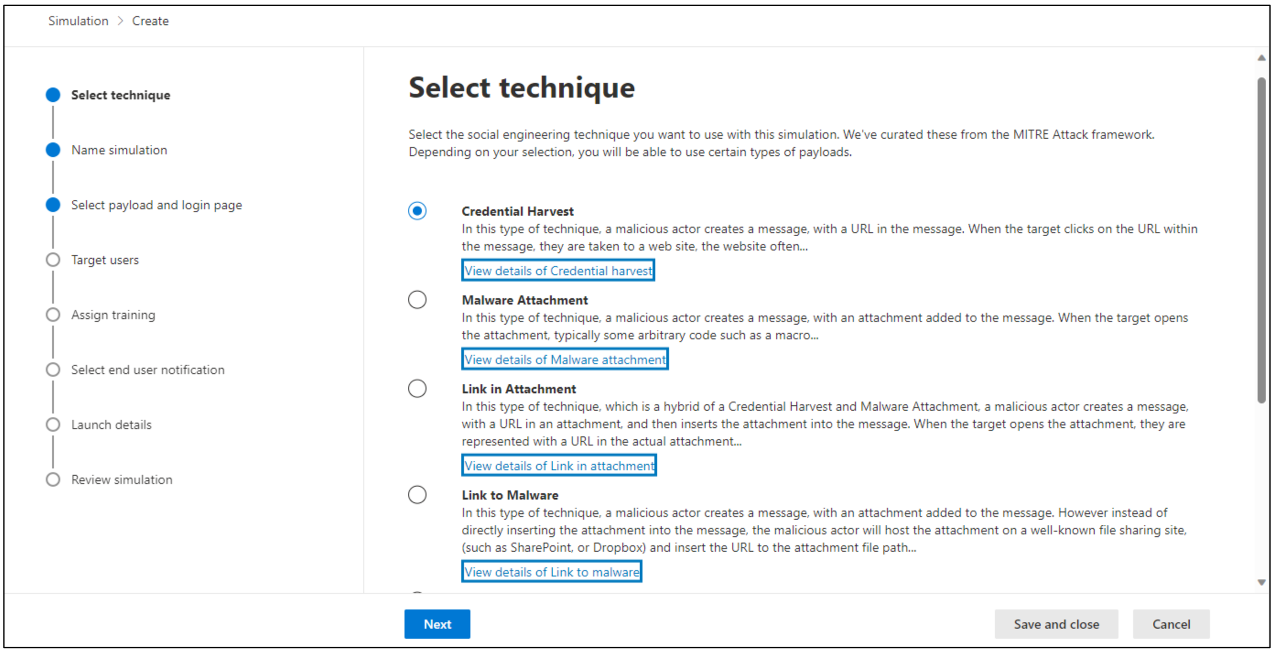
Draft	Scheduled	In progress	Completed	Failed	Cancelled
0	0	1	0	0	0

Simulation Name	Type	Platform	Launch Date	End Date	Actual Compromise R...	Predicted Compromis...	Created by

Step 3: On the **Select Technique** page, select an available social engineering technique that was curated from the MITRE ATT&CK framework. There are different payloads available for different techniques.

The available social engineering technique are:

- Credential Harvest
- Malware Attachment
- Link in Attachment
- Link to Malware
- Drive-by URL
- OAuth Consent Grant



Simulation > Create

- ● Select technique
- ● Name simulation
- ● Select payload and login page
- ○ Target users
- ○ Assign training
- ○ Select end user notification
- ○ Launch details
- ○ Review simulation

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.

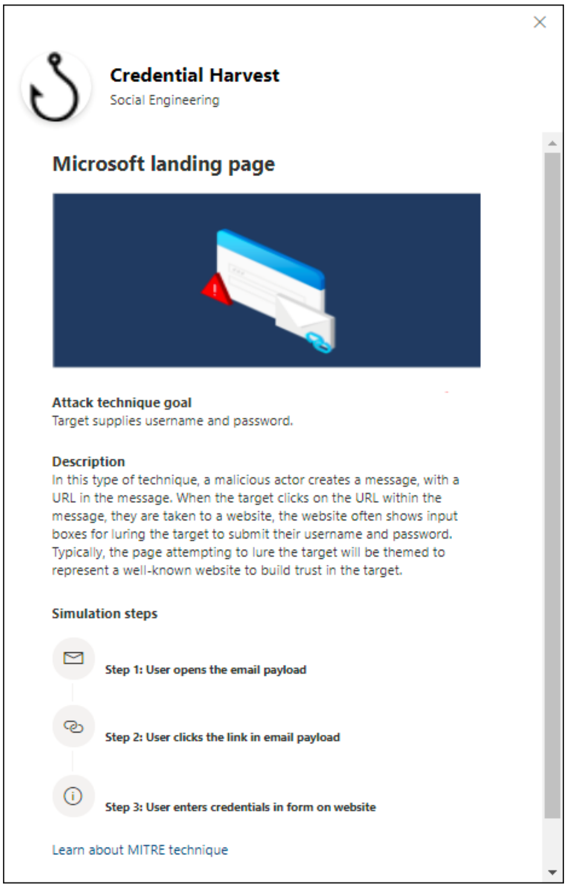
● **Credential Harvest**
In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a web site, the website often...
View details of Credential harvest

○ **Malware Attachment**
In this type of technique, a malicious actor creates a message, with an attachment added to the message. When the target opens the attachment, typically some arbitrary code such as a macro...
View details of Malware attachment

○ **Link in Attachment**
In this type of technique, which is a hybrid of a Credential Harvest and Malware Attachment, a malicious actor creates a message, with a URL in an attachment, and then inserts the attachment into the message. When the target opens the attachment, they are represented with a URL in the actual attachment...
View details of Link in attachment

○ **Link to Malware**
In this type of technique, a malicious actor creates a message, with an attachment added to the message. However instead of directly inserting the attachment into the message, the malicious actor will host the attachment on a well-known file sharing site, (such as SharePoint, or Dropbox) and insert the URL to the attachment file path...
View details of Link to malware

If **View details link** in the description is selected, it describes the technique and the simulation steps resulting from the technique.



Credential Harvest
Social Engineering

Microsoft landing page

Attack technique goal
Target supplies username and password.

Description
In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a website, the website often shows input boxes for luring the target to submit their username and password. Typically, the page attempting to lure the target will be themed to represent a well-known website to build trust in the target.

