Deutschland: Stand der Forschung zum Betrugsuniversum 2024

Verbreitungsgrad und Auswirkungen von Betrug

- Mehr als die Hälfte der Deutschen (51 %) gibt an, entweder selbst Opfer eines Online-Betrugs geworden zu sein oder jemanden zu kennen, der davon betroffen war.
  - Jüngere Befragte (18–24 Jahre und 25–34 Jahre) haben mit 59 % bzw. 66 % eher direkte oder indirekte Erfahrungen mit Betrug gemacht und geben an, Opfer zu sein oder jemanden zu kennen, der Opfer geworden ist.
  - Ältere Gruppen, insbesondere die 55–64-Jährigen (41 %) und die über 65-Jährigen (45 %), berichten seltener von Erfahrungen mit Betrug.
  - Die Altersgruppe der 25- bis 34-Jährigen ist besonders stark betroffen, wobei sowohl die direkte Viktimisierung (34 %) als auch die Kenntnis von Betroffenen (35 %) höher sind als in den meisten anderen Altersgruppen.
- Von den Personen, die Opfer eines Online-Betrugs wurden, haben 85 % durch den Betrug Geld verloren.
  - Deutsche berichten von einem durchschnittlichen Verlust von 1.283 Euro durch Online-Betrug
  - 34 % verloren über 480 Euro
  - 4 % verloren über 9.610 Euro
  - Der durchschnittliche Verlust ist in der Gruppe der 55- bis 64-Jährigen am höchsten (1.730 Euro).
  - Jüngere Befragte (18–24 Jahre) melden die niedrigsten durchschnittlichen Verluste (1.029 Euro).
- Auf die Frage, wie lange es gedauert hat, bis sie merkten, dass es sich um einen Betrug handelte, gaben Personen, die Opfer eines Online-Betrugs geworden waren, Folgendes an:
  - 12 % gaben 5 Minuten an,
  - 32 % weniger als 30 Minuten,
  - 44 % weniger als eine Stunde,
  - 65 % weniger als 24 Stunden,
  - 90 % weniger als eine Woche,
  - 95 % weniger als einen Monat und
  - 98 % weniger als ein Jahr.

    - Junge Erwachsene erkennen Betrugsversuche am schnellsten, mit durchschnittlich nur 2,1 Tagen bis zur Erkenntnis. 35 % erkannten, dass sie betrogen wurden, in weniger als 30 Minuten, was deutlich höher ist als bei älteren Gruppen.
    - Die Gruppe der 35- bis 44-Jährigen erkennt Betrugsversuche etwas langsamer (16,7 Tage) als jüngere Erwachsene, aber schneller als ältere Gruppen. Die Gruppe der 45- bis 54-Jährigen ist mit einer durchschnittlichen Zeit von 22,9 Tagen bis zur Erkennung eines Betrugs die langsamste von allen.
    - Die Gruppe der 55- bis 64-Jährigen hat die längste durchschnittliche Zeit bis zur Erkennung (30,4 Tage), was auf eine erhöhte Anfälligkeit bei der Betrugserkennung hindeutet. Befragte ab 65 Jahren erkennen Betrug schneller als Befragte im Alter von 55 bis 64 Jahren, mit einer durchschnittlichen Zeit von 12,8 Tagen.
- Opfer von Online-Betrug berichteten, dass der Diebstahl von Geld oder persönlichen Daten oft schnell erfolgte, sobald sie mit einem Betrüger in Kontakt getreten waren. Dies unterstreicht die Dringlichkeit einer schnellen Aufklärung und Maßnahmen zur Vermeidung von Verlusten. Die Umfrage ergab, dass:
    - 13 % angaben, dass es 5 Minuten dauerte,
    - 32 % angaben, dass es weniger als 30 Minuten dauerte,
    - 53 % angaben, dass es weniger als eine Stunde dauerte,
    - 71 % angaben, dass es weniger als 24 Stunden dauerte
    - 84 % sagten, weniger als eine Woche
    - 88 % sagten, weniger als einen Monat
    - 96 % sagten, weniger als ein Jahr
    - Frauen gaben eine höhere durchschnittliche Zeit an, bis ein Betrug „vorbei“ war (36,9 Tage), als Männer (26 Tage), was auf mögliche Verzögerungen bei der Identifizierung oder Eindämmung von Betrugsfällen hindeutet.
    - Betrugsfälle bei jungen Erwachsenen wurden im Durchschnitt viel schneller aufgeklärt (12,1 Tage), wobei 35 % der Befragten angaben, dass der Fall innerhalb von 30 Minuten und 22 % innerhalb von 1 Stunde aufgeklärt wurde.
- 37 % der Deutschen, die Opfer eines Online-Betrugs wurden, wurden innerhalb von 12 Monaten Opfer eines weiteren Online-Betrugs.
    - Die Altersgruppen der 18- bis 24-Jährigen (57 %) und der 25- bis 34-Jährigen (62 %) weisen die höchsten Raten an wiederholter Viktimisierung auf.
    - Bei den Befragten im Alter von 45 bis 54 Jahren (22 %), 55 bis 64 Jahren (31 %) und 65+ (29 %) ist die Wahrscheinlichkeit einer wiederholten Viktimisierung deutlich geringer.

