

Sicher vor Betrug

am Telefon, an der Haustür und im Internet

Großdruck-Fassung des Infoblatts · Erstfassung, Stand: 28. Oktober 2026

Dieses Infoblatt soll Euch eine Hilfestellung sein, um Gefahren rechtzeitig zu erkennen. Als Obmann des Zivilschutzverbands Bezirk Neunkirchen möchte ich meine Mitmenschen resilienter, also widerstandsfähiger, gegen Betrug machen.

Das ist eine Erstfassung. Trotz sorgfältiger Prüfung können Fehler enthalten sein. Wenn Euch etwas auffällt, meldet es bitte an **office@zivilschutz-nk.at**.

Christoph Polleres, Obmann des Zivilschutzverbands Bezirk Neunkirchen

Im Notfall:

Polizei-Notruf

133

Euro-Notruf

112

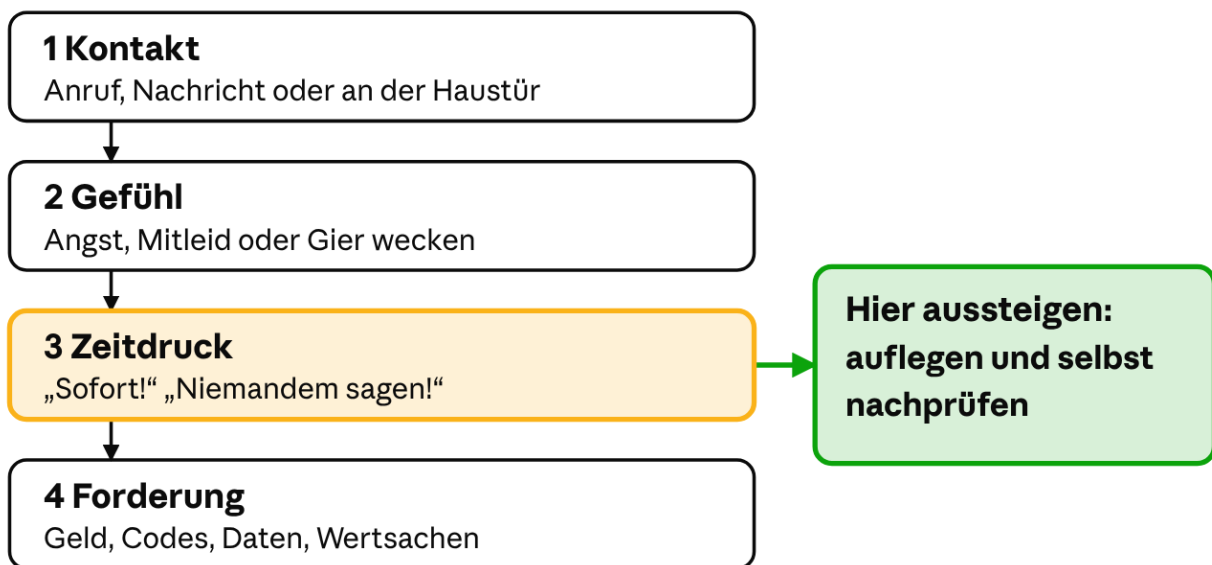
Bankomatkarte sperren

0800 204 88 00

Betrüger arbeiten heute mit echten Daten, gefälschten Telefonnummern und sogar mit künstlich erzeugten Stimmen. Mit ein paar einfachen Regeln könnt Ihr Euch und Eure Familie trotzdem gut schützen.

In Österreich wurden 2025 laut Bundeskriminalamt 63.459 Straftaten im Bereich Internetkriminalität angezeigt. Betroffen sind oft ganz normale Menschen, die von den Tätern unter Zeitdruck gesetzt wurden. Niemand muss sich schämen, wenn er hereinfällt. Am besten schützt Ihr Euch, wenn Ihr die Tricks kennt und im Zweifel kurz innehaltet.

Fast jeder Betrug läuft so ab



Sechs Grundregeln

1

Zeitdruck ist das wichtigste Warnzeichen.

Wer sagt „Sofort!“, „Niemandem davon erzählen!“ oder „Sonst passiert etwas Schlimmes!“, will Euch am Nachdenken hindern. Echte Behörden und Banken verlangen am Telefon nie Codes oder Wertsachen und nie sofort Geld.

2

Auflegen und selbst nachprüfen.

Ruft selbst bei der Bank, der Polizei oder dem Angehörigen an und fragt, ob der Anruf wirklich von ihnen kam. Nehmt dafür eine Nummer, die Ihr kennt oder selbst nachgeschlagen habt. Das kann die gespeicherte Nummer im Handy sein oder die Nummer auf der Bankomatkarte. Verwendet nie die Nummer aus dem Anruf oder der Nachricht. Auch die Nummer, die am Display angezeigt wird, kann gefälscht sein.

