Google Workspace Whitelisting

There are several options in G Suite that can be adjusted to improve the Phishing Simulation Experience.

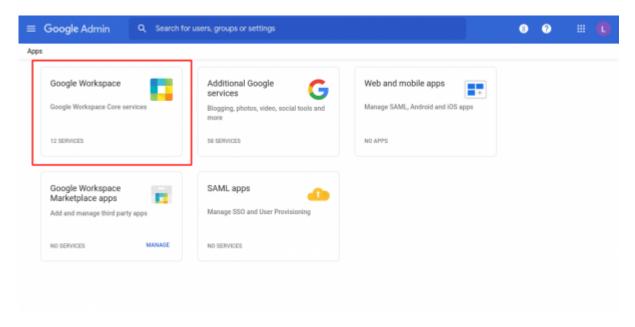
Whitelisting emails from LUCY.

Whitelist LUCY to receive emails from the appliance.

Log into admin.google.com, go to "Apps":

≡ Google Admin 9,	Search for users, groups or settings			48 ®	
 ▲ 	& Users Manage	Billing Manager subscriptions and billing ~	Froduct updates information about new features and improvements		
5 2 2	RA 🔄	Q Alerts view notifications about potential issues ∨	All. Groups Create groups for mailing lists and applying policies		
0	Delete a uner Update a uner's name or email Create an alternate email address (email alias)	LD Devices interage devices and secure your regarization's data	Account settings Manage your organization's profile and preferences		
	Create an analysist privat adjuncted (create analy	Secarity Configure security settings, and view alerts and entryfics	n Reports Maniforysur organization's user and admin activity		
	© Benains ~	Rules Interaction to set alerts and actions	Admin roles Ansign tokes to control permissions for the Admin Canada		
	Apps Adamage web and mobile app access and settings	O Support Connect with the Help Assistant			
	egg Ceganizational units Organiza users into units for applying policies				
	Buildings and resources Interage and resources Interage and monitor your buildings, rooms, and resources				

Navigate to "Google Workspace":



Go to "Gmail":

≡ Google Admin	Q Search	for users, groups or settings	3	0		
Apps > Google Workspace						
G Google		Showing status for apps in all organizational units		AL	DD SERVICE	ES
Workspace		Service Status				
		Calendar ON for everyone				1
All users in this account		Cloud Search ON for everyone				
Groups	~	Currents ON for everyone				
Organizational Units	^	Children Drive and Doos ON for everyone				
Search for organizational units	— I	Gmail ON for everyone				
		Google Chat and classic Hangouts ON for everyone		1	Learn more	
		Google Meet ON for everyone				
		Groups for Business ON for everyone				
		🗌 🤳 Jemboard ON for everyone				
		CN for everyone				
		Sites ON for everyone				
		Rows per page: 50 v	IC Page	1 of 1 <	>	

Choose the "Spam, phishing, and malware" at the very bottom of the list:

= Google Adr			480	
Alles > 0000	ple vitorlespace > dettings for tanail			_
	M Gmail	Safety Configure email and spen safety Nettures	ř	
•	Status ON for everyone	Setup Cardgare setup features	~	
		End User Access Configure end user access features	÷	
		Spars, Phishing and Malware Cardigare span, phohing and individe features	~	
		Compliance Configure compliance features	×	
		Routing Centigure routing testures	~	

Add LUCY IPv4 to "Email Whitelist". Click "Save"

Apps > 6	Google Workspace + Settings for Graall + Spare, phishing, and	Smalware	
	M Gmail	Showing settings for users in	
	Status	Sparn, phishing, and malware	^
	ON for everyone bigentrational Unit	Erzail whitelist Applied at (double-ver/21.com)	An email obtaining as inder?? Appropriate monitoring you went your severt to reactive amation. Must see them these it? addresses should not be marked as speen, in order to that full adversarial of information and the marked and the control of the second and the second and the second adversarial of the second adversarial to the second adversarial to the second adversarial of the second adversarial to the s
	Search for organizational units		Enter the iP addresses for your enail whitelist
			Imparts-street scattering and control in a few strendard, calar's more Total charges they effect in a few strendard, calar's more You cale rate prior charges in the Audit lag
			1 unsaved change CANCEL SAVE
		Enhanced pre-delivery message scanning apprecial consistences 20 cost	Lawn many Enables improved detection of suspicious content prior to delivery: 6N
		Inbound galeway	If you are verial pervays to solve incoming entail, pieces when them to response spann handling Learn more forcable CM

As the result of steps above, G Suite will not reject email messages from LUCY host, however, if you do not want them to be considered as spam, please do some additional steps:

Go to "Inbound Gateway" configuration on the same menu.