Die psychischen Auswirkungen von Betrug

- Auf die Frage nach ihren Erfahrungen und Gefühlen in Bezug auf Betrug in den letzten 12 Monaten
    - 47 % der Befragten sind jetzt vorsichtiger beim Öffnen von E-Mails oder Nachrichten von unbekannten Absendern als noch vor 12 Monaten.
        - Ältere Altersgruppen, insbesondere 55–64-Jährige (53 %) und 65 Jahre+ (55 %), geben deutlich häufiger an, beim Öffnen von Nachrichten von unbekannten Absendern vorsichtiger zu sein als jüngere Gruppen wie 18–24-Jährige (28 %) und 25–34-Jährige (40 %).
    - Proaktives Verhalten ist offensichtlich: 18 % unternehmen Schritte, um sich über das Erkennen und Vermeiden von Betrugsfällen zu informieren, und 42 % geben an, dass sie sofort melden würden, wenn sie Opfer eines Betrugs geworden sind.
        - Jüngere Befragte im Alter von 18 bis 24 Jahren (51 %) und 35 bis 44 Jahren (51 %) geben am ehesten an, dass sie sofort melden würden, wenn sie Opfer eines Online-Betrugs geworden sind, im Vergleich zu 41 % der Gruppe 65 Jahre+.
    - Die Sorgen erstrecken sich auch auf Angehörige, wobei 27 % befürchten, dass Familienmitglieder oder Freunde auf Betrug hereinfallen könnten.
    - 32 % sind der Meinung, dass ihre persönlichen Daten online heute einem größeren Risiko ausgesetzt sind als noch vor einem Jahr, was die wachsen-de Wahrnehmung der Verwundbarkeit in der digitalen Landschaft unter-streicht.
    - Die Auswirkungen ausgeklügelter Betrugsmaschen sind offensichtlich: 13% sind auf Betrugsversuche gestoßen, die als legitime Nachrichten von vertrauenswürdigen Organisationen getarnt waren, und 15 % haben eine Zunahme von KI-gesteuerten Betrugsmaschen wie gefälschten Videos oder Sprachnachrichten bemerkt.
    - 10 % haben eine Zunahme von Online-Betrügereien erlebt und beobachtet.
    - Trotz erhöhter Vorsicht fühlen sich 12 % im Vergleich zum Vorjahr weniger sicher, Betrügereien zu erkennen, während 7 % zugeben, dass sie sich schämen würden, wenn sie Opfer eines Betrugs würden.
- 30 % der Deutschen gaben an, dass es sie mäßig bis erheblich belastete, auf einen Online-Betrug hereinzufallen. Dies reichte von mäßiger Angst oder anhaltenden Schamgefühlen bis hin zu Depressionen oder schwerer Angst.
- 74 % der Deutschen gaben an, dass es sich auf ihr Selbstwertgefühl oder ihr Vertrauen in ihre Fähigkeit, Betrugsversuche zu erkennen und/oder anderen

zu vertrauen, auswirkte, wenn sie auf einen Online-Betrug hereingefallen waren.

