Social Media: Was tun bei Hacks und Sperrungen?

INFO BLATT

Sowohl das Hacking als auch die Sperrung des unternehmenseigenen Social-Media-Accounts sind ärgerliche Szenarien, die jederzeit auftreten können. Was Sie genau in solch einem Fall tun sollten und was Sie beachten müssen, ist in diesem Infoblatt dargestellt. Auch zur Vorbeugung von Sperrungen und Hacks bieten wir Ihnen Hilfestellungen in dem Leitfaden "Social Media: Hacks und Sperrungen vorbeugen":
https://digitalzentrumhandel.de/infoblatt-social-media-hacks-und-sperrungen-vorbeugen

HACKING

Das Hacking von Social-Media Unternehmensaccounts ist eine Problematik, die in den letzten Jahren zunehmend an Bedeutung gewonnen hat. Angreifer:innen können auf diese Weise Zugang zu sensiblen Informationen wie Kundendaten, Passwörtern und persönlichen Informationen erhalten. Häufig führt dies zu schwerwiegenden Konsequenzen für das betroffene Unternehmen, darunter finanzielle Verluste, Rufschädigung und Vertrauensverlust bei Kund:innen und Geschäftspartner:innen. Im Folgenden wird dargelegt, wie Sie herausfinden ob Sie gehackt wurden und was Sie im Ernstfall zu tun haben.

Mittelstand-Digital

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

WIE KANN ICH HERAUSFINDEN, OB MEIN KONTO GEHACKT WURDE?

Falls mindestens einer der folgenden Punkte auf Ihre Situation zutrifft, wurden Sie vermutlich gehackt:

- Ihr Account verschickt Nachrichten oder postet Beiträge bzw. Kommentare, von denen Sie nichts wissen
- Ihre E-Mail-Adresse oder das Passwort wurden ohne Ihr Wissen geändert. Meist erhalten Sie hierbei eine E-Mail von der Social-Media-Plattform, die Sie darauf hinweist
- Ihr Account hat Freundschaftsanfragen an Personen versendet, die Sie nicht kennen
- Ihr Name oder Ihr Geburtsdatum wurden geändert
- Zahlungen von Ihrem Facebook-Account wurden getätigt, von denen Sie nichts wissen.

Sie haben noch Zugriff auf Ihr Konto:

1. Passwort ändern

Stellen Sie fest, dass sich jemand Zugang zu Ihrem Konto verschafft hat, sollten Sie zunächst das Passwort ändern, um weiteren Schaden zu vermeiden.

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

Vorgehen Facebook: „Einstellungen und Privatsphäre“ → „Einstellungen“ → „Sicherheit und Login“ → „Passwort ändern” → „Bearbeiten“:

Hier geben Sie nun **Ihr altes und zweimal Ihr neues Passwort** ein. Bestätigen Sie das neue Passwort, indem Sie oben rechts auf das nun blau erscheinende Wort **„Speichern“ bzw. „Änderungen speichern“** klicken. Beachten Sie, dass Sie ein **sicheres Passwort** wählen, welches sich **grundlegend** vom alten Passwort **unterscheidet**.
Das Passwort wurde nun erfolgreich geändert. Anschließend werden Sie **automatisch auf allen Geräten** ausgeloggt. Sie müssen sich auf allen von Ihnen genutzten Geräten mit dem neuen Passwort wieder anmelden.

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

2. Prüfen Sie, ob eine zusätzliche fremde E-Mail-Adresse mit dem Account verknüpft ist.

Vorgehen Facebook:

„Einstellungen und Privatsphäre“ → „Einstellungen“ → „Allgemein“ → „Bearbeiten“:

Vorgehen Instagram:

„Einstellungen und Privatsphäre“ → „Kontenübersicht“ → „Persönliche Informationen”

Falls hier eine Ihnen nicht bekannte E-Mail-Adresse oder Telefonnummer aufgeführt ist, löschen Sie diese umgehend.

3. Prüfen Sie, was die Hacker:innen mit dem Account unternommen hat (Likes, Freundschaftsanfragen, …).

Löschen Sie die Vorgänge umgehend.

