

IT-Sicherheitsleitfaden

Verdächtige E-Mails & Phishing-Versuche richtig melden



Haben Sie eine verdächtige E-Mail erhalten? Handeln Sie sofort, aber richtig! Klicken Sie auf keine Links und öffnen Sie keine Anhänge.

Um Ihre IT-Infrastruktur optimal zu schützen, analysieren wir potenzielle Phishing-Mails direkt im Sicherheits-Labor. Damit alle relevanten technischen Daten (die Header-Informationen) erhalten bleiben, senden Sie uns die E-Mail bitte ausschließlich über Ihre persönliche Sicherheits-Adresse.

IHRE PERSÖNLICHE SICHERHEITS-ADRESSE
[Wird in Kürze für Sie eingetragen]

Nachfolgend finden Sie die Schritt-für-Schritt-Anleitung für die zwei am häufigsten genutzten E-Mail-Portale:

Variante 1: Microsoft Outlook (Desktop-App & Web)

In Outlook ist die Meldung besonders einfach, da die E-Mail direkt als technische Datei angehängt werden kann:

- **Schritt 1:** Starten Sie Outlook und klicken Sie auf **"Neue E-Mail"**, um eine neue, leere Nachricht zu erstellen.
- **Schritt 2:** Positionieren Sie das Fenster der neuen E-Mail so, dass Sie Ihre Posteingangs-Liste noch sehen können.
- **Schritt 3:** Klicken Sie die verdächtige E-Mail in Ihrer Liste an, halten Sie die Maustaste gedrückt und ziehen Sie die E-Mail per **Drag-and-Drop** direkt in das Textfeld der neuen E-Mail hinein. Die verdächtige Mail erscheint nun sauber als Anhang (z.B. als .msg-Datei).
- **Schritt 4:** Tragen Sie oben Ihre persönliche Sicherheits-Adresse ein und klicken Sie auf **"Senden"**.

Variante 2: Google Gmail (im Webbrowser)

Da Gmail beim normalen Weiterleiten wichtige Sicherheitsdaten abschneidet, nutzen Sie bitte diesen kurzen, sicheren Weg:

- **Schritt 1:** Öffnen Sie die verdächtige E-Mail in Ihrem Gmail-Konto.
- **Schritt 2:** Klicken Sie ganz rechts (auf einer Linie mit dem Betreff/Absender) auf die **drei vertikalen Punkte** ("Mehr").
- **Schritt 3:** Wählen Sie im Menü den Punkt **"Nachricht herunterladen"**. Gmail speichert die E-Mail nun als eigenständige Datei (Endung .eml) in Ihrem "Downloads"-Ordner auf dem Computer.
- **Schritt 4:** Erstellen Sie eine neue E-Mail in Gmail, fügen Sie die eben heruntergeladene Datei als ****Anhang**** hinzu, tragen Sie Ihre persönliche Sicherheits-Adresse ein und senden Sie die Nachricht ab.

 Wichtiger Sicherheitshinweis:

Bitte nutzen Sie niemals die normale "Weiterleiten"-Funktion Ihres Mailprogramms. Dabei gehen alle Spuren des echten Absenders verloren, was eine präzise technische Analyse der Phishing-Mail unmöglich macht.

Nach dem Absenden wird die E-Mail in unserem System isoliert geprüft. Sie erhalten in Kürze eine Rückmeldung, ob es sich um eine Gefahr oder einen Fehlalarm handelt.