E-Mail-Security-Test

2-Minuten-Check der aktuellen E-Mail-Konfiguration

Ziel: Schnelle Überprüfung Ihrer E-Mail-Sicherheit mit sofortigen Handlungsempfehlungen
Dauer: 2 Minuten
Auswertung: Automatische Risikobewertung

🔍 TEIL 1: Basis-Konfiguration (30 Sekunden)

1.1 Spam-Filter Status

Aktion: Öffnen Sie Ihren E-Mail-Client/Webmail
☐ **Spam-Ordner vorhanden und aktiv**
☐ **Letzte Spam-E-Mails im Spam-Ordner (nicht im Posteingang)**
☐ **Spam-Filter-Einstellungen zugänglich**

✅ **Grün:** Alle Punkte erfüllt
🟡 **Gelb:** 2 von 3 Punkten
🔴 **Rot:** Weniger als 2 Punkte

1.2 Verdächtige E-Mails im Posteingang

Aktion: Prüfen Sie Ihren aktuellen Posteingang
☐ **Keine E-Mails von unbekannten Absendern mit verdächtigen Betreffzeilen**
☐ **Keine E-Mails mit Anhängen von unbekannten Absendern**
☐ **Keine E-Mails mit dringenden Zahlungsaufforderungen**

❌ **Wenn Sie verdächtige E-Mails finden → NICHT ÖFFNEN!**

🔐 TEIL 2: Authentifizierung (30 Sekunden)

2.1 Multi-Faktor-Authentifizierung (MFA)

Aktion: Versuchen Sie sich auf einem neuen Gerät anzumelden

Test:
☐ **System fordert zweiten Faktor an (SMS, App, etc.)**
☐ **Login ohne zweiten Faktor nicht möglich**
☐ **MFA-Methode ist aktiv (nicht nur optional)**

Bewertung:

✅ **Grün:** Alle 3 Punkte erfüllt

🔴 **Rot:** MFA nicht aktiv oder umgehbar

2.2 Passwort-Stärke

Selbsttest Ihres E-Mail-Passworts:

☐ **Mindestens 12 Zeichen lang**

☐ **Enthält Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen**

☐ **Nicht bei anderen Diensten verwendet**

☐ **Nicht älter als 1 Jahr**

📨 **TEIL 3: E-Mail-Header-Analyse (45 Sekunden)**

3.1 SPF/DKIM/DMARC Test

Für Admins - Prüfung Ihrer Domain:

1. **Gehen Sie zu:** https://mxtoolbox.com/spf.aspx
2. **Eingabe:** Ihre E-Mail-Domain (nach @-Zeichen)
3. **Prüfung in 15 Sekunden:**

☐ **SPF-Record vorhanden** (grünes Häkchen)

☐ **DKIM aktiviert**

☐ **DMARC-Richtlinie konfiguriert**

3.2 E-Mail-Verschlüsselung

Test einer eingehenden E-Mail:

1. **Wählen Sie eine externe E-Mail**
2. **Prüfen Sie die E-Mail-Eigenschaften/Header**

☐ **TLS-Verschlüsselung bei Übertragung**

☐ **Sichere Verbindung (kein "unsicher" Hinweis)**

⚠️ **TEIL 4: Phishing-Anfälligkeit (15 Sekunden)**

4.1 Aktueller Phishing-Check

Kurze Bewertung der letzten 7 Tage:

☐ **Keine verdächtigen "Dringend"-E-Mails erhalten**
☐ **Keine unerwarteten "Bestätigungs"-E-Mails**
☐ **Keine E-Mails mit verdächtigen Links geklickt**
☐ **Keine Passwort-Anfragen von "Banken/Services"**

Wenn auch nur ein Punkt zutrifft → Sofortige Überprüfung nötig!

📊 SOFORT-AUSWERTUNG

🟢 AUSGEZEICHNET (Alle Bereiche grün)

Ihre E-Mail-Sicherheit ist vorbildlich konfiguriert!

Empfehlung:

- Vierteljährliche Überprüfung beibehalten
- Mitarbeiter-Awareness regelmäßig schulen

🟡 GUT (Überwiegend grün/gelb)

Grundschutz vorhanden, aber Verbesserungen möglich.

Sofort-Maßnahmen:

1. **MFA aktivieren** (falls nicht vorhanden)
2. **Spam-Filter optimieren**
3. **SPF/DKIM/DMARC konfigurieren**

🔴 KRITISCH (Rote Bereiche vorhanden)

Dringende Sicherheitslücken - sofortiges Handeln erforderlich!

Notfall-Maßnahmen:

1. **MFA SOFORT aktivieren**
2. **Passwörter SOFORT ändern**
3. **IT-Security-Experten kontaktieren**
4. **Mitarbeiter warnen**

🚀 SCHNELLE VERBESSERUNGEN

In 5 Minuten umsetzbar:

- ✅ **MFA aktivieren** (Authenticator-App installieren)
- ✅ **Spam-Filter-Level erhöhen**
- ✅ **Verdächtige E-Mails löschen**

In 30 Minuten umsetzbar:

- ✅ **E-Mail-Passwort ändern** (12+ Zeichen, komplex)
- ✅ **E-Mail-Regeln für Phishing erstellen**
- ✅ **Backup-Recovery-E-Mail einrichten**

In 1 Stunde umsetzbar:

- ✅ **SPF-Record für Domain einrichten**
- ✅ **DKIM aktivieren**
- ✅ **E-Mail-Archivierung überprüfen**

⚡ ERWEITERTE TESTS

Für IT-Verantwortliche:

1. DNS-Security-Check (2 Min.):

nslookup -type=TXT ihre-domain.de

Prüfung auf SPF/DMARC-Records

2. Mail-Server-Security-Scan:

- **Tool:** https://www.ssllabs.com/ssltest/
- **Eingabe:** Ihr Mail-Server
- **Ziel:** A+ Rating

3. Phishing-Simulation:

- **Interne Test-E-Mail** an 5 Mitarbeiter senden
- **Reaktionen beobachten**
- **Klickrate messen**

🎯 CHECKLISTE FÜR REGELMÄSSIGE TESTS

Monatlich:
☐ Spam-Filter-Effizienz prüfen
☐ Verdächtige E-Mails analysieren
☐ MFA-Logs überprüfen

Quartalsweise:
☐ DNS-Records aktualisieren
☐ E-Mail-Richtlinien überprüfen
☐ Phishing-Simulation durchführen

Jährlich:
☐ Vollständiger Security-Audit
☐ Mitarbeiter-Schulung
☐ Incident-Response-Plan testen

⭐ BONUS-TIPPS

Sofortige Sicherheit:

1. **"Externe E-Mail" Warnung aktivieren**
2. **Automatische Bild-Download deaktivieren**
3. **Makros in Anhängen blockieren**
4. **Link-Preview deaktivieren**

Profi-Tipp: Richten Sie eine **separate E-Mail für kritische Services** ein:

- Banking
- Cloud-Services
- Administrative Zugänge

Nächster Test empfohlen: In 30 Tagen zur Erfolgskontrolle