Simulation steps

Step 1: User opens the email payload

Step 2: User clicks the link in email payload

Step 3: User enters credentials in form on website

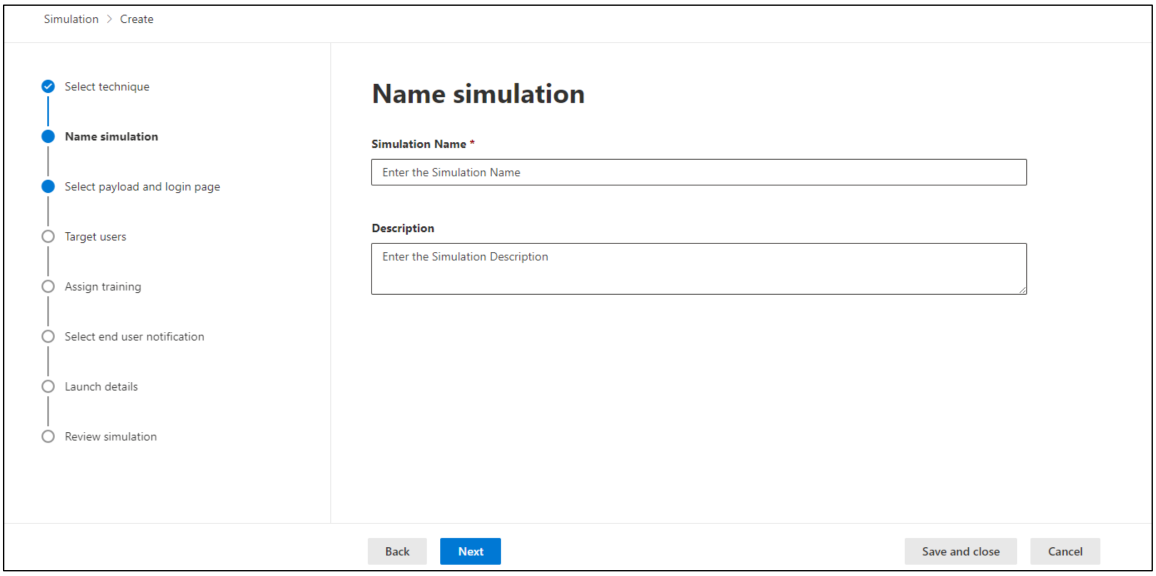
Learn about MITRE technique

Once done, select **Next**.

Step 4: On the **Name simulation** page, configure the following settings:

- Name: Enter a unique, descriptive name for the simulation.
- Description: Enter an optional detailed description for the simulation.

When you have completed the configuration on the **Name simulation** page, select **Next**.



Simulation > Create

- Select technique
- **Name simulation**
- Select payload and login page
- Target users
- Assign training
- Select end user notification
- Launch details
- Review simulation

Name simulation

Simulation Name *

Enter the Simulation Name

Description

Enter the Simulation Description

Step 5: On the **Select payload and login** page, select an existing payload, or create a new payload.

For the **Credential Harvest** or **Link in Attachment** social engineering techniques, you can also view the login page that is used in the payload, select a different login page to use, or create a new login page to use.

To find a payload in the list, type part of the payload name in the Search box and then press the ENTER key.

If you select ▽ , the following filters are available:

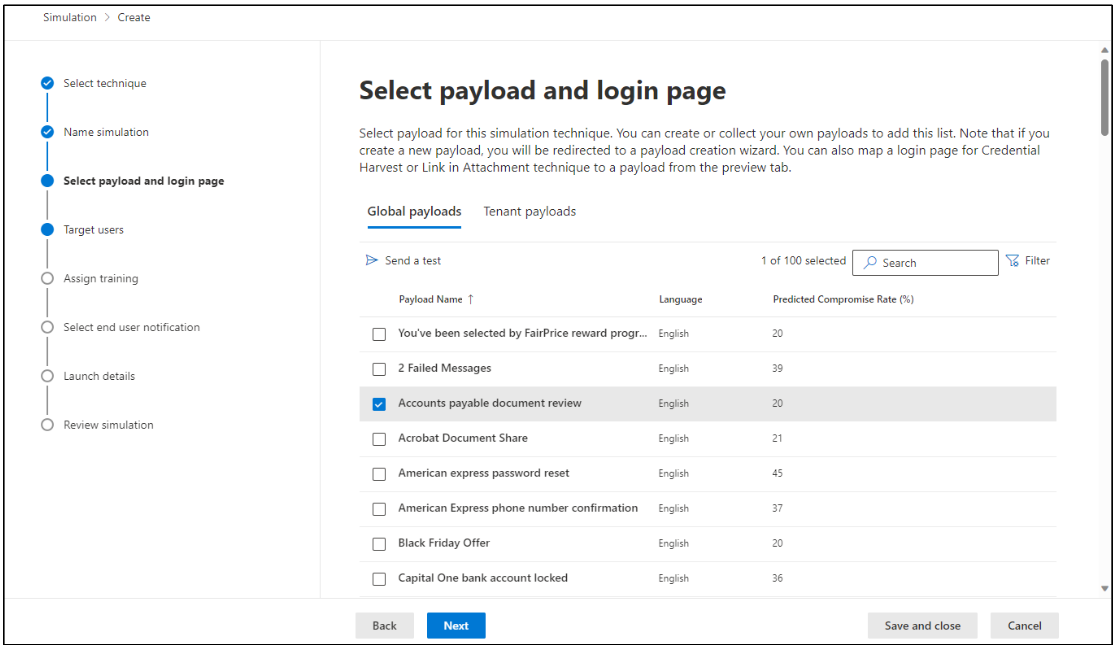
- Source
- Complexity
- Filter by theme
- Filter by brand
- Filter by industry

When you are finished configuring filters, select Apply, Cancel, or ▽ Clear filters.

If you select a payload by selecting the check box next to the name, a **Send a test** button appears above the list of payloads. You can use this button to send a copy of the payload email to yourself (the currently logged in user) for inspection.

Click on **Next** to proceed.

Example: Accounts payable document review



Simulation > Create

- Select technique
- Name simulation
- **Select payload and login page**
- Target users
- Assign training
- Select end user notification
- Launch details
- Review simulation

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.

	Payload Name ↑	Language	Predicted Compromise Rate (%)
☐	You've been selected by FairPrice reward progr...	English	20
☐	2 Failed Messages	English	39
☑	Accounts payable document review	English	20
☐	Acrobat Document Share	English	21
☐	American express password reset	English	45
☐	American Express phone number confirmation	English	37
☐	Black Friday Offer	English	20
☐	Capital One bank account locked	English	36

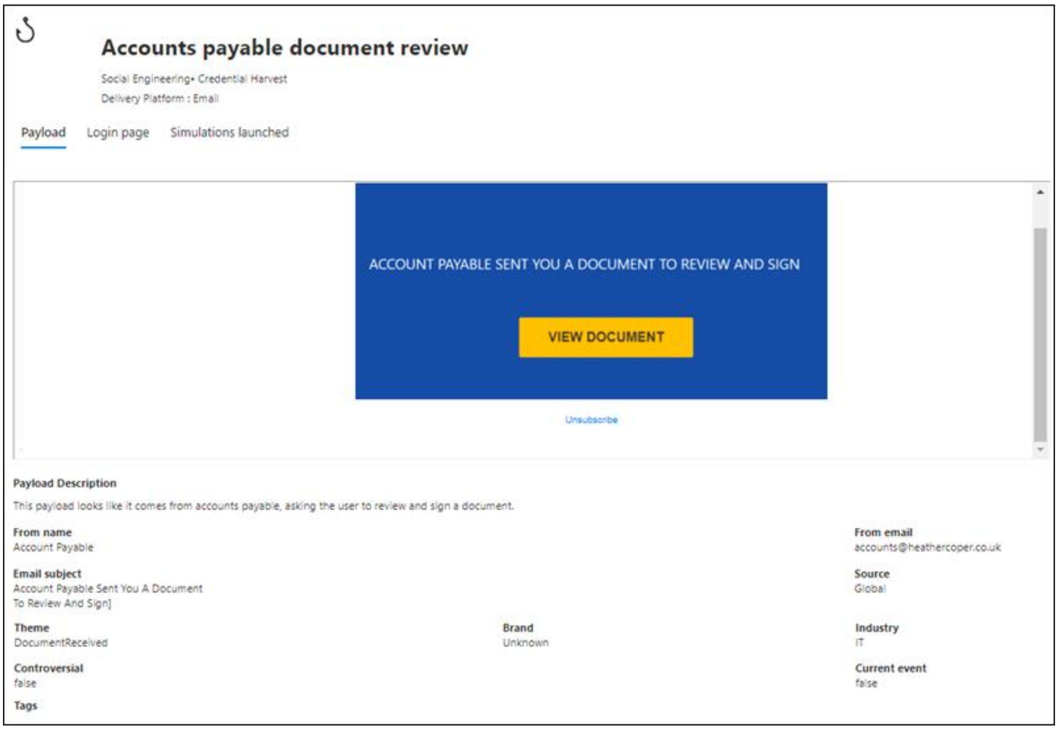
If there are no payloads available that fit the requirements, a custom payload can be created, select **Tenant payloads tab**, select **Create a payload**. For more information on custom payloads, see Payloads in Attack simulation training.

