# MINIMIERUNG VON PHISHING-FEHLALARMEN

## KURZREFERENZ

## INHALT

# ÜBERSICHT

**Was ist ein falsches Positiv?**

Ein False Positive ist ein Fehler, der auftritt, wenn ein System ein Ereignis meldet, z. B. dass eine Zielperson auf eine Phishing-E-Mail geklickt hat, das in Wirklichkeit nicht eingetreten ist. Falsch positive Ergebnisse treten bei allen Arten von Phishing-Simulationssystemen auf und sind nicht auf einen bestimmten Anbieter oder ein bestimmtes Tool beschränkt.

**Was ist ein Klick?**

Um zu verstehen, wie falsch-positive Ergebnisse zustande kommen, muss man wissen, wie das System Reaktionen misst. Ein "Klick" ist definiert als jede Interaktion mit einem Link, z. B. ein Mausklick des Benutzers. Dies kann jedoch auch ein System umfassen, wie z. B. eine E-Mail-Sicherheitssoftware, die eine E-Mail prüft, bevor sie den Posteingang erreicht.

**Häufige Ursachen**

Falschmeldungen werden in der Regel von den Sicherheitsfiltern der E-Mail-Anbieter verursacht. Filter prüfen den Inhalt von E-Mails, bevor sie in den Posteingang des Empfängers gelangen. Für das Phishing-Tool wird dies als Klick registriert und als solcher gemeldet.

# LÖSUNGEN

VENZA ist sich der Bedeutung genauer Daten bewusst und ergreift aktive Maßnahmen, um Fehlalarme zu vermeiden. Wichtige Schritte umfassen:

1. **IP-Whitelisting**

Whitelisting ist ein Begriff aus der Cybersicherheit und der Informationstechnologie (IT), der sich darauf bezieht, dass bestimmte E-Mail-Domänen (z. B. example@domain.com) und Internetprotokolle (IPs) durch die Schutzmaßnahmen eines Unternehmens hindurch zugelassen werden.

Wenn Sie die IPs der eingehenden VENZA-Kampagnen in die Whitelist Ihres Netzwerks aufnehmen, können Sie verhindern, dass Ihre E-Mail-Sicherheitssysteme Fehlalarme auslösen.

2. **Interne IP-Filterung**

Stellen Sie Ihrem Customer Success Coach eine Liste mit internen IP-Adressen zur Verfügung, die in einem internen Filterprozess verwendet werden können.

## WHITELISTING CISCO

**Zielsetzung**: Mit Hilfe der Cisco Ironport Sicherheitssoftware können Sie VENZA auf eine sichere Liste setzen (Whitelist), damit Ihre Benutzer unsere simulierten Phishing- und System-E-Mails erhalten können.

Wenn Sie Probleme mit dem Safelisting in Cisco Ironport haben, empfehlen wir Ihnen, sich zunächst direkt an Cisco zu wenden, um Hilfe zu erhalten.

- ### WHITELISTING VERWENDEN

**Schritte**:

1. Navigieren Sie in der Verwaltungskonsole von Cisco Ironport zur Registerkarte **Mail Policies**.
2. Wählen Sie **HAT Overview** und stellen Sie sicher, dass **InboundMail lister** ausgewählt ist.
3. Klicken Sie auf **WHITELIST**. Wenn Sie **WHITELIST** nicht sehen, können Sie Ihre Gruppe mit diesem Titel erstellen.
4. Klicken Sie auf **Absender hinzufügen** und fügen Sie die VENZA IP (108.163.193.74) hinzu.
5. Klicken Sie auf **Senden** und dann auf **Änderungen übernehmen**.

- ### ÜBERSPRINGEN VON AUSBRUCHSFILTER-SCANS

**Schritte**:

1. Navigieren Sie in der Verwaltungskonsole von Cisco Ironport zur Registerkarte **Mail Policies**.
2. Geben Sie unter dem Abschnitt **Message Modification** in der Tabelle **Bypass Domain Scanning** die VENZA IP (108.163.193.74) ein.
3. Klicken Sie auf **Senden** und dann auf **Änderungen übernehmen**.

