

Account Sicherheit: Sicherheitsmaßnahmen

Beschreibung

In einer zunehmend digitalen Welt ist der Schutz persönlicher und beruflicher Online-Konten wichtiger denn je. Cyberangriffe wie Phishing, Identitätsdiebstahl oder Datenlecks können erhebliche finanzielle, rechtliche und persönliche Schäden verursachen. Account-Sicherheit ist daher nicht nur eine technische Notwendigkeit, sondern eine zentrale Säule digitaler Eigensicherung und Privatsphäre.

Die Sicherheit der Online-Konten beginnt mit starken Passwörtern und wird durch Zwei-Faktor-Authentifizierung entscheidend verbessert.

Sichere Passwörter – das erste Schutzschild

Was macht ein Passwort sicher?

- Länge vor Komplexität: Ein sicheres Passwort sollte mindestens 12 Zeichen lang sein
- Kombinationen nutzen: Verwenden Sie Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
- Keine persönlichen Informationen: Vermeiden Sie Geburtstage und Namen
- Einzigartigkeit ist entscheidend: Für jedes Konto ein anderes Passwort verwenden

Wie erstelle ich ein sicheres Passwort?

- Methode 1: Wörter-Kombination – Kombinieren Sie mehrere Wörter mit zusätzlichen Sonderzeichen, die sie sich gut merken können (z.B. „Giraffe+!Apfel99_Beamer“)
- Methode 2 Satz-Methode – denken Sie sich einen Satz aus (z.B. „Ich mag es im Jahr2024, 3Kaffee zu trinken!“) → erstellen Sie darauf ein Passwort („lmeij2024,3Kzt!“)
- Methode 3: Passwort-Generatoren – Nutzen Sie einen Passwort-Manager, um lange und zufällige Passwörter zu generieren. Es ist wie ein digitales Notizbuch, in dem Benutzernamen und verschiedene Passwörter gespeichert werden und das mit einem Master-Passwort verschlossen ist. Anstatt mehrerer Passwörter muss man sich nur das Master-Passwort merken.

Zwei-Faktor-Authentifizierung – das zweite Schutzschild

Was ist Zwei-Faktor-Authentifizierung (2FA)?

Die Zwei-Faktoren-Authentifizierung ergänzt Ihr Passwort, um eine zweite Sicherheitsebene, die Sie bestätigen müssen. Selbst wenn ein Angreifer Ihr Passwort kennt, kann er ohne den zweiten Faktor nicht auf Ihr Konto zugreifen.

Welche 2FA-Methoden gibt es?

1. Biometrische Methoden:
Anhand biologischer Merkmale des Nutzers - Fingerabdruck, Gesichts- bzw. Stimmerkennung oder Iris-Scan - kann dieser verifiziert werden.

2. Authentifizierungs-Apps:
Diese stellen eine Methode zur Identitätsprüfung dar, die durch Generierung von Zahlencodes funktioniert, die zusammen mit den Anmeldeinformationen eingegeben werden müssen.
3. SMS/E-Mail-Codes:
Ein Code wird per SMS bzw. E-Mail-Nachricht versendet. Bietet eine geringere Sicherheit als die Biometrische Methode, Authentifizierungs-Apps und Hardware-Token ist aber auf Grund der leichteren Handhabung gegenüber keiner 2FA zu bevorzugen.
4. Hardware-Token:
Der Token ist ein eigenständiges Gerät, dass unabhängig von anderen Systemen besteht und somit schwer manipulierbar ist. Die Identität des Benutzers wird damit authentifiziert und unbefugter Zugriff verhindert.

Wie aktiviere ich 2FA?

- Loggen Sie sich in Ihr Konto (E-Mail-Account, Bankkonto, Smartphone, etc.) ein und suche Sie in den Einstellungen nach „Sicherheit“ oder „2FA“.
- Wählen Sie eine bevorzugte 2FA-Methode (z.B. Authentifizierungs-App, SMS/E-Mail-Codes).
- Folgen Sie den Anweisungen, um die Einrichtung abzuschließen.
- Speichern Sie Notfallcodes sicher, um auch bei Verlust des 2FA-Geräts Zugriff zu behalten.