Step 6 (Optional): Make changes to the selected payload.

Check on a payload box, example: Accounts payable document review, and click on it again. Select a **login page** to be used in Credential Harvest or Link in Attachment payloads. **

NOTE: **If the simulation does not use Credential Harvest or Link in Attachment payloads, or there is no need to view or edit the login page that is used, **move to Step 7** to continue.

Click anywhere in the row other than the checkbox of the selected payload to view more details.



Accounts payable document review

Social Engineering• Credential Harvest

Delivery Platform : Email

Payload Description

This payload looks like it comes from accounts payable, asking the user to review and sign a document.

From name
Account Payable

From email
accounts@heathercoper.co.uk

Email subject
Account Payable Sent You A Document To Review And Sign]

Source
Global

Theme
DocumentReceived

Brand
Unknown

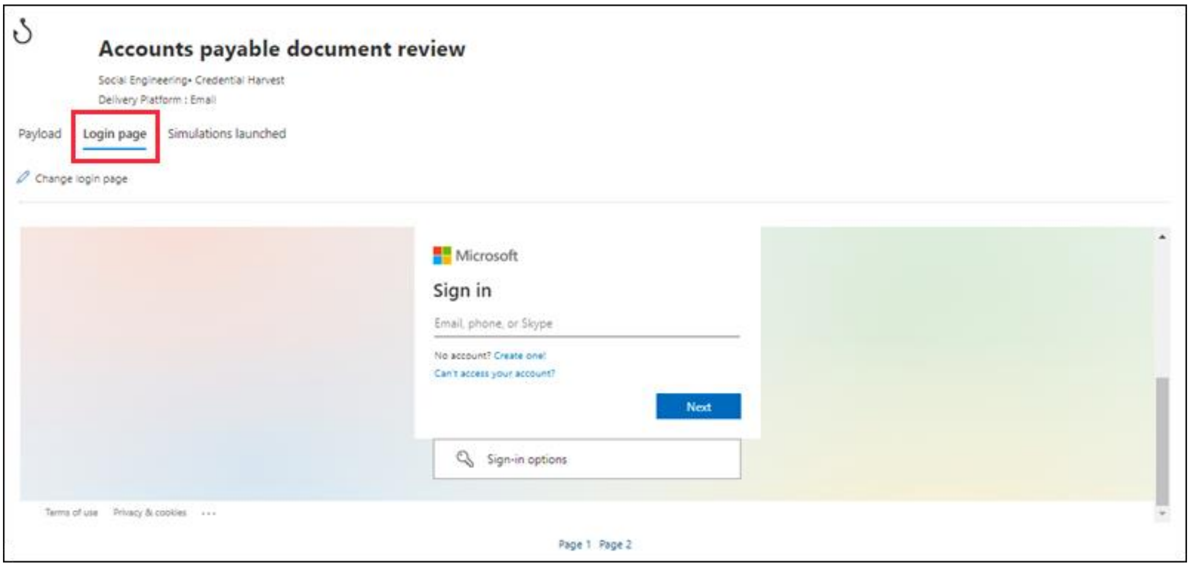
Industry
IT

Controversial
false

Current event
false

Tags

The Login page tab shows the login page that is currently selected for the payload.



Accounts payable document review

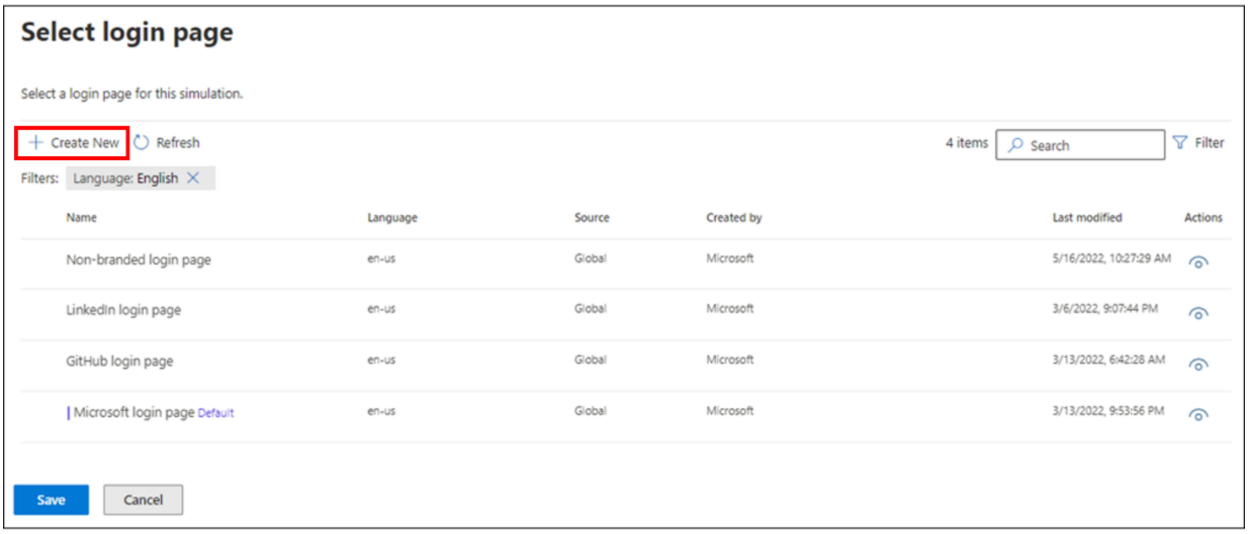
Social Engineering• Credential Harvest

Delivery Platform : Email

Use the Page 1 and Page 2 links at the bottom of the page for two-page login pages.

Optional: To find another login page in the list, click on **Change login page**, type part of the login page name in the Search box and then press the **Save** key.

Optional: If a custom login page must be created, click on **Change login page**, select Create **new**. For more information on custom login page, see Login Pages in Attack Simulation Training.



