it4med

Checkliste für Ihre Ordination:

8 Tipps für sichere Passwörter

Ihre Checkliste zum Abhaken!

Verwenden Sie niemals das gleiche Passwort für unterschiedliche Zwecke

Die Verwendung desselben Passworts für unterschiedliche Konten führt rasch dazu, dass die Sicherheit des Passworts reduziert wird. Warum? Findet ein Hacker die Kombination aus Username und Passwort heraus, wird er es bei vielen verschiedenen Konten ausprobieren. Um das zu vermeiden, empfehlen wir, **unterschiedlichste Passwortkombinationen** für jedes einzelne Konto zu verwenden.

Verwenden Sie keine Begriffe, die mit Ihrer Person zusammenhängen

Wir teilen unser Leben online auf diversen Social-Media-Kanälen und geben so viele Informationen über uns preis. **Persönliche Daten, wie z.B. das Geburtsdatum, Spitznamen** oder auch die Namen der Ehepartner oder der Kinder sind damit auch für Hacker leicht herauszufinden. Vermeiden Sie daher Begriffe oder Zahlenkombinationen, die direkt mit Ihnen als Person zusammenhängen.

Vermeiden Sie simple Passwörter

„Passwort", „12345", „00000" oder „hallo" sind wirklich keine Option. Sollten Sie eines davon in Verwendung haben, ändern Sie es umgehend. Das Gleiche gilt für die Wahl von **„Administrator" oder „Admin" als Benutzername.**

Verwenden Sie Zahlen und Sonderzeichen

Statt sich für ein Passwort zu entscheiden, das nur aus Buchstaben oder Zeichen besteht, sollten Sie **Kombinationen aus Buchstaben, Zahlen und Sonderzeichen** (%, @, $) verwenden.

Weiterlesen auf Seite 2

Sie haben **Fragen** oder brauchen **Unterstützung?**

Melden Sie sich gerne bei uns: wir beraten Sie bei allen Themen rund um Hard- und Software.

Mag. Markus Dittrich
Geschäftsführung

office@casc.at
01 924 05 28

Ihr Passwort sollte aus mindestens acht Zeichen bestehen

Rund ein Drittel aller Passwörter für sensible Konten bestehen aus nur sieben oder noch weniger Zeichen. **Acht Zeichen sind das absolute Minimum** für ein sicheres Passwort, besser sind Passwörter mit etwa 15 Zeichen.

Ändern Sie Ihre Passwörter in regelmäßigen Abständen

Je länger Sie Ihr Passwort verwenden, umso mehr Zeit haben die Hacker, um es zu knacken. Spätestens wenn ein Schadprogramm auf dem PC oder dem IT-System ist, müssen alle Passwörter geändert werden, da diese Programme Zugangsdaten aufzeichnen und an Dritte übermitteln können. Außerdem sollten Passwörter **geändert werden, sobald sie von einem Diensteanbieter dazu aufgefordert werden** oder sie Informationen von seriösen Nachrichtendiensten zu bestimmten Angreifern, Spam- oder Pishing-Mails erhalten.

Teilen oder notieren Sie Ihre Passwörter niemals

Um zu vermeiden, dass Ihr Passwort in falsche Hände gerät, sollten Sie es **nicht speichern oder das Kontrollkästchen „Erinnern" im Browser aktivieren** – vor allem wenn Sie einen öffentlichen Computer verwenden.

Verwenden Sie einen Passwort-Manager

Verwenden Sie einen Passwort-Manager, zum Beispiel https://1password.com

Für den Alltag in der Arztpraxis gilt: sensibilisieren sie alle Mitarbeiter und legen sie eine **Passwortrichtlinie** fest. Geben Sie Passwörter nicht weiter und verwenden Sie in der Praxis **keine Klebezettel** oder sonstiges. Ändern Sie alle voreingestellten Passwörter ab. Wenn möglich nutzen Sie eine 2-Faktor-Authentifizierung, so kann ein Zugriff auf das System verhindert werden, auch wenn das Passwort geknackt wurde, da eine Information an den Nutzer gesendet wird und dieser bspw. einen **Verifizierungscode** eingeben muss, um sich eindeutig zu identifizieren.

Geschafft! Sicher online, mit diesen Passwörtern!

Sie haben **Fragen** oder brauchen **Unterstützung?**

Melden Sie sich gerne bei uns: wir beraten Sie bei allen Themen rund um Hard- und Software.

Mag. Markus Dittrich
Geschäftsführung

office@casc.at
01 924 05 28