Spam, phishing, and malware						^
Email whitelist Applied at a	spam. In order to take ful	I advantage of 0 I should be add	Smail's spam filtering ed to Inbound Gatewa		ification result	these IP addresses should not be marked as ts, IP addresses of your mail servers that are
Enhanced pre-delivery message scanning Applied at	Learn more Enables improved det	lection of sus	picious content pri	or to delivery: ON		
Inbound gateway	If you use email gateway Enable: ON	s to route incom	ning email, piease ente	r them here to improve spam h	andling Learn	more
Spam	Description	Status	Source	Actions	ID	Values
	whitelist	Enabled	Locally applied	Edit - Disable - Delete	-	Aggressive spam filtering: OFF Bypass internal senders: ON Bypass approved senders: ON Quarantine message: OFF
						ADD ANOTHER RULE
	Most changes take You can view prior		minutes. Learn more Audit log			
Blocked senders	Block or approve spe	cific senders l	based on email add	fress or domain.		CONFIGURE
	Most changes take You can view prior		minutes. Learn more Audit log			

- Add LUCY IPv4.
- Activate Message Tagging.
- Add a random set of symbols to the Regular Expression field. Only emails with a header like this
 expression will be considered as spam.
- Check "Disable Gmail spam evaluation on mail from this gateway; only use header value".
- Click "Save"

Inbound gateway	If you use email gateways to route incorning email, please enter them here to improve spam handling Learn more
	C Enable
	1. Gateway IPs
	IP addresses / ranges
	No IP address added yet. Add
	ADD
	Automatically detect external IP (recommended)
	Reject all mail not from gateway IPs
	Require TLS for connections from the email gateways listed above
	2. Message Tagging
	Message is considered spam if the following header regexp matches
	Regexp Learn more
	randomsetofchars
	Test expression
	Message is spam if regexp matches
	 Regexp extracts a numeric score
	Disable Gmail spam evaluation on mail from this gateway; only use header value
	Most changes take effect in a few minutes. Learn more

Bypassing spam by Email Header.

Inside of a campaign, it is possible to set a custom X-Mailer Header. G Suite can analyze the header to bypass SPAM detection.

Steps to configure: Log into admin.google.com, go to "Apps".

≡ Google Admin	Q, Search for users, groups or settings			480 = 0
a *	& Users Manage	Billing V V	Product updates Information about new features and improvements	
3 II II	PAD a user	Alerts View notifications about potential issues	LEL Groups Create groups for mailing lists and applying policies	
9	Delete a user Update a user's name or ensail Create on offernate ensail oddress (ensail olias)	ED Devices Manage devices and secure your organization's data	Account settings Manage your organization's profile and preferences	
		Security Configure security settings, and view alerts and analytics	$\label{eq:rescaled} \vec{n}_{ii} = \frac{\text{Reports}}{\text{Mentor your organization's user and administratively}}$	
	S Benains v	Rules Manage rules to set alerts and actions	Admin roles Assign roles to control permissions for the Admin Canade	
	H Appn Manage web and mobile opp access and settings	Support Connect with the Help Assistant		
	Organizational units Organizational units for applying policies			
	Baildings and resources hassage and monitor your buildings, rooms, and resources			

Go to "Google Workspace".

5/13

	users, groups or settings		8 ?	. 0
Apps Google Workspace Google Workspace Core services	Additional Google services G Blogging, photos, video, social tools and	Web and mobile apps		
12 SERVICES	more se services	ND APPS		
Google Workspace Marketplace apps Add and manage third party apps	SAML apps			
NO SERVICES MANAGE	NO SERVICES			

Go to "Gmail".

≡ Google Admin	Q Sear	ch for users, groups or settings	8 ?
ops > Google Workspace			
G Google		Showing status for apps in all organizational units	ADD SERVICE
Workspace		Service Status	
		Calendar ON for everyone	
All users in this account		Cloud Search ON for everyone	
Groups	~	Currents ON for everyone	
Organizational Units	^	Crive and Doos ON for everyone	
Search for organizational units		Gmail ON for everyone	
 Your Software Name 		Google Chat and classic Hargouts ON for everyone	Learn more
		Google Meet ON for everyone	
		Groups for Business ON for everyone	
		Jamboard ON for everyone	
		Keep ON for everyone	
		Sites ON for everyone	
		Rows per page: 50 v	I< Page1of1 < >

Go to "**Compliance**" at the very bottom.

= Google A	dimin 9, Search for users, groups or s	etting	0 8	0 = 0
Appe > G	cogle Workspace + Settings for Gmail			
25 A 15	M Gmail	Safety Configure enail and spars safety features	÷	
0	Status Only for everyone	Setup Configure setup Instance	÷	
□ © ⊕		End User Access Configure end user access features	÷	
		Sparn, Phishing and Malware Configure spars, phishing and malware features	Ŷ	
		Compliance Configure compliance testures	v	
		Routing Configure routing features	÷	

Go to "Content Compliance" and click "Configure".