Select login page

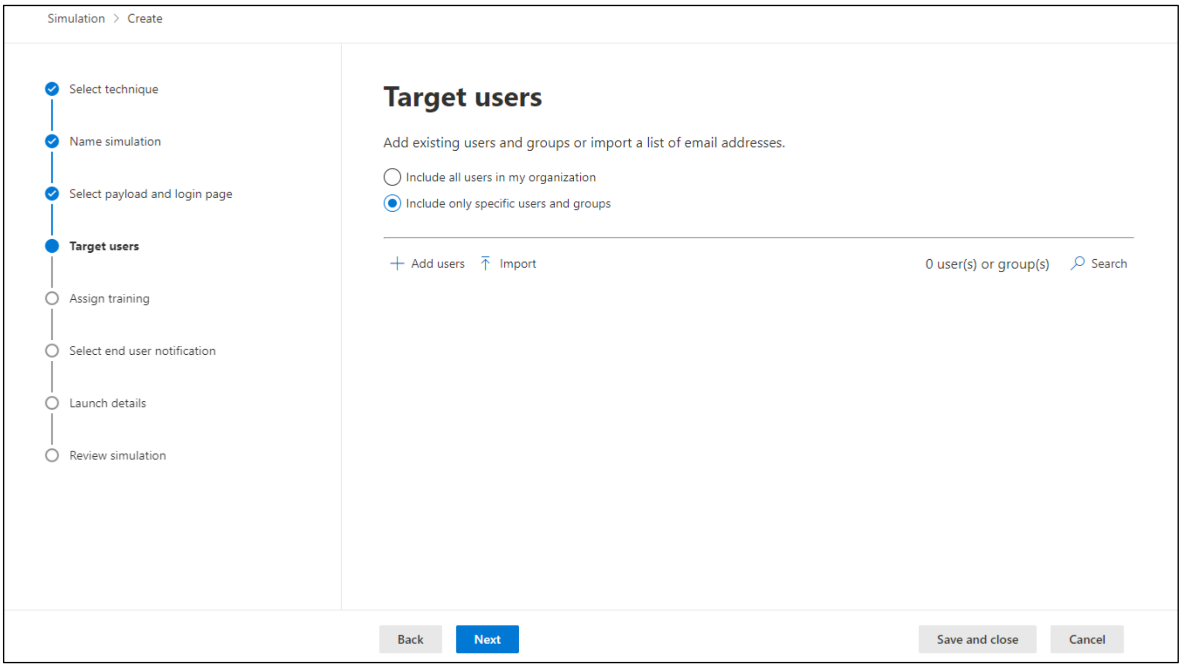
Select a login page for this simulation.

Name	Language	Source	Created by	Last modified	Actions
Non-branded login page	en-us	Global	Microsoft	5/16/2022, 10:27:29 AM	👁
LinkedIn login page	en-us	Global	Microsoft	3/6/2022, 9:07:44 PM	👁
GitHub login page	en-us	Global	Microsoft	3/13/2022, 6:42:28 AM	👁
Microsoft login page Default	en-us	Global	Microsoft	3/13/2022, 9:53:56 PM	👁

Verify the selected login page and click **Save**.

Once done, select **Next**.

Step 7: On the Target users page, select the users involved in the simulation.



Target users

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

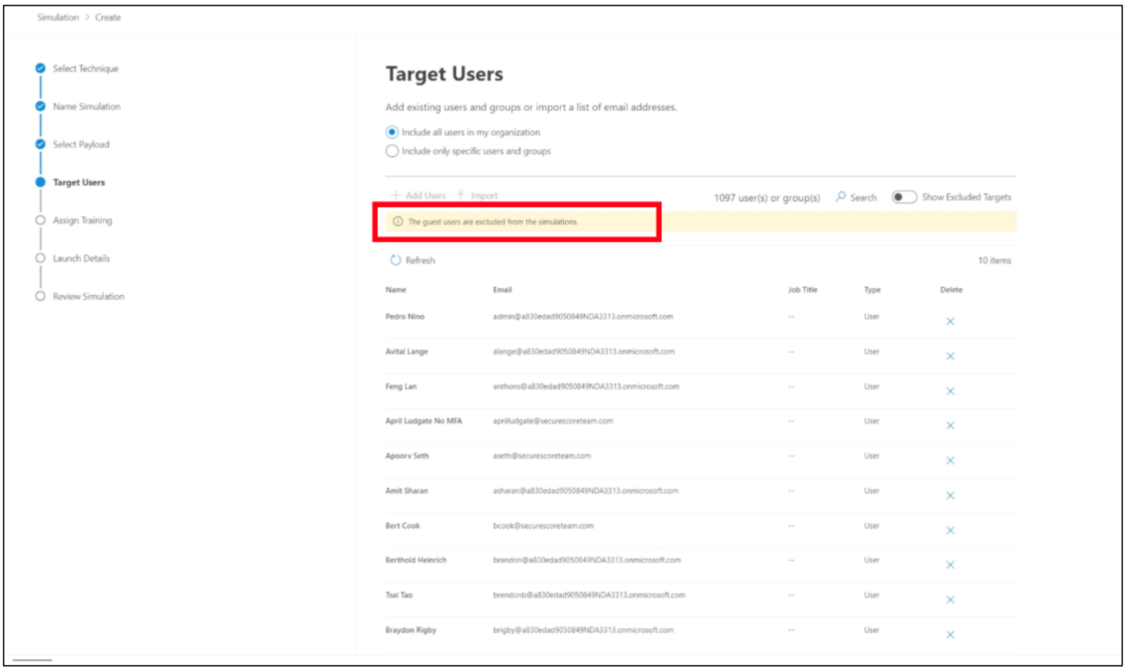
○ Include all users in my organization

● Include only specific users and groups

To add more users and groups, select **Add users** or **Import**.

To import, specify a CSV file that contains one email address per line which will be imported and shown on the Targeted Users page.

To exclude users, select **Exclude some of the targeted users from this simulation** to exclude users that would otherwise be included based on previous selections on the Target Users page.



Target Users

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

● Include all users in my organization

○ Include only specific users and groups

1097 user(s) or group(s)

ⓘ The guest users are excluded from the simulations.