3

Eine bekannte Stimme beweist nichts mehr.

Mit künstlicher Intelligenz (KI) lassen sich Stimmen und sogar Videos täuschend echt nachmachen. Vereinbart deshalb in der Familie ein Codewort.

4

Kein Geld, keinen Schmuck und keine Bankomatkarten an Fremde übergeben.

Das gilt auch für angebliche Polizisten, Bankmitarbeiter oder Boten. Die echte Polizei holt nie Geld oder Wertsachen zur Aufbewahrung ab.

5

Codes und Passwörter bleiben geheim.

Gebt niemandem eine TAN (den Bestätigungscode fürs Online-Banking), einen Code aus einer SMS oder Eure PIN weiter, auch nicht am Telefon. Keine Bank fragt danach. In der Bank-App gebt Ihr nur frei, was Ihr selbst veranlasst habt.

6

Lieber einmal zu viel nachfragen.

Redet mit der Familie oder den Nachbarn. Wollt Ihr bei der Polizei nachfragen, ob ein Anruf echt war, oder einen verdächtigen Anruf melden, ruft die Polizei-Servicenummer **059 133** an. Den Notruf **133** wählt Ihr nur bei akuter Gefahr, zum Beispiel wenn jemand vorbeikommen will, um Geld oder Wertsachen abzuholen.

Sechs Regeln schützen vor vielen Betrugstricks

1

Zeitdruck = Warnzeichen

Echte Stellen drängen nicht.

2

Erst auflegen

Selbst prüfen, ob es stimmt.

3

Stimme beweist nichts

Nach dem Codewort fragen.

4

Nichts übergeben

Kein Geld, keine Karten.

5

Codes bleiben geheim

PIN, TAN, SMS-Code: niemandem.

6

Im Zweifel nachfragen

Familie oder Polizei 059 133.

Die häufigsten Maschen

Fast alle Maschen laufen nach demselben Muster ab. Zuerst wecken die Täter Angst, Mitleid oder Gier, dann setzen sie Euch unter Zeitdruck.

Auf diesen vier Wegen kommen Betrüger zu Euch

Am Telefon

- Schockanruf mit KI-Stimme
- Falsche Polizei
- Falsche Bank oder PayPal: „Abbuchung stoppen“
- Angeblicher Computer-Support

Per Nachricht und E-Mail

- „Hallo Mama, neue Nummer“
- „Stimm für meine Tochter ab“ (WhatsApp)
- Paketdienst, Amt, Gesundheitskasse, Bank
- Neue Bankverbindung, Erpressungs-Mail

Im Internet

- Gefälschter Online-Shop und Kleinanzeigen
- Geldanlage mit Promi-Video, Liebe im Internet
- Jobangebot als „Finanzagent“

An der Haustür

- Falsche Handwerker, falsches Wasserwerk
- Angebliche Amtspersonen
- Unbekannte Spendensammler

Fast immer: erst ein starkes Gefühl wecken, dann Zeitdruck machen.

Schockanruf mit KI-Stimme

So klingt es: Die vertraute Stimme von Kind oder Enkel weint: „Ich hatte einen Unfall, ich brauche sofort Geld für die Kautions.“

So reagiert Ihr: Nach dem Familien-Codewort fragen. Dann auflegen und Kind oder Enkel selbst unter der gespeicherten Nummer anrufen.

Falsche Polizei

So klingt es: „Hier Kriminalpolizei. In Ihrer Gegend wird eingebrochen, wir stellen Ihr Geld sicher.“

So reagiert Ihr: Auflegen und bei der Polizei selbst nachfragen, unter der Polizei-Servicenummer **059 133** oder bei Eurer Polizeiinspektion. Kündigt jemand an, Geld oder Wertsachen abzuholen, wählt sofort den Notruf **133**. Die echte Polizei holt nie Geld oder Wertsachen zur Aufbewahrung ab.

Falsche Bank oder PayPal

So klingt es: „Hier ist Ihre Bank. Auf Ihrem Konto gibt es verdächtige Abbuchungen. Bestätigen Sie die Meldung in Ihrer Bank-App, dann stoppen wir das.“ Oder eine Bandansage: „Bei PayPal wurde Geld von Ihrem Konto abgebucht. Drücken Sie die Taste 1, um die Zahlung zu stoppen.“ Seltener: „Erzeugen Sie am Bankomaten einen QR-Code und schicken Sie uns ein Foto.“

So reagiert Ihr: Auflegen und keine Taste drücken. In der Bank-App nichts bestätigen, was Ihr nicht selbst veranlasst habt. Keinen Code und kein QR-Code-Foto weitergeben. Kein Programm installieren, mit dem Fremde auf Euer Handy oder Euren Computer zugreifen können. Dann selbst in der App oder auf der Webseite nachsehen, ob es die Abbuchung wirklich gibt. Oder die Bank unter der Nummer aus der Bank-App anrufen.

