Social Media Manager

Intensivtraining für alle, die Social Media für Apotheken umsetzen möchten

mit **Sandra Staub**

Unser Fahrplan

20.05. 13.30h	27.05. 13.30h	03.06. 13.30h	10.06. 16.00h	17.06. 13.30h	24.06. 16.00h	01.07. 13.30h	15.07. 13.30h
Social Media Basiswissen & Strategie	Persönliche Facebook-Sicherheit	Meta Orga im Hintergrund	Instagram optimieren	Rechts-vorlesung	Redaktions-planung	Trolle & Shitstorms	Abschluss-Veranstaltung mit 2 Impulsen
mit Sandra	mit Sandra	mit Sandra	mit Michelle	mit Sandra	mit Michelle	mit Sandra	mit Michelle & Sandra

Es gilt das Prinzip **5 von 7** – ihr müsst nicht bei jeder Einheit dabei sein, aber Kontinuität lohnt sich.

Unser Fahrplan heute

20.05. 13.30h	**27.05. 13.30h**	**03.06. 13.30h**	**10.06. 16.00h**	**17.06. 13.30h**	**24.06. 16.00h**	**01.07. 13.30h**	**15.07. 13.30h**
Social Media Basiswissen & Strategie	Persönliche Facebook-Sicherheit	Meta Orga im Hintergrund	Instagram optimieren	Rechts-vorlesung	Redaktions-planung	Trolle & Shitstorms	Abschlussveranstaltung
mit Sandra	mit Sandra	mit Sandra	mit Michelle	mit Sandra	mit Michelle	mit Sandra	mit Michelle & Sandra

Heute: **Social Media Basiswissen & Strategie** – wir legen das Fundament für alle weiteren Einheiten.

Unsere Stationen heute

1. **Passwortsicherheit -** Was macht ein Passwort sicher?
2. **Facebook-Profil absichern** - Warum & wie schütze ich mein privates Profil?
3. **Passwortmanager-Software -** Nie wieder Passwörter vergessen
4. **Instagram sichern** - Login-Einstellungen richtig setzen
5. **2FA & Passkeys** - Die stärkste Schutzebene aktivieren
6. **Mitarbeiter-Sicherheit** - Wer hat Zugriff auf was?
7. **Fake-Mails erkennen** - Ist diese E-Mail wirklich von Facebook?

Ist dein Passwort sicher?

Oder ist dein Passwort das Geburtsjahr deines jüngsten Kindes plus der Name und dann ein Rufzeichen? Nutze besser generierte Passworte oder absurde Sätze als Gedächtnisstütze (Margret Thatcher is 100% sexy!)

Unsichere vs. sichere Passwörter

UNSICHER	SICHER
✗ 123456	✓ H@ndK@ff33&Rezept!
✗ Christine12062014!	✓ ApothekeKaffee4Morgen!
✗ password	✓ Tr0ub4dor&3
✗ qwertz	✓ 9#bX$mK2pL7@qR
✗ 11.11.1990	
✗ ApothekeMuenchen	

Mindestens 12 Zeichen · Groß- & Kleinbuchstaben · Zahlen · Sonderzeichen · Kein Name, kein Geburtsdatum

Passworte niemals im Browser speichern

Der Browser kann gehackt werden – und dann sind alle gespeicherten Passwörter weg oder noch besser im Internet für Geld zu kaufen.

Hast Du Passworte im Browser gespeichert?

So prüfst du später schnell, ob dein Browser Passwörter gespeichert hat – und exportierst oder entfernst sie:

Chrome

chrome://password-manager/passwords

Firefox

about:preferences#privacy

Safari

Einstellungen ⟶ Passwörter (Mac-Passwort verwenden)

Edge

3 Punkte ⟶ Einstellungen ⟶ Profile ⟶ Passwörter

Was ist ein Passwortmanager – und warum brauche ich ihn?

Komplexe Passwörter merken sich von selbst

Er generiert und speichert automatisch sichere, einzigartige Passwörter für jedes Konto.

Wiederverwendung vermeiden

Jeder Login bekommt sein eigenes Passwort. Wird ein Konto gehackt, sind die anderen sicher.

