PLAYBOOK FOR THE CONDUCT OF PHISHING SIMULATION EXERCISES

A collaboration between

CSA SINGAPORE
Cyber Security Agency of Singapore

Google

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 Google Workspace email management services. 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 cyber criminals to fraudulently obtain sensitive information such as account credentials, personal information, or financial details by impersonating a legitimate individual or reputable organisation in digital communications. 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 in the victim's name. 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. 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 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 Google Workspace

There are two methods to execute phishing training exercises with Gmail:

- Deliver messages through Gmail API (Recommended)
- Deliver messages through traditional means (SMTP), and add spam bypasses and disabling safety settings (Proceed with Caution)

Each of the two strategies has its own advantages and disadvantages. Google generally recommends the second option, which involves delivering messages through the Gmail API.

Please see the sections below for a detailed explanation of the pros and cons of each strategy, as well as implementation strategies.

7.1 Gmail API phishing exercises

This strategy involves delivering (or rather, "inserting") messages directly into recipients' mailboxes using Gmail API.

Since the messages are not being delivered through traditional SMTP methods, the spam filter will not evaluate them and will not issue any spam/phishing verdicts or banners.

This route is optimal from a security standpoint but requires some additional effort to implement the exercise.

Pros	• Messages will appear in recipients' mailboxes and will automatically bypass spam and phishing filtering • No need for spam bypasses or special rules • No need to deactivate phishing protections - users remain safe and secure throughout the exercise
Cons	• Requires API authorisation (having an account with permissions to insert messages into domain users' mailboxes) • Requires technical skills to execute Gmail API calls • Gmail rules configured in Admin console will not be triggered • User mailbox filters will not be triggered

7.1.1 Implementation of Gmail API phishing exercises:

Documentation for implementing message insertion via Gmail API is documented in the Gmail for Developers portal.

Administrators will then use this API method to insert messages into each recipient's mailbox.

7.2 SMTP phishing exercises

SMTP is a standard/protocol used to deliver electronic mail and is the primary means by which mail is transported between senders and recipients.

SMTP phishing tests are convenient, in the sense that traditional email delivery mechanisms are used; sender sends the message and recipient receives the message.

This solution requires a number of domain setting changes, including deactivation of features that normally protect users from spam and phishing.

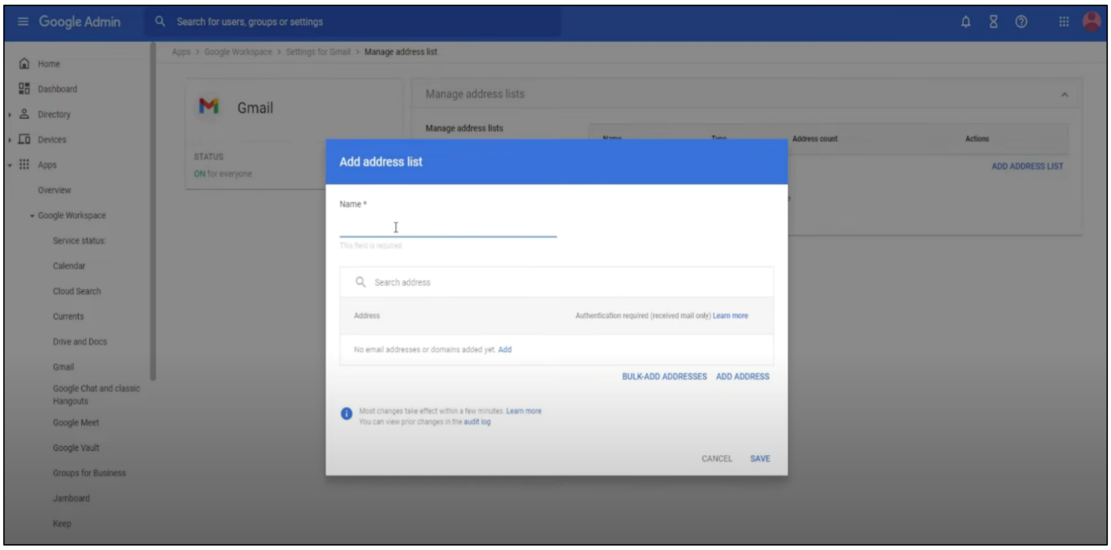
Pros	• Message delivery doesn't require any coding or architectural changes • User spam markings are reported through the Security Investigation Tool
Cons	• Spam bypasses are required to maximize the likelihood of delivery • Some messages may still get rejected if they contain decisively malicious content, despite the bypasses/allowlists • Some messages may still get classified as phishing • Safety settings may need to be deactivated in the recipients' OUs to reduce likelihood of spam/phishing banners • Recipients will lose protection from real phishing emails as long as these settings are disabled • Some warning/danger banners may show up despite these Safety settings being disabled and spam bypasses being configured

In conclusion, this approach is "easy" but is riddled with security-related compromises. Administrators must proceed with cautions with this option considering the potential security risks associated with the production users.

