

ANLEITUNG: ZUSTELLUNG VON PHISHING-E-MAILS IN OFFICE 365 ERWEITERN

INHALTSVERZEICHNIS

03 ALLOWLISTING VON PHISHING-URLS

- 03 Sicherheit
- 03 Richtlinien & Regeln



ZUSTELLUNG ERWEITERN

Sicherheit

Loggen Sie sich in die Office 356 Admin-Konsole ein und wählen Sie den Menüpunkt Sicherheit.

← Zurück		
P Alle Ihre Apps durchsuchen		
Neu	Sicherheitsinformation	Kennwort
• 🐴 Admin	Q _a	Q
• 🦁 Compliance	10	-J
Sicherheit	Halten Sie Ihre Uberprüfungsmethoden und Sicherheitsinformationen auf dem neuesten Stand.	Verstärken Sie die Kennwortsicherheit, oder ändern Sie Ihr Kennwort, wenn jemand anderes Kenntnis darüber hat.
Microsoft 365		VENNIMORT ÄNDERNI

Richtlinien & Regeln

Wählen Sie rechts im Menü den Punkt **Richtlinien und Regeln** aus. Es öffnet sich eine neue Oberfläche – hier klicken Sie auf den Punkt **Bedrohungsrichtlinien**.

Ģ	Explorer		III Microsoft 365 Defender		
	Überprüfen		=		
0	Kampagnen		 Startseite Vorfälle & Warnungen 	~	Richtlinien und Regeln Richten Sie Richtlinien ein, um Geräte zu verwalten, sich vor Bedrohungen zu schütz
\approx	Bedrohungs-Tracker		Aktionen und Übermittlung	. ~	
	Exchange-Nachrichtenablaufverf		☑ Sicherheitsbewertung☑ Testversionen		Name
	Richtlinien und Regeln	Richtlinien und Regeln	🖾 E-Mail & Zusammenarbeit	^	Warnungsrichtlinie
			🛱 Untersuchungen		Aktivitätsbenachrichtigungen

In den Bedrohungsrichtlinien wählen Sie die Option Erweiterte Zustellung aus.

9	E-Mail-Authentifizierungseinstellungen	Einstellungen für Authenticated Received Chain (ARC) und DKIM in Ihrer Organisation.
9	DKIM	Fügen Sie Ihren Domänen DKIM-Signaturen (DomainKeys Identified Maii) hinzu, damit die Empfänger wissen, dass E-Mails tatsächlich von Ihren Benutze
⊕ ≋	Erweiterte Zustellung	Außerkraftsetzungen verwalten für spezielle Systemanwendungsfälle.
76	Erweiterte Filterung	Konfigurieren Sie die EOP-Überprüfung (Exchange Online Protection) so, dass sie richtig funktioniert, wenn der MX-Eintrag Ihrer Domäne E-Mail nicht zu
ъ	Quarantäne-Richtlinien	Anwenden von benutzerdefinierten Regeln auf in Quarantäne befindliche Nachrichten, indem Sie Standard-Quarantäne-Richtlinien verwenden oder Ihre

Klicken Sie auf den Menüpunkt **Phishing-Simulation** und wählen Sie die Option **Bearbeiten** aus.

 Erweiterte ZPhishing-Simulation 	~	Erweiterte Zustellung	
SecOps-Postfach Phishing-Simulation	^	S Stfach Phishing-Simulation	



Fügen Sie unter **Domäne** folgende Domain ein: **1ys.de**

	wergen.	
q	Domäne (0 Elemente) ^①	^
	1ys.de	
	1 1ys.de	
	IP (0 Elemente) wird gesendet	~

Fügen Sie unter IP wird gesendet folgende IP-Adresse ein: 5.1.76.150

	IP (0 Elemente) wird gesendet	^
	5.1.76.150 5.1.76.150	
keine Phishing-Simulationen von Drittanbietern konfiguriert.	Simulations-URLs, die (0 Elemente) zulassen $^{\bigcirc}$	\checkmark

Fügen Sie unter Simulations-URLs, die (X Elemente) zulassen folgende URLs ein:

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

(Bitte beachten Sie, die URLs jeweils einzeln einzufügen)

urde



Klicken Sie auf **Speichern** und **schließen** Sie anschließend den Bearbeitungsmodus.

Simulations-URLs, die (7 Elemente) zulassen \oplus	^ .	*.service.vacations/* *.the-pas.de/*	
📀 *.platform-iys.de/* 🛛 🏹 📀 *.plattform-iys.com/* 🗡	ie	".your-pas.de/"	
ho *.plattform-iys.de/* $ imes$ $ ho$ *.platform-iys.com/* $ imes$	st	0 wurde entfernt	
.service.vacations/ × 💿 *.the-pas.de/* × 💿 *.your-pas.de/*	× /ir		
	e ut		Q
	æ		Ģ
Speichern Abbrechen	_	Schließen	