Auf allen Geräten verfügbar

Am PC, auf dem Handy, im Browser – immer synchronisiert.

Nur ein Master-Passwort merken

Statt 30 verschiedener Passwörter brauchst du nur noch eines: dein Master-Passwort.

Möglichkeiten: Bitwarden, KeePass, 1Password, LastPass

Warum ist das private Facebook-Profil so wichtig?

Das private Profil ist das Türschloss zur Facebook-Seite der Apotheke!

Admin-Zugang über privates Profil

Wer die Facebook-Seite der Apotheke verwaltet, ist mit dem privaten Profil verknüpft. Wird das Profil gehackt → Seite gehackt.

Hacker übernehmen die Apotheken-Seite

Sie posten Fake-Inhalte, löschen Inhalte, sperren Admins aus. Das ist schon vielen Apotheken passiert.

Mitarbeitende als Risiko

Wenn Mitarbeitende Zugang haben, aber ihr Profil unsicher ist, ist die Apothekenseite gefährdet.

Privates ≠ Unwichtig

Viele denken: "Ich bin ja privat." Aber das private Profil ist der Schlüssel zu allem.

Facebook-Profil absichern – Schritt für Schritt

Gehe zu: Einstellungen & Privatsphäre → Einstellungen → Privatsphäre

1

Wer sieht deine Beiträge?

Auf "Freunde" oder "Nur ich" stellen – nicht "Öffentlich"

2

Wer kann dich als Freund hinzufügen?

Auf "Freunde von Freunden" einschränken

3

Wer kann dein Profil suchen?

Einschränken, dass man dich nicht per E-Mail/Telefon finden kann

4

Profilbild & Titelbild

Auf "Nur Freunde" setzen – nicht öffentlich sichtbar lassen

5

Kommentare & Markierungen

Markierungsüberprüfung aktivieren: Du bestätigst, bevor Posts auf deinem Profil erscheinen

6

Vergangene Beiträge einschränken

Alte öffentliche Posts auf einmal auf "Freunde" setzen

Instagram-Konto absichern – die wichtigsten Einstellungen

Gehe zu: Einstellungen → Konto → Passwort & Sicherheit

1

Passwort überprüfen

Hast Du das Passwort noch zur Hand und wer hat es noch aller? → jetzt wechseln! accountscenter.facebook.com/password_and_security

2

Handynummer hinterlegen

Pflicht! Nur so kannst du deinen Account wiederherstellen, wenn du ausgesperrt wirst.

3

Verknüpfte Apps überprüfen

Einstellungen → Sicherheit → Apps & Websites → alte, unbekannte Apps entfernen

4

Login-Aktivitäten prüfen

Einstellungen → Sicherheit → Anmeldeaktivitäten → fremde Geräte sofort ausloggen!

5

E-Mail-Adresse aktuell halten

Stell sicher, dass deine hinterlegte E-Mail aktiv und gesichert ist.

6

2FA aktivieren (kommt gleich!)

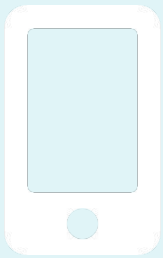
Der wichtigste Schritt überhaupt – wir zeigen gleich wie.

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

2FA = Zwei Schlösser statt einem

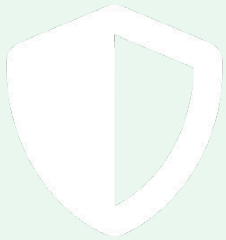
Faktor 1
Passwort

+



Faktor 2
Handy / App

=



Konto
sicher!

Selbst wenn jemand dein Passwort stiehlt – ohne deinen zweiten Faktor kommt er trotzdem nicht in dein Konto. Du auch nicht.

2FA-Methoden im Vergleich

SMS-Code

Schwach

✓ Einfach einzurichten

i SIM-Karte kann gehackt werden (SIM-Swapping). Nur als Notlösung!

Authenticator App

Gut

✓ Google Authenticator, Microsoft Authenticator, Authy

i Handy muss dabei sein. Empfehlung: Authy (mit Cloud-Backup)

Hardware-Token (YubiKey)

Sehr sicher

✓ Physischer USB-Stick – kann nicht aus der Ferne gehackt werden

i Kostet ca. 50–60 €. Für Agenturen & mehrere Apotheken ideal.

