Mittelstand-Digital
Zentrum
Handel

INFOBLATT

Social Media: Hacks und Sperrungen vorbeugen

Ein leidiges Szenario mit teils schwerwiegenden wirtschaftlichen Folgen – Ihr Instagram- oder Facebook-Unternehmensaccount könnte gehackt oder gesperrt werden. Es gibt jedoch Möglichkeiten zur Prävention, mit denen Sie die Wahrscheinlichkeit in eine solche Situation zu geraten deutlich verringern können. In diesem Infoblatt wird dargestellt, wie Sie Ihren Account vor Hackangriffen schützen können oder was mögliche Gründe für eine Sperrung sind.

Wurde Ihr Account bereits gehackt oder gesperrt? Auch hierzu bieten wir Ihnen Hilfestellungen in dem Leitfanden "Social Media: Was tun bei Hacks und Sperrungen?": https://digitalzentrumhandel.de/infoblatt-social-media-was-tun-bei-hacks-und-sperrungen

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Wie kann ich einen Hackerangriff vorbeugen?

1. Vorbeugung Allgemein

Vorsicht ist besser als Nachsicht heißt die Devise im Internet und sie gilt auch hier.
Um das Hacken Ihrer Accounts so gut wie möglich zu vermeiden, sind einige Punkte zu beachten:

a) Sichere Passwörter

Am besten schützen Sie sich, indem Sie ausschließlich Passwörter verwenden, die länger als **12 Zeichen** sind. Es sollte sich dabei **nicht** um **Namen oder Wörter** aus dem Wörterbuch handeln. Gute Passwörter enthalten **Sonderzeichen und Zahlen**. Passwörter für die **Systemverwaltung** sollten bestenfalls aus **mehr als 16 Zeichen** bestehen. Um die sicheren und komplexen Passwörter unternehmensintern verwalten zu können, eignet sich zum Beispiel ein **Passwortmanager**, welcher einen sicheren Zugriff auf verschiedene Passwörter ermöglicht. Außerdem sollten Sie darauf achten für jedes Konto ein eigenes Passwort zu verwenden.

b) Antworten Sie nicht auf Phishing-Mails

Betrüger:innen nutzen Phishing-Mails, um vertrauliche Daten abzugreifen. Hierbei geben Sie eine falsche Identität vor (z.B. einer Institution) und fordern von Ihnen die Eingabe eines Passwortes.
Solche E-Mails sind zu **löschen** und dürfen **nicht beantwortet** werden. Geben Sie das Passwort unter **keinen Umständen** ein. Sollten Sie einmal ein Passwort auf diese Weise eingeben, dann sollten Sie dieses umgehend in der App bzw. auf dem Social-Media Kanal ändern.

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

c) Verwenden Sie die zweistufige Authentifizierung

Bei der zweistufigen Authentifizierung sind zwei unterschiedliche Authentifizierungsfaktoren zur Bestätigung der Identität erforderlich. Hier gilt: Nur wenn Sie auf **zwei verschiedene** Arten Ihre Identität bestätigen, erhalten Sie Zugriff auf Ihren Account.
Dies dient dem Schutz Ihres Accounts, da Unberechtigte so zwei Zugriffspunkte hacken müssen, um Zugriff zu erlangen.
Bei Facebook kann eine zweite Authentifizierung mit Hilfe einer **Authentifizierungs-App**, **einer SMS oder einem Sicherheitsstick** erfolgen. Bei Instagram sind die beiden erstgenannten Verfahren möglich. Falls diese Sicherheitsmethoden nicht verfügbar sind, werden Anmeldeanfragen gesendet oder die Anmeldung kann anhand von Backup-Codes erfolgen.

Vorgehen bei Facebook:
„Einstellungen und Privatsphäre“ → „Kontenübersicht“ → „Passwort und Sicherheit“ → „Zweistufige Authentifizierung“

Vorgehen bei Instagram:
Profil → Drei-Strich-Menü → „Einstellungen und Privatsphäre“ → „Kontenübersicht” → „Passwort und Sicherheit“ → „Zweistufige Authentifizierung“

SICHERHEITSSTICK

Dabei handelt es sich um einen USB-Stick bzw. kleines Gerät, mit einem U2F- oder FIDO2-Sicherheitsschlüssel. Dieses Gerät muss zunächst bei einem Drittanbieter erworben werden. Je nach Variante, muss das Gerät an eine USB- oder Lightning-Buchse angeschlossen werden oder sich lediglich in der Nähe des Computers / Handy befinden.

ANMELDEANFRAGEN

Anmeldeanfragen können per E-Mail oder auf bereits eingeloggten Geräten erfolgen. Hierbei fragt Facebook, ob Sie sich bei Ihrem gewünschten Gerät einloggenwollen. Falls es sich hierbei um Ihren Zugriff handelt, können Sie die Anfrage bestätigen.

