



Phishing-Mails erkennen – 6 Tipps

Phishing-Mails kommen manchmal sehr gut getarnt daher. Diese sechs Tipps helfen Ihnen, die kriminellen Mails zu erkennen und die Gefahren zu umgehen:

1. **Falsche Rechtschreibung und Grammatik:** Am einfachsten erkennen Sie Phishing-Mails, die in unkorrektem Deutsch verfasst und schlecht übersetzt sind oder zum Teil in Englisch oder Französisch erscheinen.
2. **Dringender Handlungsbedarf:** Wenn Sie aufgefordert werden, sofort tätig zu werden, etwa weil Ihr Kundenkonto angeblich gesperrt sei oder Sie eine Zahlung tätigen müssen, sollten Sie skeptisch sein.
3. **Daten eingeben:** Ein Hinweis auf Phishing ist zudem, dass Sie dazu aufgefordert werden, über einen Link aus der Mail heraus Daten einzugeben, seien es Passwörter oder Zahlungsdaten.
4. **Links anklicken:** Generell sollten Sie darauf verzichten, aus solchen Mails heraus Links anzuklicken. **Falls Sie sich trotzdem unsicher sind:** Rufen Sie die Webseite des Anbieters direkt auf, und zwar nicht über den Link aus der Mail, sondern tippen Sie diese selbst in den Browser ein oder rufen die App auf. Loggen Sie sich ein und sehen in Ihrem Kundenkonto nach, ob es dort Unregelmäßigkeiten gibt. Falls nicht, müssen Sie sich auch keine Gedanken machen, dass irgendwelcher Handlungsbedarf besteht.

5. **Fehlender oder falscher Name:** Zwar werden Phishing-Mails immer geschickter, doch viele erkennt man daran, dass Ihr Name in der Anrede gänzlich fehlt. Dann werden Sie beispielsweise mit „Sehr geehrter Kunde“ angesprochen. Manchmal steht auch ein Name in der Anrede, doch er stimmt nicht mit dem überein, wie Sie auf der betreffenden Webseite (etwa Amazon) angesprochen werden.
6. **Mailheader:** Selbst wenn alles seriös erscheint, die Mail in flüssigem Deutsch verfasst ist und der Absender unauffällig aussieht, kann es sich trotzdem um eine Phishing-Mail handeln. Aufschluss gibt der Mailheader, denn dort verstecken sich eindeutige technische Informationen, die nicht auf den ersten Blick sichtbar sind. [Hier finden Sie eine Anleitung](#), wie Sie auch als Laie einen Mailheader auslesen und verstehen können.

Quelle: <https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/merkmale-einer-phishingmail-6073>