CHECKLISTE

Der Mittelstand.
BVMW e.V.
Bundesverband

Phishing-Mails erkennen & richtig handeln

Wie erkenne ich Phishing-Mails?

- ☐ **Unbekannter oder gefälschter Absender:** Die E-Mail-Adressen wirken vertraut, sind aber leicht verändert (z. B. „name@firma-secure.com“ statt „name@firma.com“).
- ☐ **Unpassende Ansprache:** Allgemeine Anreden wie „Sehr geehrter Kunde“ oder fehlerhafte Schreibweise von Namen.
- ☐ **Rechtschreibfehler:** Häufig enthalten die E-Mails auffällige Schreib- und Grammatikfehler.
- ☐ **Dringlichkeit:** Aufforderungen wie „Sofort handeln!“ oder „Ihr Konto wird gesperrt!“ sollen Druck ausüben.
- ☐ **Anfragen zu sensiblen Daten:** Forderungen nach Passwörtern, Kontodaten oder anderen vertraulichen Informationen.
- ☐ **Ungewöhnliche Links:** Links führen zu unbekannten oder verdächtigen Webseiten (prüfen Sie diese durch Mouseover, ohne zu klicken).
- ☐ **Anhänge mit Risiken:** Unbekannte, nicht angeforderte Anhänge sowie Links zu Filehosting-Dienstleistern wie Dropbox können Schadsoftware enthalten.
- ☐ **Identitätsdiebstahl:** E-Mails scheinen von einer bekannten Person (z. B. Vorgesetzten oder Kollegen) zu kommen, enthalten aber ungewöhnliche Bitten (z. B. Überweisungen oder vertrauliche Informationen).

Stellen Sie sich auch diese Fragen:

- ☐ Kenne ich den Absender der E-Mail?
- ☐ Erwarte ich eine E-Mail von dem Absender der E-Mail?
- ☐ Passt der Inhalt der E-Mail zu meiner Erwartungshaltung, wenn ich E-Mails von der Person bekommen sollte?
- ☐ Kommt mir die Handlungsaufforderung verdächtig vor, also werden Dateien zur Verfügung gestellt, nach denen ich nicht gefragt habe?

Wie verhalte ich mich bei dem Verdacht auf eine Phishing-Mail?

- ☐ **E-Mail überprüfen:** Hinterfragen Sie und prüfen Sie Absenderadresse und Linkziele genau.
- ☐ **Nicht öffnen:** Klicken Sie keine verdächtigen Anhänge oder Links (auch zu Filesharing-Anbietern, z. B. Dropbox) an.
- ☐ **Keine Daten preisgeben:** Geben Sie keine Passwörter, Bankdaten oder andere sensible Informationen weiter.
- ☐ **Persönliche Rücksprache:** Fragen Sie bei ungewöhnlichen Bitten angeblicher Kolleginnen, Kollegen oder Vorgesetzter immer telefonisch oder persönlich nach – antworten Sie nicht per E-Mail auf die verdächtige E-Mail.
- ☐ **IT-Abteilung informieren:** Melden Sie verdächtige E-Mails sofort an die IT-Abteilung oder den Sicherheitsbeauftragten.
- ☐ **E-Mail löschen:** Löschen Sie die betreffende E-Mail bei Verdacht dauerhaft – auch aus dem Papierkorb.

Wem sollte ich Phishing-Mails melden?

- ☐ **Unternehmensintern:** Melden Sie den Verdacht auf eine Phishing-E-Mail unverzüglich an Ihre IT-Abteilung oder Ihren Sicherheitsbeauftragten.
- ☐ **Externe Stellen (falls erforderlich):** Informieren Sie bei größeren Vorfällen ggf. die Datenschutzbehörde oder den IT-Dienstleister Ihres Unternehmens.
- ☐ **Ggf. weitere Betroffene:** Stellen Sie fest, dass Ihre E-Mail-Adresse von einem Identitätsdiebstahl betroffen ist, empfiehlt es sich, alle Personen im Adressbuch über den Identitätsdiebstahl und die über das Postfach versendeten Phishing-Mails in Kenntnis zu setzen.