„Hallo Mama, neue Nummer“

So klingt es: Eine Nachricht per WhatsApp oder SMS: „Mein Handy ist kaputt, das ist meine neue Nummer. Kannst du schnell eine Rechnung zahlen?“

So reagiert Ihr: Unter der **alten** Nummer anrufen oder eine persönliche Frage stellen. Nichts überweisen.

„Stimm für meine Tochter ab“

So klingt es: Ein Bekannter schreibt auf WhatsApp: „Bitte stimme beim Tanzwettbewerb für die Kleine ab.“ Auf der Abstimmungsseite soll man die Handynummer eingeben. Danach soll man einen Code in WhatsApp eintippen oder einen QR-Code scannen.

So reagiert Ihr: Nie einen Code von einer fremden Seite in WhatsApp eintippen. Keinen fremden QR-Code mit WhatsApp scannen. Damit verbindet Ihr Euer Konto mit dem Gerät der Betrüger.

Gefälschte Nachricht von Paketdienst, Behörde oder Bank

So klingt es: „Ihr Paket wartet, Zollgebühr offen.“ „Ihre ID Austria läuft ab.“ „Sie bekommen Geld von der Gesundheitskasse zurück.“

So reagiert Ihr: Nicht auf Links tippen. App oder Webseite selbst öffnen und dort nachsehen. Eine ID Austria läuft tatsächlich nach einigen Jahren ab. Prüft das deshalb selbst in der App oder auf oesterreich.gv.at, nie über den Link.

Neue Bankverbindung

So klingt es: Eine echt wirkende Rechnung oder E-Mail eines bekannten Handwerkers, Vereins oder Amts: „Unser Konto hat sich geändert.“

So reagiert Ihr: Bei geänderter Kontonummer immer beim Absender anrufen, und zwar unter der Nummer, die Ihr schon kennt.

Gefälschter Online-Shop und Kleinanzeigen

So klingt es: Ein Online-Shop bietet Markenware weit unter dem üblichen Preis an. Beahlt wird nur im Voraus. Oder ein angeblicher Käufer schickt Euch einen Link zum „sicheren Bezahlen“.

So reagiert Ihr: Bei auffallend günstigen Angeboten zuerst im Internet nach Erfahrungen mit dem Shop suchen. Nie über einen zugeschickten Link Bankdaten eingeben.

Geldanlage mit Promi-Video

So klingt es: Ein bekanntes Gesicht empfiehlt im Video eine „sichere“ Anlage mit hohen Gewinnen.

So reagiert Ihr: Solche Promi-Empfehlungen sind häufig gefälscht, oft mit KI. Echte Nachrichtensendungen zeigen keine Promis, die für Anlage-Plattformen werben. Nichts einzahlen.

Jobangebot als „Finanzagent“

So klingt es: „Verdienen Sie leicht dazu: Geld über Ihr Konto weiterleiten oder Pakete annehmen und weiterschicken.“

So reagiert Ihr: Ablehnen. Wer Geld weiterleitet, hilft bei Geldwäscherei. Wer Pakete weiterschickt, hilft oft bei Bestellbetrug. In beiden Fällen kann man sich selbst strafbar machen.

Erpressungs-Mail

So klingt es: „Ich habe Sie über Ihre Kamera gefilmt. Zahlen Sie in Bitcoin, sonst schicke ich das Video an Ihre Kontakte.“

So reagiert Ihr: Nicht antworten, nicht zahlen, löschen. Diese Mails werden massenhaft verschickt. In aller Regel gibt es kein Video. Wurdet Ihr aber nach einem echten Video-Chat erpresst: nicht zahlen, nichts löschen und Anzeige erstatten.

Liebe im Internet

So klingt es: Eine neue Bekanntschaft schreibt monatelang liebevoll. Dann braucht sie plötzlich Geld für einen Notfall oder ein Ticket.

So reagiert Ihr: Kennt Ihr jemanden nur aus dem Internet und er will Geld, brecht den Kontakt ab. Überweist nichts. Auch Videoanrufe lassen sich heute mit KI fälschen.

Angeblicher Computer-Support

So klingt es: „Ihr Computer ist infiziert, wir helfen. Installieren Sie bitte dieses Programm.“

So reagiert Ihr: Auflegen, egal ob sich der Anrufer als Microsoft, Apple oder eine andere Firma ausgibt. Microsoft ruft nach eigenen Angaben nie unaufgefordert an, um Computerprobleme zu beheben. Niemanden über das Internet auf Euren Computer zugreifen lassen.

An der Haustür

So klingt es: „Wir sind vom Wasserwerk und müssen die Leitung prüfen.“ Oder ein „Handwerker“ mit dringender Reparatur. Oder ein Spendensammler.

