

# Sicherer Umgang mit privaten E-Mail-Accounts

Immer wieder melden Konsument/innen dem Internet Ombudsmann, dass ihnen der **Zugriff** auf ihre **privaten, meist kostenlosen E-Mail-Accounts** bei Anbietern wie GMX, Yahoo, Hotmail oder Gmail **verwehrt** wird. Dies kann unterschiedliche Gründe haben, die von einer Sperre seitens der Anbieter wegen verdächtiger Zugriffe über gehackte E-Mail-Konten bis hin zu vergessenen Zugangsdaten reichen. Nicht selten geht damit der **Zugang zu wichtigen Dokumenten und Kontakten verloren**.



Zahlungsmittel - Informationen, Kontaktdaten, Dokumente, Fotos etc.).

- Auch besteht die Gefahr, dass der E-Mail-Account missbraucht wird, um **Spam- bzw. Phishing-Mails** oder sonstige **betrügerische E-Mails** (siehe z.B. Watchlist Internet-Bericht „Abgezockt von den eigenen Freunden?!“) **im Namen des Betroffenen** an die im E-Mail-Account gespeicherten Kontakte zu versenden. Dies ist vor allem problematisch, wenn die E-Mail-Adresse auch für **berufliche Zwecke** genutzt wird: Denn dann erhalten auch Geschäftspartner oder Vorgesetzte entsprechende unseriöse E-Mails.

Verliert man den Zugang zu seinem E-Mail-Account, kann der Zugriff meist durch die **Beantwortung von Sicherheitsfragen** oder die **Anforderung eines Links zur Passwort-Wiederherstellung** an eine alternative E-Mail-Adresse wiederhergestellt werden. Dabei ergeben sich jedoch oft folgende Probleme:

In der Praxis wird die Problemlösung oft erschwert, weil viele der E-Mail-Accounts mittlerweile einige Jahre in Verwendung sind und von den Nutzer/innen nicht regelmäßig gewartet werden.

Wurde ein E-Mail-Account **gehackt** bestehen zusätzliche Risiken:

- So können Dritte **Zugriff auf** die im E-Mail-Account gespeicherten, teils sensiblen **Daten** erlangen (z.B. Passwörter,

Vor allem wenn eine lange Zeit seit der Einrichtung des E-Mail-Accounts vergangen ist, können die **Sicherheitsfragen** häufig **nicht mehr beantwortet** werden, meist weil die Antworten schlicht vergessen wurden. Dies ist vor allem dann der Fall, wenn die Fragen nicht wahrheitsgetreu beantwortet wurden.



# Sicherer Umgang mit privaten E-Mail-Accounts

- Die hinterlegte **alternative E-Mail-Adresse** kann außerdem bereits seit längerer Zeit **nicht mehr existieren** bzw. der Zugang zu dieser kann ebenfalls nicht mehr gegeben sein. Beispielsweise weil alternative E-Mail-Adressen kaum benutzt werden und somit das zugehörige Passwort vergessen oder der E-Mail-Account wegen Inaktivität gesperrt wurde.
- Beim Anlegen einer E-Mail-Adresse werden nicht selten **falsche Daten** zur eigenen Person angegeben. In diesem Fall kann die **eigene Identität** gegenüber dem E-Mail-Anbieter auch durch das Übersenden einer Ausweiskopie **nicht nachgewiesen werden**.

## Tipps

- Speichern Sie wichtige Dokumente und Kontaktdaten immer auch extern ab.
- Geben Sie immer eine gültige und aktive alternative E-Mail-Adresse an.
- Halten Sie Ihren E-Mail-Account immer am neuesten Stand, überprüfen Sie die Einstellungen regelmäßig (alternative E-Mail-Adresse, wichtigste Angaben zu Ihrer Person etc.)
- Geben Sie bei der Einrichtung eines E-Mail-Accounts keine fiktiven Daten an, dies kann im Fall von Zugriffsproblemen eine Lösung erheblich erschweren.
- Beantworten Sie die Sicherheitsfragen so, dass Sie sich diese merken können. Speichern Sie diese Angaben sicher ab (z.B. in einem Passwort-Safe auf dem Smartphone).
- Beachten Sie die Hinweise im Hilfebereich des jeweiligen Anbieters, wenn Sie Probleme mit Ihrem E-Mail-Account haben.
- Verwenden Sie sichere Passwörter und ändern Sie diese regelmäßig, um das Risiko zu minimieren, dass der Account gehackt wird. Sollten Sie den Verdacht haben, dass Ihr Account gehackt worden sein könnte, ändern Sie das Passwort schnell, wenn das noch möglich ist!
- Beachten Sie, dass Sie bei kostenlosen Anbietern in der Praxis kaum Chancen haben Ansprüche geltend zu machen, wenn es zu Datenschutzverletzungen oder Datenverlust kommt.