## WHITELISTING FORTINET

**Zielsetzung**: Mit der Sicherheitssoftware von Fortinet können Sie VENZA auf eine Whitelist setzen, damit Ihre Benutzer unsere simulierten Phishing- und System-E-Mails empfangen können.

Wenn Sie Probleme mit dem Safelisting in Fortinet haben, empfehlen wir Ihnen, sich zunächst direkt an Fortinet zu wenden, um Hilfe zu erhalten.

- ### STATISCHE URL-FILTER VERWENDEN

**Schritte**:

1. Melden Sie sich bei Ihrem Fortinet-Konto an.
2. Navigieren Sie zu **Sicherheitsprofile** > **Webfilter**.
3. Erstellen Sie einen neuen Webfilter oder wählen Sie einen zur Bearbeitung aus.
4. Erweitern Sie **Statischer URL-Filter**, aktivieren Sie **URL-Filter**, und wählen Sie **Erstellen**.
5. Geben Sie URLs ohne "https." ein. Eine Liste der URLs befindet sich am Ende dieser Kurzanleitung.
6. Typ auswählen: **Einfach**.
7. Wählen Sie die Aktion, die bei übereinstimmenden URLs durchgeführt werden soll: **Zulassen**.
8. Bestätigen Sie, dass der **Status "**Aktiviert" ist.

## WHITELISTING VON GOOGLE MAIL

**Zielsetzung**: Diese Anweisungen helfen Ihnen, die Übermittlung von Phishing-Simulationen Dritter an Google Gmail zu konfigurieren.

**Hinweis**: Sie müssen über ein Administratorkonto verfügen, um diesen Vorgang durchführen zu können, und es kann bis zu 24 Stunden dauern, bis die Änderungen wirksam werden.

- ### HINZUFÜGEN EINER IP-ADRESSE ZU IHRER ZULASSUNGSLISTE

**Schritte**:

1. Melden Sie sich bei Ihrer Google Admin-Konsole an.
2. Gehen Sie in der Verwaltungskonsole zu **Menü** > **Apps** > **Google Workspace** > **Google Mail** > **Spam, Phishing und Malware**.
3. Wählen Sie auf der linken Seite die Organisation der obersten Ebene aus. Dies ist normalerweise Ihre Domäne.
4. Blättern Sie auf der Registerkarte **Spam, Phishing und Malware** zu der Einstellung **E-Mail-Zulassungsliste**. Oder geben Sie in das Suchfeld **E-Mail-Zulassungsliste** ein.

5. Geben Sie die IP-Adresse für VENZA Phishing™ ein: 108.163.193.74
6. Klicken Sie unten auf der Seite auf **Speichern**.

- ### ERSTELLEN EINER LISTE ZUGELASSENER ABSENDER ZUR UMGEHUNG VON SPAM-FILTERN

**Schritte**:

1. Melden Sie sich bei Ihrer Google Admin-Konsole an.
2. Gehen Sie in der Verwaltungskonsole zu **Menü** > **Apps** > **Google Workspace** > **Google Mail** > **Spam, Phishing und Malware**.
3. Wählen Sie auf der linken Seite eine Organisationseinheit aus.
4. Zeigen Sie auf **Spam** und klicken Sie auf **Konfigurieren**.
5. Geben Sie für eine neue Einstellung einen eindeutigen Namen oder eine Beschreibung ein.
6. Aktivieren Sie das Kontrollkästchen **Spamfilter für Nachrichten umgehen, die von Adressen oder Domänen innerhalb dieser Listen zugelassener Absender empfangen werden**.
7. Klicken Sie auf **Erstellen oder Bearbeiten**, um eine Liste der zugelassenen Absender zu erstellen.
8. Führen Sie einen Bildlauf zum unteren Rand von **Adresslisten verwalten durch**, und klicken Sie auf Adressliste **hinzufügen**.
9. Geben Sie einen Namen für die neue Liste ein.
10. Klicken Sie auf **Adresse hinzufügen**.
11. Geben Sie E-Mail-Adressen oder Domänennamen ein. Verwenden Sie ein Leerzeichen oder Komma zwischen den einzelnen Einträgen.
12. Klicken Sie auf **Speichern**, um die neue Adressliste zu speichern.

