

Attack Simulation Training

Simulating an attack within your organization, identifying vulnerable users giving them the correct training they need.

← → ↻ https://admin.microsof

Microsoft 365 admin center

Health

Admin centers

- Security
- Compliance
- Endpoint Manager
- Azure Active Directory
- Exchange
- SharePoint
- Teams
- All admin centers

Microsoft 365 Defender

- Learning hub
- Trials

Email & collaboration

- Investigations
- Explorer
- Submissions
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules

- Learning hub
- Trials

- Email & collaboration**
- Investigations
- Explorer
- Submissions
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules

Attack simulation training

- Overview
- Simulations
- Payloads
- Simulation automations
- Payload automations
- ...

Take note

i RBAC roles to access Attack Simulation Training should be assigned from Azure Active Directory. Details [here](#).

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

Click to go back (Alt+Left arrow), hold to see history

- Learning hub
- Trials
- Email & collaboration**
- Investigations
- Explorer
- Submissions
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules

Attack simulation training

Overview Simulations Payloads Simulation automations Payload automations ...

Take note
In order for Attack simulation training to have reporting capabilities, auditing needs to be enabled. [please see here for details](#)

A list of all your simulations and their status.



+ Launch a simulation

0 items Refresh Search Customize columns

Simulation Name	Type	Platform	Launch Date	End Date
-----------------	------	----------	-------------	----------

How to turn on Audit

Microsoft 365 admin center

Health

Admin centers

- Security
- Compliance
- Endpoint Manager
- Azure Active Directory
- Exchange
- SharePoint
- Teams
- All admin centers

Reports

Policies

Permissions

Trials

Solutions

- Catalog
- Audit
- Content search
- Communication compliance
- Data loss prevention
- eDiscovery
- Information governance

Audit

[Learn about audit](#) [Remove from navigation](#)

Search Audit retention policies



Start recording user and admin activity

Date and time range *

Start Sun Feb... 00:00

Activities

Show results for all activities

File, folder, or site

Add all or part of a file name, folder

End Sun Feb... 00:00

Users

Search

Search

Clear all

compliance

Your organization settings need to be updated. Do you want to continue?

Yes

No



Overview Simulations Payloads Simulation automations Payload automations ...

 In order for Attack simulation training to have reporting capabilities, auditing needs to be enabled. [please see here for details](#) 

A list of all your simulations and their status.

 Draft **0**  Scheduled **0**  In progress **0**  Completed **1**  Failed **0** Show excluded simulations

 Cancelled **0**

  Launch a simulation

1 item  Refresh

 Search

 Customize columns

Simulation Name	Type	Platform	Launch Date	End Date
Credential harvesting	Social Engineering	Email	2/20/2022, 2:23:08 PM	2/22/2022, 2:23:08 PM



Select Technique

Name Simulation

Select Payload

Target Users

Assign Training

Select end user notification

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...

Next

Save and close

Cancel



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

- Select Technique**
- Name Simulation
- Select Payload
- Target Users
- Assign Training
- Select end user notification

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

Next

Save and close

Cancel

- ✓ Select Technique
- Name Simulation**
- Select Payload
- Target Users
- Assign Training
- Select end user notification

Name Simulation

Simulation Name *

Description

Back




Next

Save and close

Cancel

Simulation > Create

- Select Technique
- Name Simulation
- Select Payload**
- Target Users
- Assign Training
- Select end user notification

 Send a test  Create a payload 1 of 106 selected  Filter

Payload name	Language	Click rate	Predicted Compro...	Simulations launch
Accounts payable document rev...	English	0	20	0
Address Incorrect	Other	0	20	0
<input checked="" type="checkbox"/> American express password reset	English	0	45	0
American Express phone numbe...	English	0	37	0
Capital One bank account locked	English	0	36	0

Back Next Save and close Cancel

Send Test Email



Clicking Confirm below will send this payload to the currently logged in user for formatting validation. It will not be included in any simulation reporting and will not work as part of an end to end simulation scenario.

Confirm

Cancel

Send Test Email



Test email successfully sent, please check your mailbox in a few minutes.



New message



Delete



Archive



Junk



Sweep



Move to



Categorize



Snooze



Folders

Inbox 2

Drafts

Sent Items

Deleted Items

Junk Email

Archive

Notes

Conversation His...



