

**AK
YOUNG**

FAQ
FREQUENTLY ASKED QUESTIONS

**15 HÄUFIG
GESTELLTE
FRAGEN**



SMART AM HANDY

**LASS DICH NICHT
VON KRIMINELLEN TÄUSCHEN:
SO NUTZT DU DEIN SMARTPHONE SICHER**

SCHÜTZE DEIN HANDY!

AUF DEINEM HANDY SIND DEINE WICHTIGSTEN DATEN GESPEICHERT: PASSWÖRTER, KONTONUMMER, KONTAKTE, FOTOS, VIDEOS UND MEHR. GERÄT DEIN HANDY IN FALSCH E HÄNDE, KANN DAS BÖSE ENDEN.



WIE KANNST DU DEIN HANDY SCHÜTZEN?

Sperre dein Handy

Entweder mit einem alphanumerischen Code – z. B. MkSw218Ja!, einem Fingerabdruck (Touch ID) oder einer Gesichtserkennung (Face ID)



EINEN CODE MERKST DU DIR AM BESTEN MIT EINEM MERKSATZ, Z. B.: MEINE KLEINE SCHWESTER WURDE 2021 8 JAHRE ALT! DAS ERGIBT ALS CODE: MkSw218Ja!

Stelle ein, dass sich Betriebssystem und Apps automatisch updaten

Mach ein Back-Up und sichere deine Daten

So verlierst du bei Verlust oder Diebstahl keine persönlichen Informationen.

Sperre deine Nummer für ...

Dritt- oder Content-Anbieterdienste, Roaming-Dienste im Ausland, Anrufe und SMS außerhalb der EU und Mehrwert-SMS und -Anrufe

Blockiere in den Handy-Einstellungen Spam-Nachrichten und -Anrufe



2

BRAUCHST DU EIN ANTIVIREN-PROGRAMM?

Das hängt von deinem Betriebssystem ab.

Beim iPhone (iOS) nicht unbedingt, denn das Betriebssystem ist nur teilweise offen. Vieles bleibt geheim.

Bei einem Android-Handy können alle einsehen, wie das Betriebssystem funktioniert. So können Sicherheitslücken leicht ausgenutzt werden.



**WELCHE ANTIVIREN-APP
GERADE DIE BESTE IST,
FINDEST DU IM INTERNET
HERAUS.**

3

SIND QR-CODES UND SMS-LINKS GEFÄHRLICH?

An sich nicht. Aber: Sie können auf betrügerische Websites führen und dort schädliche Programme herunterladen.

WIE ERKENNST DU, OB EIN QR-CODE ODER EIN LINK SICHER IST?

Überprüfe die Adresse: Achte auf Rechtschreibfehler, zusätzliche Buchstaben oder ungewöhnliche Endungen der Webadresse.

Vergleiche:

www.musterseite.at (richtig 😊)

www.mustersaitexy.at (fake 😞)

**4**

WIE TÄUSCHEN DICH KRIMINELLE?

Sie geben vor, dass sie von der Polizei, einer Bank oder einer anderen Einrichtung sind. Durch falsches Vertrauen gibst du dann persönliche Informationen wie Kontonummer, PIN oder TAN bekannt. Damit plündern Betrüger dann dein Konto oder nutzen deine Daten für Verbrechen unter deinem Namen.

IST DEINE TELEFONNUMMER FÜR KRIMINELLE SCHON BEKANNT?

Das kannst du auf diesen Websites nachschauen:

 <https://leakchecker.uni-bonn.de>

 <https://sec.hpi.de/ilc/search>

 <https://haveibeenpwned.com>



**SAG DEINEM MOBILFUNKANBIETER,
DASS DEINE NUMMER NICHT IM
TELEFONBUCH AUFSCHWEINEN SOLL.**

DU BEKOMMST KOMISCHE ANRUFEN UND NACHRICHTEN?

Lege auf, wenn die Polizei, die Bank oder eine andere Einrichtung nach Geld oder deiner Kontonummer fragt. Echte Behörden machen das nicht!

Auch in diesen Fällen sei skeptisch:

- Bei Geldversprechen durch Gewinnspiele, Online-Trading oder Coachings, die dir für zunächst wenig Geld ein hohes Einkommen garantieren
- Bei seltsamen Nachrichten von Paketdiensten, Banken und Unternehmen
- Klicke keine unbekannten Links an, damit du angebliche Pakete orten oder Geld für irgendetwas zahlen kannst



Gib niemals Infos an Unbekannte weiter und blockiere betrügerische Nummern. Lade keine Apps oder Dateien von unbekannten Quellen herunter und ignoriere komische Links.