Trends bei Betrugsnachrichten

- 53 % der Deutschen gaben an, dass sie die meisten Betrugsnachrichten per E-Mail, 15 % per SMS und 21 % über soziale Medien erhalten. 11 % erhielten die meisten Nachrichten auf einer anderen Plattform.
    - Ältere Befragte, insbesondere die Altersgruppen 55–64-Jährige (68 %) und 65 Jahre+ (58 %), geben deutlich häufiger an, dass E-Mails das Hauptmedium für den Erhalt von Betrugsnachrichten sind, als jüngere Gruppen wie 18–24-Jährige (33 %) und 25–34-Jährige (34 %).
    - Befragte im Alter von 25 bis 34 Jahren (40 %) und 18 bis 24 Jahren (31 %) geben viel häufiger Social-Media-Plattformen als Hauptquelle für Betrugsnachrichten an als ältere Gruppen wie 55 bis 64 Jahre (8 %) und 65 Jahre + (14 %).
    - Jüngere Altersgruppen wie 18–24-Jährige (26 %) und 25–34-Jährige (19 %) geben häufiger an, betrügerische Nachrichten per Textnachricht erhalten zu haben, als ältere Gruppen, bei denen diese Quelle deutlich seltener ist (z. B. 10 % bei 55–64-Jährigen).
- Die durchschnittliche Person in Deutschland sieht täglich durchschnittlich 10 betrügerische Nachrichten und Deepfakes in sozialen Medien sowie per Textnachricht und E-Mail. Darin enthalten sind:
    - 2,4 Betrugsnachrichten über soziale Medien pro Tag.
        - Die meisten Betrugsnachrichten erhalten Befragte im Alter von 25 bis 34 Jahren und 35 bis 44 Jahren, durchschnittlich 3,3 pro Tag. Im Gegensatz dazu berichten Befragte im Alter von 55 bis 64 Jahren und 65+ von viel niedrigeren Durchschnittswerten (1,7).
    - 2,2 Deepfake-Videos täglich online.
        - Die Befragten im Alter von 18 bis 24 Jahren berichten von der höchsten durchschnittlichen Exposition, wobei sie täglich 3,7 Deepfake-Videos sehen, gefolgt von 25 bis 34 Jahren mit 3,4.
        - Die durchschnittliche Anzahl der gesehenen Deepfake-Videos nimmt in den Altersgruppen stetig ab, wobei die Gruppe der über 65-Jährigen den niedrigsten Tagesdurchschnitt (1,4) angibt.
        - Jüngere Befragte (18–24 und 25–34) sehen mit größerer Wahrscheinlichkeit täglich 20+ Deepfake-Videos; in älteren Altersgruppen kommt dies fast nicht vor.
    - 2 betrügerische SMS-Nachrichten täglich.
        - Jüngere Altersgruppen, insbesondere 18–24 (durchschnittlich 2,3) und 25–34 (durchschnittlich 2,6), melden eine höhere

