SABU

SICHERHEITSLEITFADEN FÜR FACEBOOK BUSINESS KONTEN

Facebook ist ein mächtiges Werkzeug für Unternehmen, um ihre Zielgruppen zu erreichen und ihre Markenbekanntheit zu steigern. Doch mit den vielen Möglichkeiten kommen auch Sicherheitsrisiken.

Die Sicherheit deines Facebook-Kontos ist entscheidend, um deine Investitionen zu schützen und das Vertrauen deiner Kunden zu wahren. Dieser Leitfaden bietet praktische Tipps und bewährte Verfahren, um dein Konto vor unautorisierten Zugriffen und anderen Bedrohungen zu schützen.

DARUM IST ES SO WICHTIG AUF DIE SICHERHEIT DES FACEBOOK-KONTOS ZU ACHTEN

- **Schutz vor finanziellen Verlusten:** Unautorisierte Zugriffe können zu unerwünschten Werbeausgaben führen, die erhebliche finanzielle Schäden verursachen.
- **Datensicherheit:** Sicherstellen, dass sensible Unternehmens- und Kundendaten nicht in die falschen Hände geraten.
- **Vermeidung von Rufschädigung:** Sicherheitsverletzungen können das Vertrauen der Kunden untergraben und dem Ansehen deines Unternehmens schaden.
- **Compliance und rechtliche Anforderungen:** Einhaltung von Datenschutzgesetzen und Vorschriften, um rechtliche Konsequenzen zu vermeiden.
- **Sicherstellung der Kampagnenintegrität:** Gewährleistung, dass deine Werbekampagnen wie geplant laufen und keine unautorisierten Änderungen vorgenommen werden.

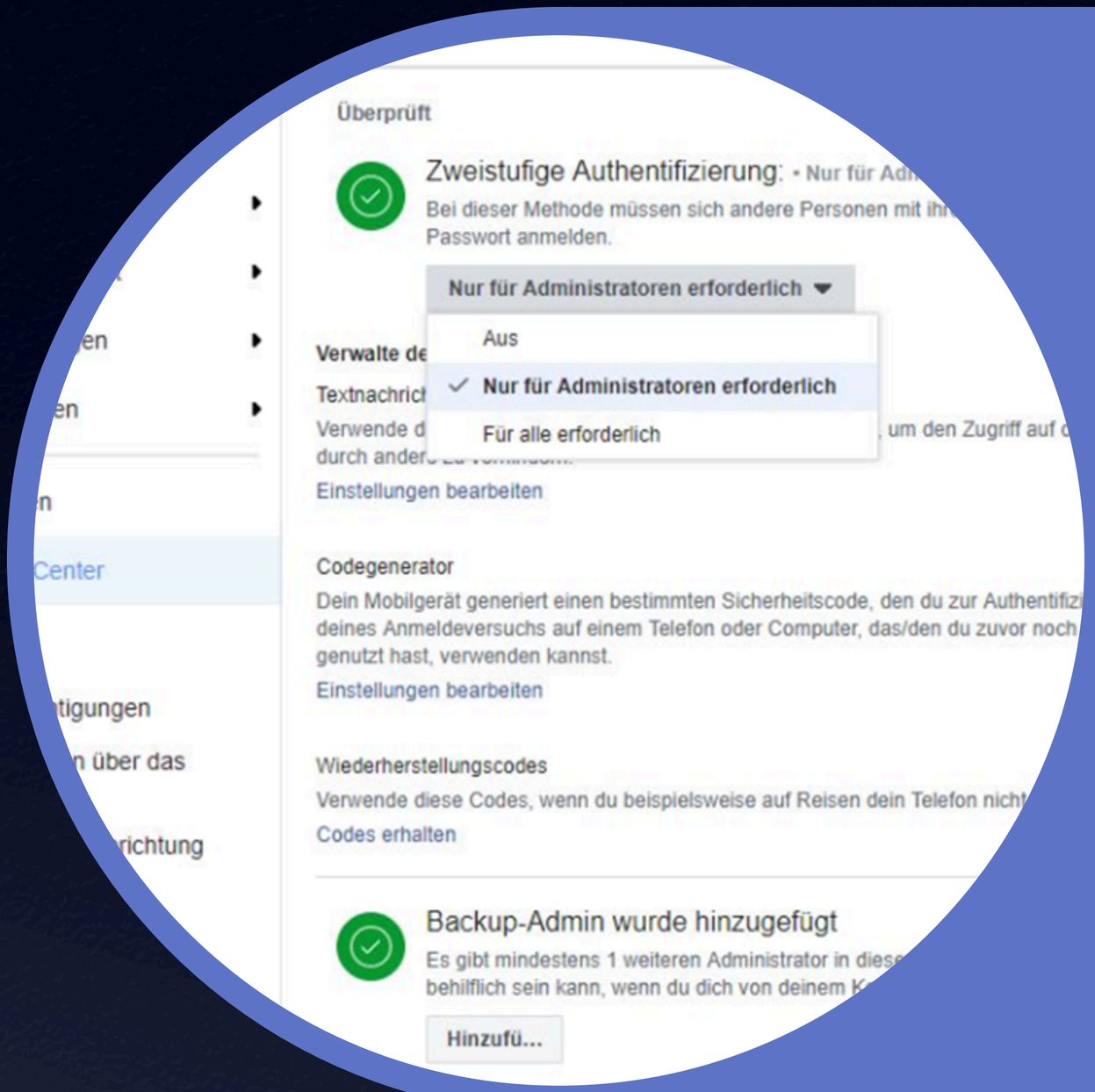
DIE ZWEISTUFIGE AUTHENTIFIZIERUNG NUTZEN

