Am Blümlingspfad 115
53359 Rheinbach
(02226) 899 7646
mail@digihelp.de

Benutzerkonten und-profile

Inhaltsverzeichnis

digiHelp IT Beratung

Am Blümlingspfad 115
53359 Rheinbach
(02226) 899 7646
mail@digihelp.de

Einleitung

Bei der Einrichtung von Geräten wie Smartphones, Tablets oder PC mit den Betriebssystemen Android [Google], iOS [Apple] oder Windows 11 [Microsoft] wird der Besitzer aufgefordert, ein Benutzerkonto anzulegen oder ein bestehendes Konto anzumelden. Auch beim Besuch von Webseiten mit einem Browser oder bei der Nutzung von vielen Apps auf dem Smartphone bzw. Tablet ist eine Anmeldung zur persönlichen Identifikation und Wiedererkennung erforderlich.

Grundlage für alle Anmeldungen ist eine eigene E-Mail-Adresse[1] (gelegentlich auch eine Telefonnummer oder Kundenummer) in Verbindung mit einem Passwort. Dabei gibt es aber einiges zu beachten, damit der Betrieb dauerhaft möglichst reibungslos und sicher verläuft.

- Auswahl eines geeigneten E-Mail-Providers (Anbieters), Stichwort Datenschutz. Hier empfiehlt sich die Inanspruchnahme eines europäischen Anbieters, bei dem die Einhaltung der EU-Datenschutzgrundverordnung (DSGVO) am ehesten gewährleistet ist.
- Besuchen Sie die Sicherheitseinstellungen Ihres Profils und machen die dort erbetenen ergänzenden Angaben zum E-Mail-Nutzer Profil; damit Sie immer Herr Ihrer E-Mail-Adresse bleiben.
- Neue Anmeldeverfahren zur Verbesserung der Sicherheit und Nutzbarkeit wie die Zweifaktor-Authentifizierung (Passwort + Gesichtserkennung, Fingerabdruck, Wischmuster, TAN) und seit 2025 zunehmend den Passkeys
- Wie und womit soll auf Mails zugegriffen werden?
- Wie SPAM erkannt wird

Vorgehensweise bei der Wahl und Anlage von E-Mail-Adressen

- Legen Sie eine Liste an von allen Anbietern, bei denen Sie eine Mailadresse als Identifikation verwendet haben oder neuerdings verwenden. Diese Liste dient als Verwendungsnachweis. Vor der evtl. Kündigung einer Mail-Adresse, erkennen Sie so schnell, wo diese Adresse verwendet wurde. Vor der Kündigung muss diese Mailadresse überall geändert werden, wo sie verwendet wurde.
- Verzichten Sie, soweit möglich auf außereuropäische E-Mail-Anbieter
- Sollten Sie bereits Adressen wie gmail.com, icloud.com, aol.com o.ä. verwenden, legen Sie eine neue EU-Adresse an und benutzen Sie diese fortan
- Teilen Sie Ihren Kontakten die neue Adresse mit. Warten Sie ca. ein Jahr, bis niemand mehr die bisherige Adresse verwendet
- Kündigen Sie die nicht mehr zu verwendende E-Mail-Adresse, sobald Sie darüber keine Mails mehr erhalten bzw. sich mit dieser Adresse nirgendwo mehr anmelden.
- Verwenden Sie berufliche E-Mail-Adressen niemals für private Angelegenheiten und umgekehrt. Ihr Arbeitgeber ist verpflichtet, E-Mails zu archivieren und kann diese u. U. nach vielen Jahren noch einsehen – auch nach Ihrem Austritt.
- Besuchen Sie die Profil-Verwaltung bei Ihrem E-Mail-Anbieter und ergänzen Sie alle erforderlichen Informationen2, um bei einem plötzlichen Versagen des üblichen Anmeldeverfahrens wieder Zugriff auf Ihr E-Mail-Konto zu bekommen.

[1] Dies kann die gebräuchliche E-Mailadresse sein. Es muss keine neue Adresse sein.
[2] Alternative E-Mail-Adresse, SMS-fähige Telefonnummer wie z. Bsp. Ihre Mobilfunknummer

digiHelp IT Beratung

Am Blümlingspfad 115
53359 Rheinbach
(02226) 899 7646
mail@digihelp.de

Einrichten von Benutzerkonten und -profilen bei Apple, Google, Microsoft sowie E-Mail und anderen Konten

Ein Benutzerkonto (englisch user account), kurz Nutzerkonto oder Account, ist eine Zugangsberechtigung zu einem zugangsbeschränkten IT-System. Üblicherweise muss ein Benutzer sich beim Anmelden mit Benutzernamen und Kennwort/ Passwort authentifizieren.

