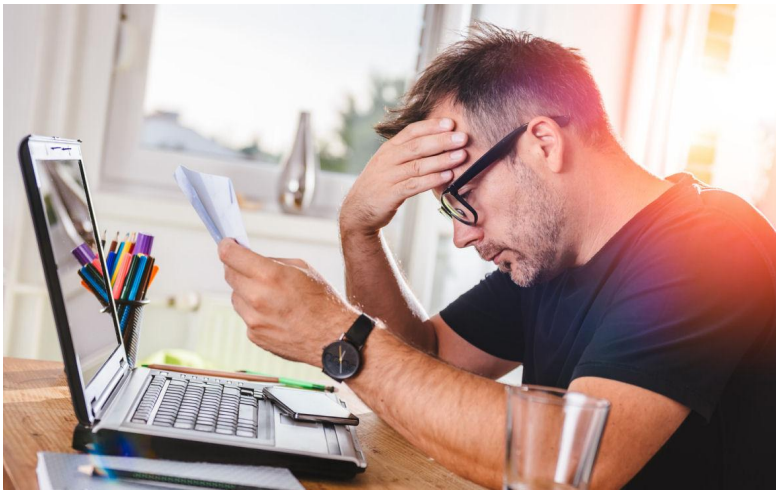
Verbraucherzentrale
Hamburg

Identität geklaut und Account gehackt? Das sollten Sie tun!

Seien Sie wachsam beim Umgang mit persönlichen Daten im Netz! Immer wieder kommt es zu Identitätsdiebstahl oder Identitätsmissbrauch, der hohe Rechnungen nach sich zieht. Bei gehackten Accounts ist schnelles Handeln gefragt. So gehen Sie vor. Mit Notfall-Check für die Suche nach den richtigen Kontaktdaten von Unternehmen.



DAS WICHTIGSTE IN KÜRZE

1. Betrüger nutzen persönliche Daten, um im Netz einzukaufen und Verträge auf Kosten ihrer Opfer zu schließen.

2. Wurde ein Account gehackt, ist schnelles Handeln gefragt. Die Verbraucherzentrale unterstützt mit einem Tool bei der Suche nach den richtigen Kontaktdaten von Unternehmen (z.B. Telekommunikationsdienstleister, Social-Media-Plattformen, Online-Shops). Betroffene sollten diese umgehend informieren und Strafanzeige bei der Polizei erstatten.
3. Die Verbraucherzentrale rät zur besonderen Vorsicht im Internet. Dem Identitätsdiebstahl lässt sich mit verschiedenen Maßnahmen vorbeugen.

Stand: 26.09.2025

An die Verbraucherzentralen wenden sich immer wieder Ratsuchende, deren Online-Konto gehackt und Identität missbraucht wurde. Das bedeutet: Kriminelle bestellen unter Verwendung des Namens einer anderen Person und ihrer persönlichen Daten Waren oder Dienstleistungen. Die Betroffenen erhalten dann Rechnungen, Inkassoschreiben oder sogar Mahnbescheide. Mit jeder einzelnen Forderung muss man sich auseinandersetzen.

So erkennen Sie, ob Ihr Online-Konto gehackt wurde

Wir alle nutzen zahlreiche Online-Konten. Dazu gehören das E-Mail-Postfach, Social-Media-Accounts, Online-Konten bei verschiedenen Shops oder Marktplätzen wie Ebay oder Amazon und das Online-Banking. Hacker können jedes dieser Konten angreifen. Es gibt verschiedene Hinweise darauf, dass Ihr Online-Konto einem Hackerangriff zum Opfer gefallen ist:

- Ihr Anbieter hat Ihnen zum Beispiel per E-Mail mitgeteilt, dass sich jemand mit einem anderen Gerät bei Ihrem Konto angemeldet hat und Sie waren das nicht.
- Sie haben eine Mail erhalten, in der Sie über Änderungen der E-Mail-Adresse, mit der das Online-Konto verknüpft ist, oder des entsprechenden Passwortes informiert wurden.
- Sie kommen gar nicht mehr in Ihren Account.
- Ihre Daten, die Sie in Ihrem Online-Account angegeben haben, wurden geändert.

- Es gibt gelesene Nachrichten, die Sie nicht geöffnet haben.
- Nachrichten, Anfragen oder ähnliches versenden sich scheinbar wie von selbst an andere.
- Sie erhalten plötzlich gar keine Nachrichten mehr, obwohl eigentlich täglich neue Nachrichten in Ihrem Account eingehen müssten.
- Sie erhalten Bestellbestätigungen, obwohl Sie keine dazu passenden Bestellungen getätigt haben.
- Sie erhalten Mahnungen oder Inkassobriefe, die Sie nicht zuordnen können.
- Sie werden erpresst und sollen Geld bezahlen, um Ihr Online-Konto wiederherzustellen.

Das sollten Sie bei einem gehackten Konto bzw. Identitätsmissbrauch tun

Wenn Sie vermuten oder wissen, dass eines Ihrer **Online-Konten gehackt** wurde, ist schnelles Handeln erforderlich. Trotzdem sollten Sie Ruhe bewahren.

