



Familienpaket

Ihre Familie gemeinsam gegen Betrug schützen

Codewort

Erklären

Notfallplan

Digital

Checkliste

Kostenlos heruntergeladen von schluss-mit-betrug.de

Keine Werbung · Keine Datenweitergabe

Das Familien-Codewort

Die einfachste und wirkungsvollste Schutzmaßnahme gegen KI-Betrug.

Warum ist das so wichtig?

KI-Programme können heute Stimmen täuschend echt kopieren – mit nur wenigen Sekunden Aufnahme, z. B. aus einem Instagram-Video. Ein Codewort, das nur Ihre Familie kennt, lässt sich nicht fälschen.

1 Codewort jetzt wählen

Wählen Sie zusammen ein Wort: leicht zu merken, schwer zu erraten, nicht auf Social Media. Z. B. ein Urlaubsort oder Lieblingstier.

2 Allen Familienmitgliedern mitteilen

Sagen Sie das Codewort persönlich oder per Telefon jedem, den Sie schützen möchten. Nie per SMS oder E-Mail.

3 Im Notfall konsequent anwenden

Wenn jemand anruft und behauptet, Ihr Kind zu sein: Fragen Sie nach dem Codewort. Kennt die Person es nicht – sofort auflegen und zurückrufen.

4 Niemals am Telefon verraten

Das Codewort darf nur persönlich oder auf einem Zettel weitergegeben werden. Kein seriöses Familienmitglied fragt Sie am Telefon danach.

Unser Familien-Codewort:

Hier eintragen – dann sicher aufbewahren!

So erkläre ich es meinen Eltern

Einfache Formulierungen für schwierige Themen – verständlich erklärt.

Das Gespräch über Betrug ist nicht immer einfach. Ältere Menschen fühlen sich manchmal bevormundet. Diese Formulierungen helfen, das Thema respektvoll und klar anzusprechen.

Einstieg

"Ich habe etwas Wichtiges gelesen und möchte es dir zeigen – damit du sicher bist."

"Ich will nicht, dass dir das passiert, was ich kürzlich gehört habe."

Enkeltrick & KI-Stimmen erklären

"Betrüger rufen an und tun so als wären sie ich – die Stimme klingt echt, ist aber eine KI-Aufnahme."

"Deshalb haben wir jetzt ein Codewort. Frag immer danach!"

Phishing (E-Mail-Betrug) erklären

"Manchmal kommt eine E-Mail, die aussieht wie von der Bank. Klick niemals auf den Link – ruf direkt bei der Bank an."

"Ich zeige dir, wie du den Unterschied erkennst."

Computer-Betrug erklären

"Wenn jemand anruft und sagt, dein Computer hat ein Problem: Sofort auflegen! Echte Techniker melden sich nie von selbst."

"Lass niemanden Fremden auf deinen Computer."

Abschluss des Gesprächs

"Wenn du dir jemals nicht sicher bist: Ruf mich sofort an. Ich helfe dir gerne."

"Es ist kein Problem, Fragen zu stellen. Betrüger sind Profis – da kann sich jeder täuschen lassen."

Was tun, wenn Betrug passiert?

Schnell und richtig handeln – Schritt für Schritt.

Wichtig: Ruhe bewahren. Betrug ist keine Schande.

Betrüger sind professionell. Wer schnell handelt, kann oft noch Schlimmeres verhindern.

1 Sofort auflegen oder Tür schließen

Sie müssen sich nicht rechtfertigen. Kein seriöser Anrufer wird beleidigt sein.

2 Vertraute Person anrufen

Rufen Sie sofort Ihr Kind, Nachbarn oder Ihre Vertrauensperson an. Schildern Sie, was passiert ist.

3 Kein Geld mehr übergeben

Warten Sie ab, auch wenn der Druck groß ist. Übergebenes Geld ist meist für immer weg.

4 Polizei: 110 anrufen

Erstatten Sie Anzeige – auch wenn kein Schaden entstanden ist. Jede Meldung hilft, andere zu schützen.

5 Bank sofort informieren (bei Überweisung)

Rufen Sie sofort Ihre Bank an (Sperrnotruf: 116 116). In manchen Fällen kann eine Überweisung noch gestoppt werden.

