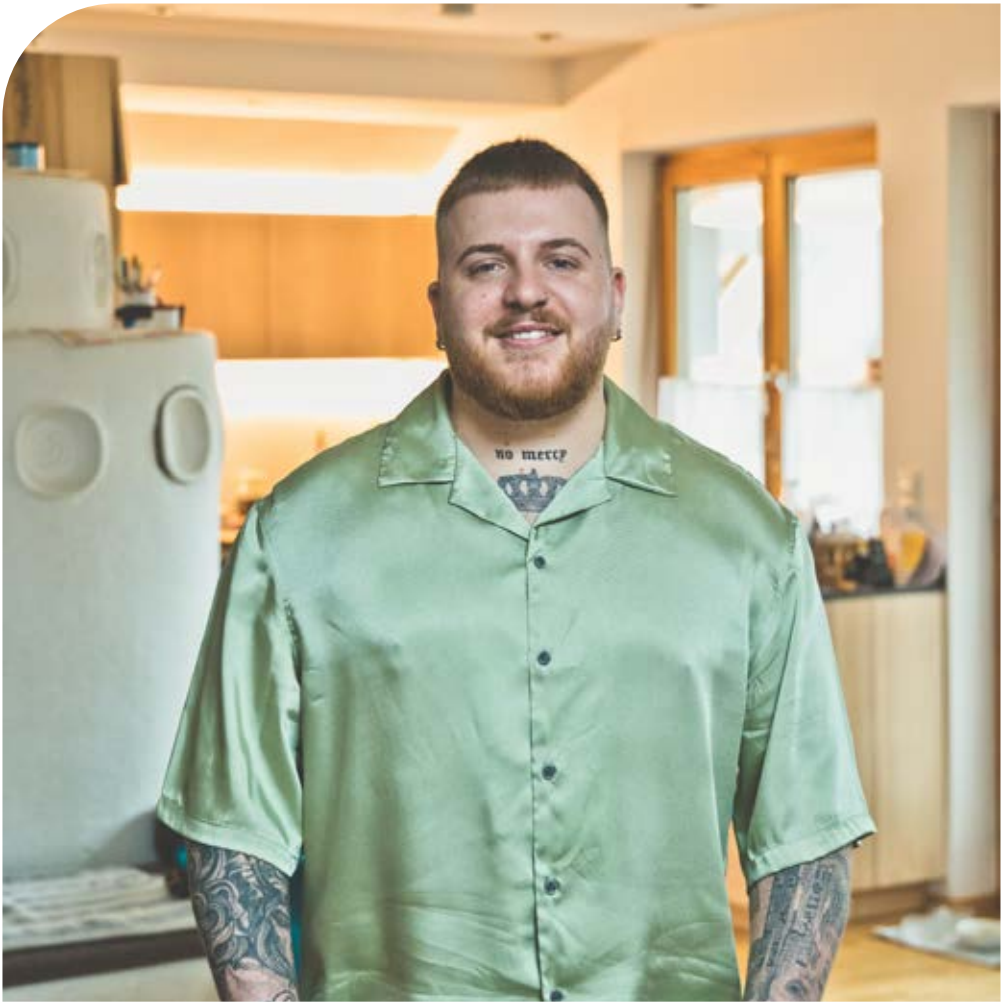

Tatort Internet

Fake-Profile, Bestellbetrug & Co:
Verbrechen unter fremdem Namen

AK VORARLBERG

⋆ **Mathias**
AK Mitglied seit: 2012

Sie finden unsere
Broschüren auch online
ak-vorarlberg.at

TATORT INTERNET

FAKE-PROFILE, BESTELLBETRUG & CO: VERBRECHEN UNTER FREMDEM NAMEN

Verbrechen unter falschem Namen sind keine Seltenheit. Deshalb: Schützen Sie Ihre Daten! Wie das geht und was Sie tun können, wenn Ihr Namen für Verbrechen missbraucht wird, erfahren Sie in diesem Ratgeber.