	Most changes take effect in a few minutes. Learn more You can view prior changes in the Audit log	
Restrict delivery	Restrict the domains that your users are allowed to exchange email with.	CONFIGURE
	Most changes take effect in a few minutes. Learn more You can view prior changes in the Audit log	
Content compliance	Configure advanced content filters based on words, phrases or patterns.	CONFIGURE
	Most changes take effect in a few minutes. Learn more You can view prior changes in the Audit log	
Objectionable content	Configure content filters based on word lists.	CONFIGURE
	Most changes take effect in a few minutes. Learn more You can view prior changes in the Audit log	

- Add description (e.g. "Lucy Email Phishing")
- Check "Inbound"
- Check "Internal receiving"
- Select "If ANY of the following match the message"

Add setting
Content compliance Learn more
Lucy Email Phishing
1. Email messages to affect
Inbound -
Outbound
Internal - Sending
Internal - Receiving
2. Add expressions that describe the content you want to search for in each message If ANY of the following match the message 🐨
Expressions
No expressions added yet. Add
ADD
3. If the above expressions match, do the following Modify message
CANCEL SAVE

- Click Add Expression → Advanced content match → Headers + Body → Contains text.
 Content → Input your LUCY X-Mailer Header¹⁾ (e.g. "LucyHeader") and click Save.

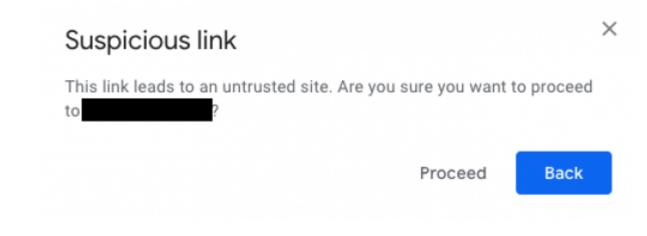
Add setting	
Advanced content match 👻	
Location	
Headers + Body 👻	
Match type	
Contains text 🔍	
Content	
LucyHeader	
	CANCEL SAVE

Scroll down to the "Spam" section and activate "Bypass spam filter for this message".
Click "Save".

Add setting	
Prepend custom subject	
Route	
Change route	
Envelope recipient	
Change envelope recipient	
Spam	
Bypass spam filter for this message	
Attachments	
Remove attachments from message	
Also deliver to	
Add more recipients	
Encryption (onward delivery only)	
Require secure transport (TLS)	
Show options	
	CANCEL SAVE

Suspicious link issue

Sometimes a warning pop-up window appears when you are trying to open link from LUCY email.



First of all, please enable SSL in LUCY campaign. More info can be found here.

It can be that Let's Encrypt certificate is not enough, so we recommend to obtain a paid certificate. You can contact our support team via support@lucysecurity.com or any SSL vendor you like.

However, there are known cases when even a paid certificate can not solve the issue. In this case, you can try to disable this pop-up on G Suite side. Untrusted domains from suspicious emails still will be not affected. "Gmail clients will show a warning prompt when users click on any link in email to untrusted domains (does not work on IMAP/POP email clients). If you don't activate this feature, warnings will only be shown for clicks to untrusted domains from suspicious emails."

Steps to configure: Log into admin.google.com, go to "Apps".

≡ Google Admin Q	Search for users, groups or settings				
 ▲ 	g Users Marage	 Billing Manage subscriptions and billing 	G Product updates information about new features and improvements		
20 21 21	PA 🔊	Alerts View notifications about potential issues	284 Groups Create groups for mailing tots and applying policies		
0	Delete a user Update a user's name or email Create on oftensete ensuit oddress (email often)	Devices bianage devices and secure your organization's data	Account settings Manage your organization's profile and preferences		
		Security Configure security settings, and view alerts and analytics	Benefits Mentor your organization's user and administratively		
	S Bonains V	Rules Manage rules to set alerts and actions	Admin roles Assign toles to control permissions for the Admin Cansole		
	Hanage web and mobile app access and settings	Connect with the Help Assistant			
	Granizational units Granization units for applying policies				
	Balldings and resources Manage and monitor your buildings, roome, and resources				

Navigate to "Google Workspace":

≡ Google Admin Q Search for	users, groups or settings		8 ?	
Apps				
Google Workspace	Additional Google G services Blogging, photos, video, social tools and more	Web and mobile apps		
12 SERVICES	58 SERVICES	ND APPS		
Google Workspace Marketplace apps Add and manage third party apps	SAML apps			
NO SERVICES MANAGE	NO SERVICES			

Go to "Gmail".