5

ANRUF MIT UNBEKANNTER NUMMER?

Vorsicht vor unbekannten Anrufen mit ausländischer Vorwahl! Hebe nicht ab, rufe nicht zurück und blockiere die Nummer sofort. Warum? Es können hohe Kosten entstehen. Deshalb: Sperre Anrufe und SMS außerhalb der EU bei deinem Mobilfunkanbieter.





6

WAS MACHST DU BEI SPAM-ANRUFEN?

Am iPhone: unbekannte Personen stummschalten

- 📞 Einstellungen
- 📞 Telefon
- 📞 Unbekannte Anrufer stumm – aktiviere den Regler

Am Android Handy: unbekannte Personen blockieren

- 📞 Telefonsymbol – öffne das Menü
- 📞 Einstellungen
- 📞 Blockierte Nummern – aktiviere Unbekannt



BEACHTET: NICHT ALLE UNBEKANNTEN NUMMERN SIND GEFÄHRLICH. AKTIVIERST DU DIE FUNKTIONEN, KÖNNTEST DU AUCH WICHTIGE ANRUFEN VERPASSEN.

7

WAS MACHST DU BEI SPAM-NACHRICHTEN?

Am iPhone kannst du Nachrichten von unbekannten Personen filtern. Dadurch scheinen derartige Mitteilungen in einem eigenen Ordner auf (Einstellungen – Nachrichten – Nachrichtenfilter – Option: Unbekannte Absender filtern). Bei Android kannst du Nachrichten von fremden Nummern nicht automatisch filtern. Aber du kannst unbekannte Personen blockieren.

WORAUF MUSST DU BEI SPAM NOCH AUFPASSEN?

Du erhältst eine Nachricht, dass du deine Bankdaten, deinen Netflix- oder Spotify-Account aktualisieren sollst. Das ist ein Fake! Rufe auf keinen Fall die verlinkte Website auf. Gib dort auch niemals deine Bankdaten und Sicherheitscodes bekannt. Sonst ermöglichst du es Datendieben, dass sie deine Zahlungsdaten für ihr Apple Pay-Konto stehlen. Und damit auf deine Kosten einkaufen können.

8

EINE FREMDE PERSON MÖCHTE ZUGRIFF AUF DEIN HANDY?

Alarmglocken! Zum Beispiel, wenn dir jemand per Anruf oder SMS sagt: Du sollst was auf deinem Handy installieren. Die Fake-Personen bieten dir so vermeintliche Hilfe an und wollen dadurch Zugang zu deinem Handy bekommen. Installiere nichts! Leg auf! Und blockiere die Nummer!

Kriminelle können ansonsten mit dem Programm auf dein Handy zugreifen. Und so zum Beispiel Geld stehlen, deinen Freunden Fake-Nachrichten schreiben oder dich mit deinen Fotos erpressen.

9

WAS, WENN DU DEIN HANDY VERLIERST?

Bei Apple gibt es „Find my iPhone“, bei Android „Find my Device“. Wenn du dein Handy verlierst, kannst du es damit wiederfinden, Daten löschen oder sperren.



Achtung: Es gibt auch betrügerische Websites zur Handy-Ortung, die viel Geld kosten. Nutze also nur die offiziellen Angebote.



WhatsApp, INSTAGRAM & CO UND ZOCKEN AM HANDY

**WHATSAPP SPAMGRUPPEN, GESPERRTER INSTAGRAM-ACCOUNT,
TEURE HOTLINES ODER MEHRERE HUNDERT EURO FÜR LEVEL-PAKETE –
SO SCHÜTZT DU DICH:**

10

WIE MACHST DU WHATSAPP SICHER?