BACKUP-CODES

Bei der Aktivierung des zweistufigen Authentifizierungs-Verfahrens bietet Facebook die Möglichkeit Ihnen 10 Wiederherstellungscodes zu nennen. Diese müssen sie sich aufschreiben und an einem sicheren Ort verfahren. Sollten Sie einmal keinen Zugriff auf Ihr Konto bzw. Gerät haben, so können Sie sich mit diesen Backup-Codes einloggen. Jeder Code kann nur einmal verwendet werden, sollten Sie die Codes verlieren oder bereits alle genutzt haben, so können Sie jeder Zeit neue Wiederherstellungscodes erhalten, indem Sie auf “Neue Codes erhalten” klicken.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

d) Führen Sie mehrere E-Mail-Adressen

Für Ihre Social-Media-Kanäle sollten Sie eine **zusätzliche** E-Mail-Adresse verwenden.
Dies hat zum einen den Vorteil, dass ihre Haupt-E-Mail-Adresse geschützt ist, falls ihre Social-Media-Accounts gehackt werden.

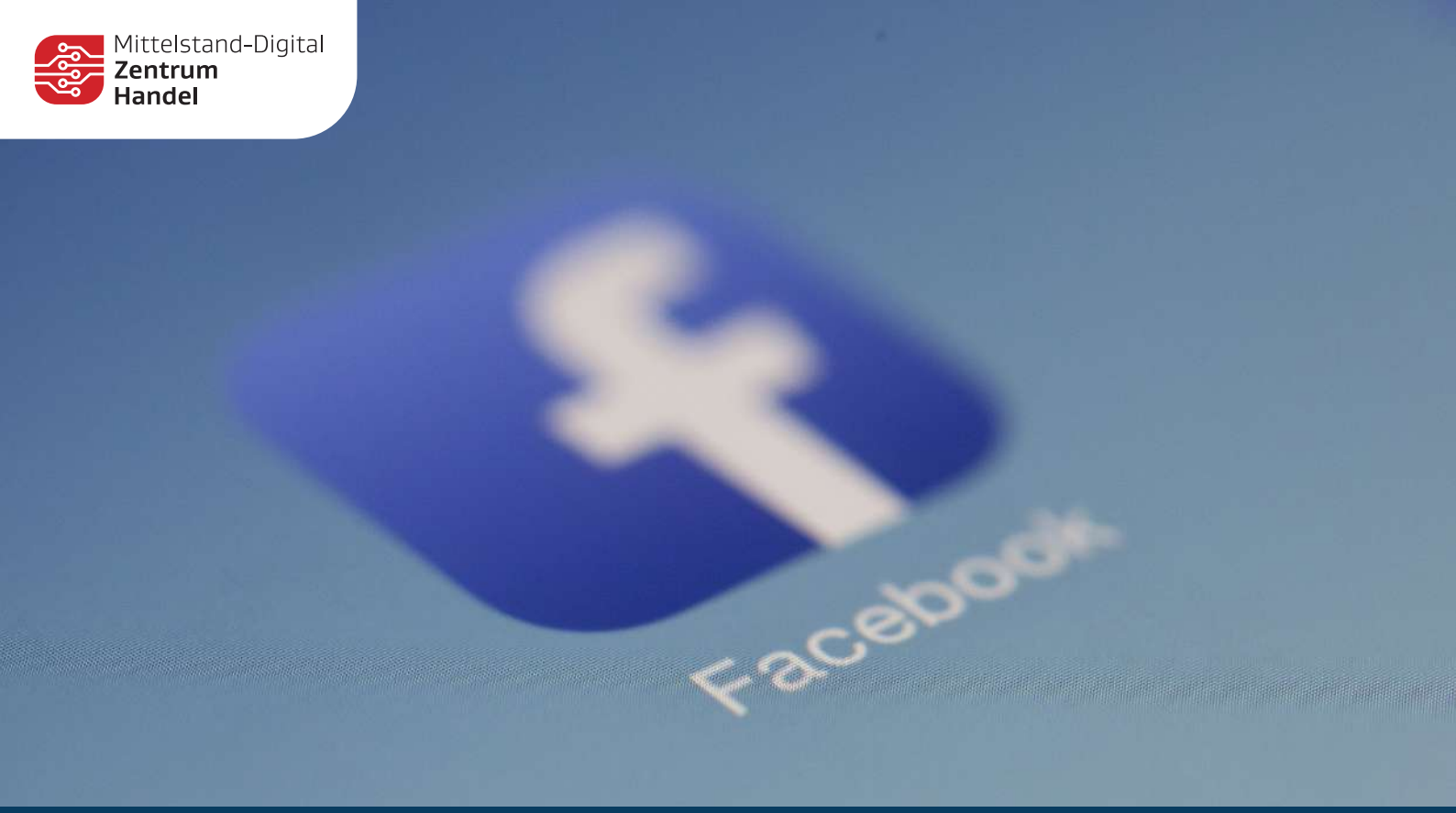
e) Prüfen Sie auf Leaks (undichte Stelle)