So reagiert Ihr: Keine Unbekannten hereinlassen. Dienstausweis zeigen lassen und beim Amt oder Betrieb selbst anrufen, unter einer Nummer, die Ihr selbst nachgeschlagen habt. Nicht die Nummer auf dem Ausweis oder einem Zettel verwenden. Kein Bargeld an der Tür.

Gut zu wissen: Bei einem Datenleck werden Kundendaten bei Firmen gestohlen oder gelangen ungewollt ins Internet. Danach kennen Betrüger oft Euren Namen, Eure Adresse und Euer Geburtsdatum. Wenn jemand diese Daten nennt, beweist das noch nicht, dass er echt ist.

E-Mails und Nachrichten prüfen

Am sichersten ist es, selbst in der App oder auf der bekannten Webseite nachzusehen oder anzurufen, statt etwas in der Nachricht anzuklicken.

Fünf Warnzeichen verraten diese gefälschte Bank-Mail

Von: Kundenservice Ihrer Bank service@ihre-bank.sicherheit-pruefung.example	1
Betreff: DRINGEND – Konto wird in 24 Std. gesperrt	2
Sehr geehrter Kunde, wir haben verdächtige Zugriffe festgestellt. Bestätigen Sie Ihre Daten sofort, sonst wird Ihr Konto gesperrt.	3
Jetzt Konto bestätigen	4
Anhang: Rechnung_Oktober.zip	5

- 1 **Falscher Absender**
Die Adresse gehört nicht zur Bank.
- 2 **Drohung und Zeitdruck**
Echte Banken drohen nicht so.
- 3 **Unpersönliche Anrede**
Ein Hinweis, aber kein Beweis.
- 4 **Link zum Anmelden**
Führt auf eine gefälschte Seite.
- 5 **Gepackter Anhang**
Kann ein Schadprogramm enthalten.

Beispiel frei erfunden. Echte Betrugs-Mails wirken oft professioneller.

Absender genau ansehen

- Die ganze Absenderadresse lesen, nicht nur den angezeigten Namen. Eine Mail von „Ihre Bank“ kann in Wahrheit von service@ihre-bank.sicherheit-pruefung.example kommen.
- Auch eine echt aussehende Adresse oder Telefonnummer kann gefälscht sein. Und dass der Absender Euren Namen, Eure Adresse oder Kundennummer kennt, beweist ebenfalls nichts.

Links nicht anklicken

- Am Computer mit der Maus über den Link fahren, ohne zu klicken. Je nach Programm erscheint dann unten im Fenster oder neben dem Mauszeiger die echte Zieladresse. Passt sie nicht zum Absender, nicht anklicken.
- Am Handy öffnet Ihr besser gleich die App des Absenders, statt auf den Link zu tippen.

Anhänge nur öffnen, wenn Ihr sie erwartet

- Anhänge mit Namen wie „Rechnung“, „Mahnung“, „Vorladung“ oder „Urheberrechtsverletzung“ sind typische Lockmittel. Darin können Schadprogramme stecken, also Programme, die Euren Computer ausspionieren oder sperren.
- Besonders gefährlich sind gepackte Dateien (der Dateiname endet auf .zip) sowie Word- oder Excel-Dateien, die zum „Aktivieren von Inhalten“ auffordern.
- Im Zweifel beim Absender anrufen: „Haben Sie mir das wirklich geschickt?“

Nachrichten von Ämtern und Versicherungen

Gefälschte Nachrichten zu ID Austria, Finanzamt oder Krankenkasse enthalten oft Links zu nachgemachten Anmeldeseiten. Ob eine Nachricht echt ist, seht Ihr, wenn Ihr Euch selbst auf der offiziellen Seite oder in der offiziellen App anmeldet. Den Link in der Nachricht verwendet Ihr dafür nie.

QR-Codes

- QR-Codes sind die kleinen gemusterten Quadrate, die man mit der Handykamera scannt. Auf Briefen, Zetteln, Parkautomaten oder Ladestationen für E-Autos können sie überklebt oder gefälscht sein.

- Nach dem Scannen zuerst die angezeigte Adresse prüfen und dort nie Bank- oder Anmeldedaten eingeben.
- Einen QR-Code, den Ihr am Bankomaten oder in der Bank-App erzeugt habt, nie fotografieren und weiterschicken.

Konten und Geräte schützen

Ein paar Einstellungen, die Ihr nur einmal machen müsst, machen es Fremden deutlich schwerer, Eure Konten zu übernehmen. Gemeint sind hier Eure Zugänge zu E-Mail, Online-Banking, WhatsApp oder Facebook.