Muss man alle Probleme immer alleine lösen? Muss man nicht.

Nutze unser
kostenloses
Serviceangebot.
ak-vorarlberg.at

AK VORARLBERG

21 Fragen und Antworten zu Datenklau, Identitätsmissbrauch und Bestellbetrug

Fremde Identitäten sind für Kriminelle ein begehrtes Gut.
Denn so können sie unter falschem Namen Straftaten begehen und bleiben selbst unentdeckt.

1

Verbrechen unter fremdem Namen:

Welche Verbrechen sind möglich?

Wenn Kriminelle an Ihre Daten gelangen, können Sie damit zahlreiche Verbrechen begehen, zum Beispiel:

- Fake-Profile von Ihnen erstellen
- Andere täuschen, wodurch Opfern ein Schaden entsteht und Sie verdächtigt werden
- Den Ruf Ihrer Person schädigen
- Sie erpressen – z. B. mit der Androhung, Ihre privaten Daten zu veröffentlichen
- In Ihrem Namen einkaufen, ohne zu zahlen

2

Verbrechen unter fremdem Namen:

Wie kommen Kriminelle an Ihre Daten?

Da gibt es viele Möglichkeiten: Sie bringen Sie mit gefälschten Nachrichten, E-Mails oder Fake-Anrufen dazu, persönliche Angaben zu machen. Oder Sie installieren als Reaktion auf eine gefälschte Aufforderung Schadsoftware, die Ihre Daten stiehlt. Kaufen Sie auf Fake-Seiten ein, verfügen Betrüger ebenso über Ihre Daten. Haben Sie öffentliche Profile, können Kriminelle diese auch einfach so kopieren und für Verbrechen nutzen. Ebenso ist ein Datenabfluss bei Unternehmen denkbar.

Aber auch das Knacken Ihrer Konten ist möglich, wenn Sie ein unsicheres Passwort haben und keine Zwei-Faktor-Authentifizierung nutzen.

3

Verbrechen unter fremdem Namen:

Wo können Sie überprüfen, ob Ihre Daten noch sicher sind?

- leakchecker.uni-bonn.de
- sec.hpi.de/ilc/search
- haveibeenpwned.com

Dazu müssen Sie Ihre E-Mailadresse eingeben. Danach erhalten Sie Auskunft, ob Ihre Daten gehackt worden sind und was Sie in diesem Fall tun können, um mögliche Schäden abzuwenden.

Unternehmen müssen Sie informieren, wenn sie Ihre Daten an Kriminelle verloren haben. Nehmen Sie solche Benachrichtigungen ernst und ergreifen Sie Vorkehrungen, damit der Schaden nicht größer wird!

4

Verbrechen unter fremdem Namen:

Was können Sie tun, wenn Ihre Daten nicht mehr sicher sind?

Passwort
Ist Ihr Passwort bekannt geworden, ändern Sie es – siehe Frage 9

Zwei-Faktor-Authentifizierung
Sichern Sie Ihre Konten, Messenger-Dienste etc. mit der Zwei-Faktor-Authentifizierung ab – siehe Frage 11

Fake-Profile
Informieren Sie Ihre Freunde, dass sie auf keine Nachrichten reagieren sollen. Melden Sie Fake-Profile von Ihnen und lassen Sie diese löschen – siehe Frage 13

Erpresserische Nachrichten
Reagieren Sie nicht darauf und zahlen Sie nichts. Am besten blockieren Sie das Verbrecherkonto – nachdem Sie zum Beweis der Erpressung Screenshots der Nachrichten gemacht haben - und erstatten Anzeige.

Bankkonto und Kreditkarte
Ist Ihr Bankkonto oder Ihre Kreditkarte bekannt geworden, melden Sie sich sofort bei Ihrer Bank und klären Sie ab, ob Sie Ihre Karte sperren lassen sollen.