7.2.1 Implementation of SMTP phishing exercises:

If the administrator wishes to pursue this route, the following settings should be changed:

1. Add sending IPs to the "Email whitelist" rule in Admin console (Help Center)



Add address list

Name *

This field is required

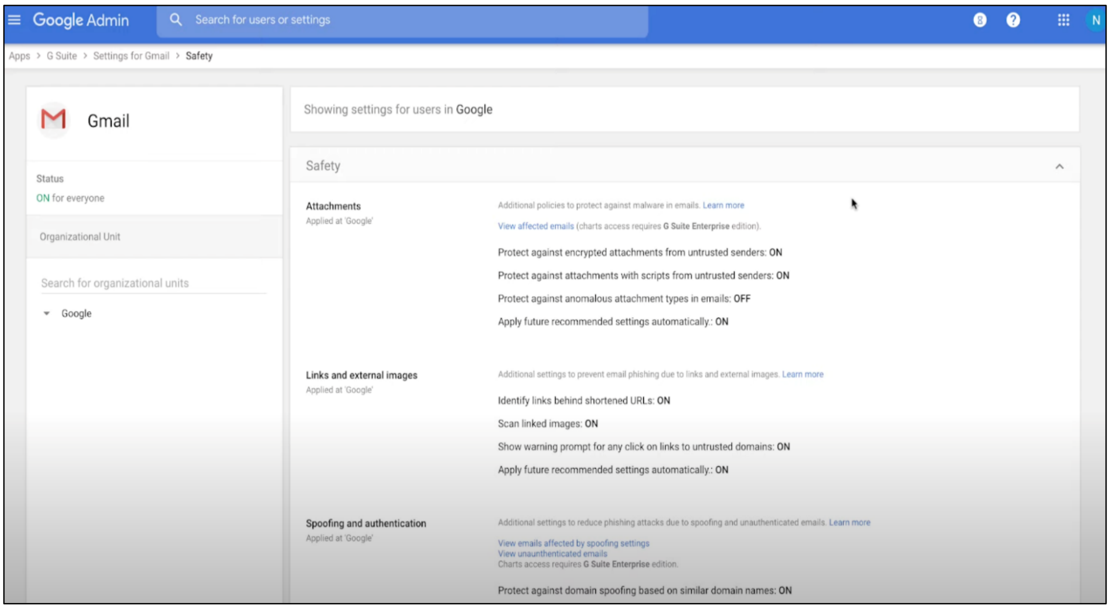
Address — Authentication required (received mail only) Learn more

No email addresses or domains added yet. Add

Most changes take effect within a few minutes. Learn more
You can view prior changes in the audit log

- Do not use the Approved Senders List (ASL) for this purpose; ASL will override spam verdicts, but will deliver the message with a grey banner stating that the message was not marked as spam due to organisational settings. Use IP-based allow listing as described above to avoid the grey banner. To understand what Gmail banner looks like, refer to the Blog

2. Disable 'Safety' settings in Admin console (Help Center)


Google Admin
Search for users or settings
Apps > G Suite > Settings for Gmail > Safety
Gmail
Status
ON for everyone
Organizational Unit
Search for organizational units
Google
Safety

Showing settings for users in Google

Attachments
Applied at 'Google'

Additional policies to protect against malware in emails. Learn more
View affected emails (charts access requires G Suite Enterprise edition).

Protect against encrypted attachments from untrusted senders: ON
Protect against attachments with scripts from untrusted senders: ON
Protect against anomalous attachment types in emails: OFF
Apply future recommended settings automatically.: ON

Links and external images
Applied at 'Google'

Additional settings to prevent email phishing due to links and external images. Learn more

Identify links behind shortened URLs: ON
Scan linked images: ON
Show warning prompt for any click on links to untrusted domains: ON
Apply future recommended settings automatically.: ON

Spoofing and authentication
Applied at 'Google'

Additional settings to reduce phishing attacks due to spoofing and unauthenticated emails. Learn more
View emails affected by spoofing settings
View unauthenticated emails
Charts access requires G Suite Enterprise edition.