- **Sichere Passwörter wählen.** Je länger, desto besser: mindestens 12 Zeichen. Am leichtesten merkt man sich mehrere zufällige Wörter, verbunden mit Zahlen oder Zeichen. Ungeeignet sind Namen, Geburtsdaten, Haustiere, die eigene Adresse, „123456“ oder „Passwort“. Auch Kombinationen wie Vorname und Geburtsjahr erraten Betrüger schnell.
- **Für jedes Konto ein eigenes Passwort.** Sonst kommen Betrüger mit einem einzigen gestohlenen Passwort auch in alle anderen Konten.
- **Passwörter nie offen speichern.** Nicht als Notiz im Handy, nicht in einer Word- oder Excel-Datei und nicht in einer E-Mail an Euch selbst. Schickt Passwörter auch nie per E-Mail, SMS oder WhatsApp weiter. Ein Zettel am Bildschirm ist ebenso tabu.

- **Einen Passwortsafe verwenden.** Ein Passwortsafe, auch Passwort-Manager genannt, ist ein Programm, das alle Passwörter verschlüsselt aufbewahrt. Ihr müsst Euch dann nur noch ein einziges, gutes Hauptpasswort merken. Viele Handys haben so einen Safe bereits eingebaut. Passwörter einfach im Internetprogramm (Browser) speichern zu lassen, ist dagegen weniger sicher. Schützt den Safe zusätzlich mit dem zweiten Schritt bei der Anmeldung.
- **Zweiten Schritt bei der Anmeldung einschalten.** In den Einstellungen heißt das oft „Zwei-Faktor“ oder „2FA“. Zusätzlich zum Passwort braucht es dann eine Bestätigung am Handy. Das gibt es bei E-Mail, Online-Banking, Facebook und den meisten anderen Diensten.
- **WhatsApp absichern.** Öffnet die WhatsApp-Einstellungen (am iPhone unten rechts, je nach Version „Du“ oder „Einstellungen“, am Android-Handy über die drei Punkte oben rechts). Unter „Konto“ schaltet Ihr die **Verifizierung in zwei Schritten** ein und legt eine eigene 6-stellige PIN fest. Den 6-stelligen Code, den WhatsApp per SMS schickt, gebt Ihr nie weiter, auch nicht an Freunde. Und tippt nie einen Code in WhatsApp ein, den Euch eine fremde Webseite anzeigt. Schaut außerdem ab und zu unter „Verknüpfte Geräte“ nach. Steht dort ein Gerät, das Ihr nicht kennt, tippt es an und wählt „Abmelden“.
- **Updates sofort installieren,** am Handy genauso wie am Computer und am WLAN-Router. Diese Aktualisierungen schließen Sicherheitslücken, über die Betrüger sonst eindringen.

- **Wichtiges doppelt sichern.** Fotos und Dokumente zusätzlich auf einer externen Festplatte speichern und die Festplatte danach wieder abstecken. Dann kommen auch Erpressungsprogramme, die Eure Dateien sperren und Lösegeld verlangen, nicht an diese Kopie heran.

In drei Schritten schützt Ihr Euer WhatsApp vor Fremden

1 Einstellungen öffnen

iPhone: unten rechts („Du“ bzw. „Einstellungen“) · Android: Menü ☰ oben rechts



2 „Konto“ antippen

dann „Verifizierung in zwei Schritten“ wählen



3 Einschalten

eigene 6-stellige PIN festlegen und gut merken

Den 6-stelligen Code aus der WhatsApp-SMS gebt Ihr nie weiter, auch nicht an Freunde.

Wenn Eure Daten im Umlauf sind

Ein Datenleck heißt nicht automatisch, dass jemand auf Eure Konten zugreifen kann. Betrüger nutzen die echten Daten aber, um glaubwürdig zu wirken.

Wer Eure Daten kennt, ist deshalb noch nicht echt

Name, Geburtsdatum, Adresse

- Daraus wird:** persönliche Anrede in Mails, Briefen und Anrufen
- Eure Antwort:** Anrede mit Namen ist kein Echtheitsbeweis

Bankverbindung (IBAN)

- Daraus wird:** gefälschte Abbuchungen oder falscher „Bank-Anruf“
- Eure Antwort:** Bank selbst anrufen, Kontoauszüge prüfen

Ausweisnummer

- Daraus wird:** Verträge oder Konten in Eurem Namen
- Eure Antwort:** Anzeige erstatten, fremden Rechnungen widersprechen

E-Mail-Adresse

- Daraus wird:** gezielte, echt wirkende Betrugs-Mails
- Eure Antwort:** Absender genau prüfen, Zwei-Faktor einschalten

- Seid besonders vorsichtig, wenn Anrufer oder Absender Euren Namen, Euer Geburtsdatum oder Eure Adresse kennen. Das beweist nicht, dass sie echt sind.
- Kontoauszüge und Post regelmäßig ansehen. Unbekannte Abbuchungen, Verträge, Bestellungen oder Mahnungen sofort bei der Bank oder der jeweiligen Firma klären.
- Sind Daten aus Eurem Ausweis oder Reisepass betroffen und vermutet Ihr Missbrauch, erstattet Anzeige bei der Polizei. Wegen eines Datenlecks allein müsst Ihr kein neues Dokument beantragen.
- Passwörter ändern, wenn Ihr erfahrt, dass Eure Zugangsdaten betroffen sein könnten. Das ist besonders wichtig, wenn Ihr dasselbe Passwort für mehrere Konten verwendet habt.