Inbox



Filter



American Express

[EXT] Confirmation: Your One-Ti... 11:53 AM

Let us know if you did not make this reques...

Last week



Microsoft Audio Conferencing

You now have Audio Conferencin... Tue 2/15

- You now have Audio Conferencing for Mic...

You recently called us and requested that we send a One-Time Password so that you could proceed with a transaction on your account.

If you requested this One-Time Password, no further action is required.

If you did not request this One-Time Password, [click here](#) to secure your account immediately

Thank you for your Card Membership,

American Express Customer Care

Select Technique

Name Simulation

Select Payload

Target Users

Assign Training

Select end user notification



Send a test + Create a payload

1 of 106 selected



Payload name	Language	Click rate	Predicted Compro...	Simulatio
Accounts payable document rev...	English	0	20	0
Address Incorrect	Other	0	20	0
<input checked="" type="checkbox"/> American express password reset	English	0	45	0
American Express phone numbe...	English	0	37	0
Capital One bank account locked	English	0	36	0

Back

Next

Save and close

Include the target users for this simulation



Select Technique

Name Simulation

Select Payload

Target Users

Assign Training

Select end user notification

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



+ Add Users



Import

0 user(s) or group(s)



Se

Back

Next

Save and close

C

Search for Users or Groups



Enter User or Group Name. Type at least 3 characters and hit enter to search.

Filter Users by categories

Suggested User Groups (0)

All Suggested User Groups

Users not targeted by a simulation in the last three months


Repeat offenders

User tags (0)

Add 0 User(s)

Clear All Selections

Search for Users or Groups

 alexw@m365x62234438.onmicrosoft.com

Add Filters

User List

Selected (1/1) User(s)

<input checked="" type="checkbox"/>	Name ↑	Email
<input checked="" type="checkbox"/>	Alex Wilber	AlexW@m365x62234438.OnMicrosoft.com

Add 1 User(s)

Clear All Selections



- Select Technique
- Name Simulation
- Select Payload
- Target Users**
- Assign Training
- Select end user notification

- Include all users in my organization
- Include only specific users and groups

+ Add Users ↑ Import

1 user(s) or group(s) 🔍 Search

📄 1 user(s) or group(s) with valid and unique email addresses have been added.

🔄 Refresh

1 ite

Name	Email	Job Title	Type	Delete
Alex Wilber	AlexW@M365x62234438.On...	Marketing Assistant	User	✕

Back

Next

Save and close

Can

- ✓ Select Technique
- ✓ Name Simulation
- ✓ Select Payload
- ✓ Target Users
- Assign Training**
- Select end user notification

Preferences

Select training content preference

Microsoft training experience (Recommended) ▾

Redirect to a Custom URL

No training

Microsoft training experience (Recommended) [review these selections in the next step. Learn more](#)

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 ▾

Back

Next

Save and close

Cancel

Number of days persons should be trained by

- ✓ Select Technique
- ✓ Name Simulation
- ✓ Select Payload
- ✓ Target Users
- Assign Training**
- Landing page

Select landing page layout *

Microsoft Landing Page Template 1

Edit layout

Add logo

Select a file with extension .png, .jpeg, .gif

[Browse](#) [Remove](#)

Payload Indicators

Add payload indicators to email. They help users to learn how to identify the phishing email.

 [Open preview panel](#)

[Back](#)

[Next](#)

[Save and close](#)

[Cancel](#)



close



Company logo

`\${DisplayName}`, you were just **phished** by your security team.

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

Rather than stealing your login credentials like a cyber criminal, we have redirected you to this educational page instead and assigned you some training courses.





- ✓ Select Technique
- ✓ Name Simulation
- ✓ Select Payload
- ✓ Target Users
- ✓ Assign Training

Select end user notification

Select end user notification preferences for this simulation.

- Do not deliver notifications ⓘ None of the notifications will be delivered to the user
- Microsoft default notification (recommended) ⓘ
- Customised end user notifications ⓘ

Select default language *

English

Notifications	Language	Type
Microsoft default positive reinf...	English, German.. +10	Positive reforcem...

Do not deliver

Deliver after campaign ends

Deliver during campaign

Deliver after campaign ...