Telefonnummer
Ist Ihre Telefonnummer öffentlich, blockieren Sie unbekannte Anrufer bzw. Absender von Nachrichten. Installieren Sie keine Apps aus unbekannten Quellen, auch wenn das in Nachrichten an Sie gefordert wird.

Auskunfteien
Erkundigen Sie sich bei Auskunfteien, ob es dort Einträge gibt, die nicht von Ihnen stammen, also nicht auf Sie zurückzuführen sind – siehe Frage 19.

In Österreich wichtige Auskunfteien:
- KSV1870 Information GmbH: ksv.at
- CRIF GmbH: crif.at

5

Verbrechen unter fremdem Namen:

Was ist im Internet von Ihnen öffentlich?

Um das zu überprüfen, machen Sie einfach eine Suche nach Ihrem Namen. Sie finden Einträge, die nicht von Ihnen stammen? Lassen Sie diese beim Website-Betreiber löschen. Dazu schreiben Sie am besten die im „Kontakt“, „Impressum“ oder „Über uns“ genannte E-Mailadresse oder den in der Datenschutzerklärung angeführten Datenschutzbeauftragten an.

TIPP

Für eine automatische Benachrichtigung per E-Mail, ob es neue Inhalte von Ihnen gibt, können Sie auch einen Google-Alert einrichten: google.com/alerts

6

Schützen Sie Ihre Daten:

Was gilt grundsätzlich?

!

Die wichtigste Regel
Veröffentlichen Sie so wenig Daten wie möglich! Adresse, Telefonnummer, Passwörter etc. gehen Fremde nichts an. Seien Sie besonders sparsam mit diesen Informationen, wenn Sie sich auf Websites, für Gewinnspiele und dergleichen registrieren. Löschen Sie auch Ihre Konten, wenn Sie diese nicht mehr brauchen.

TIPP

Wann immer es möglich ist:
Verwenden Sie anonyme Nicknames anstelle Ihres richtigen Namens.

7

Schützen Sie Ihre Daten:

Machen mehrere E-Mail-Adressen Sinn?

Ja. Eine E-Mail-Adresse für wichtige Zwecke und eine andere für unwichtige Dinge. Legen Sie sich dafür bei einem Gratis-Anbieter eine zusätzliche E-Mail-Adresse an, die keine Rückschlüsse auf Ihre Person zulässt und die problemlos gelöscht werden kann. Verwenden Sie diese Adresse, wenn Sie sich z. B. auf unwichtigen Websites registrieren, in Foren diskutieren oder an Gewinnspielen teilnehmen.

8

Schützen Sie Ihre Daten:

Können Sie Ihr Endgerät sicherer machen?

Ja. Achten Sie dafür auf die Datenschutz- und Sicherheitseinstellungen Ihres Geräts und treffen Sie Auswahlmöglichkeiten, die Ihre Nutzerdaten möglichst privat halten. Bei diesen Einstellungsmöglichkeiten können Ihnen Anleitungen aus dem Internet helfen. Das Gleiche gilt auch für Apps und Ihren Einstellungsmöglichkeiten.

Weitere wichtige Schutzmaßnahmen

- Führen Sie regelmäßig Updates Ihres Systems und Ihrer Apps durch
- Verwenden Sie ein Anti-Viren-Programm und eine Firewall
- Schützen Sie Ihr Endgerät durch eine Zugriffsperre
- Erstellen Sie regelmäßige Back-Ups Ihrer Daten, damit es zu keinem Datenverlust kommen kann
- Nutzen Sie keine offenen Internetverbindungen. Lässt sich das – z. B. im Ausland – nicht vermeiden, verwenden Sie einen sicheren VPN-Dienst

9

Schützen Sie Ihre Daten:

Wie sieht ein sicheres Passwort aus?