Anzahl an betrügerischen SMS-Nachrichten pro Tag als ältere Gruppen wie 55–64 (durchschnittlich 1,5) und 65+ (durchschnittlich 1,9).
    - 3,4 betrügerische E-Mails pro Tag.
        - Die Altersgruppe der 35- bis 44-Jährigen meldet die höchste durchschnittliche Anzahl betrügerischer E-Mails pro Tag (5,2 E-Mails), die deutlich über der anderer Altersgruppen liegt.
        - Ältere Gruppen wie 65+ und 55–64 melden niedrigere Durchschnittswerte (2,9 bzw. 3,1 E-Mails).
        - Die Gruppe der 35- bis 44-Jährigen ist besonders anfällig für eine höhere Anzahl von Betrugs-E-Mails: 9 % erhalten täglich 20+ und 11 % täglich 5 E-Mails.
    - Auf die Frage, wie viel Prozent der Deepfake-Videos, die sie gesehen haben, sie für Betrug hielten, gaben 26 % weniger als 25 % an, 48 % etwa die Hälfte, 15 % zwischen 50 und 75 % und 10 % mehr als 75 %.
- 48 % der Menschen sind auf Facebook auf Deepfakes gestoßen, 39 % auf Instagram, 27 % auf TikTok, 13 % auf X, 13 % auf Snapchat, 31 % auf WhatsApp, 15 % auf Telegram, 6 % auf LinkedIn, 7 % auf Discord, 2 % auf BlueSky und 10 % auf einer anderen Plattform.
    - Männer (21 %) sind deutlich häufiger als Frauen (5 %) mit Deepfakes auf Twitter konfrontiert.
    - 67 % der 45- bis 54-Jährigen und 53 % der 55- bis 64-Jährigen (53 %) haben Deepfakes auf Facebook gesehen.
    - Instagram wird von jüngeren Altersgruppen häufiger als Ort genannt, an dem sie Deepfakes gesehen haben, wobei der höchste Anteil bei den 18- bis 24-Jährigen (50 %) und den 25- bis 34-Jährigen (52 %) liegt.
    - TikTok folgt einem ähnlichen Trend, wobei der höchste Prozentsatz der Personen, die Deepfakes auf der Plattform gesehen haben, bei den 18- bis 24-Jährigen (44 %) und den 25- bis 34-Jährigen (42 %) liegt.
- 36 % der Deutschen sind auf gefälschte (betrügerische) Social-Media-Nachrichten auf Facebook, 28 % auf Instagram, 17 % auf TikTok, 8 % auf X, 8 % auf Snapchat und 15 % auf einer anderen Plattform gestoßen.
- Auf die Frage, welche Art von Betrugsnachrichten sie erhalten haben:
    - Gefälschte Versandbenachrichtigung – Behauptet, ein Paket sei verspätet oder nicht zustellbar, mit einem Link zur „Lösung“ des Problems (35 %).
    - Gefälschte Zustellbenachrichtigung – Behauptet, Sie hätten ein Paket verpasst und fordert Sie auf, auf einen bösartigen Link zu klicken, um die Zustellung neu zu planen (31 %).

