

Checkliste: Phishing erkennen

1. Prüfen

- Kenne ich den Absender? Passt die E-Mail-Adresse zur Firma?
- Wirkt der Name vertrauenswürdig – oder „nur so ähnlich“?
- Verständlicher Text – oder komische Formulierungen?
- Dringender Ton („Sofort handeln!“) oder ungewöhnliche Aufforderungen?
- Ergibt der Betreff Sinn, wurde die Nachricht erwartet?
- Passt das zum aktuellen Geschäftsvorfall?

2. Persönliche Daten gefordert?

- Wird nach Passwort, TAN, Zugangsdaten gefragt?

👉 **Sofort löschen – seriöse Firmen fragen das nie per Mail**

3. Links prüfen

- Mit Maus über den Link fahren → stimmt die Adresse?
- Komische Domains oder Kurzlinks (bit.ly, tinyurl etc.)?

👉 **Nicht klicken, wenn du dir nicht 100 % sicher bist**

4. Check!

- Website manuell aufrufen (nicht über den Link), Firma anrufen

👉 **Grundregel: lieber einmal zu viel prüfen als einmal zu wenig**

Sofort handeln, wenn...

- du versehentlich Daten eingegeben hast
- du auf einen verdächtigen Link geklickt hast

👉 **Sofort Passwort ändern!**

