

**AK
YOUNG**

FAQ

FREQUENTLY ASKED QUESTIONS

**16 HÄUFIG
GESTELLTE
FRAGEN**

FAKE-PROFILE & BESTELLBETRUG

**HILFE! KRIMINELLE VERWENDEN
MEINEN NAMEN!**

WIE??? VERBRECHEN UNTER MEINEM NAMEN SIND MÖGLICH?

JA. WENN KRIMINELLE AN DEINE INFORMATIONEN GELANGEN, KÖNNEN SIE DAMIT ZAHLREICHE VERBRECHEN BEGEHEN.

1

WELCHE VERBRECHEN?

-  Fake-Profil von dir erstellen
-  Andere täuschen, dadurch entsteht den Opfern ein Schaden und du wirst verdächtigt
-  Dich gegenüber anderen schlechtmachen
-  Dir mit dem Online-Stellen von privaten Daten drohen
-  Dich erpressen
-  In deinem Namen einkaufen, ohne zu zahlen

2

WIE KOMMEN KRIMINELLE AN DEINE PERSÖNLICHEN INFORMATIONEN?

Da gibt es viele Möglichkeiten: Sie können dich mit gefälschten Nachrichten, E-Mails oder Fake-Anrufen dazu bringen, persönliche Angaben zu machen. Oder sie installieren Schadsoftware, die deine Daten stiehlt.

Aber auch das Knacken deiner Konten ist möglich, wenn du ein unsicheres Passwort und keine Zwei-Faktoren-Authentifizierung hast.

Kaufst du auf Fake-Seiten ein, verfügen Betrüger ebenso über deinen Namen und deine Anschrift. Genauso, wenn sie Unternehmen hacken und Kundendaten stehlen. Hast du öffentliche Profile, können sie die auch einfach so kopieren und für Verbrechen nutzen.

3

WO KANNST DU ÜBERPRÜFEN, OB DEINE DATEN NOCH SICHER SIND?

 leakchecker.uni-bonn.de

 sec.hpi.de/ilc/search

 haveibeenpwned.com

Dazu musst du deine E-Mailadresse eingeben. Die Anbieter zeigen dir dann an, ob deine Daten gehackt worden sind. Ist das der Fall, sagen sie dir, was du tun kannst, um mögliche Schäden abzuwenden.



Unternehmen müssen dich informieren, wenn sie deine Daten an Kriminelle verloren haben. Nimm solche Benachrichtigungen ernst und ergreife Vorkehrungen, damit der Schaden nicht größer wird!

4

WAS KANNST DU TUN, WENN DEINE DATEN NICHT MEHR SICHER SIND?

Passwort

Ist dein Passwort bekannt geworden, ändere es – siehe Frage 8.

Zwei-Faktoren-Authentifizierung

Sichere deine Konten, Messenger-Dienste etc. mit der Zwei-Faktoren-Authentifizierung ab, damit dich Verbrecher nicht aus deinem Konto ausschließen können.

Fake-Profile

Informiere deine Freunde, dass sie auf keine Nachrichten reagieren sollen, melde Fake-Profile von dir und lass sie löschen – siehe Frage 7.

Erpresserische Nachrichten

Reagiere nicht darauf und zahle nichts. Am besten blockierst du das Verbrecherkonto, nachdem du zum Beweis der Erpressung Screenshots der Nachrichten gemacht hast.

Bankkonto und Kreditkarte

Ist dein Bankkonto oder deine Kreditkarte bekannt geworden, melde dich sofort bei deiner Bank und kläre, ob du deine Karte sperren sollst.

Telefonnummer

Ist deine Telefonnummer bekannt, blockiere unbekannte Anrufer bzw. Absender von Nachrichten.

Auskunfteien

Erkundige dich bei Auskunfteien, ob es dort Einträge gibt, die nicht von dir stammen – siehe Frage 14.

5

WAS IST IM INTERNET VON DIR ÖFFENTLICH?

Mach einfach eine Suche nach deinem Namen. Findest du Einträge von dir, die nicht von dir stammen, dann lass sie beim Website-Betreiber löschen. Dazu schreibst du am besten die im „Kontakt“, „Impressum“ oder „Über uns“ genannte E-Mailadresse oder den in der Datenschutzerklärung genannten Datenschutzbeauftragten an.



FÜR EINE AUTOMATISCHE BENACHRICHTIGUNG PER E-MAIL, OB ES NEUE INHALTE VON DIR GIBT, KANNST DU AUCH EINEN GOOGLE-ALERT EINRICHTEN:
[google.com/alerts](https://www.google.com/alerts)

FAKE-PROFILE

FAKE-PROFILE GIBT ES LEIDER AUF ALLEN SOCIAL MEDIA PLATFORMEN.

