SICHERHEITS-LEITFADEN & PRAXIS-CHECKLISTE

Checkliste: Digitale Sicherheit im Alltag

Schritt-für-Schritt-Prüfung für Identität, Geräte, Netzwerke und Daten

> Diese praxisorientierte Checkliste führt Sie durch die fünf zentralen Schutzbereiche moderner IT-Sicherheit im privaten und beruflichen Alltag. Jeder Prüfpunkt ist als konkrete Handlungsanweisung formuliert und lässt sich systematisch abarbeiten, um typische Einfallstore für Malware und Social Engineering effektiv zu schließen.

01 1. Identität & Passwörter

02 2. Multi-Faktor-Authentifizierung (MFA)

03 3. Gerätesicherheit & Patchmanagement

04 4. Datensicherung & Recovery (3-2-1-Regel)

05 5. Phishing- & Betrugsprävention

01

1. Identität & Passwörter

Starke, einzigartige Zugangsdaten bilden die erste Verteidigungslinie gegen automatisierte Wörterbuch- und Credential-Stuffing-Angriffe. Nutzen Sie zur Vermeidung von Mehrfachnutzungen zwingend einen vertrauenswürdigen Passwort-Manager.

- [ ] Passwort-Manager einrichten: Installieren Sie einen quelloffenen oder geprüften Manager und vergeben Sie eine mindestens 16-stellige Passphrase als Master-Passwort.
- [ ] Komplexitätsregeln durchsetzen: Generieren Sie für jeden Dienst zufällige Kennwörter mit mindestens 14 Zeichen, bestehend aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.
- [ ] Passwort-Wiederverwendung eliminieren: Prüfen Sie alle bestehenden Konten und ersetzen Sie doppelt verwendete Passwörter schrittweise durch neu generierte Einträge.
- [ ] Notfallzugriff hinterlegen: Drucken Sie den Wiederherstellungsschlüssel des Managers einmalig aus und verwahren Sie diesen an einem physisch gesicherten Ort.

> **Wichtiger Hinweis zur Kennwortwahl**
>
> Verwenden Sie niemals persönliche Daten wie Geburtsdaten, Namen von Angehörigen oder geläufige Tastaturmuster in Kennwörtern.

Verwendeter Passwort-Manager & Datum der Umstellung

Sicherer Verwahrort des physischen Notfallschlüssels

02

2. Multi-Faktor-Authentifizierung (MFA)

Ein Passwort allein reicht bei Datenlecks oft nicht aus. Ein zweiter Faktor stellt sicher, dass kompromittierte Zugangsdaten Angreifern keinen direkten Systemzugriff ermöglichen.

1. **Authentisierungs-App installieren**

   Wählen Sie eine etablierte TOTP-Applikation auf Ihrem Smartphone und sichern Sie den App-Zugriff biometrisch oder per PIN ab.

2. **Sicherheitseinstellungen aufrufen**

   Navigieren Sie im Zielkonto zu den Sicherheitsoptionen und wählen Sie 'Zwei-Faktor-Authentifizierung einrichten'.

3. **QR-Code scannen und verifizieren**

   Scannen Sie den angezeigten QR-Code mit der App und geben Sie den sechsstelligen Bestätigungscode ein.

4. **Wiederherstellungscodes sichern**

   Laden Sie die Einmal-Wiederherstellungscodes herunter und speichern Sie sie geschützt außerhalb des Mobilgeräts.

- [ ] Primäre E-Mail-Konten absichern: Aktivieren Sie für Ihr zentrales E-Mail-Postfach App-basierte Einmal-Passwörter (TOTP) oder FIDO2-Sicherheitsschlüssel.
- [ ] Finanz- und Cloud-Dienste verknüpfen: Richten Sie für Banking-, Shopping- und Cloud-Speicher-Konten einen zweiten Authentisierungsfaktor ein.
- [ ] SMS-Verfahren ablösen: Bevorzugen Sie Authenticator-Apps oder Hardware-Token gegenüber SMS, um SIM-Swapping-Risiken zu minimieren.
- [ ] Backup-Codes archivieren: Speichern Sie die einmaligen Notfallcodes getrennt vom regulären Authentifikator ab.

> **Empfehlung für kritische Dienste**
>
> FIDO2/WebAuthn-Hardware-Token bieten den höchsten Schutz gegen bösartige Phishing-Seiten, da der Hostname kryptografisch geprüft wird.