## WHITELISTING VON MICROSOFT 365

**Zielsetzung**: Diese Anweisungen helfen Ihnen, die Bereitstellung von Phishing-Simulationen von Drittanbietern an Microsoft 365 Defender zu konfigurieren.

**Hinweis**: Sie müssen über Berechtigungen (Organisationsmanagement oder Sicherheitsadministrator) in Exchange Online verfügen, bevor Sie diese Verfahren durchführen können.

**Hinweis**: Benutzer können ein falsches positives Ergebnis erhalten, wenn sie eine E-Mail mit dem Add-In "Nachricht melden" melden.

- ## ERWEITERTE ZUSTELLUNG VERWENDEN

**Schritte**:

1. Öffnen Sie das Microsoft 365 Defender-Portal.
2. Gehen Sie zu **E-Mail & Collaboration** > **Richtlinien & Regeln** > Seite **Bedrohungsrichtlinien** > Abschnitt **Regeln** > **Erweiterte Zustellung**.
3. Wählen Sie auf der Seite **Erweiterte Bereitstellung die** Registerkarte **Phishing-Simulation** und führen Sie dann einen der folgenden Schritte aus:
    a. Klicken Sie auf **Bearbeiten**, oder
    b. Wenn noch keine Phishing-Simulationen konfiguriert sind, klicken Sie auf **Hinzufügen**.
4. Konfigurieren Sie in dem sich öffnenden Flyout **Phishing-Simulation eines Drittanbieters bearbeiten** die folgenden Einstellungen:
    a. **Domäne**: Erweitern Sie diese Einstellung und geben Sie mindestens eine E-Mail-Adressdomäne ein, indem Sie in das Feld klicken, einen Wert eingeben und dann die **Eingabetaste** drücken. Eine Liste der für VENZA Phishing™ erforderlichen Domains finden Sie am Ende dieser Kurzanleitung.
    b. **Sende-IP**: Erweitern Sie diese Einstellung und geben Sie eine gültige IPv4-Adresse ein, indem Sie in das Feld klicken, **108.163.193.74** eingeben und dann die **Eingabetaste** drücken.
    c. **Zuzulassende Simulations-URLs**: Erweitern Sie diese Einstellung und geben Sie URLs ein, die von Ihrem VENZA Customer Success Coach bereitgestellt werden. Hinweis: Dieses Feld ist nicht für alle Phishing-Kampagnen erforderlich.
5. Wenn Sie fertig sind, klicken Sie auf **Hinzufügen** und dann auf **Schließen**.

- ## VERWENDUNG DER IP-ZULASSUNGSLISTE

Achtung! Ohne zusätzliche Überprüfung, wie z. B. Mailflow-Regeln, werden E-Mails von Quellen in der IP-Zulassungsliste nicht auf Spam-Filterung und Absenderauthentifizierung (SPF, DKIM, DMARC) geprüft. Dadurch besteht ein hohes Risiko, dass Angreifer erfolgreich E-Mails an den Posteingang zustellen, die andernfalls gefiltert werden würden.

**Schritte**:

1. Öffnen Sie das Microsoft 365 Defender-Portal.

2. Gehen Sie zu **E-Mail & Zusammenarbeit** > **Richtlinien & Regeln** > **Bedrohungsrichtlinien** > **Anti-Spam**
3. Klicken Sie auf **Verbindungsfilterrichtlinie** und dann auf **Verbindungsfilterrichtlinie bearbeiten**.
4. Fügen Sie die unten stehende IP-Adresse in das Feld **Nachrichten von folgenden IP-Adressen oder Adressbereichen immer zulassen ein**:
    a. 108.163.193.74
5. Drücken Sie die **Eingabetaste** und klicken Sie auf **Speichern**, um die neuen Einstellungen zu aktivieren.