6

KANNST DU DICH VOR VERBRECHEN IN DEINEM NAMEN SCHÜTZEN?

Nur zum Teil: Du kannst deine Konten möglichst privat einstellen und löschen, sobald du sie nicht mehr brauchst. Geht das nicht über dein eigenes Benutzerkonto, schreibe dafür den Datenschutzbeauftragten des Anbieters an. Er kann dir bei der Löschung deiner Daten helfen.



AUF SAFERINTERNET.AT FINDEST DU LEITFÄDEN, DIE DIR ZEIGEN, WIE DU DEINE KONTEN PRIVAT EINSTELLEN KANNST!

7

WIE MELDEST DU FAKE-PROFILE?

TikTok

- 📺 Ruf das Fake-Profil auf
- 📺 Klicke oben rechts auf die 3 Punkte
- 📺 Melde das Profil



Instagram

- 📺 Ruf das Fake-Profil auf
- 📺 Klicke oben rechts auf die 3 Punkte
- 📺 Melden
- 📺 Konto melden und folge den weiteren Schritten



Snapchat

- 📺 Ruf das Fake-Profil auf
- 📺 Halte den Profil-Namen lange gedrückt
- 📺 Wähle Freundschaft verwalten aus
- 📺 Melde das Profil



8

WIE SICHERST DU DEINE KONTEN AB?



SICHERES PASSWORT UND TROTZDEM LEICHT ZU MERKEN?

SCHAU DIR DIESES VIDEO AN: www.youtube.com/watch?v=-iko8a8_fmU

- 🔒 Nutze die Zwei-Faktoren-Authentifizierung
- 🔒 Nenne eine funktionierende Alternativ-Adresse bzw. Telefonnummer, mit der du wieder Zugriff auf dein Konto erlangst – solltest du dein Passwort einmal vergessen
- 🔒 Reagiere auf keine Nachricht – E-Mail, SMS, Messenger – die dich auffordert, auf einer fremden Website deine Kundendaten zu aktualisieren bzw. eine vermeintliche App zu installieren
- 🔒 Nutze nur laufend aktualisierte Software, Apps etc., damit Kriminelle nicht so einfach Zugriff auf deine Endgeräte und Konten erlangen können

9

WAS TUN BEI FAKE-PROFILIEN?



SOS Checkliste:

- 🔒 Reagiere auf keine Erpressungsversuche der Täter
- 🔒 Sichere alle Unterlagen sowie den Schriftverkehr zu deinem Fall
- 🔒 Nimm einen Personalausweis
- 🔒 Geh zur Polizei und erstatte Anzeige
- 🔒 Melde das Fake-Profil und lass es vom Anbieter löschen



BESTELLBETRUG – JEMAND KAUFTE UNTER DEINEM NAMEN EIN

WAS DU MACHEN KANNST, WENN DU NICHT BESTELLTE EINKÄUFE ZAHLEN SOLLST.

10

WURUM GEHT ES DA?

Wenn Kriminelle an deine Informationen gelangen, können sie damit Verbrechen begehen – z. B. in deinem Namen einkaufen, ohne zu zahlen. Das bekommst du erst mit, wenn du eine nicht bestellte Ware oder eine Rechnung erhältst. Aber auch Inkassobüros, die Polizei oder das Gericht können sich in so einem Fall bei dir melden.



Nimm das ernst und denke dir nicht, das interessiert mich nicht, weil ich ja eh nichts gemacht habe. Das kann nämlich zu großen Problemen führen!



SO REAGIERST DU BEI BESTELLBETRUG RICHTIG:

youtu.be/0tZZ4HsjoeA

11

DU HAST EINE RECHNUNG BEKOMMEN, OBWOHL DU NICHTS BESTELLT HAST?

In diesem Fall gehe zur Polizei und erstatte Anzeige. Nimm dabei alle Unterlagen mit, die du hast - auch deinen Personalausweis.

Nachdem du eine Bestätigung der Anzeige hast, schreib den Shop oder Zahlungsdienstleister an. Teile ihm mit, dass du nichts eingekauft hast und es sich um ein Verbrechen in deinem Namen handelt. Er soll deshalb die Rechnung oder Mahnung ausbuchen. Füge die Bestätigung der Anzeige hinzu. Das sollte ausreichend sein. Klar ist: Wenn du nichts bestellt hast, muss du dafür auch nichts zahlen.

12

WIE VERHINDERST DU, DASS DEIN NAME IMMER WIEDER VON VERBRECHERN GENUTZT WIRD?