Protect against domain spoofing based on similar domain names: ON

These settings control the consequences that get applied to messages which exhibit phishing signals; deactivating these settings exposes users to certain types of phishing attacks but reduces the risk of banners appearing on phishing training messages.

Deliver your simulated phishing email to users through your phishing simulation service provider after disabling the security settings.

NOTE: Sending phishing emails, even as part of a simulated test, from a company mailbox without proper authorisation may violate laws and ethical standards. It can lead to legal consequences and damage the organisation's reputation.

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 includes 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 recipients who entered sensitive information into phishing websites.
- **Reporting rate**: The percentage of recipients who reported suspicious emails to the IT or security team.

The Google Workspace Security Investigation Tool (SIT) is the primary tool for evaluating the effectiveness of user behaviour on the phishing simulation. **Security Investigation Tool (SIT)** is an admin tool that lives in the Google Workspace Security Center (GSC).

NOTE: To use Security Investigation Tool, you must be a super administrator with a premium Google Workspace edition - such as Enterprise Plus or Education Plus.

The tool can be found in admin console in the following location:

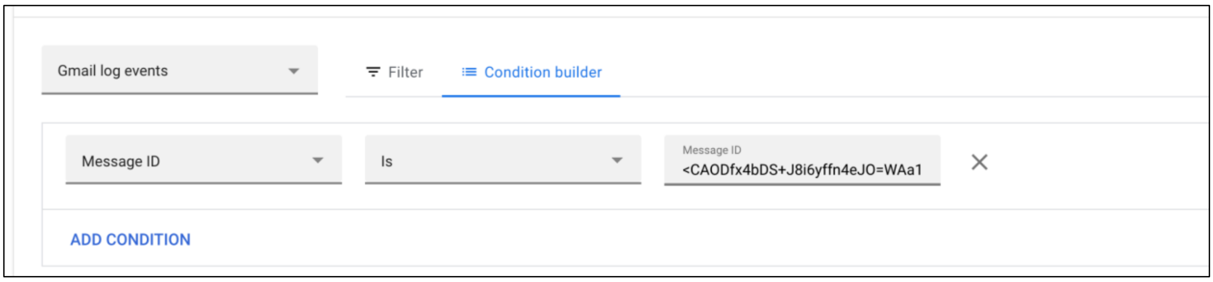
Main "hamburger" menu > Security > Security center > Investigation tool

To calculate the user response rate on phishing emails, an administrator must combine search criteria in the SIT and/or choose to export the results to a Google Sheet for advanced reporting purposes, steps are documented in below examples.

Step 1 - Search Gmail messages

Gmail log events is the primary audit log we will use for the evaluation because it provides the most comprehensive and detailed view of user activity in Gmail. The log includes information about all user actions, including sending and receiving emails, attachment view or download, and accessing and modifying email settings, delete or move to spam etc. This information can be used to identify potential security risks and to evaluate the effectiveness. Additionally, the log can be used to track user behaviour over time, which can be helpful for identifying trends and patterns.

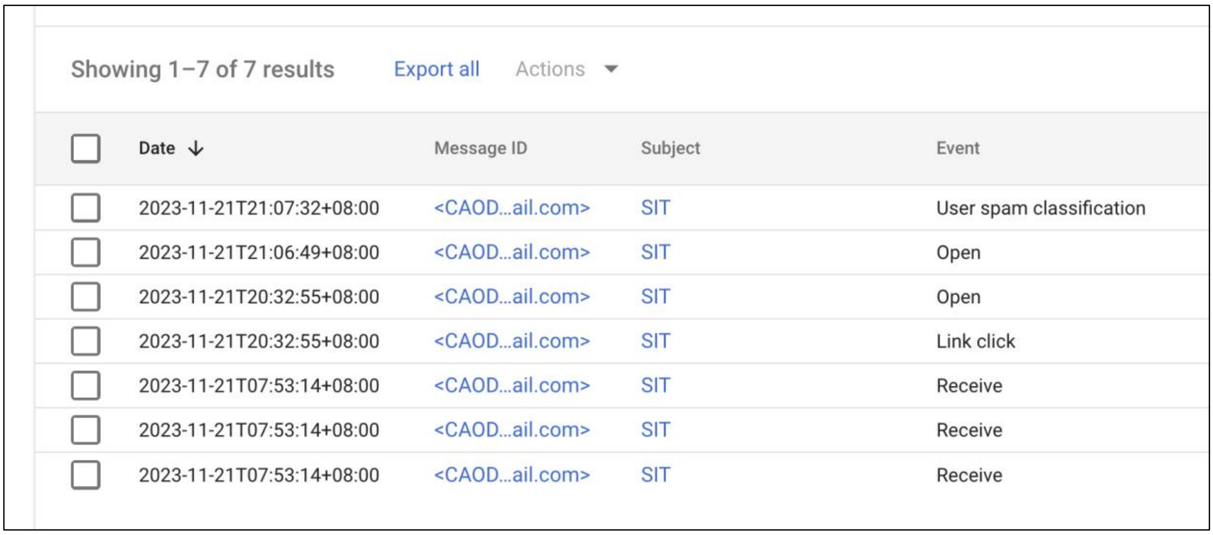
Open the SIT, and choose **Gmail log events**, in this example we search specific Gmail messages via its message ID, administrator could enter various search criteria to scope the search.