Grundsätzlich gilt: Hundertprozentigen Schutz gibt es nicht
Auch ein langes, kompliziertes Passwort kann geknackt oder durch einen Datenabfluss an Dritte öffentlich werden. Doch von Ihrer Seite aus können Sie es möglichen Angreifern schwerer machen, indem Sie Ihre Passwörter möglichst sicher gestalten:

- Je länger ein Passwort ist, desto besser ist es
- Verwenden Sie dafür keine leicht zu erratenden Informationen wie Ihr Geburtsdatum oder den Namen eines Familienmitgliedes
- Achten Sie darauf, dass Sie Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern gebrauchen
- Nutzen Sie für jedes Konto ein eigenes Passwort
- Gebrauchen Sie Passwort-Manager, damit Sie mit Ihren Passwörtern nicht durcheinander kommen

10

Schützen Sie Ihre Daten:

Welche Passwort-Strategien gibt es?

- **4-Wörter-Methode**
  Mit dieser Strategie können Sie ganz leicht lange, zufällige und dadurch komplexe Passwörter erstellen.
  Zum Beispiel: FahrradTopfenSieglindeMeeresgrund

- **Zeichen schlagen Wörter**
  Reichern Sie Ihr Passwort mit Sonderzeichen und Zahlen an.
  Zum Beispiel: Fahrrad&Topfen3Sieglinde%Meeresgrund9!

- **Minimum 12 Zeichen**
  Ihr Dienst hat gänzlich andere Vorgaben? Dann verwenden Sie ein Passwort mit mindestens 12 Zeichen. Variieren Sie Groß-und Kleinschreibung und kombinieren Sie Buchstaben, Zahlen und Sonderzeichen wie + = ? & $ % „ ( ) / * >< .

11

Schützen Sie Ihre Daten:

Was ist die Zwei-Faktor-Authentifizierung?

Das ist eine zusätzliche Sicherheits-Maßnahme zum Schutz von Benutzerkonten. Hier geben Sie zusätzlich zum Passwort beim Login z. B. einen Code ein, der bei jedem Anmeldevorgang für Sie neu erstellt und in einer App am Handy angezeigt wird.

Der Vorteil: Selbst, wenn Ihr Passwort in falsche Hände gelangt, haben Unbefugte keinen Zugriff auf Ihr Benutzerkonto.

TIPP Zahlreiche bekannte Anbieter, wie zum Beispiel Google, Amazon oder GMX, bieten diese Funktion an.
Nutzen Sie sie!

12

Fake-Profile:

Wo gibt es Fake-Profile?

Fake-Profile gibt es auf allen Social-Media-Plattformen. Können Sie sich davor schützen? Leider nur zum Teil: Sie können Ihre Konten möglichst privat einstellen und löschen, sobald Sie diese nicht mehr brauchen.

KON KRET Können Sie Ihr Konto nicht über Ihr eigenes Benutzerkonto löschen, schreiben Sie dafür den Datenschutzbeauftragten des Anbieters an.

TIPP Auf saferinternet.at/privatsphaere-leitfaeden/ finden Sie Anleitungen, wie Sie Ihre Konten privat einstellen können.

13

Fake-Profile:

Wie melden Sie Fake-Profile?

Facebook

- Rufen Sie das Fake-Profil auf
- Tippen Sie auf die 3 Punkte
- Wählen Sie „Support erhalten oder Profil melden“ aus
- Folgen Sie den Anweisungen

X

- Rufen Sie das Fake-Profil auf
- Tippen Sie auf das Mehr-Symbol
- Wählen Sie „Melden“ aus

- Folgen Sie den Anweisungen

Instagram

- Rufen Sie das Fake-Profil auf
- Klicken Sie oben rechts auf die 3 Punkte
- Wählen Sie „Melden“ aus
- Konto melden und den weiteren Schritten folgen

Snapchat

- Rufen Sie das Fake-Profil auf
- Halten Sie den Profil-Namen lange gedrückt
- Wählen Sie „Freundschaft verwalten“ aus
- Melden Sie das Profil

TikTok

- Rufen Sie das Fake-Profil auf
- Klicken Sie oben rechts auf die 3 Punkte
- Melden Sie das Profil

14

Fake-Profile:

Wie sichern Sie Ihre Konten ab?