Quelle: Wikipedia

Bei Android und iOS sind dies grundsätzlich Online Konten, d. h., die zugrundeliegenden Profile werden beim jeweiligen Hersteller gespeichert und können per Webbrowser eingesehen und gepflegt werden. Bei Microsoft kamen bis Windows 7 im Privatkundenbereich (Windows Home) nur lokale Konten ohne Profil Hinterlegung beim Hersteller zum Einsatz. Mit der Einführung von Windows 8 und seinem App Store hat sich Microsoft seinen Wettbewerbern Apple und Google angeschlossen. Über einen gut versteckten Dialog ist es zwar auch unter Windows 10/ 11 noch möglich, ein lokales Konto anzulegen aber es können dann nicht alle Möglichkeiten des Betriebssystems genutzt werden. Ein Grund hierfür ist, dass im Profil auch die Bezahldaten für App-Einkäufe hinterlegt sind.

Die Motivation hinter dieser Vorgehensweise ist u.a. das Ziel, einem Anwender auf allen seinen Endgeräten mit identischem Betriebssystem einheitliche und automatisch synchronisierte Einstellungen und Zugriffsmöglichkeiten anzubieten. Nur so ist es möglich, einmal gekaufte Apps auf allen eigenen Geräten zu benutzen und ggf. auch kostenfrei neu zu installieren – z. Bsp. nach einem Gerätetausch.

Um sich nicht selber im Fall einer Störung aus dem eigenen Gerät/ Konto auszuschließen, ist es wichtig, die geforderten Angaben im jeweiligen Profil vollständig zu hinterlegen und für den jederzeitigen Zugriff zu dokumentieren. Dazu gehören insbesondere SMS-fähige Telefonnummern, alternative E-Mail-Adressen (die auch ohne das betroffene Konto abrufbar sind) und Sicherheitsfragen nebst zugehörigen Antworten und natürlich die eigene Konto-/ Benutzer-ID mit Passwort.

Das einem persönlichen Benutzerkonto hinterlegte Benutzerprofil (Ihre Akte) bei einem Anbieter enthält identifizierende Angaben zum Benutzer, Benutzerrechte, sowie persönliche Einstellungen und Kontaktinformationen. Auch die Lizenzen für erworbene Nutzungsrechte sowie Verzeichnisse von Software/ Apps, Musik, Filmen, etc. werden hier hinterlegt. Das Profil ermöglicht u.a. die geräteübergreifende Synchronisation von persönlichen Daten und Einstellungen und erleichtert dadurch den Umstieg auf ein neues Endgerät durch Übernahme der bisherigen Daten und Einstellungen.

Die Tabelle zeigt abhängig vom Anbieter einige Links rund um die Benutzerkonten-Verwaltung:

	Apple	Google	Microsoft
Konto/ ID anlegen und pflegen	appleid.apple.com/de/	accounts.google.com	signup.live.com
An Konto anmelden	appleid.apple.com/de	accounts.google.com	login.live.com
Erläuterungen zu Konten und ID	https://support.apple.com/	support.google.com/	account.microsoft.com

digiHelp IT Beratung

Am Blümlingspfad 115
53359 Rheinbach
(02226) 899 7646
mail@digihelp.de

Bitte beachten Sie:

Nur mit Kenntnis der im Profil hinterlegten Informationen können vergessene Passwörter wiederhergestellt oder gesperrte Konten wieder geöffnet werden. Anderenfalls können sich die Schutzvorkehrungen gegen Missbrauch und Diebstahl leicht gegen den legitimen Besitzer wenden.

Cyberkriminalität ist profitabler denn je. Laut dem Bundeskriminalamt wurden im Jahr 2024 über 400.000 Phishing-Mails allein bei der Verbraucherzentrale in Nordrhein-Westfalen angezeigt. Der wirtschaftliche Schaden betrug eine Rekordsumme von mehr als 178 Milliarden Euro.

Schutz von E-Mail-Konten:

Sollte das Passwort zu einem der oben genannten Anmeldekonten, Benutzerprofile oder irgendeinem anderen Onlinedienst einmal vergessen, verloren oder ungültig sein, bietet sich die „***Passwort vergessen***“ Funktion an, um den Zugang schnell und komfortabel zu reaktivieren. Im Umkehrschluss bedeutet das aber auch, dass alle Passwörter zu E-Mail-Adressen, die für Benutzerprofile genutzt werden, besonders schutzbedürftig sind. Wer sich den Zugang zu Ihrem Mailkonto verschafft, hat via „***Passwort vergessen***“ somit auch den Zugang zu allen damit verknüpften Diensten und Profilen.

Das sollten Sie zu jedem Profil dokumentieren:

Zweck	Beispiel
Name des Dienstes/ Anbieters	Google
Name des Benutzerprofils	fritz.maier@web.de
Passwort	&Supi(#)Dupi!
Datum der letzten Änderung	12.11.2025

Die für den Profilnamen verwendete Mail-Adresse können Sie frei aus Ihrem Bestand wählen. D.h. für eine Google-ID können aber müssen Sie nicht eine Gmail-Adresse verwenden.

Empfehlung: Zum Schutz vor Missbrauch können viele Online-Konten, darunter insbesondere eMail-Konten, durch eine Zweifaktor-Authentisierung (2FA[3]) zusätzlich zum Passwort geschützt werden.

Es geht hier um Ihre persönlichen Geheimnisse, für deren Schutz vor Verlust und Missbrauch nur Sie selber verantwortlich sind.