Back

Next

Save and close

Cancel

- ✓ Select Technique
- ✓ Name Simulation
- ✓ Select Payload
- ✓ Target Users
- ✓ Assign Training
- ✓ Select end user notification

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 *

Your simulation will end on 2/22/2022


Enable region aware timezone delivery

Back Next Save and close Cancel



Review Simulation

Review your Simulation information below before you launch it. You currently have it scheduled to be launched on 2/20/2022 at 2:20:40 PM. It will end on 2/22/2022 at 2:20:40 PM.

 **Send a test**

Delivery Platform

Email

Technique

CredentialHarvesting

Name

Credential harvesting

[Edit Name](#)

Description

Credential harvesting

[Edit Description](#)



Back

Submit

Save and close

Wait until it has been successfully submitted



- ✔ Select Technique
- ✔ Name Simulation
- ✔ Select Payload
- ✔ Target Users
- ✔ Assign Training
- ✔ Select end user notification

✔ Simulation has been scheduled for launch

Your simulation Credential harvesting will be sent on 2/20/2022 at 2:23:08 PM to 1 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 >](#)

Done

Email & collaboration

- Investigations
- Explorer
- Submissions
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules
- Reports
- Audit

Attack simulation training

Overview **Simulations** Payloads Simulation automations Payload automations ...

(i) In order for Attack simulation training to have reporting capabilities, auditing needs to be enabled. [please see here for details](#) ✕

A list of all your simulations and their status.



[+ Launch a simulation](#) 1 item [Refresh](#) [Customize columns](#)

Simulation Name	Type	Platform	Launch Date	End Date
Credential harvesting	Social Engineering	Email	2/20/2022, 2:23:08 PM	2/22/2022, 2:23:08 PM

Platform	Launch Date	End Date	Actual Compromise Ra...	Predicted Compromise...	Created
Email	2/20/2022, 2:23:08 PM	2/22/2022, 2:23:08 PM	0	45	admin@

Enter the profile for Alex to see the simulated email snet

The screenshot shows the Microsoft Outlook web interface. At the top, there is a blue header bar with the Outlook logo, a search bar, and various utility icons like Teams call, chat, calendar, and settings. Below the header, a yellow notification banner states: "Your browser supports setting Outlook on the Web as the default email handler. Try it now Ask again later Don't show again".

The main interface is divided into three sections:

- Left sidebar (Folders):** Contains a list of folders: Mail, Folders, Inbox (with a count of 2), Drafts, Sent Items, Deleted Items, Junk Email, Archive, Notes, and Conversation His... There is also a "New folder" link at the bottom.
- Center pane (Inbox):** Shows the "Inbox" folder with a "Filter" dropdown. It contains two email items:
 - American Express:** Subject "[EXT] Confirmation: Your On...", received at 2:24 PM. Preview text: "Let us know if you did not make this re...".
 - Microsoft Audio Conferencing:** Subject "You now have Audio Confere...", received on Tue 2/15. Preview text: "- You now have Audio Conferencing for...".
- Right pane:** Displays a large graphic of two envelopes (one blue, one grey) with the text: "Select an item to read" and "Nothing is selected".

You recently called us and requested that we send a One-Time Password so that you could proceed with a transaction on your account.

If you requested this One-Time Password,
no further action is required.

If you did not ~~request~~ request this One-Time Password, [click here](#) to secure your account immediately

Thank you for your Card Membership,

American Express Customer Care

[PRIVACY STATEMENT](#) | [UPDATE YOUR EMAIL](#)

Your account information is included above to help you recognize this as a customer care e-mail from American Express. To learn more about e-mail security or report a suspicious e-mail, please visit us at americanexpress.com/phishing. We kindly ask you not to reply to this e-mail but instead contact us via [Customer Care](#).

© 2020 American Express. All rights reserved.

PWDENDMCVPW0005

If you would like to unsubscribe and stop receiving these emails [click here](#).

[Reply](#) | [Forward](#)



Sign in

Next

No account? [Create one!](#)

[Can't access your account?](#)



alexw@M365x62234438.onmicrosoft.com



Enter password

Back

Sign in

[Forgot my password](#)

English

Alex Wilber, you were just **phished** by your security team.

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

Rather than stealing your login credentials like a cyber criminal, we have redirected you to this educational page instead and assigned you some training courses.