Du hast eine Rechnung für einen Einkauf erhalten, den du nie gemacht hast? Nimm am besten mit dem Zahlungsdienstleister Kontakt auf und lass deine Daten für weitere Einkäufe sperren. Das wird im internen System vermerkt. Dann können Kriminelle nicht mehr unter deinem Namen einkaufen, weil das auch technisch nicht mehr möglich ist.

13

WAS IST, WENN DIR EIN INKASSOBÜRO SCHREIBT, DASS DU ZAHLEN SOLLST?

Auch in diesem Fall musst du unbedingt reagieren! Denn sonst kann es sein, dass die Rechnung als unbestritten an eine Auskunftfei gemeldet wird. Davon merkst du zunächst nichts, aber: Wenn du in Zukunft einen Vertrag abschließen oder einen Kredit haben möchtest, kann dir das wegen einer nie bezahlten Rechnung verwehrt werden – obwohl du unschuldig bist!

14

WAS SIND AUSKUNFTFEIEN UND WAS HABEN SIE VON MIR GESPEICHERT?

Auskunftfeien sammeln Informationen über dich, wenn du Rechnungen nicht bezahlst, einen Kredit aufnimmst, umzieht etc.

Damit wollen sie eine Aussage treffen können, ob du kreditwürdig bist. Du kannst bei ihnen eine sogenannte Artikel 15-Selbstauskunft beantragen. Damit erhältst du Informationen darüber, was sie alles über dich wissen. Findest du Einträge für unbezahlte Rechnungen, die nicht von dir stammen, kannst du sie löschen lassen.

15

DU SOLLST EINE AUSWEISKOPIE ZUR IDENTIFIZIERUNG SCHICKEN?

Eigentlich sollst du nie Ausweiskopien an Unbekannte senden, denn das stellt eine große Gefahr da. Manchmal aber verlangen das auch vertrauenswürdige Unternehmen, damit sie dir Auskunft über deine Daten geben können. In diesem Fall beachte:

-  Schwärze alle Informationen mit Ausnahme deines Namens und deines Geburtsdatums
-  Füge einen Text im Sinne von „Kopie für XX, Datum“ hinzu
-  Auch dein Ausweisfoto interessiert niemanden

Am besten ist es aber immer, wenn du dem Unternehmen Informationen nennst, die nur du kennen kannst, zum Beispiel deine Kundennummer, die Höhe und das Datum der letzten Rechnung etc. Damit zeigst du, dass du wirklich du bist und du Angaben machst, die nur du kennen kannst.

Du kannst Unternehmen aber auch eine mit der ID-Austria qualifiziert elektronisch signierte PDF-Datei mit deinen Daten senden. Das erfüllt den gleichen Zweck. Die ID-Austria holst du dir über die App Digitales Amt.



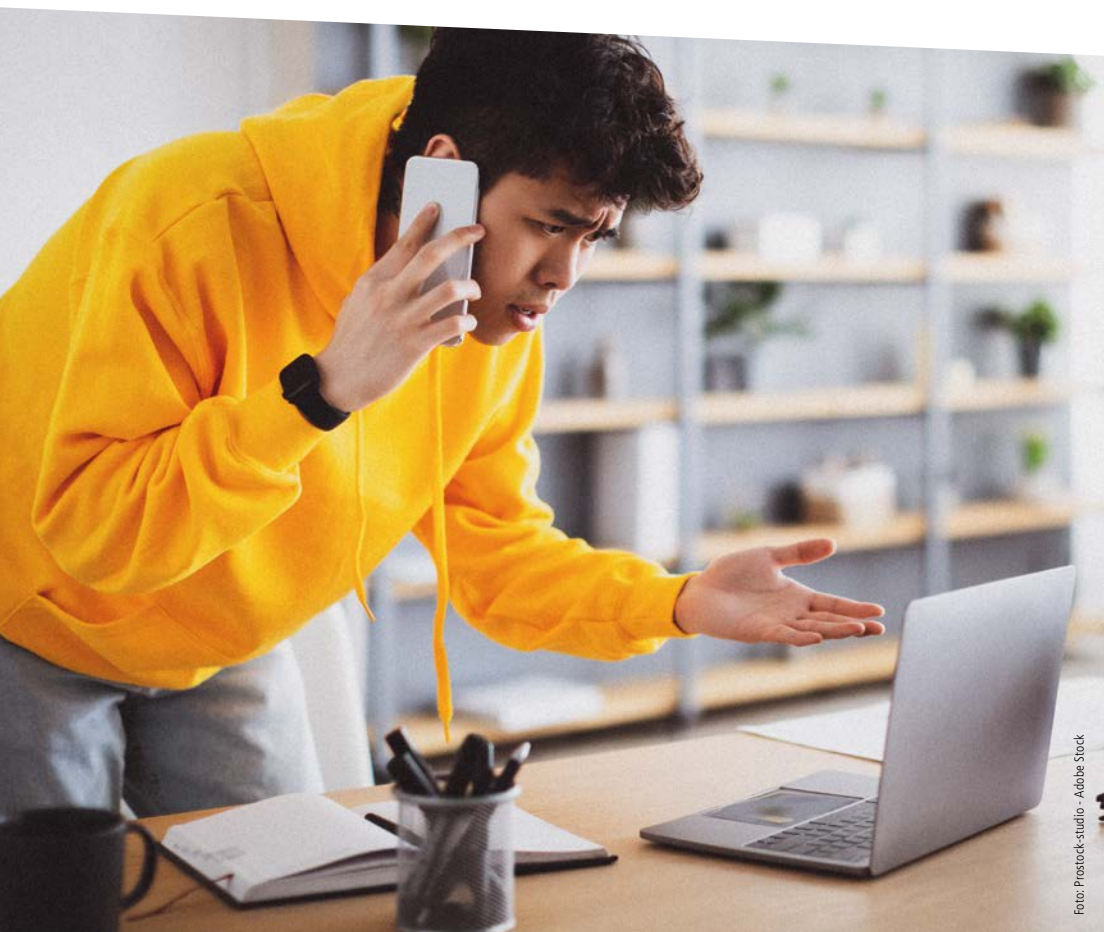
ÜBERPRÜFE IMMER: IST DAS UNTERNEHMEN BZW. DIE NACHRICHT WIRKLICH ECHT UND VERTRAUENSWÜRDIG!

