
AK YOUNG
FAQ
FREQUENTLY ASKED QUESTIONS
22 HÄUFIG GESTELLTE FRAGEN
INTERNETBETRUG
SO SCHÜTZT DU DICH IM NETZ

VORSICHT ABZOCKE!

DAS INTERNET IST EIN GUTER BODEN FÜR BETRÜGERINNEN UND BETRÜGER. DAVON GIBT ES GANZ SCHÖN VIELE, ABER DIE MEISTEN SIND NICHT BESONDERS SCHLAU. WENN DU AUF DIE FOLGENDEN DINGE ACHTEST, GIBST DU IHNEN KEINE CHANCE!

1 WANN SOLLTEST DU SKEPTISCH SEIN?

Wenn ein Angebot extrem verlockend klingt, ist irgendetwas faul. Auch im Internet schenkt dir niemand was! Original Markenware zu einem Bruchteil des üblichen Preises gibt es nicht. Also: Finger weg von Superschnäppchen!

2 WO KÖNNEN DIR UNSERIÖSE ANGEBOTE BEGEGNEN?

- In Onlineshops
- In Werbeanzeigen
- In Sozialen Medien
- Auf Portalen für Kleinanzeigen
- In E-Mails

3 WAS KANN DIR DABEI PASSIEREN?

Natürlich wird in solchen Fällen meistens verlangt, dass du vorab bezahlst. Trotz bezahlter Geldüberweisung erhältst du aber keine Gegenleistung. Oder du bekommst zum Beispiel statt des gekauften hochwertigen Produkts eine billige Fälschung. Kriminelle können deine persönlichen Daten aber auch für Verbrechen nutzen.

4 WIE KANNST DU DICH DAVOR SCHÜTZEN?

Diese einfachen Tipps helfen dir, betrügerische Angebote zu entlarven:

- Informiere dich über das Unternehmen oder die Händlerin bzw. den Händler, bevor du etwas kaufst – findest du lauter schlechte oder keine Bewertungen, hol dir das Produkt lieber woanders
- Vergleiche die Preise immer auf mehreren Plattformen, wie zum Beispiel geizhals.at, idealo.at oder preisvergleich.at – sei skeptisch bei megagünstigen Angeboten
- Wenn möglich, bezahle die Ware nicht im Voraus
- Kaufst du etwas von Privat, bestehe auf eine persönliche Übergabe von Produkt und Geld
- Sende nie Ausweiskopien an Unternehmen oder Kontakte.

5 WELCHE GEFAHREN LAUERN AM HANDY?

Textnachrichten und Werbebanner am Smartphone versprechen dir oft das Blaue vom Himmel.

Die Klassiker:

- 250-Euro-Gutschein geschenkt
- Besseres WhatsApp möglich
- Paket zur Abholung bereit
- Hol dir dein Gratis-Game
- Orte jedes Handy

6 WIE FUNKTIONIEREN DIESE „DIENSTE“?

Klickst du auf solche Werbebanner oder Textnachrichten, musst du deine Handynummer angeben oder eine App aus unbekannten Quellen herunterladen. Damit schließt du entweder ungewollt ein Abo ab, für das du dann Monat für Monat zahlen musst. Du bekommst aber gar nichts dafür, weil es das versprochene Angebot oder den Dienst dazu nicht gibt! Oder aber du installierst Schadsoftware.

Die Kosten stehen nur ganz versteckt im Kleingedruckten

7 WIE WIRD ABGERECHNET?

Monatlich über deine Handyrechnung – als teurer Mehrwertdienst

8 GIBT ES VORSICHTSMASSNAHMEN?

Ja klar! Wenn du die folgenden Regeln beachtest, bist du relativ sicher:

- Gib deine Telefonnummer nur bei seriösen Anbietern bekannt
- Mach nicht bei Gewinnspielen mit
- Gehe nicht auf verlockende Angebote ein
- Beantworte keine SMS mit „Ja“, außer du willst ein Angebot wirklich annehmen
- Übermittle nie einen TAN-Code außerhalb des Online- bzw. Mobile-Bankings
- Lass deine Rufnummer für Mehrwertdienste, Mehrwert-SMS und Mehrwert-Content Downloads sperren – ganz einfach bei deinem Mobilfunkbetreiber
- Installiere keine Daten aus unbekannten Quellen – es könnte sich um Schadsoftware handeln

KONTROLLIERE DEINE HANDYRECHNUNG IMMER GANZ GENAU!

9 WAS TUN, WENN DOCH WAS PASSIERT IST?

Solltest du auf deiner Handyrechnung eine unbekannte Abbuchung entdecken, erhebe Einspruch bei deinem Mobilfunkanbieter – schriftlich und innerhalb von 3 Monaten. Solltest du dich mit deinem Mobilfunkbetreiber nicht einigen können, beantrage bei der RTR ein kostenloses Schlichtungsverfahren.