Verlange von jedem, der Zugang zu deinem Business Manager hat, sich **für die zweistufige Authentifizierung** anzumelden und diese zu nutzen. Die zweistufige Authentifizierung schützt dein Business Konto vor Zugriff durch Unbefugte.

Jedes Mal, wenn ein Mitarbeiter beispielsweise von einem neuen Computer oder Mobiltelefon zugreift, wird er aufgefordert einen besonderen Sicherheitscode einzugeben. Um diese Sicherheitsfunktion nutzen zu können, muss eine Telefonnummer zu dem eigenen Facebook-Profil hinzugefügt werden.

So legst du fest, dass die zweistufige Authentifizierung für die Nutzer deines Business-Portfolios verpflichtend ist:

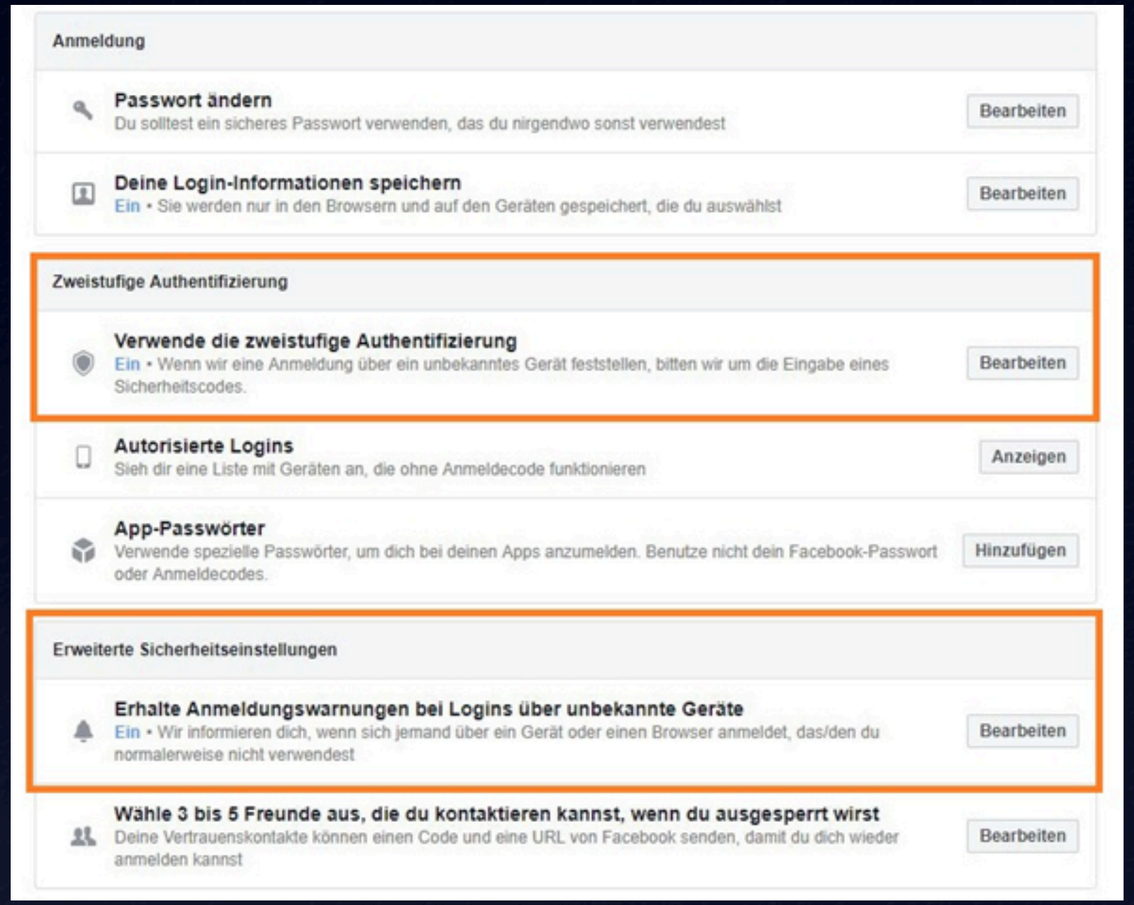
1. Gehe zu den Unternehmenseinstellungen.
2. Klicke auf Unternehmensinfos.
3. Scrolle nach unten zu Business-Optionen.
4. Klicke neben Zweistufige Authentifizierung auf das Dropdown-Menü.
5. Durch Auswahl von Nur Administratoren oder Alle legst du fest, für wen die zweistufige Authentifizierung verpflichtend ist.