- Bei der Firma oder Stelle, bei der das Datenleck passiert ist, könnt Ihr Auskunft verlangen, welche Daten sie über Euch gespeichert hat. Das Recht dazu gibt Euch die Datenschutz-Grundverordnung (Art. 15). Bei einem Leck mit hohem Risiko muss Euch die Firma in der Regel außerdem von sich aus informieren.

Kinder und Jugendliche

Am wichtigsten ist, dass sich Eure Kinder trauen, mit jedem Problem zu Euch zu kommen, ohne Angst vor Strafe oder Handyverbot.

- **Erpressung mit Fotos:** Täter geben sich als Gleichaltrige aus, überreden Jugendliche, intime Fotos zu schicken, und drohen dann, die Fotos zu veröffentlichen. Nicht zahlen, den Kontakt abbrechen und nichts löschen. Den Chat, das Profil der Täter und die Forderungen per Bildschirmfoto sichern, aber so, dass keine intimen Bilder darauf zu sehen sind. Die Bilder selbst nicht abfotografieren, speichern oder weiterleiten, denn das kann bei Bildern von Minderjährigen selbst strafbar sein. Sofort eine Vertrauensperson und die Polizei einschalten. Das Kind ist das Opfer und trägt keine Schuld.
- **Gefälschte Gewinnspiele und Gratis-Angebote:** Mit „Du hast ein Handy gewonnen“ oder angeblichem Gratis-Spielgeld für Online-Spiele wollen Betrüger an Telefonnummern, Passwörter oder Geld kommen.
- **Keine Codes weitergeben:** Auch Kinder sollen wissen, dass sie einen Code aus einer SMS nie weitergeben, egal, wer fragt.
- **Ins Codewort einweihen:** Kinder ab dem Schulalter sollten das Familien-Codewort kennen.

Stopp, sichern, sag es jemandem. Du bist nicht schuld.

1 Stopp

Nicht antworten, nichts zahlen, nichts schicken



2 Sichern

Chat und Profil sichern, keine Nacktfotos speichern



3 Sag es jemandem

Eltern, Lehrer, Polizei oder Rat auf Draht 147

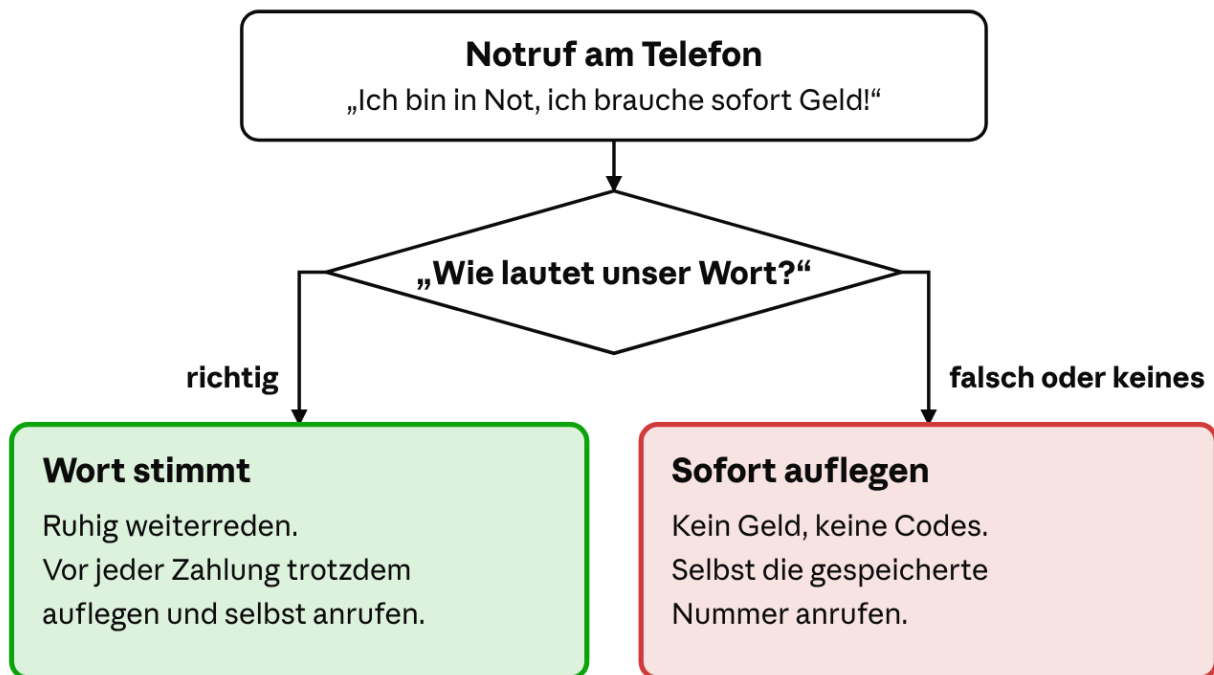
Rat auf Draht: 147 · rund um die Uhr · kostenlos · anonym

Hilfe für Kinder, Jugendliche und Eltern: **Rat auf Draht, Telefon 147**, rund um die Uhr, kostenlos und anonym.

