

## Awareness-Training: Wichtige Information

**Verteiler: alle E-Mail-Nutzer:innen & Internet-Nutzer:innen**

Sehr geehrte Damen und Herren,

in den kommenden Monaten wird in Ihrer Organisation ein Awareness-Training stattfinden, um das Bewusstsein aller E-Mail- und Internet-Nutzer:innen für IT-Sicherheit zu schärfen.

Im Rahmen dieses Trainings werden alle E-Mail-Benutzer:innen mehrere gefälschte E-Mails erhalten, die darauf abzielen, diese Benutzer:innen zum Klicken auf unbekannte Links und Dateien zu verleiten.

Das Training ist ungefährlich, da durch Klicken auf die Links und Dateien kein Hackerangriff gestartet wird. Statt dessen erhalten die Benutzer:innen eine weitere Information zum Erkennen von gefälschten E-Mails.

### **Was Sie wissen müssen:**

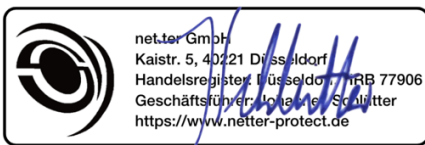
1. Gefälschte E-Mails: Sie werden E-Mails erhalten, die echt aussehen, aber in Wirklichkeit gefälscht sind. Diese E-Mails können Links oder Anhänge enthalten, die bei einem echten Angriff potenziell gefährlich sind. Im Training sind diese Link und Anhänge jedoch ungefährlich.
2. Ziel des Trainings: Das Ziel dieses Trainings ist es, Ihre Fähigkeit zu verbessern, solche Phishing-Versuche zu erkennen und entsprechend zu handeln. Es ist wichtig, dass Sie aufmerksam bleiben und verdächtige E-Mails melden.
3. Überprüfung: sofern Sie auf einen gefälschten Link klicken, wird dieses dokumentiert und sie erhalten eine kurze Information zum Thema Phishing. Sollten Sie mehrfach Links in den gefälschten E-Mails angeklickt haben, werden Sie zu einer weiteren Sensibilisierung eingeladen.

**Was Sie tun sollten:**

- Seien Sie aufmerksam: Überprüfen Sie die Absenderadresse und den Inhalt Ihrer E-Mails im Posteingang sorgfältig.
- Öffnen Sie keine unbekannten Links oder Anhänge: Klicken Sie nicht auf Links und öffnen Sie keine Anhänge, wenn Sie sich nicht sicher sind, dass die E-Mail echt ist.
- Melden Sie verdächtige E-Mails: Wenn Sie mehrfach verdächtige E-Mails erhalten, melden Sie diese sofort an die IT-Abteilung/ die EDV-Beauftragten. Nicht zu melden sind einfache SPAM-E-Mails, die Sie mittlerweile vielfach erhalten.

Wir danken Ihnen für Ihre Aufmerksamkeit und Ihre Mitarbeit bei diesem wichtigen Training. Gemeinsam können wir die Sicherheit Ihrer Organisation verbessern.

Mit freundlichen Grüßen aus Düsseldorf



Johannes Schlütter  
Datenschutzbeauftragter

## Checkliste zur Erkennung von Phishing-E-Mails

Um Ihnen zu helfen, Phishing-E-Mails zu erkennen und sicher zu handeln, haben wir eine Checkliste erstellt. Bitte verwenden Sie diese Checkliste, um verdächtige E-Mails zu identifizieren:

### 1. Absenderadresse überprüfen:

- Ist die E-Mail-Adresse des Absenders bekannt und vertrauenswürdig?
- Stimmt die Domain der E-Mail-Adresse mit der offiziellen Domain der Organisation überein?  
echte Adresse: @duesseldorf.de  
gefälschte Adresse: @duesseldorf-online.de
- Klicken Sie zum Erkennen mit Ihrer rechten Maustaste auf die E-Mail-Adresse des Absenders und schauen sich diese genau auf.

### 2. Betreffzeile und Inhalt prüfen:

- Ist die Betreffzeile ungewöhnlich oder alarmierend?
- Enthält die E-Mail Rechtschreib- oder Grammatikfehler?
- Ist der Inhalt der E-Mail unpersönlich oder allgemein gehalten?

### 3. Links und Anhänge untersuchen:

- Bewegen Sie den Mauszeiger über Links, um die tatsächliche URL anzuzeigen. Ist die URL verdächtig oder unbekannt?
- Öffnen Sie keine Anhänge, wenn Sie den Absender nicht kennen oder die E-Mail verdächtig erscheint.

### 4. Dringlichkeit und Aufforderungen hinterfragen:

- Fordert die E-Mail zu dringenden Handlungen auf, wie z.B. das sofortige Ändern von Passwörtern oder die Bereitstellung persönlicher Informationen?
- Droht die E-Mail mit negativen Konsequenzen, wenn nicht sofort gehandelt wird?

### 5. Ungewöhnliche Anfragen erkennen:

- Fordert die E-Mail sensible Informationen wie Passwörter, Bankdaten oder persönliche Daten an?
- Ist die Anfrage ungewöhnlich oder untypisch für den Absender?

### 6. Signatur und Kontaktinformationen überprüfen:

- Enthält die E-Mail eine offizielle Signatur mit vollständigen Kontaktinformationen?
- Stimmen die Kontaktinformationen mit den offiziellen Informationen der Organisation überein?

### **Was tun bei verdächtigen E-Mails?**

- Nicht klicken: Klicken Sie nicht auf Links und öffnen Sie keine Anhänge.
- Abstimmen: stimmen Sie sich mit der IT-Abteilung ab. Diese hat meist Richtlinien zum Umgang mit Phishing-E-Mails erlassen.
- Löschen: Löschen Sie die verdächtige E-Mail aus Ihrem Posteingang.