Passkey (Biometrie)

Zukunft

✓ Fingerabdruck oder Face ID = Login. Kein Passwort mehr nötig.

i Kommt gleich im nächsten Block!

2FA einrichten – bei Facebook & Instagram

Facebook

1. accountscenter.facebook.com aufrufen
2. "Passwort & Sicherheit" öffnen
3. "Zwei-Faktor-Authentifizierung" wählen
4. Konto auswählen → Methode wählen
5. QR-Code mit Authenticator-App scannen
6. Backup-Codes ausdrucken & ablegen

Instagram

1. Profil → Menü (3 Striche) öffnen
2. Einstellungen → Passwörter & Sicherheit
3. "Zwei-Faktor-Authentifizierung" tippen
4. "Erste Schritte" → Methode wählen
5. Authenticator-App empfohlen!
6. Backup-Codes drucken & ablegen!

⚠️ **Backup-Codes immer sichern – z. B. im Passwortmanager! Bei Handyverlust sonst ausgesperrt.**

Was ist ein Passkey?

Ein Passkey ersetzt das Passwort komplett.
Du loggst dich mit deinem Fingerabdruck oder Face ID ein.

Merkmal	🔑 Passwort	👁️ Passkey
Was du brauchst	Passwort merken	Fingerabdruck / Face ID
Kann gestohlen werden?	Ja – durch Phishing	Nein – bleibt auf deinem Gerät
Kann erraten werden?	Ja	Nein
Sicherheit	Mittel	Sehr hoch
Benutzerfreundlichkeit	Aufwändig	Extrem einfach

Passkey einrichten – Schritt für Schritt

Funktioniert mit: iPhone (ab iOS 16), Android (ab Version 9), Windows Hello

Facebook Passkey

1. accountscenter.facebook.com öffnen
2. Passwort & Sicherheit → Passkeys
3. "Passkey hinzufügen" tippen
4. Fingerabdruck / Face ID bestätigen
5. Fertig – kein Passwort mehr nötig!

Instagram Passkey

1. Profil → Einstellungen & Aktivitäten
2. Passwörter & Sicherheit → Passkeys
3. "Passkey erstellen" auswählen
4. Biometrische Bestätigung durchführen
5. Passkey wird im Gerät gespeichert

✓ **Passkey + 2FA = maximale Sicherheit. Beides zusammen nutzen!**

Mitarbeiter Sicherheit

Wer hat hier wirklich worauf Zugriff und ist das wirklich sicher?

Warum müssen sich Mitarbeitende absichern?

Die Apothekenseite ist nur so sicher wie das schwächste Mitarbeiter-Profil!

Mitarbeiterin mit altem Passwort

Anna verwaltet die Facebook-Seite. Ihr privates Profil hat noch das Passwort "anna2018" – ohne 2FA. Hacker übernehmen Annas Profil → die Apothekenseite ist weg.

Ehemalige Mitarbeiterin hat noch Zugriff

Lisa hat die Apotheke verlassen – aber wurde nie als Admin entfernt. Aus Frust oder Versehen kann sie Inhalte löschen oder posten.

Team-Login mit geteiltem Passwort

Alle loggen sich mit demselben Account ein. Wenn einer geht oder ein Gerät verloren geht, hat immer noch jeder Zugriff.

Das Ziel: Jeder hat sein eigenes Profil

Jede Mitarbeiterin, die postet, arbeitet über ihr eigenes, abgesichertes privates Profil. Rollen werden klar vergeben.