Plötzlich fügt dich eine fremde Person in eine WhatsApp-Spamgruppe hinzu? Vielleicht erhältst du Kettenbriefe mit Fake-News? Oder dein Profilbild wird für Fake-Bilder verwendet? Mit diesen Tipps kannst du dich schützen:



- 📱 **Wähle Einstellungen auf WhatsApp**
- 📱 **Verbirg die Anzeige von:** Zuletzt Online, Online-Status, Profil-Bild und die Lesebestätigung – gehe dazu auf Datenschutz und stelle die nötigen Funktionen ein bzw. aus
- 📱 **Aktiviere die Zwei-Stufen-Authentifizierung:** Gehe zu Konto und tippe auf Verifizierung in zwei Schritten
- 📱 **Stelle ein, dass Bilder und Videos nicht automatisch in deine Galerie kommen:** Wähle Chats, beim iPhone schaltest du „Sichern in Aufnahmen“ aus, bei Android deaktivierst du den Regler bei „Sichtbarkeit von Medien“



**UNTER DATENSCHUTZ FINDEST DU EINEN DATENSCHUTZ-CHECK –
DER HilFT DIR BEIM FINDEN DER RICHTIGEN EINSTELLUNGEN.**

11

WIE MACHST DU ALLE DEINE APPS SICHER?

Der beste Tipp: die Zwei-Faktor-Authentifizierung! Wenn du dich bei Instagram oder einer anderen App einloggst, musst du zusätzlich zum Passwort einen Code eingeben. Der wird auf dein Handy geschickt. Erst, wenn du diesen Code eingibst, erhältst du Zugang zu deinem Konto.

So können Kriminelle dein Konto nicht übernehmen oder sperren. Auch, wenn sie deine Nummer und dein Passwort kennen.



**AKTIVIERE IN ALLEN APPS SICHERE DATENSCHUTZ-EINSTELLUNGEN.
MEHR INFOS FINDEST DU HIER: saferinternet.at/privatsphaere-leitfaeden**



12

DU ZOCKST AM HANDY UND WIRST DABEI ABGEZOCKT?

Du lädst ein kostenloses Spiel runter und plötzlich musst du mehrere Hundert Euro zahlen. Weil du Level-Pakete, Spielwährung oder andere Gadgets gekauft hast. Damit dir das nicht passiert, deaktiviere In-App-Käufe auf deinem Handy.

Am iPhone geht das so:

- 📱 Einstellungen
- 📱 Bildschirmzeit
- 📱 Beschränkungen
- 📱 Käufe im iTunes & App Store
- 📱 In-App-Käufe
- 📱 Nicht erlauben



ENTFERNE AUCH GESPEICHERTE ZAHLUNGSDATEN AUS DEINEM KONTO. DAS SCHÜTZT DICH VOR UNABSICHTLICHEN KÄUFEN.

Im Android-System gehst du so vor:

- 📱 Profilsymbol in der Google Play App
- 📱 Einstellungen
- 📱 Authentifizierung
- 📱 Authentifizierung für Käufe erforderlich



13**WO LAUERN NOCH TEURE GEFAHREN?**

Du schaust nur kurz ein Video oder klickst eine Werbung weg – auch das kann teuer werden. Du erhältst eine SMS, dass du zahlen sollst: Wahrscheinlich hast du dir ein betrügerisches Abo eingefangen. Damit dir das nicht passiert, sperre deine Nummer am besten für Dritt- oder Content-Anbieter. Entweder über die Hotline deines Mobilfunkbetreibers oder direkt in deinem Kundenkonto.



**SPERRE DEINE NUMMER AUCH FÜR MEHRWERT-DIENSTE.
DAMIT KANNST DU TEURE NACHRICHTEN NICHT MEHR VERSENDEN
ODER TEURE HOTLINES NICHT MEHR ANRUFEN. DAS SPART DIR GELD!**

14**DIR WIRD GRUNDLOS GELD ABGEBUCHT?**

Kontaktiere sofort deinen Handyanbieter. Sag ihm, dass du das nie bestellt hast. Dein Handyanbieter soll dir deswegen dein Geld zurückzahlen.

15**DU VERKAUFST ETWAS ÜBER EINE APP?**

Hier gilt immer: vorsichtig sein. Kriminelle können dich nämlich dazu bringen, dass du deine Kontodaten samt Verfügernummer und TAN-Code auf einer Fake-Site nennst. Der Vorwand dabei: Das soll notwendig sein, damit du Geld erhältst. In Wahrheit stehlen sie aber so deine Online-Banking-Daten. Deshalb: Gib nie etwas frei, wenn du nicht etwas einkaufst.

**MEHR INFOS
FINDEST DU HIER:**



**DU HAST
FRAGEN ZUM
KONSUMENTENSCHUTZ?**



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



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

SMART AM HANDY Artikelnummer **584**

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

Stand: September 2023