≡ Google Admin	Q Sear	ch for users, groups or settings	8 9 📖
ops > Google Workspace			
G Google		Showing status for apps in all organizational units	ADD SERVICES
Workspace		Service Status	
All users in this account		Calendar ON for everyone	
	-	Cloud Search ON for everyone	
Groups	~	Currents ON for everyone	
Organizational Units	^	Drive and Doos ON for everyone	
Search for organizational units		Gmail ON for everyone	
 Your Software Name 		Google Chat and classic Hangouts ON for everyone	Learn more
		Google Meet ON for everyone	
		Groups for Business ON for everyone	
		Deriveryone ON for everyone	
		Keep ON for everyone	
		Sites ON for everyone	
		Rows per page: 50 v	<pre>I< Page1of1 < ></pre>

Go to "Safety".

Authenticate email Set up email authentication (DKIM)
Manage quarantines Create, modify, or remove email quarantines.
Safety Configure email and spam safety features
Setup Configure setup features
End User Access Configure end user access features

Go to "Links and external images".

Google Admin 9, 8	earch for users, groups or settings		8	0	
cs > G Suite > Settings for Gmail > Safe	Attachments	Additional policies to protect against malware in emails. Learn more			
pps > G Sutle > Settings for Gmail > Selver	Applied at 'cloudberver25.com'	View affected emails (charts access requires 0 Saille Enterprise edition).			
Gmail		Protect against encrypted attachments from untrusted senders: ON			
		Protect against attachments with scripts from untrusted senders: ON			
Status		Protect against anomalous attachment types in emails: OFF			
		Apply future recommended settings automatically. ON			
Irganizational Unit	Links and external images	Additional settings to prevent email phishing due to links and external images. Learn more			
	Applied at 'cloudberver25.com'	Identify links behind shortened URLs: ON			
earch for organizational units		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	Additional settings to reduce prishing attacks due to spoofing and unauthenticated emails. Learn more			
	Applied at cloudberver25.com	View emails affected by spoofing settings View unaanthenticoted emails Charts access requires & Sable Enterprise edition.			
		Protect against domain spoofing based on similar domain names: ON			
		Protect against spoofing of employee names: ON			
		Protect against inbound emails spoofing your domain: ON			
		Protect against any unauthenticated emails: OFF			
		Protect your Groups from inbound emails spoofing your domain: OFF			
		Apply future recommended settings automatically.: ON			

Deactivate "Show warning prompt for any click on links to untrusted domains" and click "Save".

2022/08/19 06:34	13/13	Google Workspace Whitelisting
Links and external images Applied at 'cloudserver25.com'	Additional settings to prevent email phishing due to links and external images. Learn more	
	Identify links behind shortened URLs Allow discovery of hidden malicious links behind shortened URLs.	
	Scan linked images Allow scanning of images referenced by links to find hidden malicious content.	
	Show warning prompt for any click on links to untrusted domains Gmail clients will show a warning prompt when users click on any link in email to untrus clients). If you don't activate this feature, warnings will only be shown for clicks to untrus	
	Apply future recommended settings automatically. Learn more Changes may take up to 24 hours to propagate to all users. Prior changes can be seen in Audit log	
	1 ur	nsaved change CANCEL SAVE

Gsuite can scan links inside of phishing simulation emails which can cause false-positives. The feature is called "IMAP view time protections".

M Gmail	Safety			^
	Attachments	Additional policies to protect against malware in emails. Learn more		
Itatus	Applied at 'cloudserver25.com'	View offected emails (chorts access requires Gougle Workspace Enterprise Plas editor).		
IN for everyone		Protect against encrypted attachments from untrusted senders: ON		
		Protect against attachments with scripts from untrusted senders: ON		
Organizational Unit		Protect against anomalous attachment types in emails: OFF		
		Apply future recommended settings automatically: ON		
Search for organizational units				
+ cloudserver25.com	IMAP view time protections Applied at 'claudearver25.com'	Additional settings to protect MAP-users as they interact with emails. Least, ware		
		Enable imag ink protection Enable loss protection on the messages landed via MARP protocol. This feature can scan message links at click time.		
		Changes may take up to 24 hours to propagate to all users. Prior changes can be seen in Audit log		
			CANCEL	SAV
	Links and external images	Additional settings to prevent erroril phishing due to links and external images. Learn more		
	Applied at 'doudserver25 corri	Identify links behind shortened URLs: ON		
		Scan linked images: ON		
		Show warning prompt for any click on links to untrusted domains: OFF		
	Снимок экрана	Apply future recommended settings automatically : ON		

1)

LUCY X-Mailer Header is being configured in your campaign, message section, find more here

