# ACCOUNT GEHACKT NOTFALLPLAN

## Phase 1 – Sofort handeln

Wenn dein Account gehackt wurde, ist schnelles und strukturiertes Handeln entscheidend. Dieses Dokument zeigt dir ein universelles Vorgehen, das für nahezu alle Plattformen funktioniert.

1. **Anderes Gerät verwenden**:

Nutze ein anderes Gerät (Smartphone, Tablet, anderer Computer), um die folgenden Schritte durchzuführen. Das Gerät auf dem der Angriff stattgefunden hat, könnte weiter infiziert sein.

2. **Aktive Sitzungen beenden**:

Beende alle aktiven Sitzungen des betroffenen Accounts. Dies verhindert, dass der Angreifer weiterhin Zugriff hat.

Die meisten Plattformen bieten eine Option, alle Sitzungen unter 'Sicherheit' oder 'Privatsphäre' zu beenden.

3. **Passwort des betroffenen Accounts ändern**:

Wähle ein starkes, einzigartiges Passwort. Mindestens 12 Zeichen, bestehend aus Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen. Je länger, desto besser → gerne auch 30 Zeichen ;)

Verwende kein Passwort mehrfach.

4. **Zwei-Faktor-Authentifizierung aktivieren**:

Aktiviere, wenn möglich, die Zwei-Faktor-Authentifizierung (2FA) für alle wichtigen Accounts.

**WICHTIG:** Solltest du dich hier nicht mehr anmelden können, etwa weil ein Angreifer dein Passwort bereits geändert hat, kontaktiere umgehend den zuständigen Kundenservice und informiere deine Kontakte, um weiteren Schaden zu verhindern.

## Phase 2 – Ausbreitung verhindern

1. **Passwörter bei ähnlichen Accounts ändern**:

Wenn du das gleiche Passwort für andere Accounts verwendet hast, ändere diese Passwörter sofort.

Angreifer werden direkt versuchen, dein Passwort für andere Dienste zu probieren.

2. **Verknüpfte Logins prüfen (Google, Facebook etc.)**:

Überprüfe, welche Anwendungen und Dienste Zugriff auf deinen Account haben (z.B. über Google oder Facebook Login).

Entferne unbekannte oder verdächtige Verknüpfungen.

## Phase 3 – Schaden prüfen

1. **Bankkonto und Zahlungsdienste prüfen**:

Überprüfe deine Bankkonten, Kreditkarten und Zahlungsdienste (z.B. PayPal) auf unautorisierte Transaktionen.

Falls vorhanden, direkt Kontakt mit den Ansprechpartnern aufnehmen und den Fall schildern.

2. **Bestellungen kontrollieren**:

Überprüfe deine Bestellhistorie auf verdächtige Bestellungen.

Falls vorhanden: Stornieren und Kundenservice kontaktieren.

3. **E-Mails auf ungewöhnliche Aktivitäten prüfen**:

Durchsuche deine E-Mails (Gesendet, Papierkorb) nach verdächtigen Aktivitäten, wie z.B. Phishing-Versuche an Freunde/Familie oder Passwort-Zurücksetzungen.

Informiere betroffene entsprechend.

## Phase 4 – Kontrolle zurückgewinnen

1. **Login-Verlauf prüfen**:

Überprüfe den Login-Verlauf deines Accounts (falls verfügbar).

Dieser zeigt, von welchen Geräten und Standorten aus auf den Account zugegriffen wurde.

2. **Unbekannte Geräte entfernen**:

Entferne alle unbekannten oder verdächtigen Geräte aus der Liste der verbundenen Geräte.

3. **Wiederherstellungsoptionen prüfen**:

Stelle sicher, dass deine Wiederherstellungsoptionen (E-Mail, Telefonnummer) aktuell sind und nicht verändert wurden.

Dies erleichtert die Wiederherstellung des Accounts in Zukunft.

## Phase 5 – Ursache verstehen

Versuche zu verstehen, wie der Zugriff auf deinen Account erfolgen konnte:

1. **Phishing-Mail erkannt?** Hast du auf einen Link in einer verdächtigen E-Mail geklickt und deine Anmeldedaten eingegeben?
2. **Passwort mehrfach verwendet?** Hast du das gleiche Passwort für mehrere Accounts verwendet?
3. **Datenleck möglich?** War dein Passwort Teil eines bekannten Datenlecks? Überprüfe dies zum Beispiel beim Hasso-Plattner-Institut: https://sec.hpi.de/ilc oder den Leak Checker der Uni Bonn: https://leakchecker.uni-bonn.de/de/index

## Wichtige Accounts

Das hier sind deine wichtigsten Accounts:

1. **E-Mail**

Dient als Schlüssel zu fast allen anderen Accounts, da hierüber Passwörter zurückgesetzt und wichtige Informationen empfangen werden.

2. **Banking & Zahlungsdienste**

Liefern direkten Zugriff auf dein Geld.

3. **Cloud Dienste**

Halten häufig wichtige persönliche Dokumente und Daten.

4. **Shopping**

Missbrauch kann zu finanziellem Schaden führen.

5. **Social Media**

Enthalten private Kommunikation und persönliche Inhalte, die deine Identität und dein soziales Umfeld betreffen

## Hilfeseiten der bekannter Dienste*

- **Google (Gmail, Drive, etc.)**
  - https://support.google.com/accounts/answer/6294825?hl=de
- **Apple (iCloud, Apple ID)**
  - https://support.apple.com/de-de/102560
- **Microsoft (Outlook, OneDrive)**

    - https://support.microsoft.com/de-de/account-billing/so-stellen-sie-ein-gehacktes-oder-manipuliertes-microsoft-konto-wieder-her-24ca907d-bcdf-a44b-4656-47f0cd89c245
- **Facebook**
    - https://www.meta.com/de-de/help/policies/539039418231124/
- **Instagram**
    - https://www.instagram.com/hacked/
- **WhatsApp**
    - https://faq.whatsapp.com/1131652977717250/?locale=de_DE
- **TikTok**
    - https://support.tiktok.com/de/log-in-troubleshoot/log-in/my-account-has-been-hacked
- **X (Twitter)**
    - https://help.x.com/de/forms/account-access/regain-access/hacked-or-compromised
- **Amazon**
    - https://www.amazon.de/gp/help/customer/display.html?ref_=hp_bc_nav&nodeId=GRFTMVHP4HXMESSP
- **PayPal**
    - https://www.paypal.com/de/security/report-fraud
- **eBay**
    - https://www.ebay.de/help/account/protecting-account/hilfe-und-manahmen-bei-ebaykontodiebstahl?id=4196
- **Dropbox**
    - https://help.dropbox.com/de-de/security/account-hacked
- **N26**
    - https://support.n26.com/de-de/sicherheit/kontosicherheit/was-kann-ich-tun-wenn-mein-konto-gehackt-wurde
- **Sparkasse**
    - https://blog.sparkasse-allgaeu.de/artikel/online-banking-gehackt-was-sie-tun-sollten-und-wie-sie-sich-schuetzen
- **ING**
    - https://www.ing.de/hilfe/sicherheit/betrug/#kontoaktivitaeten
- **Commerzbank**
    - https://www.commerzbank.de/hilfe/sicherheit-onlinebanking/phishing/#phishing-link-geklickt-was-jetzt-zu-tun-ist

## Nächste Schritte

Wenn du diese Schritte erledigt hast, hast du die wichtigsten Maßnahmen ergriffen, um deine Accounts wieder zu sichern und zukünftige Angriffe zu erschweren.

# ITsicher.online

Colin Brown

kontakt@itsicher.online

https://itsicher.online