

Passwort NICHT per Mail versenden

Warum wir Ihnen niemals ein Passwort per E-Mail schicken

Sie haben vielleicht schon einmal ein neues Passwort per E-Mail erhalten – von uns bekommen Sie das nicht. Das hat einen guten Grund, den wir Ihnen hier kurz erklären möchten.

Das Problem: E-Mails sind nicht sicher genug für Passwörter

E-Mails werden auf ihrem Weg durch das Internet in der Regel nicht durchgehend verschlüsselt. Sie können auf diesem Weg – oder später auf den Servern, auf denen sie gespeichert werden – von Unbefugten mitgelesen werden.

Das eigentliche Risiko entsteht dabei nicht nur im Moment des Versands. Ein einmal verschicktes Passwort liegt danach dauerhaft an mehreren Stellen: im Postausgang des Absenders, in Ihrem Posteingang, auf Mailservern und in Backups. Wird auch nur eine dieser Stellen später einmal kompromittiert – auch Monate danach – ist das Passwort weiterhin nutzbar, wenn es nicht geändert wurde.

Warum das besonders gefährlich werden kann

Sollte einmal Ihr E-Mail-Postfach selbst gehackt werden, hätten Angreifer damit automatisch Zugriff auf alle Passwörter, die jemals per Mail an Sie verschickt oder von Ihnen versendet wurden – einfach durch eine Suche im Postfach. Ein solcher Missbrauch bleibt oft lange unbemerkt, weil niemand eine Warnung erhält, wenn ein Passwort in falsche Hände gerät.

Wie wir es stattdessen machen

Damit Ihre Zugangsdaten sicher bei Ihnen ankommen, gehen wir anders vor:

- **Getrennte Übermittlungswege:** Den Benutzernamen erhalten Sie ggf. per E-Mail, das zugehörige Passwort teilen wir Ihnen telefonisch oder über einen sicheren, verschlüsselten Einmal-Link mit.
- **Einmal-Links mit Ablaufdatum:** Bei Bedarf nutzen wir Dienste, bei denen das Passwort verschlüsselt hinterlegt und nur einmalig sowie zeitlich befristet abrufbar ist. Nach dem Abruf oder Ablauf der Frist ist der Link nicht mehr gültig.
- **Sofortiger Passwortwechsel:** Wo immer technisch möglich, richten wir es so ein, dass Sie bei der ersten Anmeldung direkt aufgefordert werden, ein eigenes, individuelles Passwort zu vergeben.

Was wir Ihnen empfehlen

Auch für Ihren eigenen Schutz gilt: Geben Sie Passwörter nie per E-Mail weiter, auch nicht an Kolleginnen, Kollegen oder vermeintliche Dienstleister. Seriöse Unternehmen – auch wir – fragen niemals per E-Mail nach Ihrem Passwort.

Zusätzlich empfehlen wir:

- Nutzen Sie für wichtige Konten, wo verfügbar, die **Zwei-Faktor-Authentisierung**. Damit reicht ein gestohlenes Passwort allein nicht mehr für einen Zugriff aus.
- Verwenden Sie für jeden Dienst ein eigenes, starkes Passwort – ein **Passwort-Manager** hilft dabei, den Überblick zu behalten.
- Seien Sie misstrauisch bei E-Mails, die Sie zur Eingabe eines Passworts auffordern, auch wenn sie von einem bekannten Absender zu stammen scheinen.

Bei Fragen zur sicheren Verwaltung Ihrer Zugangsdaten sprechen Sie uns gerne an – wir beraten Sie individuell.

PC-SPEZIALIST Hannover / HIT Systempartner GmbH

Version #1

Erstellt: 2026-08-25 12:30:12 UTC von Frank Böttger

Zuletzt aktualisiert: 2026-08-25 12:30:34 UTC von Frank Böttger