Gmail log events

Message ID | Is | Message ID: <CAODfx4bDS+J8i6yffn4eJO=WAa1

SIT will then return all Gmail log events that are relevant to the email you are searching for.

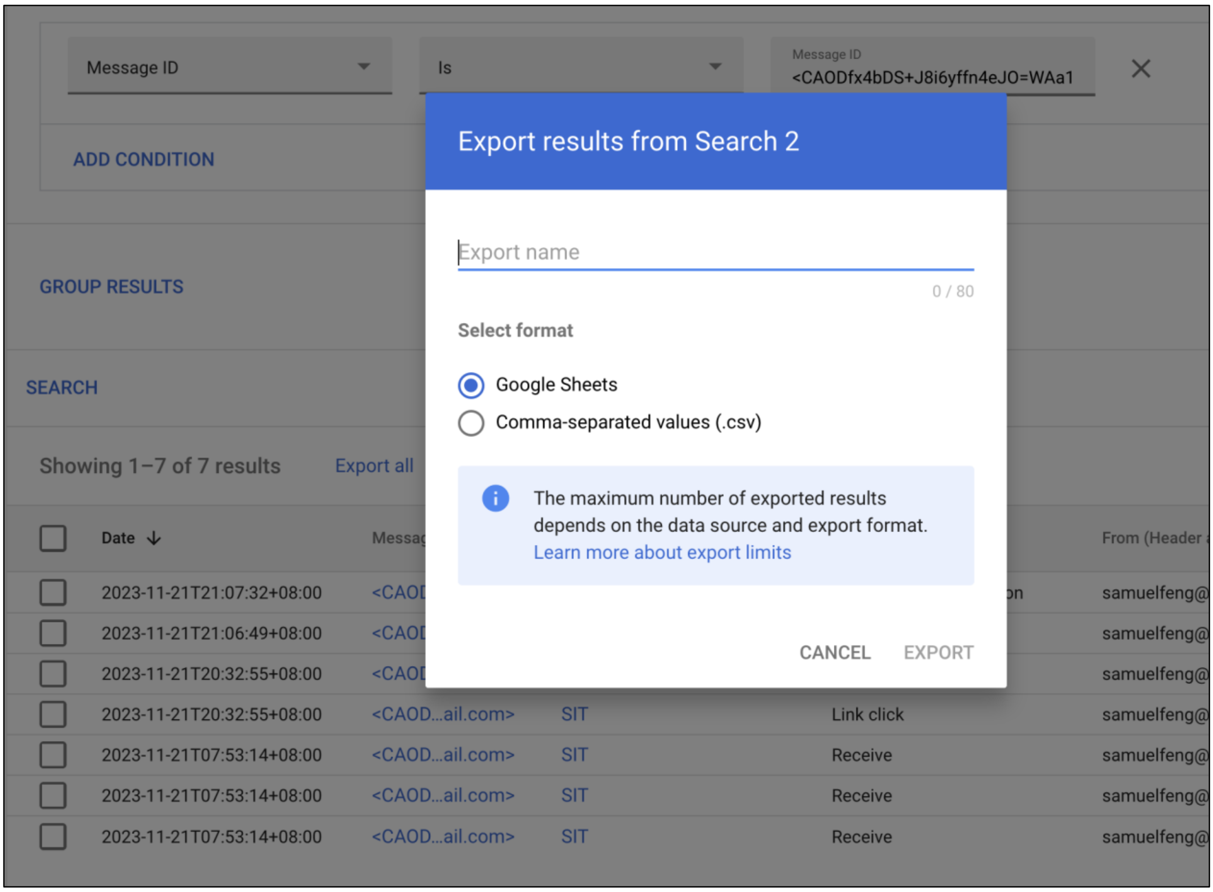


Showing 1–7 of 7 results Export all Actions ▾

□	Date ↓	Message ID	Subject	Event
□	2023-11-21T21:07:32+08:00	<CAOD...ail.com>	SIT	User spam classification
□	2023-11-21T21:06:49+08:00	<CAOD...ail.com>	SIT	Open
□	2023-11-21T20:32:55+08:00	<CAOD...ail.com>	SIT	Open
□	2023-11-21T20:32:55+08:00	<CAOD...ail.com>	SIT	Link click
□	2023-11-21T07:53:14+08:00	<CAOD...ail.com>	SIT	Receive
□	2023-11-21T07:53:14+08:00	<CAOD...ail.com>	SIT	Receive
□	2023-11-21T07:53:14+08:00	<CAOD...ail.com>	SIT	Receive

Step 2 - Export to Google Sheet for advance analysis

Choose **Export all** button to export all results to Google Sheet for further analysis.



Message ID ▾ Is ▾ Message ID <CAODfx4bDS+J8i6yffn4eJO=WAa1 ✕

ADD CONDITION

GROUP RESULTS

SEARCH

Showing 1–7 of 7 results Export all

Export results from Search 2