WAS TUN, WENN DU OPFER EINES IDENTITÄTSMISSBRAUCHS BIST?



SOS Checkliste:

- ☑️ Sichere alle Rechnungen, Dokumente und den Schriftverkehr zu deinem Fall
- ☑️ Nimm einen Personalausweis
- ☑️ Geh zur Polizei und erstatte Anzeige
- ☑️ Schreib das Unternehmen an und sag, es soll die Rechnung stornieren - schick dazu die Anzeigen-Bestätigung mit
- ☑️ Lass deine Daten für weitere Einkäufe sperren
- ☑️ Überprüfe regelmäßig dein Bankkonto, damit du verdächtige Abbuchungen entdecken und diese zurückfordern kannst
- ☑️ Reagiere immer auf weitere Rechnungen, sonst kann das zu einer Menge Probleme führen – siehe Frage 12





Artikelnummer 584

SO NÜTZT DU DEIN SMARTPHONE SICHER

➤ Einfache Tipps und Tricks,
wie du dein Smartphone absichern kannst:



Artikelnummer 582

SO SCHÜTZT DU DICH IM NETZ

➤ Wenn du auf ein paar Dinge achtest,
gibst du Betrügerinnen und Betrugern
keine Chance:



DU HAST NOCH FRAGEN?

WIR HELFEN DIR GERNE WEITER!

AK Wien

1040 Wien, Prinz-Eugen-Straße 20-22

Tel.: +43 1 501 65-0

wien.arbeiterkammer.at

akyoung.at



DU HAST FRAGEN ZUM KONSUMENTENSCHUTZ?

Alle AK YOUNG Folder kannst du kostenlos downloaden:

wien.arbeiterkammer.at/akyoung-ratgeber

Weitere Bestellmöglichkeiten:

- E-Mail: mitgliederservice@akwien.at
- Bestelltelefon: +43 1 50165-1401

FAKE-PROFILE & BESTELLBETRUG Artikelnummer **329**

WICHTIG

Wir erarbeiten alle Inhalte der AK YOUNG Folder sehr sorgfältig. Dennoch können wir nicht garantieren, dass alles vollständig und aktuell ist bzw. sich seit dem Druck keine Gesetzesänderung ergeben hat. Achte bitte deshalb auf das Erscheinungsdatum dieser Ausgabe. Die AK YOUNG Folder dienen dir als Erstinformation. Sie enthalten die häufigsten Fragen, viele anschauliche Beispiele, Hinweise auf Stolpersteine und einen Überblick über die wichtigsten gesetzlichen Regelungen. Bei individuellen Fragen steht dir unsere Hotline zur Verfügung: +43 1 501 65-0

Impressum – Medieninhaber: Kammer für Arbeiter und Angestellte für Wien, Prinz-Eugen-Straße 20–22, 1040 Wien | Telefon: (01) 501 65 0; Offenlegung gem. § 25 MedienG: siehe wien.arbeiterkammer.at/impressum
Titelfoto: © bodnarphoto – Adobe Stock, weitere Abbildungen siehe Credit beim Foto
Grafik: www.christophluger.com | Druck: Gugler GmbH, 3390 Melk

Stand: November 2023