Das Familien-Codewort

Mit einem geheimen Wort, das nur Eure Familie kennt, erkennt Ihr einen gefälschten Notruf rasch, auch wenn die Stimme täuschend echt klingt.

Ohne richtiges Codewort kein Geld und keine Daten



So richtet Ihr es ein:

1

Persönlich zusammensetzen,

zum Beispiel beim nächsten Familienessen. Nicht per Nachricht, E-Mail oder Telefon ausmachen.

2

Ein Wort oder einen kurzen Satz wählen,

den Außenstehende nicht mit Euch in Verbindung bringen können. Kein Beispiel aus einem Infoblatt oder aus dem Internet nehmen, denn das kann jeder lesen.

3

Alle einweihen, die im Ernstfall angerufen werden könnten:

Eltern, Großeltern, Kinder ab dem Schulalter, enge Vertraute.

4

Nirgends am Handy oder Computer speichern

und nie ins Internet stellen. Ein Zettel daheim in der Lade ist für ältere Angehörige in Ordnung.

5

Einmal spielerisch üben,

damit es im Stress auch wirklich abgefragt wird.

Gut geeignet sind:

- zufällige Wortpaare ohne Bezug zu Euch
- ein Satz aus einem gemeinsamen Erlebnis, das niemand im Internet finden kann
- ein Wort, das man sich auch unter Stress merkt

Ungeeignet sind:

- Namen von Haustieren, Kindern oder Straßen
- Geburtstage, Hochzeitstage, Lieblingsverein
- alles, was auf Facebook, Instagram oder in Fotos zu sehen ist

Im Ernstfall:

Ruhig nach dem Codewort fragen: „**Wie lautet unser Wort?**“

Keine Hilfe geben, etwa „Es ist doch das mit dem Garten, oder?“

Kommt das Wort nicht oder falsch, **sofort auflegen** und die Person selbst unter ihrer gespeicherten Nummer anrufen.

Wurde das Wort einmal benutzt oder vielleicht verraten, vereinbart ein neues.

Auch mit Codewort bleibt der Rückruf wichtig. Im Zweifel legt Ihr auf und ruft selbst an.

Wenn es doch passiert ist

Jetzt zählt jede Minute. Habt Ihr Geld oder Schmuck an einen Abholer übergeben, ruft sofort die Polizei unter **133** an. Wurde Geld überwiesen oder ein Code verraten, geht in dieser Reihenfolge vor. Und schämt Euch nicht, denn die Täter sind Profis.

Geld überwiesen? Zuerst Bank, dann Polizei

Sofort	1 Bank anrufen Online-Banking und Karten sperren, Rückbuchung anfragen
Gleich danach	2 Polizei: 133 oder 112 Anzeige erstatten
	3 Beweise sichern Nummer, Uhrzeit, Nachrichten, Belege
Danach	4 Passwörter ändern wenn Codes oder Passwörter verraten wurden
	5 Familie warnen Betrüger versuchen es oft noch einmal

1

Bank sofort verständigen.

Online-Banking und Karten sperren lassen und fragen, ob eine Überweisung noch zurückgeholt werden kann. Die Nummer findet Ihr in der Bank-App und auf der Webseite Eurer Bank. Bankomatkarten könnt Ihr zusätzlich über den Sperr-Notruf **0800 204 88 00** sperren lassen (aus dem Ausland +43 1 204 88 00).

2

Polizei anrufen und Anzeige erstatten:

Ist der Betrug gerade passiert, Polizei-Notruf **133** oder Euro-Notruf **112**. Sonst unter der Polizei-Service Nummer **059 133** oder bei jeder Polizeiinspektion.

3

Beweise sichern:

Telefonnummern, Uhrzeit, Nachrichten, E-Mails und Zahlungsbelege per Foto oder Bildschirmfoto festhalten. Nichts löschen.

4

Passwörter ändern:

Wurden Passwörter oder Codes verraten, diese von einem sicheren Gerät aus sofort ändern.

5

Familie warnen:

Betrüger versuchen es oft mehrmals oder bei weiteren Angehörigen.