► Tips to identify the phishing message

DISCLAIMER: The message you just clicked on is a phishing message simulation. It is not a real message from the owner of the trademark or logo featured in the simulation. The trademarks and logos featured in the simulation may be the property of their respective owners and are in no way associated or affiliated with the simulation, nor have the owners of such trademarks and logos authorized, sponsored or endorsed the use of such trademarks and logos in the simulation.

From: American Express <alerts@americanexpresps.com>

To: Alex Wilber

Subject: [EXT] Confirmation: Your One-Time Password



**AMERICAN
EXPRESS**

Dear CARD MEMBER, **Did you recently request a One-Time Password?**

You recently called us and requested that we send a One-Time Password so that you could proceed with a transaction on your account.

If you requested this One-Time Password,
no further action is required.

If you did not request this One-Time Password, [click here](#) to secure your account immediately

Thank you for your Card Membership,


American Express Customer Care

DON'T *live life* WITHOUT IT™

PRIVACY STATEMENT | UPDATE YOUR EMAIL

Your account information is included above to help you recognize this as a customer care e-mail from American Express. To learn more about e-mail security or report a suspicious e-mail, please visit us at americanexpress.com/phishing. We kindly ask you not to reply to this e-mail but instead contact us via Customer Care.

AMERICAN
EXPRESS

We've assigned you  some training to learn how to avoid this in the future.

Go to training

Add to calendar

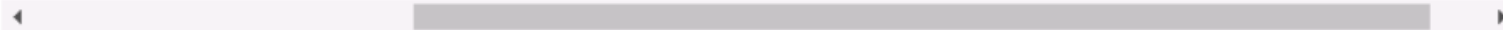


Web Phishing

ou? Can you recognize web phishing and, more importantly do you know
to avoid being hooked? Find out by trying this scenario.

Start

p with Microsoft





Go through the whole video and sign out of Alex

← → ↻ 🔒 https://security.microsoft.com/attacksimulator?viewid=overview

Microsoft 365 Defender Search

- Investigations
- Explorer
- Submissions
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules
- Reports
- Audit

[View all simulations](#) [Launch a simulation](#)

Behavior impact on compromise rate

0 users less susceptible to phishing

0% better than predicted rate

Category	Rate
Actual Compromised Rate	0%
Predicted Compromised Rate	48%

[View simulations and training efficacy report](#)