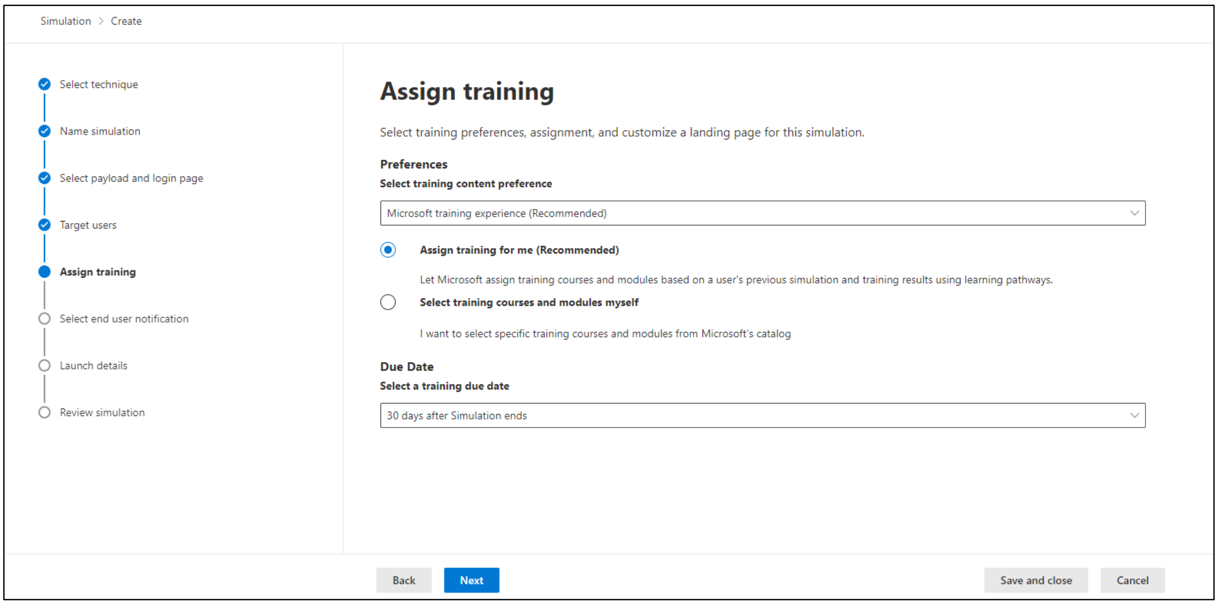
10 items

Name	Email	Job Title	Type	Delete
Pedro Nino	admin@a830edad9050849NDA3313.onmicrosoft.com	--	User	×
Avital Lange	alange@a830edad9050849NDA3313.onmicrosoft.com	--	User	×
Feng Lan	anthons@a830edad9050849NDA3313.onmicrosoft.com	--	User	×
April Ludgate No MFA	aprilludgate@securescoreteam.com	--	User	×
Apoorv Seth	aseth@securescoreteam.com	--	User	×
Amit Sharan	asharan@a830edad9050849NDA3313.onmicrosoft.com	--	User	×
Bert Cook	bcook@securescoreteam.com	--	User	×
Berthold Heinrich	brandon@a830edad9050849NDA3313.onmicrosoft.com	--	User	×
Tsai Tao	brendonb@a830edad9050849NDA3313.onmicrosoft.com	--	User	×
Braydon Rigby	brigby@a830edad9050849NDA3313.onmicrosoft.com	--	User	×

Once done, select **Next**.

Step 8: On the **Assign training** page, assign trainings for the simulation. There are three fields namely:

- **Assign training for me (Recommended)**: This is the default value where Microsoft assigns trainings based on a user's previous simulation and training results.
- **Select training courses and modules myself**: If this option is selected, a wizard will be opened where users can find and select trainings.
- **Due Date**: Default value is 30 days after simulation ends.



Simulation > Create

- Select technique
- Name simulation
- Select payload and login page
- Target users
- **Assign training**
- Select end user notification
- Launch details
- Review simulation

Assign training

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

Preferences

Select training content preference

Microsoft training experience (Recommended)

● **Assign training for me (Recommended)**

Let Microsoft assign training courses and modules based on a user's previous simulation and training results using learning pathways.

○ **Select training courses and modules myself**

I want to select specific training courses and modules from Microsoft's catalog

Due Date

Select a training due date

30 days after Simulation ends

Once done, select **Next**.

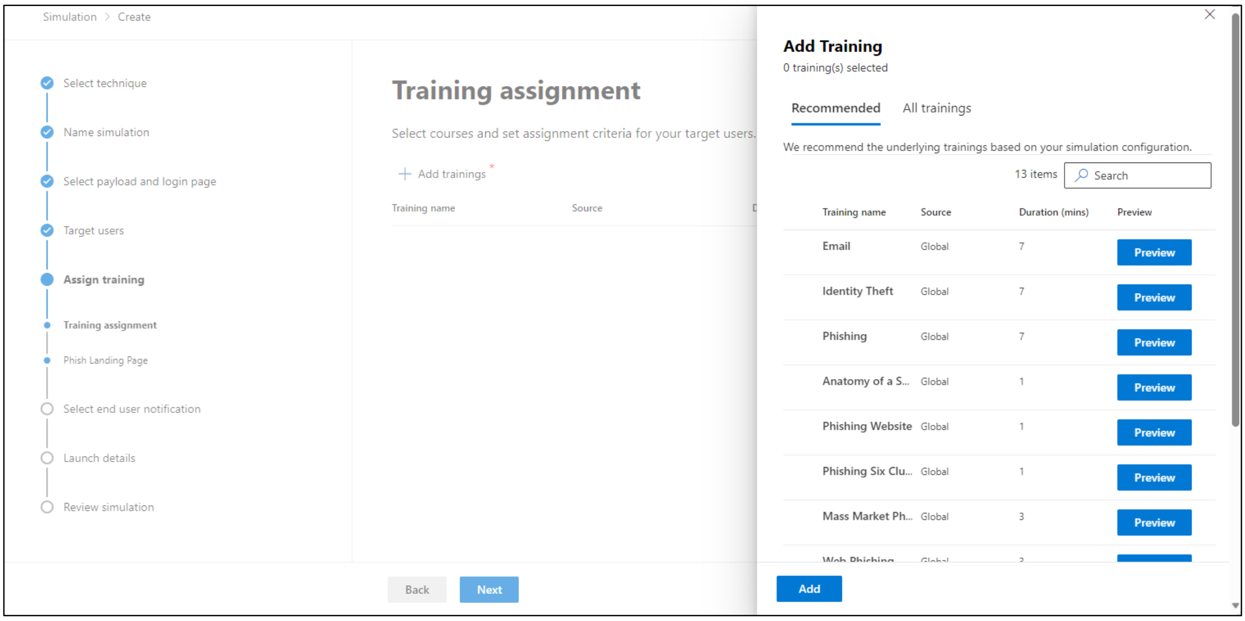
Step 9 (Optional): On the Phish Landing Page, select the trainings to add to the simulation by clicking **Add trainings**. **

NOTE: ** Applicable if **Select training courses and modules myself** option was selected on the Assign training page.

If the option was not selected, **continue to Step 10.**

Use the following tabs to select trainings to include in the simulation:

- Recommended tab: Shows the recommended built-in trainings based on the simulation configuration. These are the same trainings that would have been assigned if **Assign training for me (Recommended)** option was selected on the previous page.
- All trainings tab: Shows all built-in trainings that are available.



Simulation > Create

- Select technique
- Name simulation
- Select payload and login page
- Target users
- **Assign training**
  - Training assignment
  - Phish Landing Page
- Select end user notification
- Launch details
- Review simulation

Training assignment

Select courses and set assignment criteria for your target users.

+ Add trainings *

Training name | Source

Back | Next

Add Training

0 training(s) selected

Recommended | All trainings

We recommend the underlying trainings based on your simulation configuration.