Sicherheits-Checkliste für jede Mitarbeiterin

✓	**Sicheres Passwort für Facebook & Instagram setzen** Mindestens 12 Zeichen, Passwortmanager nutzen	Mitarbeiterin
✓	**Handynummer im Facebook-Konto hinterlegen** Notwendig für Kontowiederherstellung	Mitarbeiterin
✓	**2FA aktivieren (Authenticator App)** Google Authenticator oder Authy	Mitarbeiterin
✓	**Passkey einrichten (wenn Gerät es unterstützt)** iPhone ab iOS 16 oder Android ab v9	Mitarbeiterin
✓	**Sicherheitscheck durchführen** accountscenter.facebook.com/password_and_security	Mitarbeiterin
✓	**Login-Aktivitäten prüfen** Fremde Geräte sofort ausloggen!	Mitarbeiterin
✓	**Backup-Codes sichern** Im Passwortmanager oder ausgedruckt sicher aufbewahren	Mitarbeiterin
⚠	**Bei Austritt: Admin-Rechte sofort entfernen** Verantwortung der Leitung / Inhaberin. Nicht warten!	Leitung

Du hast eine Mail von Facebook bekommen. Wirklich?

Ich habe so eine Mail bekommen. Ein Urheberrechtsverstoß – und dann haben wir alle Reels mit Musik gelöscht. Wir wollten einfach kein Risiko eingehen.

Das hätte nicht sein müssen. Einstweilige Verfügungen kommen IMMER per Post. Dann: Nichts unterschreiben, Medienanwälte kontaktieren.

Woran erkenne ich eine Fake-Mail von "Facebook"?

Verdächtige Absender-Adresse

Echter Meta-Absender: @facebookmail.com oder @metamail.com
Fake: support-facebook.net · fb-security.com · meta-admin@gmail.com

Künstliche Dringlichkeit & Drohungen

"Dein Konto wird in 24 Stunden gesperrt!"
"Sofortiger Handlungsbedarf!" → Nie sofort klicken!

Link führt NICHT zu facebook.com

Vor dem Klicken: Maus über den Link halten → URL prüfen!
Alles außer facebook.com / instagram.com / meta.com ist fake.

So prüfst du es richtig

Gehe DIREKT zu facebook.com im Browser (nicht über den Link!)
Echte Nachrichten von Meta: Einstellungen → Sicherheitscenter → E-Mails von Facebook

Echte E-Mail-Adressen von Meta – die Liste

Meta hat diese Seite selbst – überprüfe echte Absender hier: facebook.com/business/help/372703956148310

Echte Absender-Domain	Wofür genutzt
✓ @facebookmail.com	Standard-Benachrichtigungen, Passwort-Reset, Sicherheits-E-Mails
✓ @metamail.com	Neuere Meta-Kommunikation, Business-Benachrichtigungen
✓ @support.facebook.com	Support-Antworten (selten, nur auf Anfragen)
✓ @fb.com	Interne Kurzform – kommt sehr selten vor

Eindeutige FAKE-Adressen – niemals klicken!

fb-support@gmail.com nmeta-security@outlook.com support-facebook.net facebooksecurity.com instagram-help@yahoo.com

Wo hängst Du? Was hindert Dich, sicher zu werden?

Lass mich all die Einwände hören! Maximal 3 Personen können Ihren Bildschirm teilen, damit wir die richtigen Einstellungen zeigen können. Habt bitte Eure Passworte dabei und seid euch bewusst: Es wird aufgezeichnet. Passworte bleiben unsichtbar.

1 **Mach dich selbst sicher**

Suche Dir jetzt im Kalender 30 ruhige Minuten für diese Einstellungen.

2 **Mach Mitarbeiter sicher**

Nutze die Checkliste oder gib sie direkt weiter.

Vertiefungsaufgabe 3: Bitte beantworte meine Umfrage kurz. https://forms.gle/VqgN4r6xbzKcBdT66 Damit kann ich auch unsere nächste Session zum Thema Organisation besser vorbereiten.

Bevor wir auseinander gehen...

1. **Wie oft hast Du dir gedacht: Oh, das betrifft genau mich?**
2. **Wie oft hast Du dich schon gefragt, ob eine Mail von Meta echt war?**
3. **Was steht auf deiner To-Do Liste nach dieser Session?**

Bis zum nächsten Mal

03.06. · 13.30 Uhr

Thema: Meta Orga im Hintergrund

⚠ **Bitte seid am PC dabei, wenn ihr selbst gleich parallel Einstellungen machen wollt.** Ein zweiter Monitor und ein Erfrischungsgetränk werden empfohlen.