



## Anleitung Email gehackt – was tun

### E-Mail gehackt? Das müssen Sie tun!



Ihr E-Mail-Konto ist mit vielen anderen Konten verknüpft. Wenn Fremde Zugriff haben, müssen Sie daher schnell handeln.

Wurde Ihr E-Mail-Konto gehackt, müssen Sie schnell sein, damit nicht noch mehr passiert. COMPUTER BILD erklärt, was zu tun ist und wie Sie sich künftig absichern.

#### Inhaltsverzeichnis

- [E-Mail-Account gehackt: Virenscan durchführen](#)
- [E-Mail-Konto gehackt: Passwörter ändern](#)
- [Outlook: Eigenes Passwort auslesen](#)
- [Kontakte warnen](#)
- [Kontoeinstellungen überprüfen](#)
- [Vorsorge treffen](#)

Haben Hacker Ihr E-Mail-Konto gehackt? Dann sollten Sie schnellstmöglich reagieren, damit die Angreifer nicht noch mehr Konten übernehmen. In diesem Ratgeber erfahren Sie Schritt für Schritt, was zu tun ist und wie Ihr Konto künftig sicher bleibt.

#### Antivirenprogramme

[Komplette Liste: Antivirenprogramme](#)

#### **E-Mail-Account gehackt: Virenscan durchführen**

Möglicherweise waren Keylogger und andere Schadprogramme am Hack Ihres Kontos beteiligt. Scannen Sie daher Ihren PC gründlich mit einer Schutzsoftware, noch bevor Sie neue Passwörter festlegen – sonst spielen Sie die neuen Zugangsdaten möglicherweise direkt den Angreifern zu. Während Sie die folgenden Schritte ausführen, lassen Sie auch auf allen anderen PCs, Tablets und Smartphones Virens cans laufen.

#### **E-Mail-Konto gehackt: Passwörter ändern**



Es mag trivial klingen, doch wenn auch nur der bloße Verdacht besteht, dass Ihr E-Mail-Konto gehackt sein könnte, sollten Sie schleunigst Ihr Zugangspasswort zum Mail-Postfach ändern! So lässt sich möglicherweise Schlimmeres verhindern. Tipps zur Wahl sicherer Passwörter bietet das obige Video. Können Sie sich gar nicht mehr anmelden, weil Ihr Kennwort geändert wurde? Dann wenden Sie sich an den Kundendienst des Mail-Anbieters, um Ihre Identität zu bestätigen und wieder Zugang zu erlangen. Ist das geschafft, ändern Sie möglichst auch alle anderen Passwörter, denn über Ihren Posteingang haben Angreifer möglicherweise bereits Zugriff auf andere Konten erlangt. Wichtig: Verwenden Sie für jede Anmeldung im Internet ein abweichendes Passwort, denn sonst gilt: Ist ein Konto gehackt, haben die Angreifer sofort Zugriff auf die anderen. Auch ein [Passwort-Manager](#) hilft unter Umständen dabei, ohne Kopfzerbrechen sichere Passwörter einzusetzen. Um auf Nummer sicher zu gehen, ändern Sie zusätzlich Ihre Antworten auf Sicherheitsfragen

## **Passwort-Manager**

[Komplette Liste: Passwort-Manager](#)

## **Outlook: Eigenes Passwort auslesen**

Falls Sie Ihr E-Mail-Passwort nicht mehr wissen, lässt sich das über Outlook auslesen. Das können Hacker übrigens auch, sofern sie direkten Zugriff auf Ihren PC haben. Wie es genau funktioniert, erklärt COMPUTER BILD in einem [Tipp](#). Achtung: Machen Sie das nur mit eigenen Passwörtern. Kennwörter anderer Personen auf diese Weise auszulesen, ist unter Umständen strafbar.

## **Kontakte warnen**

Ist Ihr Postfach erst einmal geknackt, nutzen die Ganoven es möglicherweise als Malware-Schleuder mit Vertrauensbonus: Erhalten Freunde und Verwandte E-Mails mit dubiosen Anhängen von Ihrem Konto, sind sie vielleicht eher gewillt, die digitalen Anlagen zu öffnen. So hoffen die Missetäter, auch Konten oder gar gesamte PCs weiterer Opfer zu kapern. Wirken Sie dem entgegen, indem Sie Freunde und Verwandte über den Hack informieren und vor möglichen betrügerischen E-Mails warnen.

## **Kontoeinstellungen überprüfen**

Haben Sie (wieder) Zugang zu Ihrem E-Mail-Konto, stellen Sie sicher, dass dort keine Signatur oder Abwesenheitsnotiz eingerichtet ist, die unbekannte Links enthält. Prüfen Sie sicherheitshalber auch, ob Einstellungen in sozialen Netzwerken verändert wurden, etwa bei Facebook, und ob dort möglicherweise falsche Freunde hinzugekommen sind. Sollte dasselbe E-Mail-Konto bereits mehrfach gehackt worden sein, bietet der E-Mail-Anbieter möglicherweise eine unzureichende Sicherheit. In diesem Fall sollten Sie einen Anbieterwechsel erwägen. Prüfen Sie zudem, ob die Hacker eine [Weiterleitung Ihrer E-Mails](#) eingerichtet haben. Darüber würden alle Passwort-Änderungsmails auch an die Kriminellen gehen, und sie könnten sich direkt wieder Zugang zu Ihren Online-Konten beschaffen – selbst wenn sie mittlerweile aus dem E-Mail-Konto ausgesperrt sind. Ist eine fremde Weiterleitung eingerichtet, löschen Sie diese.

## **Vorsorge treffen**

Sind alle anderen Maßnahmen getroffen, wappnen Sie sich für die Zukunft, um eine Wiederholung des Hacks zu vermeiden. Prüfen Sie etwa, ob sich Sicherheitseinstellungen im E-Mail-Konto verschärfen lassen, und aktivieren Sie die Zwei-Faktor-Authentifizierung, sofern verfügbar. Um künftig informiert zu werden, falls Ihre Zugangsdaten bei einer Datenpanne öffentlich geworden sind, nutzen Sie den [COMPUTER BILD-Account-Alarm](#). Den erhalten



**DIETMAR WALKER - PC-BLITZHELFER - NOTDIENST**  
**Nationalgasse 14 • 72124 Pliezhausen • Ø Tel. 07127 / 89194 - Fax 89118**  
**Internet: <http://www.pc-blitzhelfer.de> – Mobil 0172-882 79 55**

---

Sie kostenlos über den obigen Link. Es ist aber auch möglich, dass die Angreifer die Zugangsdaten direkt bei Ihnen abgegriffen haben. Durch **Phishing** oder Malware auf Ihren Geräten können die Angreifer Ihre Daten stehlen und selbst verwenden. Installieren Sie daher ein aktuelles Virenschutzprogramm und informieren Sie sich über gängige Phishing-Tricks und wie Sie diese erkennen. Zudem sollten Sie prüfen, ob Sie für jedes Konto ein eigenes, sicheres Passwort verwenden. Nutzen Sie dafür am besten einen **Passwort-Manager**.

Quelle: <https://www.computerbild.de/artikel/cb-Tipps-Software-Outlook-Passwort-anzeigen-31502537.html>