# SAFE

## **Office 365 whitelisting**

#### Solution:

The fix for this issue is definitely on office 365 side and we need to whitelist simulated phishing by doing the following:

- 1. Login to <u>https://security.microsoft.com/advanceddelivery</u> with your administrator account
- 2. On the left menu click on **«Policies & rules»**
- 3. Then click on "Threat policies"

_	) Policies & rules - Microsoft 36	65 : <b>X</b>	+
	$\rightarrow$ C	08	https://security.microsoft.com/securitypoliciesandrules
	Microsoft 365 Defender		
	Email & collaboration Investigations Explorer Review Campaigns	^	Policies & rules Set up policies to manage devices, protect against threats, and receive alerts about various activities in your organization. Learn more Name
ß	Threat tracker		
	Exchange message trace		Alert policy
- <u>0-</u>	Policies & rules		Policies & rules Crivity alerts
Ł	Reports		
R	Audit		
$\otimes$	Health		
0	Permissions		
ŝ	Settings		



# 4. Scroll and click on "Advanced Delivery "

	Microsoft 365 Defender				©
-72	nivesugations	N/LL			,
Ģ	Explorer	Û	Safe Attachments	PREMIUM	Protect your organization from malicious content in email attachments and files in ShareP
	Review	ଡ	Safe Links	PREMIUM	Protect your users from opening and sharing malicious links in email messages and Office
0	Campaigns				
⊵	Threat tracker	Rules			
	Exchange message trace	Θ	Tenant Allow/Block Lists		Manage allow or block entries for your organization.
-0	Policies & rules	Q	DKIM		Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know the
k	Reports	⊜⊧	Advanced delivery		Manage overrides for special system use cases.
Ē	Audit	76	Enhanced filtering		Configure Exchange Online Protection (EOP) scanning to work correctly when your domai
$\otimes$	Health	よ	Quarantine policies		Apply custom rules to quarantined messages by using default quarantine policies or creatin
9	Permissions				
ŝ	Settings	Others			
(i)	More resources		User reported message settings		Enable end users to report spam and malicious email for review and analysis
			Evaluation mode		Configure Microsoft Defender for Office 365 without impacting your production environm
Ø	Customize navigation				

# 5. Once in the Advanced delivery then click on **Phishing simulation**

				ģ
㎡ Inals				
	Advanced dollar	1		
Dinvestigations	Phishing simulation	_		
D Explorer	SecOps mailbox Phishing simulation			
Review	🖉 Edit 💍 Refresh	_		0 items
Campaigns	Value	Type	Date	
2 Threat tracker	Yunut	ιμν	Date	
Exchange message trace				
Policies & rules				
✓ Reports				
है Audit				
🏵 Health				
Rermissions		No Third Party Phishing Simulation Configured.		
🖇 Settings	Sele	ect 'Add' to configure your third party phishing simulations. A	A phishing	_
D More resources	simi trainin a	ination is an attack orchestrated by your security team that is g and learning. Simulations help identify vulnerable users an ind can lessen the impact of malicious attacks on your organ	d behaviors, ization.	1
Customize navigation		Add		



#### 6. Then click on the Add button

7. When you click on the Add button a window will slide from the right of your screen, then you need to add **all those** domains :

- trkr.ch
- newsl.ch
- scan-to-me.ch
- c-mail.ch
- t1nder.ch
- beardband.ch
- nimtendo.ch
- mail-auth.ch
- mail-check.ch
- mail-checked.com
- mail-list.ch
- safe-mail.ch
- survey-monkey.ch
- survey-monky.com
- notification-post.ch

### for your phishing campaigns and the IP address it is using to send from:

	Microsoft 365 Defender		© ?	BB
Ŭ	Inals			Х
	Email & collaboration	Advanced delivery	Add Third Party Phishing Simulations	Close
Ģ	Investigations		Phishing simulations are attacks orchestrated by your security team and used for	-
Ģ	Explorer	SecOps mailbox Phishing simulation	training and learning. Simulations can help identify vulnerable users and lessen the impact of malicious attacks on your organization.	
	Review	🖉 Edit 💍 Refresh	Third-party phishing simulations require at least one <b>Sending domain</b> entry [sour	ce
0	Campaigns	) ( due	entries are optional, and prevent the simulated phishing URLs from being blocked a time of disk.	at
⊵	Threat tracker	value		/
	Exchange message trace		Domain (3 items) 🛈	`
	Policies & rules		● trkr.ch × ● newsl.ch × ● scan-to-me.ch×	]
k	Reports			
£	Audit			
$\otimes$	Health	· · · · · · · · · · · · · · · · · · ·	Sending IP (4 items)	<b>`</b>
9	Permissions	No Third Party Phish	149.72.94.128×	1
٢	Settings	Select 'Add' to configure your third simulation is an attack orchestrate		0
(i)	More resources	training and learning. Simulations he and can lessen the impact of m		Ģ
Ø	Customize navigation		Add Cancel	

• 149.72.94.128

# SAFE

8. Once you Add these domains and Ips and close the window, each of these Ips and domains will be displayed as a separate rule in the phishing simulation window.



This procedure has been created from this page.