- ## VERWENDUNG DER LISTEN "ERLAUBTER ABSENDER" ODER "ERLAUBTE DOMÄNE

Vorsicht! Bei dieser Methode besteht ein hohes Risiko, dass Angreifer erfolgreich E-Mails in den Posteingang einspeisen, die andernfalls gefiltert würden. Die Listen der zugelassenen Absender oder der zugelassenen Domänen verhindern jedoch nicht, dass Malware oder hochvertrauliche Phishing-Nachrichten gefiltert werden.

Schritte:

1. Öffnen Sie das Microsoft 365 Defender-Portal
2. Gehen Sie zu **E-Mail & Zusammenarbeit** > **Richtlinien & Regeln** > **Bedrohungsrichtlinien** > **Anti-Spam**
3. Klicken Sie auf **+**, um eine Richtlinie zu erstellen, und wählen Sie in der Dropdown-Liste die Option **Eingehend aus**.
4. Der Richtlinienassistent wird geöffnet. Konfigurieren Sie auf der Seite **Name Ihrer Richtlinie** diese Einstellungen:
    a. **Name**: Geben Sie einen eindeutigen, beschreibenden Namen für die Richtlinie ein.
    b. **Beschreibung**: Geben Sie eine optionale Beschreibung für die Richtlinie ein.

    Wenn Sie fertig sind, klicken Sie auf **Weiter**.

5. Bestimmen Sie auf der Seite **Benutzer, Gruppen und Domänen** die internen Empfänger, für die die Richtlinie gilt (Empfängerbedingungen):
    a. **Benutzer**: Die angegebenen Postfächer, E-Mail-Benutzer oder E-Mail-Kontakte.

b. **Gruppen**: Mitglieder der angegebenen Verteilergruppen oder mail-aktivierten Sicherheitsgruppen.
c. **Domänen**: Alle Empfänger in den angegebenen akzeptierten Domänen in Ihrer Organisation.

Wenn Sie fertig sind, klicken Sie auf **Weiter**.

6. Konfigurieren Sie auf der angezeigten Seite **Massen-E-Mail-Schwellenwert & Spam-Eigenschaften die** erforderlichen Einstellungen. Wenn Sie fertig sind, klicken Sie auf **Weiter**.
7. Auf der daraufhin angezeigten Seite "**Aktionen"** können Sie die gewünschten Einstellungen vornehmen.
8. Klicken Sie im eingeblendeten Flyout der **Liste Erlauben & Blockieren** auf **Erlaubt** > **Domains** > **Erlaubte** Domains.
9. Klicken Sie auf **+**, um **Domänen hinzuzufügen**.
10. Geben Sie die am Ende dieser QRG aufgeführten Domänen in das Feld **Domäne** ein.
11. Klicken Sie auf **Domänen hinzufügen** und dann auf **Weiter**, wenn Sie fortfahren möchten.
12. Überprüfen Sie auf der daraufhin angezeigten Seite **Überprüfung** Ihre Einstellungen. Sie können in jedem Abschnitt auf **Bearbeiten** klicken, um die Einstellungen innerhalb des Abschnitts zu ändern. Sie können auch auf **Zurück** klicken oder die entsprechende Seite im Assistenten auswählen.

    Wenn Sie fertig sind, klicken Sie auf **Erstellen**.

## MIMECAST AUF DIE WHITELIST SETZEN

**Zielsetzung**: Mit Hilfe der Mimecast Sicherheitssoftware können Sie VENZA auf eine Whitelist setzen, damit Ihre Benutzer unsere simulierten Phishing- und System-E-Mails erhalten können.

Wenn Sie Probleme mit dem Safelisting in Mimecast haben, empfehlen wir Ihnen, sich zunächst direkt an Mimecast zu wenden, um Hilfe zu erhalten.

### • ERSTELLEN EINER RICHTLINIE FÜR ZUGELASSENE ABSENDER

Wir empfehlen, eine neue Richtlinie für zugelassene Absender in Ihrer Mimecast-Konsole zu erstellen, um VENZA auf eine sichere Liste zu setzen.