PRIVATE FACEBOOK-KONTEN SCHÜTZEN

Auch im eigenen Profilbereich können du und deine Mitarbeiter Maßnahmen zur Kontosicherheit ergreifen.

- **Ein sicheres Passwort nutzen**! Und das ist dann nicht Schuh80 oder 1234, sondern beispielsweise ein über einen Generator erstelltes Passwort mit Zahlen, Sonderzeichen sowie Groß- und Kleinbuchstaben. Zudem sollte das Passwort regelmäßig geändert werden. Empfehlenswert ist außerdem einen Passwort-Manager zu nutzen. Mehr dazu: **KLICK**!
- **Das persönliche Profil über eine zweistufige Authentifizierung schützen**. Dabei ist das Vorgehen ähnlich wie bei dem Business Manager: sollte über einen neuen Computer oder ein neues Telefon ein Zugriff erfolgen, muss ein Code, der beispielsweise über eine SMS verschickt wird, eingegeben werden. Zusätzlich können auch Codes manuell abgespeichert und ausgedruckt werden – falls beispielsweise das Telefon nicht zur Hand ist. Mehr dazu: **KLICK**!
- **Warnung über fremde Zugriffe** sollte unbedingt aktiv sein, sodass bei Vorfällen direkt gehandelt werden kann, falls ungewöhnliche Browser oder ähnliches genutzt werden. Mehr dazu: **KLICK**!
- **Keine Freundschaftsanfragen von unbekannten Personen** annehmen und **Augen nach verdächtigen Links und Schadsoftware** offen halten. Mehr dazu hier: **KLICK!**