Wird eine Webseite gehackt, so gelangen Daten (Benutzernamen, Passwörter, …) schnell ins Darknet (Netzwerk mit verschlüsselter Kommunikation, in dem Nutzer anonym bleiben). Um herauszufinden, ob Ihre Daten bereits im Umlauf sind, gibt es seriöse Webseiten wie: https://haveibeenpwned.com, die Ihnen bei Eingabe Ihrer E-Mail-Adresse sagen können, ob diese inklusive Passwörter bereits im Umlauf ist.
Falls dies der Fall sein sollte, so **ändern** Sie bitte Ihre **Passwörter** und vermeiden Sie das Nutzen von gleichen Passwörtern.

f) Führen Sie Updates durch

Updates stellen **sicherheitsrelevante Faktoren** dar. Mit Hilfe von Updates werden Lücken im System geschlossen bzw. das System verbessert, wodurch der Zugang für Hacker:innen erschwert wird. Sollten Sie nicht die neuste Version einer Anwendung besitzen, so kann sich der:die Betrüger:in gegebenenfalls leichter in Ihr Gerät einschleusen.
Updates sollten daher **zeitnah** durchgeführt werden. Am besten lassen Sie dafür in Ihrem App-Store automatische Updates zu.

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages



Hackerangriff bei Facebook vorbeugen

2. Vorbeugung Facebook

Um Hackerangriffe bei Facebook vorzubeugen, finden Sie im Folgenden sech spezifische Maßnahmen.

Öffnen Sie die Facebook-Website und befolgen Sie zunächst die Schritte: „Einstellungen und Privatsphäre“ → „Einstellungen“. Diese gelten als Ankerpunkt für das weitere Vorgehen, welches Sie in den folgenden Gliederungspunkten (a-f) vorfinden.

a) Vermeiden Sie „Single sign on“

Facebook bietet die Möglichkeit sich mit dem Facebook-Account bei anderen Websites anzumelden (sog. „Single sign on“). Gelangt ein:e Betrüger:in an Ihre Anmeldedaten für Facebook, so kann diese:r auch Zugang zu Ihren weiteren Accounts bei den anderen Websites erlangen.

Klicken Sie auf: „Apps und Websites“

Hier können Sie prüfen, wo Sie sich per Facebook registriert haben und können dies bei Bedarf löschen.

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

b) Richten Sie einen Hacker-Alarm ein

Sobald Außenstehende den Zugang zu Ihrem Facebook-Accounts erlangt haben, werden Sie von Facebook gewarnt. Hier können Sie auch eine zusätzliche E-Mail-Adresse anlegen, über die Sie gewarnt werden. Dies dient erneut zum Schutz, falls Hacker:innen bereits Ihren E-Mail-Account beschlagnahmt haben sollten.
Vorgehen: „Sicherheit und Login“ → „Erweiterte Sicherheitseinstellungen“ → „Warnungen bei Logins über unbekannte Geräte erhalten“ → „Bearbeiten“ → Aktivieren Sie hier alle Optionen und legen Sie am besten noch eine weitere E-Mail-Adresse an.

c) Überprüfen Sie die Geräteliste

Facebook führt eine Liste, in der Sie sehen können, auf welchen Geräten Sie derzeit angemeldet sind. Sie können sich über diese Liste auch bei einzelnen oder allen Geräten gleichzeitig abmelden.
Vorgehen: „Sicherheit und Login“ → „Hier bist du aktuell angemeldet“

d) Überprüfen Sie die Accountzugriffe

Neben den derzeit angemeldeten Geräten können Sie außerdem sehen, wann Sie sich an- und abgemeldet haben. Hierbei wird auch die IP-Adresse aufgeführt. Über dieses Protokoll können Sie verfolgen, ob externe Anmeldungen erfolgt sind.
Vorgehen: „Deine Facebook-Informationen“ → „Zugriff auf deine Informationen“ → „Sicherheits- und Login-Informationen“ → „An- und Abmeldungen“

e) Chronik und Markierungen

Die Chronik eines Profils ist für alle Nutzer:innen zugänglich. Damit Fremde Sie nicht mit unangenehmen Inhalten in Verbindung bringen, indem sie auf Ihre Chronik posten bzw. Sie auf nicht angebrachten Fotos markieren, sollte diese Voreinstellung geändert werden.
Vorgehen: „Profil und Markierungen“: Hier sollten Sie alle Einstellungen von „Öffentlich“ auf „Freunde“ abändern.