Export name

0 / 80

Select format

● Google Sheets

○ Comma-separated values (.csv)

The maximum number of exported results depends on the data source and export format. Learn more about export limits

CANCEL EXPORT

□	Date ↓	Messag			From (Header
□	2023-11-21T21:07:32+08:00	<CAOD		on	samuelfeng@
□	2023-11-21T21:06:49+08:00	<CAOD			samuelfeng@
□	2023-11-21T20:32:55+08:00	<CAOD			samuelfeng@
□	2023-11-21T20:32:55+08:00	<CAOD...ail.com>	SIT	Link click	samuelfeng@
□	2023-11-21T07:53:14+08:00	<CAOD...ail.com>	SIT	Receive	samuelfeng@
□	2023-11-21T07:53:14+08:00	<CAOD...ail.com>	SIT	Receive	samuelfeng@
□	2023-11-21T07:53:14+08:00	<CAOD...ail.com>	SIT	Receive	samuelfeng@

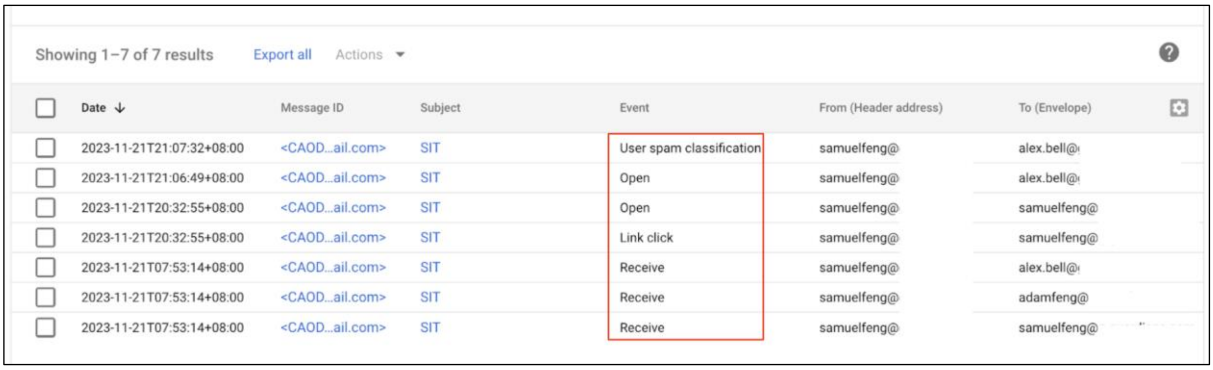
Step 3 - Choose proper event to assess the result

To evaluate the effectiveness of this email phishing campaign, you will need to focus on the appropriate event. As a minimum requirement, we suggest that the administrator assess the **email click rate, conversion rate and reporting rate**.