6 BSI-Hotline: 0800 274 1000 (kostenlos)

Das BSI berät kostenlos zu Cyberbetrug und nächsten Schritten. Mo–Do 8–17 Uhr, Fr 8–16 Uhr.

Emotionale Unterstützung anbieten

"Es ist nicht deine Schuld. Du hast das nicht verdient. Wir lösen das zusammen." – Das ist das Wichtigste.

Digitale Sicherheit – einfach erklärt

Die wichtigsten Schutzmaßnahmen für Computer, Smartphone und E-Mail.

E-Mail & Phishing

- Nie auf Links in E-Mails von Banken oder Behörden klicken.
- Immer direkt auf die Webseite gehen (selbst eintippen).
- Anhänge von Unbekannten nie öffnen.
- Banken fragen nie per E-Mail nach Passwörtern.

Passwörter

- Für Bank und E-Mail eigene, starke Passwörter nutzen.
- Passwörter nie am Telefon oder per E-Mail weitergeben.
- Tipp: Satz als Passwort, z. B. "Mein1.AutoWarBlau!"
- Passwörter auf Papier zu Hause aufschreiben ist OK.

WhatsApp & SMS

- Neue Nummer des "Kindes": Immer direkt zurückrufen!
- Gutscheinkarten-Bitte per WhatsApp = immer Betrug.
- Unbekannte in Gruppen können Sie ignorieren.
- Video-Anrufe: Fragen Sie nach dem Codewort.

Computer & Viren

- Kostenloses Antivirenprogramm installieren (Avira Free).
- Windows-Updates immer installieren.
- Kein Fremder darf Ihren Bildschirm fernsteuern.
- "Microsoft" ruft Sie nie unaufgefordert an.

Online-Shopping

- Nur auf bekannten Seiten kaufen (Amazon, Zalando etc.).
- Https:// und Schloss-Symbol in der Adresszeile prüfen.
- Zu gute Angebote sind meist Betrug.
- Kreditkarte nie per E-Mail oder Telefon weitergeben.

Soziale Medien

- Keine Adresse, Telefonnummer oder Reisepläne teilen.
- Anfragen von Unbekannten ablehnen.
- Fotos können für Deepfakes verwendet werden.
- Einstellungen auf "Nur Freunde" setzen.

Checkliste: Das Familiengespräch

Diese Punkte helfen Ihnen, das Gespräch vollständig und ruhig zu führen.

Vorbereitung (vor dem Gespräch)

- ☐ Ich habe mir Zeit und Ruhe genommen – kein Stress, kein Druck.
- ☐ Ich habe diese Checkliste und das Schutzpaket dabei.
- ☐ Ich habe das Codewort schon in meinem Kopf.

Das Codewort vereinbaren

- ☐ Wir haben gemeinsam ein Codewort gewählt.
- ☐ Alle Familienmitglieder kennen das Codewort.
- ☐ Das Codewort wurde sicher aufbewahrt (z. B. Notfallkarte).
- ☐ Wir haben besprochen: Kein Fremder darf das Codewort kennen.

Betrugsmaschen erläutert

- ☐ Ich habe den Enkeltrick erklärt.
- ☐ Ich habe KI-Stimmenklon-Betrug erklärt.
- ☐ Ich habe den Schockanruf erklärt.
- ☐ Ich habe Phishing und E-Mail-Betrug erklärt.
- ☐ Ich habe den Microsoft-/Tech-Support-Betrug erklärt.

Technische Maßnahmen erledigt

- ☐ Antivirenprogramm installiert oder geprüft.
- ☐ Wichtige Nummern gespeichert: 110, 116 116 (Bank), 0800 274 1000 (BSI).
- ☐ Besprochen: Unbekannte Anrufe erst zurückrufen.
- ☐ WhatsApp-Datenschutz-Einstellungen geprüft.

Notfallplan besprochen

- ☐ Wir haben besprochen: Bei Verdacht sofort auflegen.
- ☐ Die Vertrauensperson ist bekannt: _____
- ☐ Die Notfallkarte liegt bereit (neben dem Telefon).
- ☐ "Du kannst mich jederzeit anrufen" – das wurde gesagt.