- Betrug bei der Kontoverifizierung – Behauptet, Ihr Konto (z. B. Google, PayPal) werde gesperrt, wenn Sie nicht auf einen Link klicken und Ihre Daten eingeben (25 %).
- Lotterie- oder Preisbetrug – Behauptet, Sie hätten einen Preis gewonnen, verlangt aber eine Zahlung oder persönliche Informationen, um den Preis zu erhalten (23 %).
- Betrug mit Bankwarnungen – Gibt vor, Ihre Bank zu sein, warnt vor verdächtigen Aktivitäten und fordert Sie zur Kontoverifizierung auf (21 %).
- Betrügerische Bank: Gibt sich als Ihre Bank aus und fordert Anmeldedaten oder persönliche Informationen an, um Ihr Konto zu „sichern“ (21 %).
- Gefälschte Nachrichtenvideos: Verbreitet erfundene Nachrichten, in denen um Spenden oder persönliche Unterstützung gebeten wird (20 %).
- Betrug mit familiären Notfällen: Behauptet, ein geliebter Mensch sei in Schwierigkeiten und brauche dringend Geld (18 %).
- Betrug mit gefälschten Rechnungen – Es werden Rechnungen für Produkte oder Dienstleistungen gesendet, die Sie nicht bestellt haben, und Sie werden unter Druck gesetzt, diese zu bezahlen (18 %).
- „Hey, wie geht es dir?“-Betrug – Ein Fremder sendet eine freundliche SMS und bittet Sie nach einem Gespräch um Geld für eine gefälschte Investition oder einen Liebesbetrug (18 %).
- Sonderangebot oder Deal – Es werden massive Rabatte oder Gratisgeschenke versprochen, aber die E-Mail enthält Links zu Phishing-Websites (18 %).
- Betrug bei der Abonnementverlängerung – Es wird gewarnt, dass ein Abonnement (z. B. Netflix, Amazon) abläuft, und um Zahlung für die Verlängerung gebeten (15 %).
- Betrug bei der Abonnementverlängerung – Sie werden aufgefordert, die Zahlungsdaten für ein Abonnement wie Streaming-Dienste oder Antivirensoftware zu aktualisieren (13 %).
- Produktwerbung oder Werbegeschenke von Prominenten – Es wird ein gefälschtes Video von einem Prominenten gezeigt, der ein Produkt bewirbt oder ein Werbegeschenk veranstaltet, um Zahlungsdaten zu stehlen (13 %).
- Betrug mit Social-Media-Konten – Es wird vorgegeben, dass die Nachricht von Plattformen wie Facebook oder Instagram stammt, und Sie werden aufgefordert, Ihr Konto zu verifizieren (13 %).
- Betrug mit Krediten oder Finanzdienstleistungen – Es werden gefälschte Finanzberatungen oder -dienstleistungen über ausgefeilte KI-generierte Videos angeboten (12 %).

- Betrug mit Spenden für wohltätige Zwecke – Katastrophen oder Tragödien werden ausgenutzt, um per SMS um Spenden für gefälschte Wohltätigkeitsorganisationen zu bitten (10 %).
- Betrug durch technischen Support – Es wird vorgegeben, von einem Technologieunternehmen zu stammen, und behauptet, Ihr Telefon sei mit einem Virus infiziert, und es wird um Fernzugriff oder Zahlung für eine „Reparatur" gebeten (10 %).
- E-Mail-Betrug durch technischen Support – Es wird vorgegeben, von einem Technologieunternehmen zu stammen, vor Sicherheitsverletzungen gewarnt und um Fernzugriff gebeten (9 %).
- Betrug durch gefälschte Umfragen – Es wird eine Belohnung für die Beantwortung einer Umfrage angeboten, aber um Kreditkartendaten gebeten, um den Preis zu erhalten (9 %).
- Betrug mit gefälschten Identitätsvideos: Gefälschte Live- oder aufgezeichnete Videos von Personen, die Sie kennen, bitten um Geld oder sensible Informationen (9 %).
- Spenden- oder Wohltätigkeitsbetrug – Es wird fälschlicherweise behauptet, eine Wohltätigkeitsorganisation oder Hilfsaktion zu vertreten, und um Spenden gebeten (9 %).
- Betrug mit Kryptowährungsinvestitionen – Es werden Deepfake-Videos von Persönlichkeiten des öffentlichen Lebens verwendet, die „garantierte" Renditen anpreisen, um Opfer dazu zu verleiten, in gefälschte Systeme zu investieren (9 %).
- Betrug mit Stellenangeboten – Es werden hoch bezahlte Fernarbeitsplätze versprochen, aber persönliche Informationen, die Bezahlung von Schulungen oder andere Vorabkosten verlangt (8 %).
- Betrug per geschäftlicher E-Mail – Es wird vorgegeben, Ihr Chef oder Kollege zu sein, und um Überweisungen oder sensible Daten gebeten (8 %).
- Betrug durch KI-Stimmenklon – Die Stimme eines geliebten Menschen wird in einem Video simuliert, um gefälschte Notfälle überzeugender zu machen (7 %).
- Betrug durch Steuerrückerstattung – Es wird behauptet, dass Ihnen eine Steuerrückerstattung zusteht, und um Ihre Daten gebeten, um diese zu bearbeiten (6 %).
- Betrug durch Versorgungsunternehmen – Es wird damit gedroht, die Strom- oder Wasserversorgung zu unterbrechen, wenn Sie nicht sofort bezahlen (5 %).
- Betrug mit der Fahrzeuggarantie – Es wird fälschlicherweise behauptet, dass Ihre Fahrzeuggarantie abläuft, und Sie werden unter Druck gesetzt, sie zu verlängern (5 %).

