INMODIS
IT-Sicherheit für Ihr Unternehmen

PASSWORT CHECKLISTE

- [ ] **Passwörter nicht wiederverwenden**
- [ ] **Passwörter nicht teilen**
- [ ] **Möglichst lang, möglichst großer Zeichensatz**
- [ ] **Passwort Manager verwenden**
- [ ] **2 Faktor Authentifizierung einrichten**
- [ ] **Regelmäßig auf Sicherheit prüfen**
- [ ] **Keine vorhersehbaren Änderungen**
- [ ] **Passwort rücksetzen Funktion absichern**

INMODIS
IT-Sicherheit für Ihr Unternehmen

PASSWORT CHECKLISTE

Passwörter nicht wiederverwenden
Für jeden Service sollte ein eigenes Passwort erstellt werden. Zur Verwaltung bietet sich ein Passwort Manager an.

Passwörter nicht teilen
Passwörter sollten nie geteilt werden. Auch nicht wenn die "IT-Abteilung" anruft und einen neuen Account freischalten will.

Möglichst lang, möglichst großer Zeichensatz
Je länger ein Passwort und je größer der Zeichensatz (Groß-, Kleinbuchstaben, Zahlen, Zeichen) umso schwerer zu knacken.

Passwort Manager verwenden
Um den Überblick über alle Passwörter zu behalten kann ein Passwort Manger verwendet werden.

2 Faktor Authentifizierung einrichten
Für wichtige Services sollte eine 2FA (z.B. per Code aufs Handy) aktiviert werden um diese zusätzlich zu sichern.

Regelmäßig auf Sicherheit prüfen
Mit Haveibeenpwned.com/passwords können Passwörter überprüft werden. Unsichere Passwörter nicht mehr verwenden!

Keine vorhersehbaren Änderungen
Falls regelmäßige Änderungen verlangt werden, sollten diese zufällig sein (NICHT passwort+1 in passwort+2 usw. ändern).

Passwort rücksetzen Funktion absichern
Email Accounts besonders absichern, bei Sicherheitsfragen aufpassen, dass diese nur durch einen selbst beantwortet werden können.

www.inmodis.de | +49 (0) 9491 / 74 29 885-0