Vorgehen Facebook:

„Einstellungen und Privatsphäre“ → „Aktivitätenprotokoll“

Vorgehen Instagram:

Drei-Strich-Menü → „Deine Aktivität“

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

Sie haben keinen Zugriff mehr auf das Konto:

Option 1:

Bei einer Passwortänderung erhalten Sie eine E-Mail von Instagram / Facebook, in der Sie gefragt, ob Sie diese Änderung vorgenommen haben. Dort klicken Sie auf den entsprechenden Text, der besagt, dass Sie das nicht waren. Folgen Sie anschließend den dort aufgezeigten Schritten.

Option 2:

Hat der:die Hacker:in bereits die hinterlegte E-Mail-Adresse in Ihrem Account geändert, so erhalten Sie auch hier eine E-Mail von Instagram / Facebook mit dem Hinweis. In dieser E-Mail klicken Sie auf „secure your account here“. Sie werden zu Instagram / Facebook weitergeleitet und müssen Ihre Identität bestätigen. Anschließend erhalten Sie einen Sicherheitscode, mit dem Sie Ihre E-Mail-Adresse zurücksetzen können.

Option 3:

Sollten Sie keine E-Mail erhalten haben und trotzdem keinen Zugriff auf Ihr jeweiliges Konto haben, so ist nun das Vorgehen zwischen Instagram und Facebook zu unterscheiden.

Vorgehen Instagram:
Öffnen Sie die Instagram-App. Vermutlich sehen Sie nur noch den Anmeldebildschirm.
Gehen Sie wie folgt vor:
„Passwort vergessen?“ → Geben Sie den Instagram-Benutzernamen ein → „Benötigst du weitere Hilfe?“:
Hier öffnet sich nun ein Fenster, in dem Sie sich einen Anmeldelink zusenden lassen können. Dies können Sie durchführen, falls das Konto noch mit ihrer E-Mail-Adresse verknüpft ist oder Sie eine Handynummer hinterlegt haben. Sollte dies nicht der Fall sein, tippen Sie unten auf „Ich habe keinen Zugriff auf diese E-Mail-Adresse bzw. Telefonnummer“.

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

Sie werden zur Support-Anfrage an Instagram weitergeleitet. Hier geben Sie den Grund **"gehackter Account"** sowie eine E-Mail-Adresse an, auf die Sie Zugriff haben. An diese E-Mail-Adresse erhalten Sie von Instagram anschließend weitere Anweisungen, um Ihre Identität zu bestätigen. Somit erhalten Sie wieder Zugriff auf Ihr Konto.

Sollte diese Vorgehensweise nicht funktionieren, so nutzen Sie die Webseite https://www.instagram.com/hacked um Instagram über Ihr gehacktes Konto zu benachrichtigen.

Vorgehen Facebook:
Sollten Sie keine E-Mail erhalten haben und trotzdem keinen Zugriff auf Ihr Facebook-Konto mehr haben, öffnen Sie die Website https://www.facebook.com/hacked. Hier können Sie sich mit Ihrem alten Passwort anmelden. Wählen Sie „Jemand anderes hat sich ohne meine Erlaubnis bei meinem Konto angemeldet“ und folgen Sie den Anweisungen.

Was ist als Nächstes zu tun?

Sobald Sie wieder Zugang zu Ihrem Instagram- bzw. Facebook-Account erlangt haben, löschen Sie alle Vorgänge, die die Betrüger mit ihrem Account unternommen hat. Wie dies funktioniert, wird oben bereits erklärt (3. Prüfen Sie, was die Hacker:innen mit dem Account unternommen haben).

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

Wichtiger Hinweis für Facebook-Unternehmenskonten:

Sobald ein:e Betrüger:in sich den Zugang zu einem privaten Profil verschafft, hat er:sie Zugriff auf die verknüpften Unternehmensseiten und den Business Manager. Wurde der Admin einer Unternehmensseite bei Facebook gehackt, so melden Sie dies sofort unter der Website: https://www.facebook.com/hacked.

Sobald Sie wieder auf Ihr privates Konto zugreifen können, besuchen Sie den Facebook Hilfebereich. Dort finden Sie eine Auflistung aller Facebook-Seiten, auf die Ihr Konto vor dem Angriff Zugriff hatte. Wählen Sie das Unternehmensprofil aus und klicken Sie auf „Senden“. Facebook überprüft, ob das Konto gehackt wurde und wird sich mit einer E-Mail an den entsprechenden Admin Account melden. Die Überprüfung kann jedoch einige Tage oder Wochen dauern.