03

3. Gerätesicherheit & Patchmanagement

Angreifer nutzen regelmäßig bekannte Softwareschwachstellen aus. Ein konsequentes Patch- und Systemmanagement schließt Sicherheitslücken zügig und verringert die Angriffsfläche erheblich.

- [ ] Automatische Updates aktivieren: Schalten Sie Auto-Updates für Betriebssysteme (Windows, macOS, Linux, iOS, Android) standardmäßig ein.
- [ ] Browser und Plug-ins pflegen: Aktualisieren Sie Webbrowser täglich und entfernen Sie nicht zwingend benötigte Erweiterungen.
- [ ] Festplattenverschlüsselung aktivieren: Schalten Sie BitLocker (Windows), FileVault (macOS) oder LUKS (Linux) für alle mobilen Rechner ein.
- [ ] Standard-Adminrechte reduzieren: Arbeiten Sie im Alltag mit einem Benutzerkonto ohne administrative Privilegien.

Inventarisierte Geräte (Rechner, Mobiltelefon, Tablet) und Verschlüsselungsstatus

04

4. Datensicherung & Recovery (3-2-1-Regel)

Ransomware-Vorfälle und Hardwaredefekte bedrohen digitale Bestände. Eine nachvollziehbare Sicherungsstrategie garantiert, dass Sie im Ernstfall arbeitsfähig bleiben.

- Drei Kopien vorhalten: Führen Sie mindestens den Primärdatensatz und zwei vollständige Datensicherungen.
- Zwei unterschiedliche Medien: Nutzen Sie voneinander getrennte Medientypen (beispielsweise interne NVMe-SSD und externes USB-Laufwerk).
- Eine externe Kopie (Offsite): Lagern Sie eine verschlüsselte Sicherung räumlich getrennt oder in einem vertrauenswürdigen Cloud-Speicher.
- Wiederherstellungstests durchführen: Überprüfen Sie mindestens vierteljährlich das Einspielen eines Datenbestands auf ein Testsystem.

> **Schutz vor Ransomware**
>
> Trennen Sie externe Sicherungsfestplatten nach dem Backup physisch vom Computer, um ein Überschreiben durch Schadsoftware zu verhindern.

Protokoll letzter erfolgreicher Wiederherstellungstest (Datum, geprüfte Daten)

05

5. Phishing- & Betrugsprävention

Social-Engineering-Angriffe zielen darauf ab, menschliches Vertrauen oder Zeitdruck auszunutzen. Gezielte Prüfschritte verhindern das unbedachte Öffnen manipulierter Links oder Anhänge.

Wie verhalten Sie sich bei einer verdächtigen Nachricht mit Handlungsaufforderung?

Die Nachricht fordert zur sofortigen Passworteingabe auf einer verlinkten Seite auf.

Klicken Sie nicht auf den Link. Öffnen Sie die offizielle Website des Anbieters manuell über das Lesezeichen im Browser und prüfen Sie den Kontostatus dort.

Die E-Mail enthält einen unangekündigten Rechnungs- oder Lieferanhang (z. B. .zip, .exe oder Makro-PDF).

Laden Sie den Anhang nicht herunter. Kontaktieren Sie den vermeintlichen Absender über einen separaten, bekannten Kommunikationskanal (z. B. Telefon).

Sie haben versehentlich Zugangsdaten auf einer fremden Website eingetragen.

Ändern Sie das betroffene Passwort umgehend auf der echten Website, beenden Sie alle aktiven Sitzungen und aktivieren Sie sofort MFA.

- [ ] Absenderadresse verifizieren: Prüfen Sie den vollständigen Domainnamen im 'Von'-Header auf Vertipper oder atypische Top-Level-Domains.
- [ ] Link-Ziele kontrollieren: Fahren Sie mit dem Mauszeiger über Links, ohne zu klicken (Hover-Test), um die echte Ziel-URL vorab zu sehen.
- [ ] Dringlichkeit hinterfragen: Seien Sie besonders wachsam bei Benachrichtigungen, die mit Kontosperrung, rechtlichen Schritten oder Geldverlust drohen.
- [ ] Dateianhänge isolieren: Öffnen Sie unaufgeforderte Makro-Dokumente (.docm, .xlsm) oder Archivdateien (.zip, .iso) nicht ohne vorherige Rücksprache.