13 items | Search

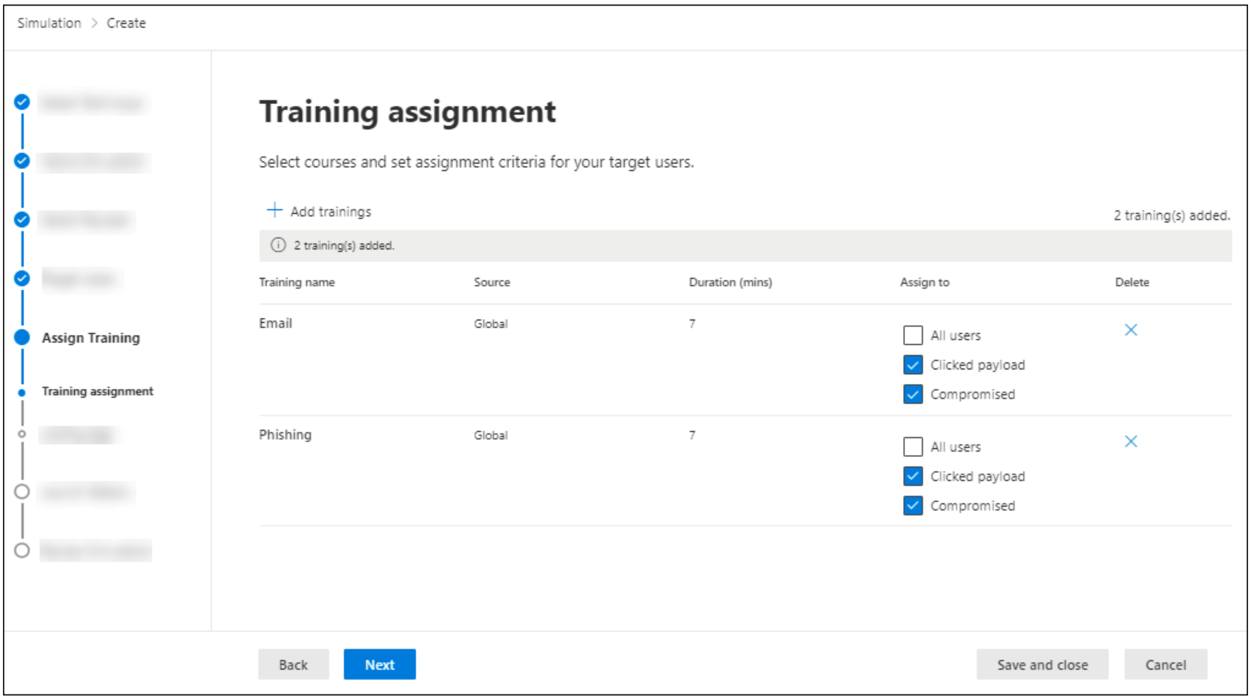
Training name	Source	Duration (mins)	Preview
Email	Global	7	Preview
Identity Theft	Global	7	Preview
Phishing	Global	7	Preview
Anatomy of a S...	Global	1	Preview
Phishing Website	Global	1	Preview
Phishing Six Clu...	Global	1	Preview
Mass Market Ph...	Global	3	Preview
Web Phishing	Global	3	

Add

Use the Search box to find trainings. Type part of the training name and press the ENTER key.

On either tab, select one or more trainings by clicking in the blank area next to the Training name column. Once done, select **Add**.

Back on the Training assignment page, the selected trainings are now listed.



Simulation > Create

- **Assign Training**
  - **Training assignment**

Training assignment

Select courses and set assignment criteria for your target users.

+ Add trainings | 2 training(s) added.

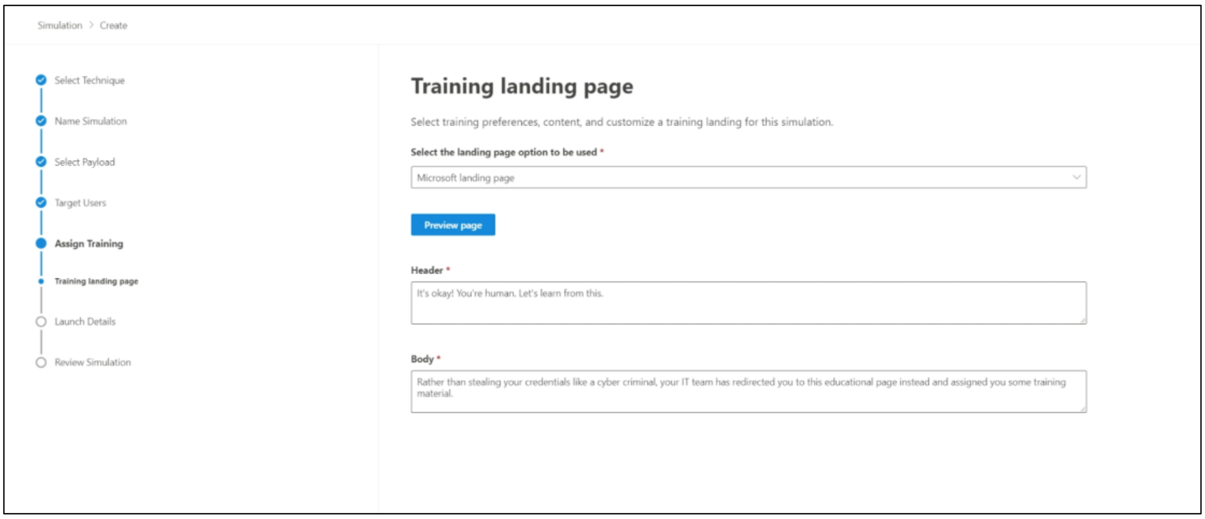
ⓘ 2 training(s) added.

Training name	Source	Duration (mins)	Assign to	Delete
Email	Global	7	□ All users ☑ Clicked payload ☑ Compromised	✕
Phishing	Global	7	□ All users ☑ Clicked payload ☑ Compromised	✕

Back | Next | Save and close | Cancel

Once done, select **Next**.

Step 10: On the **Select Phish landing page**, configure the web page that users are taken to if they open the payload in the simulation.



Training landing page

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

Select the landing page option to be used *

Microsoft landing page

Header *

It's okay! You're human. Let's learn from this.

Body *

Rather than stealing your credentials like a cyber criminal, your IT team has redirected you to this educational page instead and assigned you some training material.

Select one of the following options:

- Use landing pages from library (built-in)
- Use a custom URL

Under **Use landing pages from library:** The following options are available:

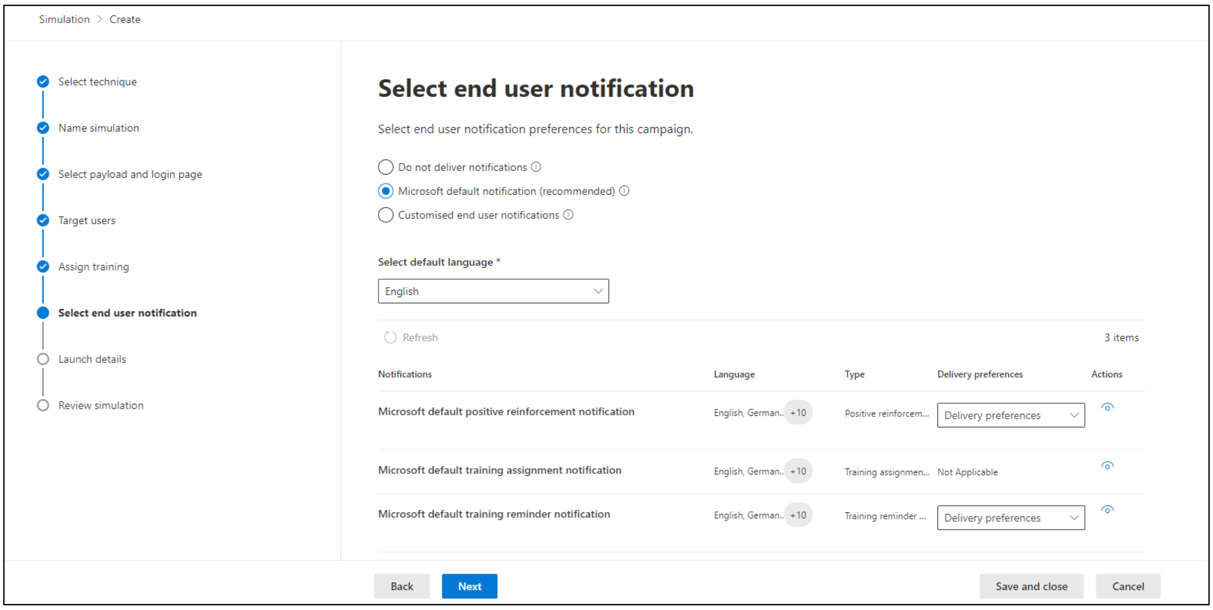
- Payload indicators: Select **Add payload indicators to email** to help users learn how do identify phishing email.

There are two remaining tabs on the Selecting phish landing page where you select the landing page to use:

- Global landing pages tab: Contains the built-in landing pages. When you select a built-in landing page to use by selecting the check box next to name.

Once done, select **Next**.

Step 11: On the **Select end user notification** page, select from the provided notification options.



Select end user notification

Select end user notification preferences for this campaign.

○ Do not deliver notifications ⓘ
● Microsoft default notification (recommended) ⓘ
○ Customised end user notifications ⓘ

Select default language *: English

Refresh — 3 items

Notifications	Language	Type	Delivery preferences	Actions
Microsoft default positive reinforcement notification	English, German.. +10	Positive reinforcem...	Delivery preferences	👁
Microsoft default training assignment notification	English, German.. +10	Training assignmen...	Not Applicable	👁
Microsoft default training reminder notification	English, German.. +10	Training reminder ...	Delivery preferences	👁

The notification options are:

- **Do not deliver notifications**: Users will not receive Training assignment notifications, Training reminder notifications or Positive reinforcement notifications from the simulation.
- **Microsoft default notification (recommended):** The notifications that users will receive are as follows:
  - Microsoft default positive reinforcement notification
  - Microsoft default training assignment notification
  - Microsoft default training reminder notification
- **Customized end user notifications**: Select a Training assignment notification, a Training reminder notification, and (optionally) a Positive reinforcement notification to use for the simulation. **

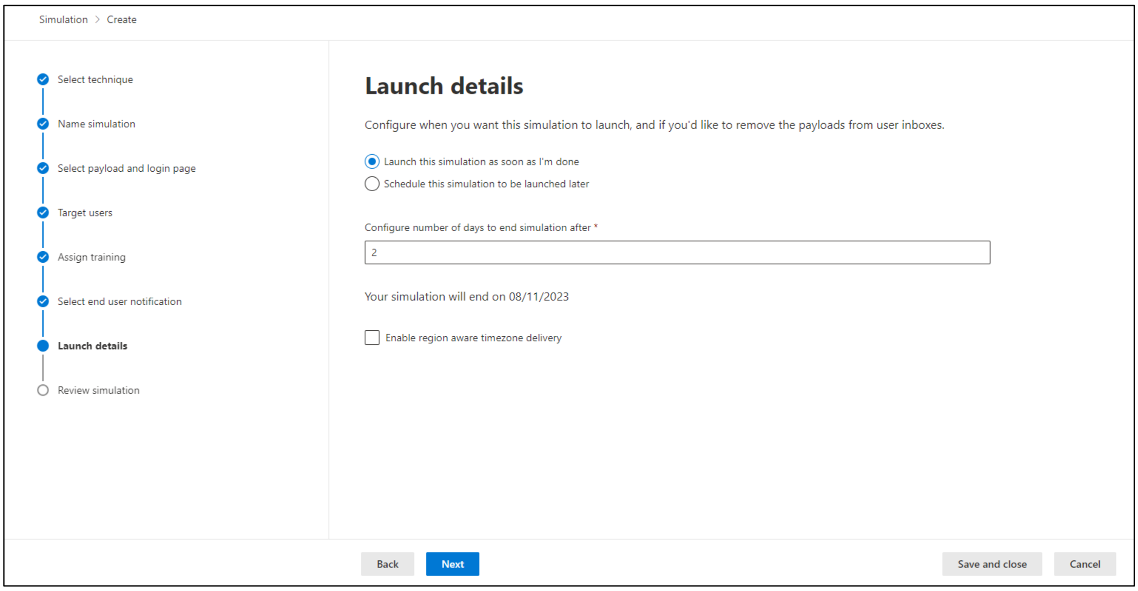
> **NOTE:** ** Select a training assignment notification page, select a training reminder notification page, and select a positive reinforcement notification page will only be available if **Customized end user notification** is selected. For more information, see End-user notifications for Attack simulation training.

Step 12: On the **Launch details** page, choose when to start and end the simulation.

Choose one of the following values:

- Launch this simulation as soon as I'm done
- Schedule this simulation to be launched later: This value has the following associated options to configure:
    - Select launch date
    - Select launch time hour
    - Select launch time minute
    - Select time format: Select AM or PM.

The default value for Configure number of days to end simulation after is 2 days, which is also the minimum value. The maximum value is 30 days. The interaction of the simulation will not be captured after the end date specified.



Launch details

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

● Launch this simulation as soon as I'm done

○ Schedule this simulation to be launched later

Configure number of days to end simulation after *

2

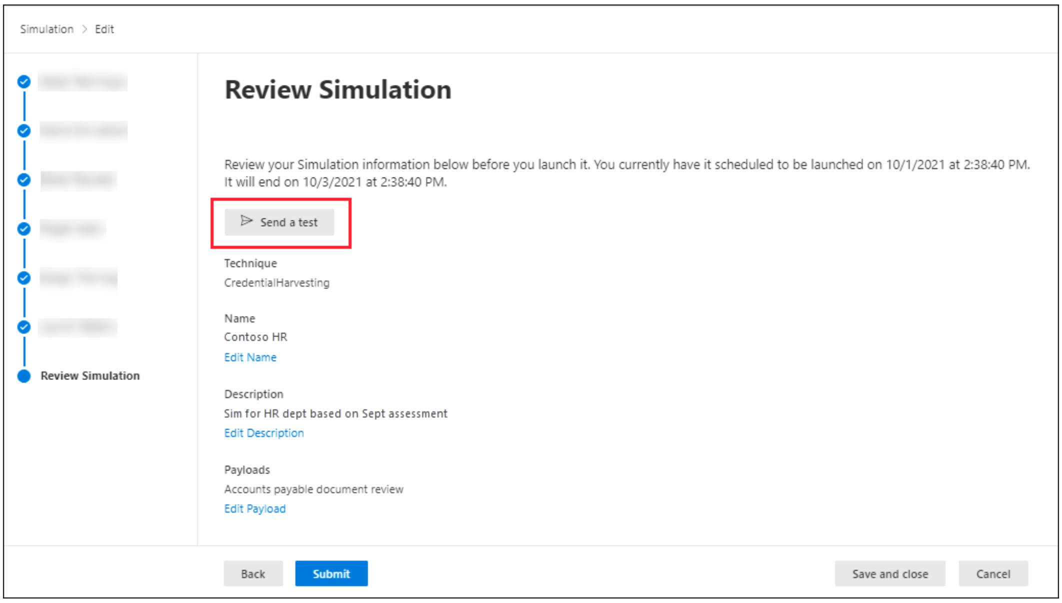
Your simulation will end on 08/11/2023

□ Enable region aware timezone delivery

If **Enable region aware time zone delivery** is selected, the simulated attack messages are delivered to users during their regional working hours.

