

Passwort-Regeln

© DATEV e.G.

Passwörter sichern die Einsatzfähigkeit des PC-Arbeitsplatzes. Sie schützen die eigenen und die Mandantendaten. Und sie garantieren, dass Mitarbeiter nur auf Programme und Daten zugreifen, die sie für ihre Aufgaben benötigen.

Sichere Passwörter sollten deshalb folgende Voraussetzungen erfüllen:

Länge

Das Passwort muss aus mindestens acht Zeichen bestehen.

Kombination

Verwenden Sie für das Passwort bitte eine Kombination aus Zahlen und Buchstaben, optional zusätzlich mit Sonderzeichen (\$, #) oder Groß- und Kleinschreibung. Vermeiden Sie nebeneinander liegende Tastenkombinationen ("QWERTZ" ist einfach zu tippen, aber leider auch einfach zu "knacken").

Inhalt

Verwenden Sie Passwörter ohne persönlichen Bezug (bitte keine Namen von Verwandten, Freunden, Kfz-Kennzeichen, Geburtstage usw.).

Schreibweise

Bilden Sie Ihr Passwort z. B. aus den Anfangs-/Endbuchstaben eines nur Ihnen bekannten Merksatzes: "**E**infache **P**asswörter sind **24** **S**tunden lang ein **S**icherheitsrisiko" = "EPs24SlSr". Eine Anmerkung: Bilden Sie sich Ihre eigene Gedanken-Brücke, die eben genannte stellt bereits eine Sicherheitslücke dar.

Zusätzlich sollten Sie noch beachten:

- Passwörter sollten grundsätzlich weder aufgeschrieben (keine gelben Zettel am Monitor bzw. unter der Tastatur...) noch abgespeichert werden. Bitte merken Sie sich Ihre Passwörter.
- Verwenden Sie unterschiedliche Passwörter für unterschiedliche Arbeitsvorgänge wie z.B. für Netzwerk-Anmeldung, DATEVnet, DATEV e:secure, Online-Banking usw. Beachten Sie hierbei auch, dass Sie Kanzlei-Passwörter nicht privat (und umgekehrt) verwenden.
- Bildschirmpasswörter allein sind nicht sicher genug. Sie bieten jedoch beim Verlassen des Zimmers einen gewissen Schutz und können zudem schnell aktiviert werden („kurze Wartezeit" einstellen).
- Um das unbefugte Starten eines PCs generell zu verhindern, sollte ein BIOS-Kennwort verwendet werden.
- Auch wenn das jeweilige Betriebssystem in manchem Anmeldefenster ein **automatisches Speichern von Passwörtern** anbietet, sollten Sie auf diesen fragwürdigen Komfort (da die Passwörter in der Regel unverschlüsselt abgelegt werden) **verzichten**.
- Wechseln Sie regelmäßig (ca. 2 x im Jahr) Ihr Passwort und verwenden Sie dabei neue Passwörter (kein Passwort-„Recycling").