Die Kombination als Lösung – Passkeys – das ultimative Schutzschild

Passkeys sind eine moderne und sichere Methode zur Authentifizierung von Nutzern ohne Verwendung von Passwörtern beim Login. Sie bestehen aus einem Schlüsselpaar – einem öffentlichen und einem privaten Schlüssel. Dabei wird auf dem eigenen Gerät ein sogenannter geheimer Schlüssel erstellt und abgespeichert, gleichzeitig wird ein passender öffentlicher Schlüssel auf dem Online-Konto hinterlegt. Bei der Anmeldung wird ein weiterer Sicherheitsfaktor (z.B. Fingerabdruck) abgefragt, anschließend erfolgt eine verschlüsselte Bestätigung zwischen den beiden Schlüsseln

- **Erhöhte Sicherheit:** Passkeys eliminieren die Gefahr von Passwortdiebstahl und Phishing-Angriffen, da keine Passwörter mehr übermittelt oder gespeichert werden.
- **Benutzerfreundlichkeit:** Keine Notwendigkeit, sich komplexe Passwörter zu merken oder regelmäßig zu ändern.
- **Schutz vor Erraten von Passwörtern durch Hackerangriffe:** die kryptografische Authentifizierung ist gegen Angriffe durch zufälliges Raten oder Wörterbuchlisten - Angriffen geschützt.
- **Komfort:** Passkeys können einfach über Geräte wie Smartphones oder Laptops verwendet werden und sind in der Regel schneller als herkömmliche Anmeldeprozesse.

Checkliste zur Account-Sicherheit – Sicherungsmaßnahmen

- Haben Sie für jedes Konto ein einzigartiges, starkes Passwort?
- Verwenden Sie „2FA“ bei Ihren (wichtigsten) Konten?
- Nutzen Sie einen Passkey oder Passwort-Manager?
- Haben Sie Sicherheits-Backups für den Fall eines Geräteverlusts?
- Bleiben Sie wachsam gegenüber Phishing-Versuchen und ungewöhnlichen Aktivitäten?

Präventionsempfehlungen der Polizei

- **Starke Passwörter verwenden** – Verwenden Sie niemals dasselbe Passwort für mehrere Konten – wenn ein Konto gehackt wird, bleiben die anderen sicher. Ändern Sie voreingestellte Passwörter sofort. Nutzen Sie Dienste wie „[have I been pwned](#)“ um zu prüfen, ob Ihre Passwörter in Datenlecks aufgetaucht sind.
- **Verwenden Sie Passkeys oder einen Passwort-Manager:** Speichern Sie Passwörter sicher und generieren Sie automatisch starke Passwörter
- **Zwei-Faktor-Authentifizierung ist unumgänglich für Account Sicherheit:** Aktivieren Sie „2FA“ bei allen (wichtigen) Konten.
- **Bewusstsein und Verhalten stärken:** Phishing vermeiden indem Links in E-Mails und Nachrichten kritisch geprüft werden, bevor Sie daraufklicken – Melden Sie sich nur direkt über die Webseite oder die App eines Dienstes an, nicht über externe Links. Wenn Sie ungewöhnliche Benachrichtigungen erhalten, ändern Sie sofort Ihr Passwort und informieren Sie den Dienstanbieter. Halten Sie alle Geräte und Apps aktuell, um Schwachstellen zu vermeiden.
- **Netzwerksicherheit ist ein weiterer Faktor:** Vermeiden Sie öffentliche WLANs

Weiterführende Links

- [BSI - Sichere Passwörter erstellen](#)
- [BSI - Passkeys - anmelden ohne Passwort](#)
- [sichere passwoerter faktenblatt.pdf](#)
- [Have I Been Pwned: Check if your email has been compromised in a data breach](#)