So spricht Ihr mit Eltern und Großeltern darüber

Ältere Menschen sind besonders oft Ziel solcher Anrufe, weil die Täter gezielt ihr Vertrauen und ihre Hilfsbereitschaft ausnutzen.

Wer ohne Vorwürfe fragt, erfährt eher von einem Betrug

Statt: „Du fällst da sicher drauf rein.“

Lieber: „Das täuscht sogar Fachleute. Lass uns gemeinsam vorsorgen.“

Statt: „Gib nie wieder etwas heraus!“

Lieber: „Du darfst jederzeit auflegen und mich anrufen.“

Statt: „Wie konnte dir das passieren?“

Lieber: „Gut, dass du es mir sagst. Wir kümmern uns gemeinsam.“

1

Auf Augenhöhe beginnen,

etwa so: „Ich habe von einer neuen Masche gehört, die sogar Fachleute täuscht. Lass uns gemeinsam vorsorgen.“
Besser nicht: „Du fällst da sicher drauf rein.“

2

Ein konkretes Beispiel erzählen

statt einer langen Regelliste, etwa den Anruf mit der weinenden Enkelstimme.

3

Das Codewort gemeinsam festlegen

und dieses Infoblatt beim Telefon lassen.

4

Ausdrücklich erlauben, aufzulegen:

„Du darfst jederzeit auflegen und mich anrufen. Damit störst du nie.“ Viele bleiben aus Höflichkeit in der Leitung.

5

Ohne Vorwürfe nachfragen:

Ab und zu fragen, ob seltsame Anrufe kamen. Wer Angst vor Vorwürfen hat, verschweigt einen Betrug lieber. Dann kann es zu spät sein, das Geld zurückzuholen.

Hilfe und Meldestellen

Akute Gefahr, Betrug läuft gerade

Polizei: **133** · Euro-Notruf: **112**

Polizei ohne Notfall, Beratung zur Vorbeugung

Polizei-Servicenummer: **059 133**

Bankomatkarte sperren

Sperr-Notruf: **0800 204 88 00**, aus dem Ausland +43 1 204 88 00

Hilfe für Opfer von Straftaten

Opfer-Notruf (Weisser Ring): **0800 112 112**, kostenlos

Hinweise auf Internetbetrug melden (ersetzt keine Anzeige)

Meldestelle für Internetkriminalität (Bundeskriminalamt):
against-cybercrime@bmi.gv.at

Betrugsversuche und gefälschte Online-Shops melden, aktuelle Warnungen

Watchlist Internet: watchlist-internet.at

Missbrauchte Telefonnummern, Lock- und Betrugsanrufe

RTR: rufnummernmissbrauch.at

Probleme beim Online-Einkauf

Internet Ombudsstelle: ombudsstelle.at

Allgemeine Tipps zur Online-Sicherheit

onlinesicherheit.gv.at

Kinder, Jugendliche und Eltern

Rat auf Draht: **147**, rund um die Uhr, kostenlos und anonym

Hinweis und Quellen

Dieses Infoblatt dient der allgemeinen Information und Vorsorge. Es ersetzt keine Rechts-, Finanz- oder Sicherheitsberatung im Einzelfall. Alle Angaben wurden sorgfältig geprüft, erfolgen aber ohne Gewähr; Stand: 28. Oktober 2026.

Die beschriebenen Maschen sind typische Muster. Betrüger missbrauchen dabei die Namen echter Behörden, Banken und Unternehmen. Diese sind selbst nicht die Absender. Die genannten Stellen sind öffentliche Melde- und Beratungsangebote; für deren Inhalte sind ausschließlich die jeweiligen Betreiber verantwortlich.

Ihr dürft dieses Infoblatt gerne unverändert und kostenlos ausdrucken und weitergeben, zum Beispiel an Eltern, Großeltern und Nachbarn. Veränderte Fassungen, vor allem mit anderen Telefonnummern oder Links, dürfen nicht unter unserem Namen verbreitet werden.

Impressum: Medieninhaber und Verleger: Zivilschutzverband – Bezirk Neunkirchen, ZVR-Zahl 1927110656, Sitz: Reichenau an der Rax. Hersteller: Medieninhaber (Eigenvervielfältigung). Verlags- und Herstellungsort: Reichenau an der Rax. Offenlegung nach § 25 Mediengesetz: www.zivilschutz-nk.at/impressum.html. Datenschutz: www.zivilschutz-nk.at/datenschutz.html

Quellen: Bundeskriminalamt (Cybercrime-Report 2025), Oesterreichische Nationalbank (25.08.2026), oesterreich.gv.at (Sperr-Notruf), Salzburg24 (Oktober 2026), Verbraucherzentrale (02.03.2026), Watchlist Internet

(09.10.2026, 16.09.2026, 26.05.2026, #10TageGegenPhishing),
Saferinternet.at (Rechtliche FAQs Cybergewalt), onlinesicherheit.gv.at.