Benutzerkonten vor unbefugtem Zugriff absichern

Zu Ihrer Sicherheit bei Aktivitäten im Internet, ist es sehr wichtig, den Zugang zu Ihren Konten- und Profilen vor Hackern und Missbrauch zu schützen. Die höchste Priorität hat dabei der Schutz Ihrer E-Mail-Konten. Denn, wer immer Zugang zu Ihrem Mail-Konto hat, kann sich über die „Passwort zurücksetzen“ Funktion auch den Zugang zu anderen Konten mit der jeweiligen Mail-Adresse als Benutzer-ID verschaffen.

Schutz des E-Mail-Kontos:

1. Auswahl des Anbieters
   1.1. Wählen Sie einen Mail-Provider aus dem Geltungsbereich der europäischen DSGVO. Das schließt Mail-Konten von Apple, Google, Microsoft und anderen nichteuropäischen Anbietern für die allgemeine Verwendung aus.

[3] Beim Online Banking obligatorisch.

Am Blümlingspfad 115
53359 Rheinbach
(02226) 899 7646
mail@digihelp.de

1.2. Die oft als kostenlose Beigabe verfügbaren Mail-Adressen der Internetzugangs- oder Mobilfunkbetreiber sind zwar bequem, müssen aber bei einem Wechsel des Providers geändert werden (hoher Verwaltungs- und Dokumentationsaufwand).
1.3. Die Mail-Adressen unabhängiger Mail-Provider gelten theoretisch ein Leben lang und stellen bei einem Umzug eine Konstante in der Erreichbarkeit dar. (Zum Beispiel: GMX, WEB.DE. Posteo, Mail.de u. a.)

2. Absicherung des Zugangs
   2.1. Verwenden Sie ausschließlich sichere Passwörter.
   2.2. Dokumentieren Sie die Zugangsdaten auf Papier oder verschlüsselt in einem Passwort-Manager.
   2.3. Nutzen Sie die Zwei-Faktor-Authentifizierung (2FA) und Passkeys, wo immer möglich.

Das wichtige Konzept bei der 2FA lautet im Englischen: *"What you have, what you know, what you are."* Übersetzt heißt das:

1. **Was Sie haben (Besitzfaktor):** Ein physischer Gegenstand, den nur Sie besitzen. Das kann Ihr Smartphone sein, eine Chipkarte oder ein spezieller USB-Stick zum Freischalten.
2. **Was Sie wissen (Wissensfaktor):** Dabei handelt es sich klassisch um Ihr Passwort oder die PIN, die natürlich auch möglichst sicher gewählt sein sollten. Bei Passwörtern genügen zum Beispiel acht Zeichen oft nicht mehr.
3. **Was Sie sind (Inhärenzfaktor):** Damit sind biometrische Merkmale gemeint, also ein Fingerabdruck oder die Gesichtserkennung.

Es geht darum, dass Sie mindestens **zwei verschiedene dieser Faktoren** miteinander kombinieren. Nur dann sind Ihre Accounts durch 2FA wirklich geschützt.

Quelle: CHIP

Am Blümlingspfad 115
53359 Rheinbach
(02226) 899 7646
mail@digihelp.de

Links zum Thema

Passwort-Manager:	Keepass, KeepassXC
2FA Authentifikator App:	Google Authenticator, Microsoft Authenticator, 2FA Authenticator 2FAS (Empfehlung!)

Tipps

Vermeiden Sie …

- die Passwortspeicherung in einem Browser wie Edge, Chrome, Firefox u.a.
- kommerzielle Passwortmanager (siehe auch hier)

Passwortregeln:

Ein sicheres Passwort besteht immer aus min. drei der vier unten genannten Zeichengruppen.

Formale Anforderungen an ein sicheres Passwort

- Große Buchstaben (A, B, C, …)
- Kleine Buchstaben (a, b, c, …)
- Ziffern (0,1,2, …)
- Sonderzeichen (+, -, #, :, /, …)
  Was erlaubt ist, bestimmt der Anbieter

Vermeiden Sie Umlaute zur Vermeidung von Inkompatibilitäten!

Länge und Komplexität: zwei entscheidende Merkmale (Quelle: BSI)

Ein starkes Passwort kann "kürzer und komplex" oder "lang und weniger komplex" sein. Doch wie lang und wie komplex sollte es mindestens sein? Folgende Beispiele geben Orientierung:

Ein Passwort ist sicher, wenn es beispielsweise

- 20 bis 25 Zeichen lang ist und zwei Zeichenarten genutzt werden (beispielsweise eine Folge von Wörtern). Es ist dann lang und weniger komplex.
- 8 bis 12 Zeichen lang ist und vier Zeichenarten genutzt werden. Es ist dann kürzer und komplex.
- 8 Zeichen lang ist, drei Zeichenarten genutzt werden und es zusätzlich durch eine Mehr-Faktor-Authentisierung abgesichert ist (beispielsweise durch einen Fingerabdruck, eine Bestätigung per App oder eine PIN). Dies ist generell empfehlenswert.

Tipps finden Sie in unserem Faktenblatt zu sicheren Passwörtern – im praktischen DINA4-Format passt es an jede Pinnwand: Hier geht es zum Download des Faktenblattes