- Verwenden Sie ein sicheres Passwort – siehe Frage 9
- Nutzen Sie die Zwei-Faktor-Authentifizierung – siehe Frage 11
- Nennen Sie eine funktionierende Alternativ-Adresse bzw. Telefonnummer, mit der Sie wieder Zugriff auf Ihr Konto erlangen können – sollten Sie Ihr Passwort einmal vergessen

- Reagieren Sie auf keine Nachricht – E-Mail, SMS, Messenger – die Sie auffordert, auf einer fremden Website Ihre Kundendaten zu aktualisieren bzw. eine App zu installieren

- Nutzen Sie nur aktuelle Software, Apps etc., damit Kriminelle nicht so einfach Zugriff auf Ihre Endgeräte oder Konten erlangen können

15

Fake-Profile:

Wie sieht die SOS Checkliste aus?

- Reagieren Sie auf keine Erpressungsversuche der Täter
- Sichern Sie alle Unterlagen sowie den Schriftverkehr zu Ihrem Fall
- Gehen Sie zur Polizei und erstatten Sie Anzeige
- Melden Sie das Fake-Profil und lassen Sie es vom Anbieter löschen

16

Bestellbetrug:

Worum geht es beim Bestellbetrug?

Kurz: Jemand kauft unter Ihrem Namen ein, ohne zu bezahlen.

Das bekommen Sie erst mit, wenn Sie auf einmal nicht bestellte Ware oder eine Rechnung erhalten. Aber auch Inkassobüros, die Polizei oder das Gericht können sich in so einem Fall bei Ihnen melden.

Nehmen Sie das ernst und denken Sie sich nicht:
Das interessiert mich nicht, weil ich ja eh nichts gemacht habe. Das kann nämlich zu großen Problemen führen!

TIPP Richtig reagieren bei Bestellbetrug: youtu.be/0tZZ4HsjoeA

17

Bestellbetrug:

Sie bekommen eine Rechnung, obwohl Sie nichts bestellt haben?

In diesem Fall: Gehen Sie zur Polizei und erstatten Sie Anzeige. Mit der Anzeigenbestätigung schreiben Sie den Shop oder Zahlungsdienstleister an – je nachdem, wer Ihnen die Rechnung sendet. Teilen Sie dem Unternehmen mit, dass Sie nichts gekauft haben und es sich um ein Verbrechen in Ihrem Namen handelt – die Anzeigenbestätigung fügen Sie als Nachweis dafür bei. Die Rechnung soll aus diesen Gründen ausgebucht werden.

Wiederholter Bestellbetrug
Wie verhindern Sie, dass Ihr Name wiederholt von Verbrechern genutzt wird? Nehmen Sie mit dem Händler oder Zahlungsdienstleister Kontakt auf und lassen Sie Ihre Daten für weitere Einkäufe sperren.

18

Bestellbetrug:

Was tun, wenn ein Inkassobüro schreibt?

Auch in diesem Fall müssen Sie unbedingt reagieren! Denn sonst kann es sein, dass die Rechnung als unbestritten an eine Auskunftei gemeldet wird. Davon merken Sie zunächst nichts, aber: Wenn Sie in Zukunft einen Vertrag abschließen oder einen Kredit haben möchten, kann Ihnen das wegen einer nie bezahlten Rechnung verwehrt werden – obwohl Sie unschuldig sind!

19

Bestellbetrug:

Was sind Auskunfteien und was haben sie von Ihnen gespeichert?

Auskunfteien sammeln Informationen über Sie, wenn Sie Rechnungen nicht bezahlen, einen Kredit aufnehmen, umziehen etc.

Damit wollen Auskunfteien eine Aussage treffen können, ob jemand kreditwürdig ist. Sie können bei ihnen kostenlos eine sogenannte Artikel 15-Selbstauskunft gemäß DSGVO beantragen. Damit erhalten Sie Informationen darüber, was alles über Sie bekannt ist. Finden Sie Einträge für unbezahlte Rechnungen, die nicht von Ihnen stammen bzw. auf Sie zurückzuführen sind, können Sie diese löschen lassen.

