E-Mail, Links und Anhänge

5.1 Links prüfen

Ein Link kann anders aussehen als sein tatsächliches Ziel. Deshalb sollte bei unerwarteten Nachrichten nicht blind geklickt werden. Besonders Anmeldeseiten verdienen Aufmerksamkeit.

Vergleich aus dem Alltag

Ein Wegweiser kann „Bahnhof“ tragen und trotzdem in die falsche Richtung zeigen.

Beispiel aus dem Arbeitsalltag

Der sichtbare Text nennt Microsoft 365, das tatsächliche Ziel gehört aber zu einer unbekannten Domain.

Was soll ich tun?

Der Text eines Links und sein tatsächliches Ziel können verschieden sein.

> **Merke:** Im Zweifel den Dienst über das bekannte Lesezeichen oder die selbst eingegebene Adresse öffnen.

5.2 Dateianhänge

Dateianhänge können normalen Inhalt, aber auch schädliche Programme oder präparierte Dokumente enthalten. Entscheidend ist deshalb nicht nur der Dateiname, sondern auch, ob die Nachricht und der Anhang erwartet wurden.

Vergleich aus dem Alltag

Ein Paket kann gefährlich sein, obwohl außen ein harmloser Aufkleber klebt.

Beispiel aus dem Arbeitsalltag

Eine unerwartete Bewerbung, Rechnung oder Versandinformation enthält eine ungewöhnliche Datei.

Was soll ich tun?

Erwartet und plausibel ist wichtiger als ein vertraut klingender Dateiname.

> **Merke:** Bei Unsicherheit nicht öffnen und die Nachricht an die vorgesehene Supportstelle melden.

5.3 Makros und ausführbare Dateien

Bestimmte Dateien können Programmcode enthalten oder ausführen. Wenn ein Dokument unerwartet verlangt, Makros oder besondere Sicherheitsfunktionen zu aktivieren, ist Vorsicht geboten.

Vergleich aus dem Alltag

Ein normales Blatt Papier verlangt nicht, dass du zuerst die Alarmanlage abschaltest, bevor du es lesen kannst.

Beispiel aus dem Arbeitsalltag

Ein unbekanntes Office-Dokument fordert nach dem Öffnen dazu auf, Inhalte oder Makros zu aktivieren.

Was soll ich tun?

Sicherheitswarnungen nicht wegklicken, nur damit ein Dokument funktioniert.

> **Merke:** Nicht aktivieren und bei unerwarteten Dateien die IT fragen.

5.4 Geschäftliche Daten an den richtigen Empfänger

Ein Sicherheitsvorfall kann auch ohne Hacker entstehen: Eine E-Mail an den falschen Empfänger oder der falsche Anhang kann vertrauliche Informationen offenlegen.

Vergleich aus dem Alltag

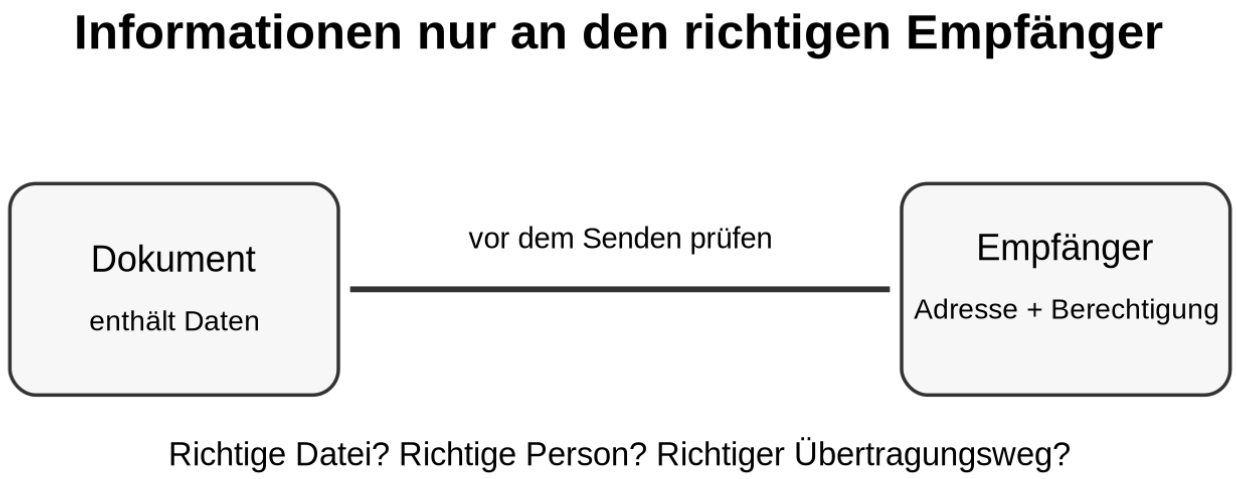
Ein falsch adressierter Brief erreicht ebenfalls die falsche Person – nur lässt sich eine E-Mail oft noch schneller verschicken.

Beispiel aus dem Arbeitsalltag

Vor dem Versand enthält die Nachricht mehrere ähnlich klingende Empfänger oder einen automatisch ergänzten Kontakt.

Was soll ich tun?

Richtige Datei + richtiger Empfänger + richtiger Übertragungsweg.



> **Merke:** Vor dem Senden Empfänger, CC-Feld und Anhänge noch einmal prüfen.