

INSTRUCTIONS: ADVANCED SETTINGS FOR THE DELIVERY OF PHISHING EMAILS IN OFFICE 365

TABLE OF CONTENTS

03 ADVANCED DELIVERY

- 03 Security
- 03 Policies & rules



ADVANCED DELIVERY

Security

Log in to the Office 356 Admin Console and select the Security menu item.

← Zurück		
Alle Ihre Apps durchsuchen		
Neu	Sicherheitsinformation	Kennwort
• 🐴 Admin	Q _a	Q
• 🦁 Compliance	10	~77
Security :	Halten Sie Ihre Überprüfungsmethoden und Sicherheitsinformationen auf dem neuesten Stand.	Verstärken Sie die Kennwortsicherheit, oder ändern Sie Ihr Kennwort, wenn jemand anderes Kenntnis darüber hat.
MICROSOFT 365		VENNNORT ÄNDERNI S

Policies & rules

Select Policies & rules from the menu on the left. A new interface opens, here click on the item Threat policies.

Ę	Explorer			III Microsoft 365 Defende	Microsoft 365 Defender		
E	Review			=			
~						Policies & rules	
0	Campaigns			Incidents & alerts	\sim	Set up policies to manage devices, protect against threats, and receive alerts about various	
\leq	Threat tracker			Actions & submissions	~		
-				Secure score		Name	
E S	Exchange message trace			沓 Trials		Threat policies	
	Delizias 8 miles	Delizion (tradas				The point of	
	Policies & rules	Policies & rules		Email & collaboration	^	Alert policy	
				C Investigations		Activity alerts	
1.4	D			D			

In the threat policies, choose the **Advanced delivery** option.

9	Email authentication settings	Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
Q,	DKIM	Add DomainKeys Identified Mail (DKIM) signatures to your domains so recipients know that email messages actually came from your users
⊜ ≣	Advanced delivery	Manage overrides for special system use cases.
\⊊	Enhanced filtering	Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first
よ	Quarantine policies	Apply custom rules to quarantined messages by using default quarantine policies or creating your own

Select **Phishing simulation** in the menu and choose the **Edit** option.

\sim		\sim	
~	Advanced Chiline	~	
	SecOps mailbox Phishing simulation		SecOps mailbox Phishing simulation
^	🖉 Edit 💍 Refresh	^	C Edit C Refresh
	Value		Value



Add the following domain in the **Domain** box: **1ys.de**

	тіте от сііск.	
	Domain (0 items) ①	^
pe	1ys.de	
	1ys.de	
	Sending IP (0 items)	~

Under Sending IP, enter the following IP address: 5.1.76.150

5.1.76.150	
E 1 76 150	

Under Simulation URLs to allow enter the following URLs:

.your-pas.de/ *.the-pas.de/* *.service.vacations/* *.platform-iys.com/* *.plattform-iys.de/* *.plattform-iys.com/* *.platform-iys.de/*

(Please remember to enter each URL separately)





ld' to configure your third party phishing simulations. A phis n is an attack orchestrated by your security team that is used learning. Simulations help identify vulnerable users and bel n lessen the impact of malicious attacks on your organizatio

Select Save and Close out of the editing screen.



	.platform-iys.de/	
s	Removed 0	
2		
ir C		
		e
		Ē
	Close	