Rate calculation

The following metrics are recommended for administrators to evaluate:

- **Total number of emails sent:** The total number of emails sent out in the campaign is represented by this value. You can use the filtering condition Event = ***Receive*** to count the number of messages.
- **Number of emails open:** The number of emails that were actually clicked on by recipients is represented by the Event = ***Open*** value.
- **Email link click rate:** The percentage of recipients who tapped on the phishing links. Calculated by dividing the number of links clicked by the total number of emails open. You can use the Event = ***Link Click*** for this calculation
- **Reporting rate:** Calculated by dividing the number of user report spam classification by the number of emails open. You can use the Event = ***User spam classification*** for this calculation
- **Conversion rate:** There are two ways to calculate the conversion rate. Administrators can choose the most appropriate method depending on the situation.
  - **Basic**: This is same as the Email Click rate, under the Zero-Trust principle, a machine is considered compromised as long as a user clicks on a phishing link in an email.
  - **Advance**: Additional setup is required on the endpoint. Please refer to the next chapter for details.



Showing 1–7 of 7 results Export all Actions ▾

□	Date ↓	Message ID	Subject	Event	From (Header address)	To (Envelope)
□	2023-11-21T21:07:32+08:00	<CAOD...ail.com>	SIT	User spam classification	samuelfeng@	alex.bell@
□	2023-11-21T21:06:49+08:00	<CAOD...ail.com>	SIT	Open	samuelfeng@	alex.bell@
□	2023-11-21T20:32:55+08:00	<CAOD...ail.com>	SIT	Open	samuelfeng@	samuelfeng@
□	2023-11-21T20:32:55+08:00	<CAOD...ail.com>	SIT	Link click	samuelfeng@	samuelfeng@
□	2023-11-21T07:53:14+08:00	<CAOD...ail.com>	SIT	Receive	samuelfeng@	alex.bell@
□	2023-11-21T07:53:14+08:00	<CAOD...ail.com>	SIT	Receive	samuelfeng@	adamfeng@
□	2023-11-21T07:53:14+08:00	<CAOD...ail.com>	SIT	Receive	samuelfeng@	samuelfeng@

In this example, if you had sent out 3 emails (3 ***Receive*** event) and 2 of them were ***Opened,*** 1 of them was clicked on (1 ***Link Click***), 1 of them was reported phishing (1 ***User spam classification***), in this case, your email link click rate would be 50%, conversion rate (basic) would be 50%, reporting rate is 50%.

You can use this metric to track the performance of your email campaigns and see how effective they are at driving traffic to your website or landing pages.

8.2 Conversion Rate (Advance)

To help organisations enhance account password protections, Google Workspace has introduced Password Alert that integrates within BeyondCorp Threat and Data Protection. BeyondCorp Threat and Data Protection help to protect Google Workspace users from phishing attacks by detecting when they enter their Google passwords into any websites other than the Google sign-in page. It also provides administrators with auditing and reporting capabilities to help them identify and address potential phishing threats.

To get the most accurate conversion rate (when a user enters company information on the phishing website - such as account name, password), administrators can leverage the Password Alert Reporting and auditing function to calculate the rate after a phishing campaign.

To set this up, refer to the detailed deployment guide here.

High level deployment steps:

1. Setup Chrome Management by Google Workspace
2. Setup Chrome browser policies

3. (Optional) Enforce only company managed Chrome can access Google Workspace apps with Google Workspace Context-Aware Access
4. Enable BeyondCorp Enterprise service (additional license required)
5. Setup activity alert rules, For details: View alert details
6. View the audit log and security reports, and perform investigations, especially check the Chrome high risk users report

8.3 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.

8.4 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. Participants should be informed as soon as possible when they have clicked on a simulated phishing message, so that they are aware of the events leading up to the clicking on the simulated phishing message. 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 support 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.

8.5 Ensuring Phishing Simulations are up-to-date

The dynamic nature of the threat landscape means cybercriminals continually develop new phishing tactics. To increase the effectiveness and realism of phishing simulations, the scenarios should be updated to closely to align with current phishing trends and real-word 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). In this way, organisations will be able to provide a comprehensive exercise that prepares employees to recognise and respond to ever evolving phishing threats.

8.6 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/

Google:

- Advance Gmail Security
- Security Investigation Tool
- Protect Chrome Users with BeyondCorp Enterprise
- Chrome high risk users report
- Follow the security checklist if you feel that an account may be compromised

CSA SINGAPORE

Cyber Security Agency of Singapore

www.csa.gov.sg