Sollten Sie die Unternehmens-Facebook-Seite nicht im Dropdown Menü auffinden, so haben die Hacker das Profil des vorherigen Admins in seiner Funktion heruntergestuft. Falls dies der Fall ist, sollten Sie eine Facebook Business Partner Agentur kontaktieren.

Sobald Sie wieder Zugang zu Ihrem Unternehmenskonto haben, überprüfen Sie, ob neue Zugriffsrechte an eine oder mehrere unbekannte Personen vergeben wurden. Entfernen Sie diese Zugriffsrechte.

Weitere Punkte:

► Warnen Sie Ihre Social-Media-Kontakte, dass Ihr Account gehackt wurde. Hacker:innen könnten versuchen noch mehr Nutzerdaten abzugreifen, indem Sie mit Ihrem Account private Nachrichten an Ihre Kontakte senden.

► Eine Strafanzeige gegen den:die Täter:in ist bei der Polizei möglich. Bringen Sie bitte hierfür aussagekräftige Screenshots mit.

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

Sperrung

Die Sperrung von Social-Media Unternehmensaccounts kann verschiedenste negative Konsequenzen haben. So kann eine Sperrung dazu führen, dass Unternehmen den Zugang zu ihren Follower:innen und Kund:innen verlieren, was wiederum einen Verlust von Umsatz und Rufschädigung bedeuten kann. Was Sie konkret im Falle einer Sperrung zu tun haben, können Sie dem folgenden Abschnitt entnehmen.

WIE LÄSST SICH EINE SPERRE DES INSTAGRAM-FACEBOOK-ACCOUNTS AUFHEBEN?

Um ein unrechtmäßig gesperrtes Konto bei Instagram zu entsperren und wieder vollen Zugriff zu erhalten, können Sie **Einspruch einlegen**. Dafür gehen Sie wie folgt vor:

- Öffnen Sie Ihre Instagram-App auf dem Smartphone, Tablet oder PC.
- Geben Sie Ihren Nutzernamen und das Passwort ein.
- Das soziale Medium wird Sie direkt über das gesperrte Konto informieren. Klicken Sie auf »Mehr dazu« oder »Weiter« und anschließend auf »Einspruch einlegen«, um zum Formular für den Einspruch zu gelangen.
- Füllen Sie das Formular aus und senden Sie es dem Support-Team zu.

Mittelstand-Digital

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

Entsperren eines vorübergehend gesperrten Instagram-/Facebook-Kontos:

Ist das Konto vorübergehend gesperrt, haben Sie neben dem Einspruch noch weitere Möglichkeiten:

- Um auszuschließen, dass die Sperre an Ihrer IP-Adresse liegt, rufen Sie die App in den mobilen Daten auf
- Melden Sie sich über ein Gerät in Ihrem Konto an, dass Sie üblicherweise nicht nutzen
- Erneute Installation der App auf dem Gerät
- Um zu beweisen, dass Sie kein Bot sind, verknüpfen Sie Ihr Konto mit dem Meta Business-Manager
- Verifizieren Sie Ihr Konto über Ihre Telefonnummer
- Warten Sie die temporäre Sperre von 24-48 Stunden ab. Anschließend haben Sie wieder Zugriff auf die Funktionen.

Entsperren eines dauerhaft gesperrten Instagram-/Facebook-Kontos:

Der Zugang zu einem dauerhaft gesperrten Konto ist i.d.R. nur über einen erfolgreichen Einspruch möglich. Sie müssen zügig handeln, da ein dauerhaft gesperrtes Konto üblicherweise nach 90 Tagen von Instagram gelöscht wird. Ein Reaktivieren ist dann nicht mehr möglich.

Wiederherstellen eines gelöschten Instagram-/Facebook-Accounts:

Das Wiederherstellen eines gelöschten Kontos ist **nicht möglich** – weder durch Sie noch durch Instagram oder Facebook. Hat sich eine Person unberechtigterweise Zugang zu Ihrem Account verschafft, beispielsweise durch Phishing (Abfangen persönlicher Daten), und das Konto gelöscht, sind alle Daten unwiderruflich weg.

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: Was tun bei Hacks und Sperrungen? – 12/2023
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