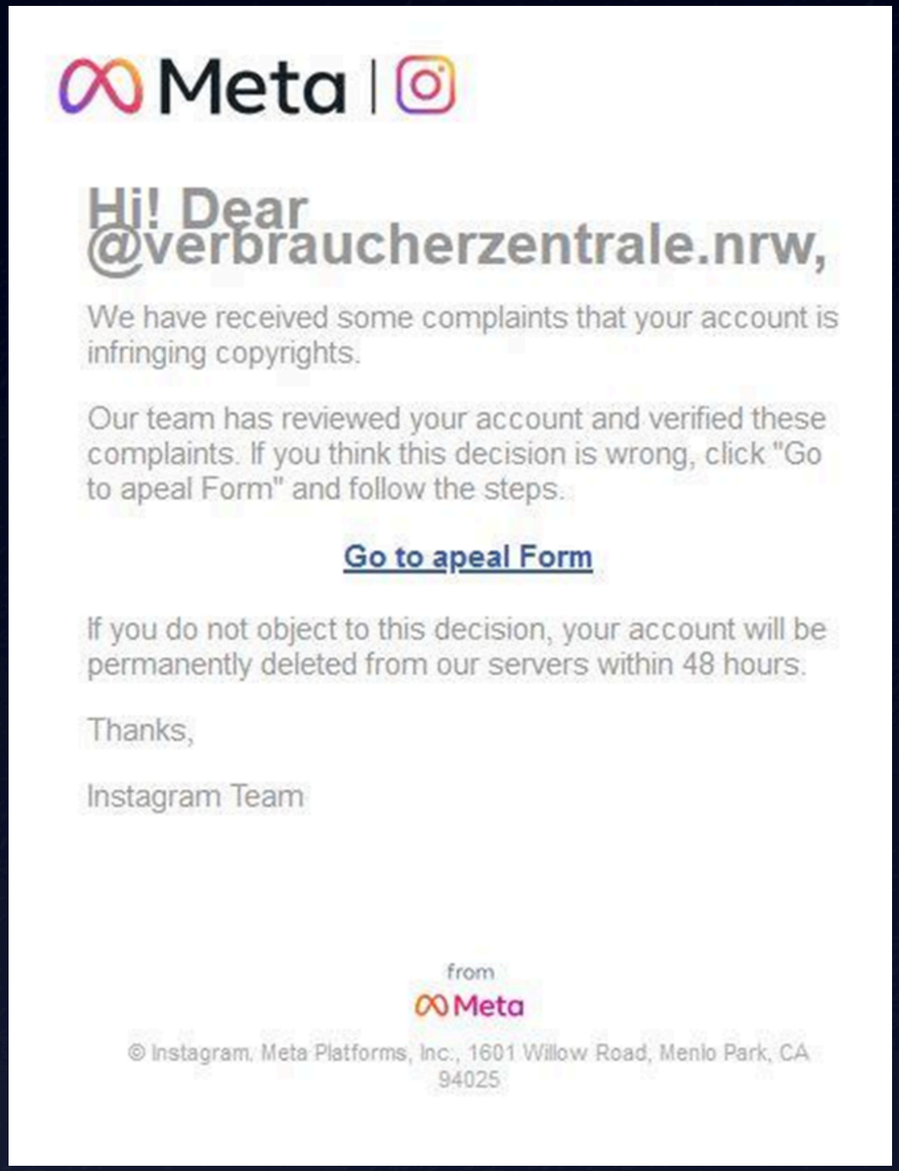


KEINE PHISHING-MAILS ÖFFNEN!

Betrüger geben sich als Meta aus, schreiben willkürlich Nachrichten an zahlreiche Empfänger und erfinden Vorwände, warum du dich bei Facebook oder Instagram anmelden solltest – und zwar über einen Link, der gleich mitgeschickt wird. Der Link führt zu einer nachgeahmten Login-Seite. Wer dort Zugangsdaten eingibt, übermittelt diese an Kriminelle.

Manchmal genügt es den Betrügern, Zugang zu deinem Konto zu haben, um dort unbemerkt „arbeiten“ zu können. Es kann aber auch vorkommen, dass die Kriminellen dein Passwort ändern und Seiten-Admins entfernen, um dich und andere Personen aus dem Konto auszusperren. Manchmal werden Werbeanzeigen erstellt, um betrügerischen Aktivitäten zu verbreiten.
Dabei ist es essentiell Folgendes zu beachten:

- Wichtige Account-Infos schicken Instagram und Facebook niemals als Direktnachricht oder SMS, sondern per E-Mail. Wenn du so eine E-Mail bekommst, achte auf den Absender! Echte E-Mails von Instagram kommen nur von @mail.instagram.com oder @facebookmail.com; Facebook schickt ausschließlich von @fb.com, @facebook.com oder @facebookmail.com. Achte auch auf abgeänderten Schreibweisen oder Fehler.
- Die Phishing-E-Mails können relativ echt aussehen. In solchen E-Mails wird behauptet, dass du gegen Copyright- oder Community-Regeln verstoßen hast und dein Konto werde gesperrt bzw. gelöscht – wenn du nicht über den blauen Button oder den Textlink Einspruch einlegen würdest. Da solltest auf keinen Fall klicken oder Anhänge herunterladen.
- In den Einstellungen von Facebook kannst du prüfen, welche E-Mails zum Thema Sicherheit wirklich verschickt wurden: **KLICK**!



KEINE FAKE-PROFILE NUTZEN

Nutze keine Fake-Privatprofile für Administration des Accounts und der Werbekonten, wie z.B. Schuhhaus XY, zu dem auch noch 10 aktuelle und ehemalige Mitarbeiter den Zugang haben. In den AGB von Facebook steht eindeutig, dass hinter jedem Nutzer eine echte Person stehen muss und auch nur ein Account pro Person erlaubt ist. Wenn es also mal richtig schlecht läuft und beispielsweise ein Konkurrent das Fake-Profil meldet, kann es also sein, dass daraufhin dein Unternehmenskonto gesperrt wird und die Konten und Seiten weg sind.