f) Kontrollieren Sie die Gesichtserkennungsfunktion

Laut Datenschutzgrundverordnung (DSGVO) soll die Gesichtserkennung als Passwort-Ersatz standardgemäß ausgeschaltet sein. Dies können Sie kontrollieren.
Klicken Sie auf: „Gesichtserkennung“ und überprüfen Sie, ob die Gesichtserkennung ausgeschaltet ist.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

3. Vorbeugung Instagram

Für das spezifische Vorbeugen von Hackerangriffen bei Instagram sind die folgenden zwei Maßnahmen hilfreich.
Hierfür öffnen Sie zunächst die Instagram-App und folgen diesen Schritten: Profil → Drei-Strich-Menü → „Einstellungen und Privatsphäre“

a) Überprüfen Sie die Kontoaktivitäten

Auch bei Instagram gibt es Möglichkeiten zur Überprüfung der Aktivität, die denen von Facebook ähnlich sind. Dafür folgen Sie bitte zunächst den Schritten: → „Kontenübersicht” → „Passwort und Sicherheit“
Folgende Menüpunkte sind für Sie wichtig:
„Passwort“: Sie sehen, wann das Passwort zuletzt geändert wurde
„Hier bist du aktuell angemeldet“: Sie sehen, wann und über welches Gerät auf den Account zugegriffen wurde und können Aktivitäten bzw. Zugriffe beenden.
„Aktuelle E-Mails“: Sie sehen, welche E-Mails Instagram an Sie gesendet hat. Somit können Sie feststellen, ob eine bei Ihnen eingegangene E-Mail tatsächlich von Instagram gesendet wurde oder ob es sich dabei um eine Phishing-Mail handelt (s.o.).

b) Kontrollieren Sie den externen Zugriff auf Ihren Account

Sobald Sie Diensten den Zugriff auf Ihren Account erlauben, können diese Ihre Daten einsehen. Bei Bedarf können Sie diesen Zugriff wieder löschen.
Klicken Sie auf: „Website-Berechtigungen” → „Apps und Websites“ und kontrollieren Sie hier die zugelassenen Dienste.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Wann sperrt Instagram/Facebook einen Account?

Wann sperrt Instagram/Facebook einen Account?

Instagram bzw. Facebook sperrt einen Account, wenn mindestens gegen eine ihrer Richtlinien (Nutzungsbedingungen von Instagram/Facebook, Musikrichtlinien, Branded-Content-Richtlinien, Gemeinschaftsrichtlinien) verstoßen wurde. Dabei kann es sich grundsätzlich um drei Arten von Verstößen handeln:

1. Phishing:

Phishing (Abfangen persönlicher Daten) oder der Verdacht besteht bei Instagram, wenn der Algorithmus davon ausgeht, dass eine unberechtigte dritte Person Ihre Zugangsdaten zum Account herausgefunden hat und diesen nun missbraucht. Dies äußert sich konkret durch:

- das Einloggen von verschiedenen IP-Adressen/Geräten und/oder Anmeldungen aus dem Ausland.
- das Benutzen von sog. Drittanbieter-Apps, die Bot-Aktivitäten wie z.B. das automatisierte Kommentieren von Beiträgen ausführen.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

2. Post mit rechtswidrigen Inhalten:

Posts und Kommentare mit rechtswidrigen Inhalten werden von **Instagram** abgestraft. Darunter fallen:

- das Posten mit Fake-Profilen
- Urheberrechtsverletzungen am Bild oder an einer Marke
- Unangemessene Beiträge (z.B. Bilder und Videos, die Gewalt in jeglicher Form verherrlichen oder dazu aufrufen aber auch unzensierte Nacktbilder/-videos)

3. Spam

Instagram / Facebook blockiert Handlungen eines Kontos, wenn diese **zu oft** innerhalb eines bestimmten Zeitraums erfolgen. Hierzu können folgende Handlungen zählen:

- das Posten von Beiträgen
- das Verschicken von Direktnachrichten
- das Liken und Kommentieren von Beiträgen
- das Folgen und kurz darauf Entfolgen anderer Accounts, um die Zahl der Abonnierenden zu steigern
- der überschwängliche Gebrauch von Automatisierung für Posts und Kommentare

Auch gekaufte Follower führen zu einer Sperre Ihres Accounts.

Das Mittelstand-Digital Zentrum Handel gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

Infoblatt: Social Media: Hacks und Sperrungen vorbeugen – 11/2023
Mittelstand-Digital Zentrum Handel
ibi research an der Universität Regensburg GmbH
Galgenbergstraße 25
93053 Regensburg

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages