iTentity erklärt:

Passwortverwaltung

Cyber Security Awareness Month

iTentity erklärt:

Best Practices für die Passwortverwaltung

Starke Passwörter erstellen:

- Verwenden einer Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
- Vermeiden von leicht zu erratenden Passwörtern wie „123456“ oder „Passwort“.

Einzigartige Passwörter für jedes Konto:

- Jedes Konto sollte ein eigenes, einzigartiges Passwort haben. Dadurch wird das Risiko minimiert, dass mehrere Konten bei einem Datenleck kompromittiert werden.

iTentity erklärt:

Best Practices für die Passwortverwaltung

Regelmäßige Passwortänderungen:

- Regelmäßiges Ändern von Passwörtern, um die Sicherheit zu erhöhen.

Passwortmanager nutzen:

- Ein Passwortmanager hilft, starke und einzigartige Passwörter zu erstellen und zu speichern. So muss man sich nur ein Master-Passwort merken.
- Passwortmanager bieten auch Funktionen wie die automatische Anmeldung und die Synchronisierung über verschiedene Geräte hinweg.

iTentity erklärt:

Best Practices für die Passwortverwaltung

Zwei-Faktor-Authentifizierung (2FA):

- Aktivieren einer Zwei-Faktor-Authentifizierung, wo immer dies möglich ist. Dies fügt eine zusätzliche Sicherheitsebene hinzu, indem ein zweiter Verifizierungsschritt erforderlich wird.