**Hinweis**: Bearbeiten Sie Ihre Standardrichtlinie für zugelassene Absender nicht. Erstellen Sie stattdessen eine neue Richtlinie.

**Schritte**:

1. Öffnen Sie in der Mimecast-Verwaltungskonsole die **Verwaltungssymbolleiste**.
    a. Wählen Sie **Gateway | Policies**.
    b. Wählen Sie **Erlaubte Absender**.
    c. Wählen Sie **Neue Richtlinie**.
2. Wählen Sie die folgenden Einstellungen unter den Abschnitten **Optionen**, **E-Mails von**, **E-Mails an** und **Gültigkeit**.
3. Weitere Informationen finden Sie unter Konfigurieren einer Richtlinie für zugelassene Absender von Mimecast.

| Option | Einstellungen |
|---|---|
| Optionen | |
| Politik-Narrativ | Phishing Erlaubte Absender |
| Option auswählen | Absender zulassen |
| Emails von | |
| Gilt für | Interne Adressen |
| Speziell | Gilt für alle internen Begünstigten |
| Gültigkeit | |
| Aktivieren/Deaktivieren | Aktivieren Sie |
| Politik als unbefristet festlegen | Immer eingeschaltet |
| Datumsbereich | Alle Zeiten |
| Aufhebung der Richtlinie | Geprüft |
| Bidirektional | Ungeprüft |
| Quell-IP-Bereiche (n.n.n.n/x) | 108.163.193.74 |

Das Hinzufügen von VENZA zur Liste der zugelassenen Absender (siehe oben) sollte das Greylisting umgehen. Wir empfehlen jedoch, die folgenden Greylisting-Schritte zu befolgen, um die Zustellbarkeit von E-Mails zu verbessern.

Schritte:

1. Öffnen Sie in der Mimecast-Verwaltungskonsole die **Verwaltungssymbolleiste**.
    a. Wählen Sie **Gateway | Policies**.
    b. Wählen Sie **Erlaubte Absender**.
    c. Wählen Sie **Neue Richtlinie**.
2. Wählen Sie die folgenden Einstellungen unter den Abschnitten **Optionen**, **E-Mails von**, **E-Mails an** und **Gültigkeit**.

| Option | Einstellungen |
|---|---|
| Optionen | |
| Politik-Narrativ | VENZA Greylist |
| Option auswählen | Keine Maßnahmen ergreifen |
| Emails von | |
| Adressen basierend auf | Die Rücksendeadresse |
| Gilt von | E-Mail-Adressen |
| Speziell | Gilt für alle externen Absender |
| Emails an | |
| Gilt für | Interne Adressen |
| Speziell | Gilt für alle internen Begünstigten |
| Gültigkeit | |
| Aktivieren/Deaktivieren | Aktivieren Sie |
| Politik als unbefristet festlegen | Immer eingeschaltet |
| Datumsbereich | Alle Zeiten |
| Aufhebung der Richtlinie | Geprüft |
| Bidirektional | Ungeprüft |
| Quell-IP-Bereiche (n.n.n.n/x) | 108.163.193.74/24 |

- ## ERSTELLEN EINER RICHTLINIE ZUR UMGEHUNG DES URL-SCHUTZES

Schritte:

1. Öffnen Sie in der Mimecast-Verwaltungskonsole die **Verwaltungssymbolleiste**.

a. Wählen Sie **Gateway | Policies**.
b. Wählen Sie **Erlaubte Absender**.
c. Wählen Sie **Neue Richtlinie**.