- Erhalten Sie beim Einloggen in Ihr Online-Konto eine Fehlermeldung, testen Sie, ob Sie sich über ein anderes Gerät anmelden können. Klappt das, versuchen Sie, das Passwort und/oder die E-Mail-Adresse, die mit dem entsprechenden Online-Account verknüpft ist, zu ändern. Außerdem: Bei nahezu jedem Online-Konto können Sie ein neues Passwort anfordern.
- Überprüfen Sie Ihre IT-Geräte (Smartphone, Tablet, PC) hinsichtlich installierter Schadsoftware. Führen Sie einen Scan mit einem seriösen Virenscanner durch, um herauszufinden, ob Schadsoftware auf Ihrem Endgerät installiert wurde.
- Handelt es sich um ein Online-Konto mit Bezahlfunktion, prüfen Sie die Bestell-Historie auf verdächtige Buchungen und informieren Sie den Shop-Betreibenden, damit Ihr Online-Konto zeitweise gesperrt wird. Das schützt Sie vor weiteren ungewollten Buchungen. Soweit möglich, stornieren Sie die Buchungen.

Haben Kriminelle **Geld von Ihrem Konto abbuchen lassen** oder selbst abgebucht, ist Schnelligkeit gefragt.

- Stellen Sie Strafanzeige bei der Polizei – das geht auch online.
- Melden Sie den gehackten Account bzw. den Identitätsmissbrauch der Schufa und anderen Auskunfteien. Die Information, dass Sie Opfer eines Identitätsbetrugs geworden sind, wird dann Unternehmen zur Verfügung gestellt, die im Falle von neuen Anträgen oder bestehenden Verträgen Daten über Sie abfragen.
- Reagieren Sie auf die Rechnungen, Zahlungsaufforderungen oder Inkassoschreiben, die Sie bekommen. Sie müssen den Vertragsschluss bestreiten. Um einen, wenn auch letztlich unberechtigten Schufa-Eintrag zu vermeiden, sollten Sie dem Vertragsschluss schriftlich per Einschreiben entgegentreten. Hierfür kann es nützlich sein, eine Kopie der Strafanzeige vorzulegen.
- Gegen einen Mahnbescheid müssen Sie innerhalb von zwei Wochen einen Widerspruch einlegen. So gehen Sie vor.

Checkliste für den Notfall erstellen

Ein gehackter Account kann großen Schaden anrichten. Unser **Notfall-Check** zeigt, wie Sie die Kontrolle über Ihr Konto zurückbekommen, wo Sie den Angriff melden sollten und welche Sofortmaßnahmen Sie schützen. Einfach Fragen beantworten und Felder ausfüllen – Checkliste herunterladen. Fertig.

Beachten Sie: In dem Tool werden persönliche Daten verarbeitet und gespeichert. Informationen dazu finden Sie in unseren Datenschutzhinweisen.

So können Sie einem Identitätsdiebstahl vorbeugen

Meist bleibt völlig unklar, wie die Täter an die digitalen Identitäten gelangen und in welchem Umfang diese genutzt oder weitergegeben werden. Bekannt ist, dass persönliche Daten mitunter über Smishing, Phishing oder Datenlecks in die Hände von Kriminellen gelangen. Klicken Sie nicht auf Links und Anhänge von unbekannten

Quellen – egal, ob in E-Mails, SMS oder auf Social Media. Wenn Sie öffentliches WLAN nutzen, seien Sie sich bewusst, dass die Verbindungen in der Regel nicht verschlüsselt sind. Jeder, der sich im gleichen Netzwerk befindet, könnte also an Ihre Daten gelangen.

Übermitteln Sie sensible Daten nicht per E-Mail. Verwenden Sie möglichst sichere Passwörter und für jedes Nutzerkonto ein eigenes. Seien Sie misstrauisch, wenn sensible Daten wie Passwörter, PINs, Bankverbindung oder Kreditkartennummern von Ihnen abgefragt werden. Verschlüsseln Sie Ihre Mails, wenn es möglich ist. Diese Vorsichtsmaßnahmen zahlen sich am Ende des Tages aus, denn von einem Identitätsklau werden Sie leider eine ganze Weile etwas haben. **Mehr erfahren:** Wie kann ich mich vor einem Identitätsdiebstahl schützen?

UNSER TIPP

Regelmäßig werden Online-Portale, Online-Shops oder die Server von Unternehmen gehackt. Die Daten, die bei solchen Datenlecks gesammelt werden, landen unter Umständen in Hacking Foren und damit in die falschen Hände. Wenn Sie wissen möchten, ob auch Ihre E-Mail-Adresse von solchen Leaks betroffen waren, können Sie das auf der Webseite Have I been pwned? oder beim Hasso-Plattner-Institut überprüfen.

Gefördert durch:

Bundesministerium
der Justiz und
für Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

https://www.vzhh.de/themen/telefon-internet/datenschutz/identitaet-geklaut-account-gehackt-das-sollten-sie-tun