Stand: Januar 2025

© Der Mittelstand. BVMW e.V. 2025. Alle Rechte vorbehalten. Transparenzregisternummer: 082217218282-59
Der Mittelstand. BVMW e.V. ist unter der Registernummer R001657 eingetragen
im Lobbyregister für die Interessensvertretung gegenüber dem Bundestag und der Bundesregierung.

CHECKLISTE

Der Mittelstand.
BVMW e.V.
Bundesverband

Was mache ich, wenn die Phishing-Mail nicht erkannt und ein Anhang geöffnet oder Link geklickt wurde?

- ☐ **Sofort handeln:** Wenn ein Link geklickt oder ein Anhang geöffnet wurde, den Rechner sofort vom Netzwerk trennen (z. B. WLAN deaktivieren oder Netzwerkkabel entfernen).
- ☐ **IT-Abteilung informieren:** Melden Sie den Vorfall sofort Ihrer IT-Abteilung und beschreiben Sie, was passiert ist.
- ☐ **Kennwörter ändern:** Falls sensible Daten preisgegeben wurden, Passwörter sofort ändern und Mehr-Faktor-Authentifizierung aktivieren. Anschließend prüfen Sie Ihr Mailingprogramm auf neu eingestellte Regeln.
- ☐ **System prüfen lassen:** Die IT-Abteilung sollte den betroffenen Rechner auf Schadsoftware überprüfen und alle notwendigen Maßnahmen einleiten.
- ☐ **Ruhe bewahren:** Schnelles und überlegtes Handeln kann weiteren Schaden verhindern.

Prävention & Schulung

- ☐ **Schulungen nutzen:** Phishing-Mails werden immer besser und sind damit schlechter als solche zu erkennen. Die regelmäßige Sensibilisierung der Mitarbeitenden, insbesondere zu Identitätsdiebstahlsangriffen und kompromittierten Accounts, sorgt für einen Basisschutz.
- ☐ **Sichere Passwörter & regelmäßige Passwortwechsel:** Stellen Sie Ihren Mitarbeitenden entsprechende Erinnerungen als Termin ein oder treffen Sie durch Ihre IT-Abteilung entsprechende Maßnahmen, damit das Passwort regelmäßig, z. B. alle 3 Monate, geändert werden muss.
- ☐ **Mehr-Faktor-Authentifizierung (MFA):** Aktivieren Sie mindestens eine 2-Faktor-Authentifizierung, um sensible Daten und Konten zusätzlich zu sichern.
- ☐ **Systeme aktuell halten:** Installieren und aktualisieren Sie Sicherheitsupdates (Patches) und Antivirensoftware regelmäßig.

Der wohl wichtigste Tipp ist aber wie an vielen anderen Stellen auch: **Lassen Sie den gesunden Menschenverstand walten.** Lassen Sie Skepsis zu und fragen lieber einmal mehr als einmal zu wenig nach. So können Sie mit persönlicher Rücksprache und Wachsamkeit Phishing-Versuche und Identitätsdiebstahlsangriffe erkennen und Ihr Unternehmen schützen. Scheuen Sie sich also nicht, Vorgesetzte, Kolleginnen und Kollegen oder Ihre IT-Abteilung anzusprechen, **denn Sicherheit ist Teamarbeit!**

Der Mittelstand. BVMW e.V. ist ein freiwillig organisierter Unternehmerverband und vertritt rund 30.000 Mitglieder. Die mehr als 300 Repräsentanten des Verbandes organisieren mehr als 2.000 Veranstaltungen pro Jahr.

Kontakt
Der Mittelstand. BVMW e.V.
Potsdamer Straße 7, 10785 Berlin
Telefon: +49 30 533206-0, Telefax: +49 30 533206-50
E-Mail: info@bvmw.de

© Der Mittelstand. BVMW e.V. 2025. Alle Rechte vorbehalten. Transparenzregisternummer: 082217218282-59
Der Mittelstand. BVMW e.V. ist unter der Registernummer R001657 eingetragen
im Lobbyregister für die Interessensvertretung gegenüber dem Bundestag und der Bundesregierung.