In Österreich wichtige Auskunfteien:

- KSV1870 Information GmbH: ksv.at
- CRIF GmbH: crif.at

20

Bestellbetrug:

Sie sollen eine Ausweiskopie zur Identifizierung schicken?

Grundsätzlich gilt: Nie Ausweiskopien an Dritte senden, denn das stellt eine große Gefahr dar. Manchmal aber verlangen das auch vertrauenswürdige Unternehmen, damit sie Auskunft über Daten geben können. In diesem Fall:

- Schwärzen Sie alle Informationen mit Ausnahme Ihres Namens und Geburtsdatums
- Fügen Sie auf dem Dokument einen Text im Sinne von „Kopie für XX, Datum“ hinzu
- Auch Ihr Ausweisfoto interessiert niemanden

Am besten ist es aber, wenn Sie dem Unternehmen Informationen nennen, die nur Sie kennen können: zum Beispiel Ihre Kundennummer, die Höhe und das Datum der letzten Rechnung etc. Damit beweisen Sie Ihre Identität. Sie können Unternehmen aber auch eine mit der ID-Austria (über die App Digitales Amt) qualifiziert elektronisch signierte PDF-Datei mit Ihren Daten senden. Das erfüllt den gleichen Zweck.

ACH TUNG Überprüfen Sie immer: Ist das Unternehmen bzw. die Nachricht wirklich echt und vertrauenswürdig!

21

Bestellbetrug:

Wie sieht die SOS Checkliste aus?

- Sichern Sie alle Rechnungen sowie den Schriftverkehr zu Ihrem Fall
- Gehen Sie zur Polizei und erstatten Sie Anzeige
- Schreiben Sie das Unternehmen an und lassen Sie die Rechnung stornieren – schicken Sie dazu die Anzeigenbestätigung mit
- Lassen Sie Ihre Daten für weitere Einkäufe sperren
- Überprüfen Sie regelmäßig Ihr Bankkonto, damit Sie verdächtige Abbuchungen entdecken und zurückfordern können
- Reagieren Sie auf jede Rechnung, sonst kann das zu einer Menge Probleme führen – siehe Frage 17

Ihre Ansprechpartner

Arbeiterkammer Vorarlberg
6800 Feldkirch
Widnau 4
T +43 (0)50 258-0
ak-vorarlberg.at

AK Vorarlberg – Konsumentenschutz

Telefonische Beratung:
T +43 (0)50 258-3000

Montag bis Donnerstag
8 – 12 Uhr und 13 – 16 Uhr

Freitag
8 – 12 Uhr

Persönliche Beratung nach vorheriger Terminvereinbarung:

konsumentenberatung@ak-vorarlberg.at
ak-vorarlberg.at

Notizen

Notizen

Wichtig
Selbstverständlich erarbeiten wir alle Inhalte unserer Ratgeber sorgfältig. Dennoch können wir nicht garantieren, dass alles vollständig und aktuell ist bzw. sich seit dem Druck keine Gesetzesänderung ergeben hat. Unsere Ratgeber dienen Ihnen als Erstinformation.

Bei individuellen Fragen stehen wir Ihnen gerne zur Verfügung
T +43 (0)50 258-0

Weitere Informationen finden Sie auch im Internet
ak-vorarlberg.at

Impressum
Herausgeber:
AK Vorarlberg
Widnau 4
6800 Feldkirch
Österreich
T +43 (0)50 258-0
kontakt@ak-vorarlberg.at
ak-vorarlberg.at

Druck:
Thurnher Druckerei GmbH,
6830 Rankweil

Stand:
Mai 2024

AK Vorarlberg
Widnau 4
6800 Feldkirch, Österreich
T +43 50 258 – 0
kontakt@ak-vorarlberg.at
ak-vorarlberg.at