



**Zwei-Faktor-
Authentifizierung
Checkliste**



01

PLANUNG

02

**FAKTOR
MENSCH**

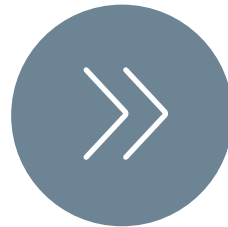
03

**TECHNISCHE
UMSETZUNG**

04

ABSCHLUSS

PLANUNG



ACCOUNTS FESTLEGEN

Müssen alle Accounts mit 2FA gesichert werden oder gibt es Ausnahmen?

☞ Überprüfe alle Benutzerkonten und entscheide, welche mit 2FA gesichert werden müssen.

💡 Beginne mit kritischen Accounts und erweitere schrittweise.

GERÄTE BEACHTEN

Gibt es Drucker oder andere Geräte, die berücksichtigt werden sollten (z.B. Scan to E-Mail)?

☞ Erstelle eine Liste aller verbundenen Geräte und überprüfe deren Kompatibilität.

💡 Informiere Dich über spezifische 2FA-Lösungen für diese Geräte.

SCHRITTE DEFINIEREN

Welche Schritte müssen ausgeführt werden, um Komplikationen zu vermeiden?

☞ Erstelle einen detaillierten Plan mit einer Checkliste für die ersten Schritte

💡 Kommuniziere diesen Plan klar an alle Beteiligten.

ALTERNATIVEN PRÜFEN

Gibt es Alternativen zur Erhöhung der Sicherheit Deiner Log-ins?

☞ Recherchiere andere Sicherheitsmassnahmen, vergleiche deren Vor- und Nachteile.

💡 Ziehe externe Beratung hinzu, um die besten Optionen zu evaluieren.

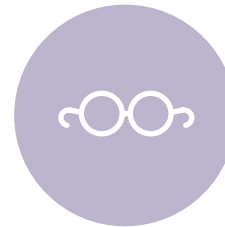
ZIELE FESTLEGEN

Was sind die Ziele der 2FA Einführung und welche Zielgruppen gibt es dafür?

☞ Definiere die Ziele der 2FA-Einführung für jede Zielgruppe.

💡 Führe Umfragen durch, um die Bedürfnisse jeder Gruppe besser zu verstehen.

MENSCHLICHER FAKTOR



KOMMUNIKATION

Hast Du klare und direkte Kommunikation über die 2FA-Einführung geführt?

☞ Plane regelmässige Meetings und Informationsveranstaltungen.

💡 Nutze verschiedene Kommunikationskanäle, um alle zu erreichen.

UNSIHERHEITEN ERNST NEHMEN

Hast Du anfängliche Unsicherheiten der Mitarbeiter ernst genommen und darauf reagiert?

☞ Führe persönliche Gespräche, um Bedenken zu klären.

💡 Erstelle ein FAQ-Dokument, das häufige Fragen beantwortet.

ZWECK ERKLÄREN

Hast Du erklärt, warum 2FA eingeführt wird und welche Vorteile es bringt?

☞ Bereite eine Präsentation vor, die den Zweck und die Vorteile erklärt.

💡 Zeige konkrete Beispiele für Sicherheitsvorfälle, die durch 2FA verhindert werden können.

UNTERSTÜTZUNG BIETEN

Hast Du Unterstützung und Anleitungen für alle Mitarbeiter bereitgestellt?

☞ Stelle Schulungsmaterialien und Handbücher zur Verfügung.

💡 Richte ein Helpdesk ein, das bei Fragen und Problemen hilft.

TECHNISCHE UMSETZUNG – 1



AUTHENTICATOR-APP WÄHLEN

Hast Du die passende Authenticator-App gewählt und auf den Geräten der Mitarbeiter installiert?

- ☞ Wähle eine geeignete Authenticator-App aus und führe diese ein.
- 💡 Teste die App vor der Einführung auf Kompatibilität.

APP AKTUELL HALTEN

Wird die Authenticator-App regelmässig aktualisiert?

- ☞ Richte automatische Updates für die App ein.
- 💡 Informiere die Mitarbeiter über die Bedeutung von Updates.

KONTEN KORREKT EINRICHTEN

Ist das richtige Konto angegeben und der korrekte Download aus dem App Store durchgeführt?

- ☞ Stelle sicher, dass alle Konten korrekt eingerichtet sind.
- 💡 Erstelle eine Schritt-für-Schritt-Anleitung für den Download und die Einrichtung.

TECHNISCHE UNTERSTÜTZUNG PRÜFEN

Hast Du den Bedarf an technischer Unterstützung geprüft?

- ☞ Überprüfe, ob zusätzlicher technischer Support erforderlich ist.
- 💡 Ziehe einen externen IT-Dienstleister hinzu, wenn nötig.

TECHNISCHE UMSETZUNG – 2



TECHNISCHE KENNTNISSE SICHERSTELLEN

Haben alle Mitarbeiter die notwendigen technischen Kenntnisse?

- ☞ Führe Schulungen durch, um die technischen Kenntnisse der Mitarbeiter zu verbessern.
- 💡 Biete Schulungen in kleinen Gruppen an, um individuellen Support zu gewährleisten.

QUALITÄTSKONTROLLEN DURCHFÜHREN

Führen Sie Qualitätskontrollen zur Überprüfung der Funktionsfähigkeit durch?

- ☞ Plane und führe regelmäßige Qualitätskontrollen durch.
- 💡 Dokumentiere alle Prüfungen und deren Ergebnisse.

BETROFFENE KOMPONENTEN PRÜFEN

Hast Du die Auswirkungen auf bestehende Log-Ins, Mobilgeräte und VPN-Verbindungen geprüft?

- ☞ Überprüfe alle betroffenen Komponenten auf Kompatibilität mit 2FA.
- 💡 Führe Tests durch, bevor die 2FA endgültig eingeführt wird.

UNSIKERHEITEN KLÄREN

Hast Du alle Unsicherheiten bei der Einrichtung der 2FA geklärt?



- ☞ Kläre alle offenen Fragen und Unsicherheiten.
- 💡 Erstelle ein Dokument mit häufig gestellten Fragen und deren Antworten

ABSCHLUSS



REGELMÄSSIGE SCHULUNGEN



Bietest Du kontinuierliche Schulungen und Updates für die Mitarbeiter an?

-  Plane regelmässige Schulungen und Informationsveranstaltungen.
-  Aktualisiere das Schulungsmaterial regelmässig.



FEEDBACK EINHOLEN

Sammelst Du Feedback zur 2FA-Nutzung und wertest es aus?

-  Führe Umfragen durch, um Feedback zur Nutzung von 2FA zu sammeln.
-  Nutze das Feedback, um die 2FA-Implementierung kontinuierlich zu verbessern.



Wenn Du mehr über die Zwei-Faktor-Authentifizierung wissen möchtest, melde Dich unter:

Telefon-Nummer: [031 511 22 33](tel:0315112233)

E-Mail-Adresse: team@plusundplus.ch

Mehr spannende Themen aus der IT-Welt findest Du unter:
plusundplus.ch/it-ratgeber