Once done, select **Next**.

Step 13: On the **Review simulation** page, review the details of the simulation.



Review Simulation

Review your Simulation information below before you launch it. You currently have it scheduled to be launched on 10/1/2021 at 2:38:40 PM. It will end on 10/3/2021 at 2:38:40 PM.

Technique
CredentialHarvesting

Name
Contoso HR
Edit Name

Description
Sim for HR dept based on Sept assessment
Edit Description

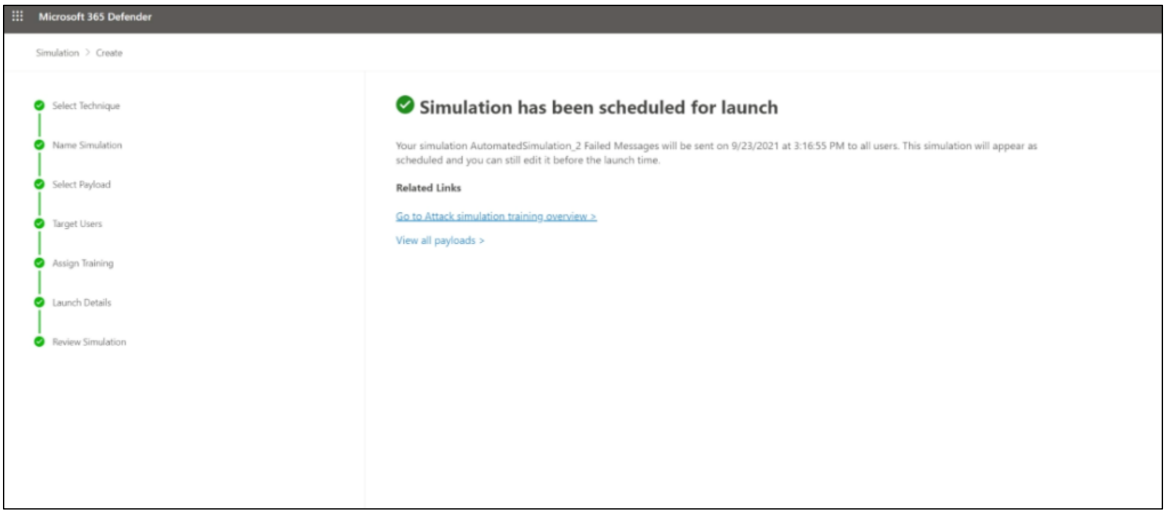
Payloads
Accounts payable document review
Edit Payload

To send a copy of the payload email, select **Send a test** for inspection.

Select **Edit** in each section to modify the settings within the section. Or select **Back** or the specific page in the wizard to modify the settings.

Once done, select **Submit**.

Step 14: On the **Simulation has been scheduled for launch** page, use the links to go to the Attack simulation training overview or to view all payloads.



Simulation has been scheduled for launch

Your simulation AutomatedSimulation_2 Failed Messages will be sent on 9/23/2021 at 3:16:55 PM to all users. This simulation will appear as scheduled and you can still edit it before the launch time.

Related Links

Go to Attack simulation training overview >

View all payloads >

Select **Done**.

Step 15: Back on the **Simulations** tab, the created simulation is now listed.

8. Next Steps After Conducting Phishing Simulations

After the phishing simulation exercises have concluded, it is important for organisations to evaluate the effectiveness of phishing simulation to identify vulnerabilities within the organisation and to determine whether the training and awareness efforts are achieving their intended goals. Here are steps organisations can take to assess the effectiveness of these exercises:

8.1 Evaluating Effectiveness of Phishing Simulation Exercises

Organisations should analyse the results collected during the phishing simulation exercise, which include metrics such as the click rates, conversion rates and reporting rates. These metrics should be compared with baseline data from previous phishing simulations, if available:

- Click rate: The percentage of recipients who clicked on phishing links.
- Conversion rate: The percentage of recipient who entered sensitive information into phishing websites.
- Reporting rate: The percentage of recipient who reported suspicious emails to the IT or security team.

8.2 Conduct Phishing Simulations Periodically

Periodic testing involves conducting simulations at regular intervals to assess how well employees continue to respond to evolving phishing threats and to reinforce cybersecurity awareness. Organisations can consider performing quarterly exercises, with the frequency of the phishing simulations tailored according to the organisation's risk profile and prior exercise results.

8.3 Continual Training and Awareness

Cybersecurity training and awareness programmes should be developed and adjusted to address specific weaknesses or concerns identified during the phishing simulation exercises. Organisations should consider implementing targeted training, concentrating on employees or departments that consistently demonstrate vulnerability to phishing attacks. These targeted efforts should provide additional resources and training to enhance the cybersecurity awareness and response among employees who are most susceptible to phishing attacks. IT administrators may take reference from CSA’s Cybersecurity Toolkits for Employees.

8.4 Ensuring Phishing Simulations are up-to-date

The dynamic nature of the threat landscape means that cybercriminals will continually develop new phishing tactics. To increase the effectiveness and realism of phishing simulations, the scenarios should be updated to closely align with current phishing trends and real-world situations. Organisations may also wish to periodically alter the type of phishing simulations performed, such as email-based, smishing (SMS phishing), or vishing (voice phishing), organisations will be able to provide a comprehensive exercise that prepares employees to recognise and respond to ever evolving phishing threats.

To check for updated information and latest steps to conduct phishing simulations in Microsoft 365, please refer to https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started.

8.5 Other Foundational Cyber Hygiene Measures

Going beyond phishing stimulations, for more holistic protection against common cybersecurity incidents, IT administrators should implement the foundational cyber hygiene measures defined in CSA Cyber Essentials or take on a risk-based framework to cybersecurity, guided by the Cyber Trust mark. IT administrators may take reference from CSA’s Cybersecurity Toolkits for IT Teams.

9. References

CSA:

- https://www.csa.gov.sg/our-programmes/cybersecurity-outreach/cybersecurity-campaigns/the-unseen-enemy-campaign/beware-of-phishing-scams
- https://www.csa.gov.sg/employee-toolkit
- https://www.csa.gov.sg/it-team-toolkit
- https://www.csa.gov.sg/cyber-essentials/
- https://www.csa.gov.sg/cyber-trust/

Microsoft:

- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection-about?view=o365-worldwide
- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide
- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-simulations?view=o365-worldwide

CSA
SINGAPORE

Cyber Security Agency of Singapore

www.csa.gov.sg