MEHRERE ADMINISTRATOREN HINZUFÜGEN

Wer den Business Manager nutzt und das sollten ebenfalls alle Unternehmen tun, die Facebook professionell betreiben, der sollte immer einen zweiten Admin aktiv haben. Hierfür bietet sich beispielsweise der Geschäftsführer oder ähnliche – mit dem Unternehmen eng verknüpfte – Mitarbeiter an. Denn gibt es nur einen einzigen Mitarbeiter, der den Admin-Zugang zum Business Manager hat und dieser z.B. nicht mehr aktiv im Unternehmen ist oder wenn sein privater Account gesperrt wird, dann ist der Business Manager so nicht mehr zu verwalten. Mehr dazu: **KLICK**!

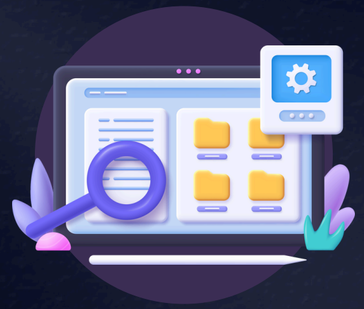
EMPFEHLUNGEN FÜR DIE REGELMÄSSIGE ÜBERPRÜFUNG DEINER KONTEN:

FÜHRE EINE SICHERHEITSÜBERPRÜFUNG DURCH

Mit dem Sicherheits-Check-Tool von Facebook kannst du dein persönliches Facebook-Konto überprüfen und noch sicherer machen.

DIE AUTORISIERTEN LOGINS ÜBERPRÜFEN

In deinen Einstellungen kannst du sehen, auf welchen Geräten du angemeldet bist, und prüfen, ob nicht autorisierte Geräte-Logins darunter sind.



KONTROLLIERE DEN ZUGRIFF AUF DIE KONTEN

In den Einstellungen des Business Manager kannst du regelmäßige Revisionen der Personen durchführen, die Zugriff auf deine Business-Manager-Konten und Anzeigenkonten haben. Ehemalige Mitarbeiter sowie Personen, die keinen Zugriff mehr benötigen, solltest du dabei entfernen.

SUCHE AUF DEINEN GERÄTEN NACH SCHADPROGRAMMEN

Überprüfe die Apps und Browser-Plugins auf deinen Geräten regelmäßig und entferne sie, falls du sie nicht mehr verwendest.

WAS TUN WENN EIN WERBEKONTO GEHACKT WIRD?

...wenn du noch Zugang zu deinem Konto hast:

- **Meta-Support kontaktieren**: Wende dich an Facebook, um deine Situation zu schildern. Auch wenn es lange dauern kann, bis der Support reagiert, muss er eingeschaltet werden.
- **Zahlungsmittel entfernen**: Um weitere Abbuchungen zu verhindern, musst du deine Zahlungsmittel entfernen.
- **Laufende Kampagnen deaktivieren**: Deaktiviere alle laufenden Kampagnen. Wurde von den Hacker:innen bereits eine Kampagne erstellt, lösche diese nicht, damit Facebook den Fall überprüfen kann.
- **Einstellungen überprüfen**: Kriminelle könnten Zugriffsrechte oder andere Einstellungen verändert haben. Überprüfe daher die Unternehmenseinstellungen. Stelle außerdem sicher, dass keine automatische Aktivierung für betrügerische Werbekampagnen eingeschaltet wurde. Klicke dafür auf „Regeln“ und „Regeln verwalten“ im Kampagnen-Bereich.
- **Weitere Personen informieren**: Alle Personen, die Zugang zu deiner Unternehmensseite haben, müssen ihr Passwort ändern.

... wenn du keinen Zugang mehr zu deinem Konto hast:

- **Meta-Support kontaktieren**: Auch wenn du ausgesperrt bist, kannst du meta über folgenden Link kontaktieren: **KLICK!**
- **Zahlungsdienstleister benachrichtigen**: Erfahrungsgemäß kann es lange dauern, bis du wieder Zugriff auf dein Konto hast. Kontaktiere daher auch deinen Zahlungsdienstleister und lasse die Zahlungsmittel sperren.
- **Weitere Personen informieren**: Informiere alle Personen, die an Deiner Unternehmensseite arbeiten. Auch wenn es unwahrscheinlich ist, kann es sein, dass noch jemand Zugang zum Werbekonto hat.