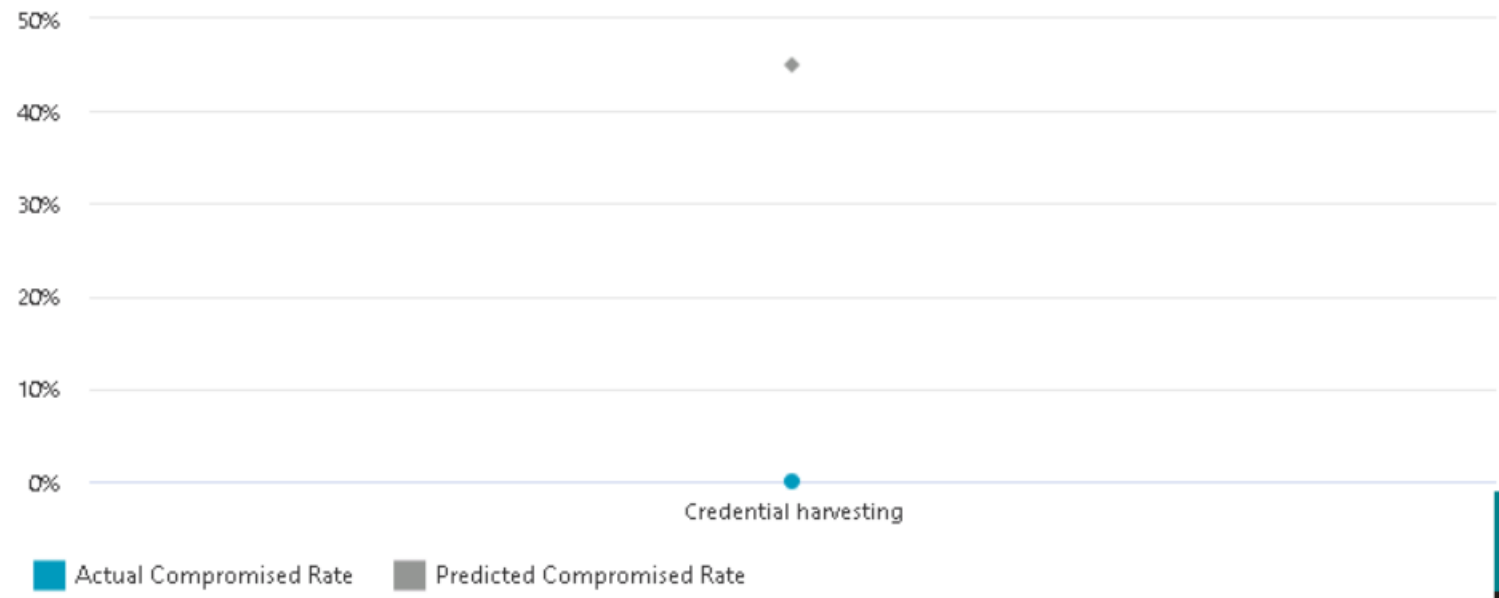
Simulation coverage

Back in Overview attack simulation page scroll down to click on the above link

- Home
 - Incidents & alerts
 - Hunting
 - Action center
 - Threat analytics
 - Secure score
 - Learning hub
 - Trials
- Email & collaboration**
- Investigations

Training Efficacy User Coverage Training Completion Repeat offenders

Showing last 1 Simulations



Export Refresh

1 item

Search

Customize columns

Simulation Name	Simulation Techni...	Simulation Tactics	Predicted Compromised Rate	Actual Compromised Rate	Tota
Credential harvesting	CredentialHarvesting	Social	45		1

Total Users Targeted

Count of Clicked Users

1

Attack simulation training > Attack Simulation Report

Training Efficacy

User Coverage

Training Completion

Repeat offenders

Simulated users



■ Simulated users ■ Non-simulated users

Simulated users	Non-simulated users
2	9

↓ Export Refresh

2 items

Search

Customize columns

User Name	Email Address	Included in S...	Date of L...	Last Simulation Re...	Count of Clicked	Count of Com...
MOD Administr...	admin@M365x62234438.On...	1	Feb 22, 20...	Passed	0	0
Alex Wilber	AlexW@M365x62234438.On...		Feb 22, 20...	Passed		



Attack simulation training > Attack Simulation Report

Training Efficacy User Coverage **Training Completion** Repeat offenders

Status

Completed In progress Incomplete

Completed In progress Incomplete
0 0 0

Export Refresh

0 items

Search

Customize columns Filter

User Name Email Address Included ... Date of L... Last Simulation Re... Name of Most... Date Completed All Trainings

No data available

Search



MA

Training Efficacy

User Coverage

Training Completion

Repeat offenders



All Credential Harvest Malware Attachment Link in Attachment Link to Malware Drive-by URL

[Export](#) [Refresh](#)

0 items

Search

[Customize columns](#)

[Filter](#)

Help icon
Chat icon

User

Repeat Count

Simulation Types

Simulations

No data available

Trials

Email & collaboration ^

Investigations

Explorer

Submissions

Review

Campaigns

Threat tracker

Exchange message trace


Attack simulation training

Policies & rules

Attack simulation training

[Overview](#)[Simulations](#)[Payloads](#)[Simulation automations](#)[Payload automations](#)

...

 RBAC roles to access Attack Simulation Training should be assigned from Azure Active Directory. Details [here](#).

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

Recent Simulations

Simulation name	Type	Status
Stealing credentials	Credential Harvest	In progress
Credential harvesting	Credential Harvest	Completed

On the overview page click on the simulation



Credential harvesting

Social Engineering . Credential Harvest

Delivery Platform : Email

Credential harvesting	Status	Launch Date	End Date	Training due date	Target users
	✔ Completed	2/20/2022, 2:23:08 PM	2/22/2022, 2:23:08 PM	3/24/2022, 2:23:08 PM	1



Simulation Impact

1 of 1 users compromised by entering credentials

Compromised



■ Entered credentials ■ Did not enter credentials

Payloads

1 payload used

Payload name	Type
American express password reset	Global

Keep scrolling down to see the data. At the end notice that you are given recommended actions.