Du kannst auch gleichzeitig mit deinem Einspruch an den Anbieter eine Meldung an die Rundfunk- und Telekom-Regulierungsbehörde (RTR) machen. Dadurch musst du nämlich den überhöhten Rechnungsbetrag in der Regel vorerst nicht bezahlen. Näheres dazu erfährst du unter: https://www.rtr.at/de/tk/TKKS_Schlichtung01

www.rtr.at/schlichtungsstelle
www.rtr.at/webformular

Foto: Rawpixel.com - AdobeStock

ACHTUNG SOCIAL MEDIA

IN DEN SOZIALEN NETZWERKEN GEHT'S NICHT IMMER SOZIAL ZU. IMMER WIEDER SIND DORT AUCH BETRÜGERINNEN UND BETRÜGER UNTERWEGS. OB ALS FALSCHE FREUNDE, ÜBER VERFÜHRERISCHE LINKS ODER WERBUNG.

10 WELCHE PLATTFORMEN SIND BESONDERS ANFÄLLIG?

Nirgendwo sonst findet Internet-Betrug so geballt statt wie bei Facebook & Co.

Du bist auf etwas Verdächtiges gestoßen? Dann melde es sofort dem Seitenbetreiber, damit die Sachen gelöscht werden können. Verdächtig können sein:

- Banner und Anzeigen
- Seiten
- Links
- Videos
- Profile
- Apps

11 WAS SIND DIE GÄNGIGEN MASCHEN?

Du bekommst einen superverführerischen Link oder ein megasensationelles Angebot. Auch extrem schockierende Videos werden immer wieder eingesetzt.

Klickst du darauf, kann dir folgendes passieren:

- Du schließt ein kostenpflichtiges Abo ab
- Du gibst deine Daten an Unbekannte weiter, die deine Daten dann weiterverkaufen
- Du installierst Schadsoftware
- Dein Profil wird gehackt und du verlierst den Zugang zu deinem Konto

12 FREUNDSCHAFTSANFRAGEN VON LEUTEN, DIE DU NICHT KENNST?

Vorsicht-Vorsicht! Wenn du Anfragen von völlig Unbekannten bekommst, ist das schon ein Grund, skeptisch zu sein. Schau dir diese Leute ganz genau an, bevor du reagierst.

Foto: NDABCREATIVITY - AdobeStock

13 WIE BIST DU SICHER UNTERWEGS?

Schütze deine Privatsphäre in den Sozialen Netzwerken und halte diese Sicherheitseinstellungen immer aktuell. Anleitungen dafür findest du bei Saferinternet.at

Wenn du Freundschaftsanfragen von Leuten bekommst, mit denen du schon befreundet bist, sei skeptisch! Nimm mit der betreffenden Freundin bzw. dem betreffenden Freund am besten über einen anderen Kanal Kontakt auf und frag nach. In den meisten Fällen kommt die erneute Anfrage gar nicht von ihr bzw. ihm, sondern von jemandem, der dir schaden will.

Außerdem: Check – Check – Double Check!
Glaub nicht alles, was du in den Social Medias liest. Sei wachsam und schalte deinen Kopf ein. Egal, ob es sich um Angebote oder News handelt.

www.saferinternet.at/leitfaden

PHISHING: VERSUCHTER DATENKLAU

DEINE ZUGANGSDATEN SIND WIE DEIN WOHNUNGSSCHLÜSSEL. WER SIE HAT, KANN ÜBERALL HINEINSCHAUEN UND ALLES MITNEHMEN, WAS ER BZW. SIE DORT FINDET. HIER LIEST DU, WIE DU DEINE DATEN SCHÜTZT.

14 WAS IST PHISHING EIGENTLICH?

Phishing heißt: Betrügerinnen bzw. Betrüger versuchen, Zugangsdaten von dir zu erbeuten.

Die begehrtesten Zugangsdaten sind die von:

- Onlinebanking
- Sozialen Netzwerken
- Google Play bzw. App Store
- E-Mail-Konten
- Onlineshops

15 WIE FUNKTIONIERT PHISHING?

Du bekommst gefälschte E-Mails, SMS oder Messenger Nachrichten mit einem Link. Die Nachrichten sehen denen deiner Bank, deiner Sozialen Plattformen oder deines E-Mail-Anbieters zum Verwechseln ähnlich.

Keinen Link öffnen

Mit unterschiedlichen Argumenten, die aber sehr nachvollziehbar klingen, wirst du aufgefordert, diesen Link zu öffnen und dort deine persönlichen Daten einzugeben. Solche Argumente sind z. B., dass du dein Konto aktualisieren, dir eine notwendige App herunterladen oder zusätzliche Features für ein Soziales Netzwerk freischalten sollst.