2. Wählen Sie die folgenden Einstellungen unter den Abschnitten **Optionen**, **E-Mails von**, **E-Mails an** und **Gültigkeit**.

| Option | Einstellungen |
|---|---|
| Optionen | |
| Politik-Narrativ | Umgehung des Phishing-URL-Schutzes |
| Option auswählen | URL-Schutz deaktivieren |
| Emails von | |
| Adressen basierend auf | Beide |
| Gilt von | Alle |
| Speziell | Gilt für alle Absender |
| Emails an | |
| Gilt für | Interne Adressen |
| Speziell | Gilt für alle internen Begünstigten |
| Gültigkeit | |
| Aktivieren/Deaktivieren | Aktivieren Sie |
| Politik als unbefristet festlegen | Immer eingeschaltet |
| Datumsbereich | Alle Zeiten |
| Aufhebung der Richtlinie | Geprüft |
| Bidirektional | Ungeprüft |
| Quell-IP-Bereiche (n.n.n.n/x) | 108.163.193.74/24 |
| Hostname(n) | Leer lassen |

## WHITELISTING VON SOPHOS

**Zielsetzung**: Mit Hilfe der Sophos Sicherheitssoftware können Sie VENZA auf eine sichere Liste setzen (Whitelist), damit Ihre Benutzer unsere simulierten Phishing- und System-E-Mails erhalten.

Wenn Sie Probleme mit dem Safelisting in Sophos haben, empfehlen wir Ihnen, sich zunächst direkt an Sophos zu wenden, um Hilfe zu erhalten.

- ## ÄNDERN VON ADD/BLOCK-LISTEN IN DER SOPHOS E-MAIL APPLIANCE

**Schritte**:

1. Navigieren Sie in Ihrem SEA-Manager zu **Konfiguration** > **Richtlinie** > **Zulassen-Listen**.
2. Klicken Sie auf die entsprechende Liste, um das Dialogfeld **Listeneditor** anzuzeigen.
3. Wählen Sie die Registerkarte **Absender**, wenn Sie einen zusätzlichen Spam-Filter vor der SEA haben. Wählen Sie die Registerkarte **Hosts, wenn Sie** keinen zusätzlichen Spam-Filter vor der SEA haben.
4. Geben Sie in das Textfeld **Einträge hinzufügen** jeden gewünschten Eintrag ein und klicken Sie auf **Hinzufügen**.
5. Geben Sie auf der Registerkarte Absender nacheinander die VENZA-Domänennamen ein. Diese Domains sind am Ende dieser Kurzanleitung aufgeführt.
6. Geben Sie auf der Registerkarte Hosts die IP-Adresse von VENZA ein. Die VENZA IP-Adresse ist am Ende dieser Kurzanleitung aufgeführt.

- ## WHITELISTING IN SOPHOS XG FIREWALLS

Schritte:

1. Melden Sie sich am Portal für die Firewall an.
2. Klicken Sie auf der linken Seite auf **Web**.
3. Klicken Sie auf **Ausnahmen**, die sich oben befinden.
4. Wenn Sie keine Ausnahmeliste haben, klicken Sie auf "**Ausnahme hinzufügen"**.
5. Geben Sie einen Namen (**VENZA**) und eine optionale Beschreibung für die Liste an.
6. Aktivieren Sie die Kästchen rechts unter **Überspringen der ausgewählten Prüfungen oder Aktionen** für Ihre gekauften Dienste.
7. **URL-Musterübereinstimmungen** prüfen.
8. Geben Sie die Phishing-Domänen zeilenweise in das Feld **Suchen/Hinzufügen ein**. Diese finden Sie am Ende dieser Kurzanleitung.
9. Klicken Sie unten auf der Seite auf **Speichern**.

# IP-ADRESSE AUF DER WHITELIST

108.163.193.74

### PHISHING-KAMPAGNE DOMAINS

| | |
|---|---|
| kontoprofil.de | hotelreview.today |
| Inkassobüro.co | humanresource.center |
| corporateoffice.biz | legalactions.org |
| discriminationweb.com | versandanzeige.de |
| dokumentenservice.de | nutzen-fedex.de |
| mitarbeitervergütungen.site | yelprating.de |
| expedia-us.com | Ihr-Konto-Login.de |

### SYSTEM-DOMÄNEN

| | |
|---|---|
| venzagrc.com | venzapeak.com |

# KONTAKT

**Helpdesk**: noreply@venzagroup.com

**Verkäufe**: sales@venzagroup.com

**Kundenerfolg**: success@venzagroup.com