Keinen Daten eingeben

Natürlich landest du auf einer ebenfalls gefälschten Website, die aber täuschend echt aussieht. Gibst du dort deine Daten ein, haben die Betrügerinnen und Betrüger genau das, was sie wollten. Nun können Sie in aller Ruhe entweder dein Bankkonto leerräumen, sich auf deinem Profil austoben oder mit deiner E-Mailadresse Schadsoftware verschicken.

Keine App herunterladen

Lädst du dir dort eine App herunter, installierst du dir damit eine Schadsoftware, die entweder deinen Computer, dein Smartphone oder dein Tablet lahmlegt oder deine Daten ausspioniert.

-16- WIE ERKENNST DU PHISHING?

Das ist ganz einfach. Denn ob Bank, Facebook oder App Store: Seriöse Unternehmen fragen niemals deine Kundendaten per E-Mail, SMS oder Messenger-Nachricht ab! Wenn du solche Nachrichten bekommst, sofort weg damit! Klicke sie nicht an, sondern wirf sie direkt in den Papierkorb.

Noch 2 Tipps, wie du deine Konten schützen kannst:

- Benütze immer die Zwei-Wege-Authentifizierung
- Installiere generell keine Apps und Programme aus unbekannten Quellen

-17- WAS IST EINE ZWEI-WEGE-AUTHENTIFIZIERUNG?

Das ist eine Schutzmaßnahme speziell für Benutzerkonten. Immer wenn du dich einloggst, wirst du aufgefordert, zusätzlich zum Passwort noch einen Code einzugeben.

Dieser Code wird dir sofort aufs Handy geschickt – je nachdem, welchen Kanal du bei der Registrierung dafür hinterlegt hast. Erst wenn du diesen Code ins Login-Feld eingegeben hast, bekommst du Zugang zu deinem Konto.

Foto: carballo - AdobeStock

HILFREICHE KONTAKTE

AN DIESE STELLEN KANNST DU DICH BEI VERSCHIEDENEN GROSSEN UND KLEINEN PROBLEMEN IM INTERNET WENDEN.

18 WER BERÄT DICH ZU ONLINE-AKTIONEN?

Die AK und die Internet Ombudsstelle. Hier bekommst du eine kostenlose Beratung bei folgenden Problemen: Onlineshopping, Internet-Betrug, Datenschutz, Urheberrecht. Die Internet Ombudsstelle bietet auch eine Streitschlichtung an.

- www.arbeiterkammer.at
- www.ombudsstelle.at

19 DIE AKTUELLEN METHODEN BEIM INTERNETBETRUG?

Auf der Watchlist Internet kannst du dich über die gerade aktuellen Maschen informieren, damit du nicht drauf reinfällst. Außerdem findest du hier interessante Fälle und Fakten.

- www.watchlist-internet.at

20 WO KANNST DU DICH ALLGEMEIN ZUM THEMA INTERNET INFORMIEREN?

Viele Tipps, Anregungen und Infos, wie du das Internet und dein Smartphone sicher benutzen kannst, findest du bei Saferinternet.at.

- www.facebook.com/saferinternetat
- www.saferinternet.at
- www.instagram.com/saferinternet.at

21 PROBLEME MIT DER HANDYRECHNUNG?

Wende dich an die Rundfunk- und Telekom-Regulierungsbehörde (RTR).

- www.rtr.at

22 DU HAST SORGEN?

Wenn du dich nicht mehr auskennst, sich das alles nicht mehr ausgeht und du einfach jemanden zum Reden brauchst, wende dich an 147 Rat auf Draht. Der Notruf für Kinder und Jugendliche ist immer für dich da! Kostenlos, rund um die Uhr und anonym.

- Telefon: **147**
- Online-Beratung, Chat: www.rataufdraht.at

Eine Leistung aus dem
ZUKUNFTSPROGRAMM
AK extra

Foto: pololia - AdobeStock

Das AK Bildungsnavi ist deine Orientierungshilfe im Bildungsdschungel!

Telefonische Beratung:
Tel.: +43 1 50165-1406
Mo und Do
9.00 bis 14.00 Uhr
Di und Mi
13 bis 18 Uhr

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
facebook.com/Arbeiterkammer
youtube.com/AKOesterreich
twitter.com/Arbeiterkammer

Alle AK YOUNG Folder kannst du kostenlos downloaden:
bildungsnavi.ak.at

Weitere Bestellmöglichkeiten:

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

INTERNETBETRUG Artikelnummer **582**

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: © pololia – Adobe Stock, weitere Abbildungen siehe Credit beim Foto
Grafik: Andreas Kuffner I Druck: Gugler GmbH, 3390 Melk

Stand: August 2020

AK 100 JAHRE GERECHTIGKEIT