Betrugserkennung, -prävention und -lösung

- 27 % der Deutschen sind im letzten Jahr Opfer eines SMS-Betrugs geworden, 31 % eines E-Mail-Betrugs und 22 % eines Betrugs mit gefälschten Videos.

Betrug mit Textnachrichten (SMS)

- 56 % der Deutschen geben an, zu wissen, wie sie sich vor SMS-Betrug schützen können. 44 % sagen, dass sie nicht sicher sind, ob sie alles richtig machen, um sich zu schützen, oder nicht wissen, wie sie sich vor diesen Betrugsmaschen schützen können.

- 70 % der Deutschen geben an, dass sie zuversichtlich sind, SMS-Betrug zu erkennen, da die Betrugsmaschen sehr offensichtlich und leicht zu erkennen sind. 30 % gaben an, dass sie sich nicht sicher sind, da die Betrugsnachrichten immer ausgefeilter und schwieriger zu erkennen sind.

E-Mail-Betrug

- 71 % der Deutschen sind sich sicher, dass sie E-Mail-Betrug erkennen können, da die Betrugsversuche sehr offensichtlich und leicht zu erkennen sind. 29 % gaben an, dass sie sich nicht sicher sind, da die Betrugsnachrichten immer ausgefeilter und schwieriger zu erkennen sind.

- 53 % der Deutschen geben an, zu wissen, wie sie sich vor E-Mail-Betrug schützen können. 47 % sagen, dass sie nicht sicher sind, ob sie alles richtig machen, um sich zu schützen, oder nicht wissen, wie sie sich vor diesen Betrugsmaschen schützen können.

Deepfake-Video-Betrug

- 62 % der Deutschen geben an, dass sie zuversichtlich sind, Deepfake-Video-Betrug erkennen zu können, da die Betrugsmaschen sehr offensichtlich und leicht zu erkennen sind. 38 % gaben an, dass sie sich nicht sicher sind, da Deepfake-Betrügereien immer ausgefeilter und schwieriger zu erkennen sind.

- Auf die Frage, ob sie Deepfakes in den sozialen Medien erkennen können, gaben 70 % an, dass sie dies können, und 30 % waren sich nicht sicher.

- Von denjenigen, die auf ein gefälschtes Profil, eine Anzeige, ein Foto oder ein Video stießen, das KI-generiert zu sein schien, und feststellten, dass es gefälscht oder manipuliert war:

- 29 % erkannten dies, weil die Behauptungen übertrieben waren – zum Beispiel Anzeigen, die unrealistische Rabatte, Vorteile oder Ergebnisse ohne klare Details versprachen.
- 26 % erkannten dies, weil Produkte oder Personen verzerrt aussahen, ungewöhnliche Texturen aufwiesen oder seltsame Proportionen hatten, die nicht real wirkten, oder weil es unscharfe Hintergründe oder ungewöhnliche Schatten oder Reflexionen gab.
- 34 % bemerkten dies, weil die Links auf der Website verdächtig aussahen oder nicht zu einer offiziellen Unternehmens- oder persönlichen Domain passten.
- 30 % bemerkten dies, weil das Bild oder Video zu perfekt schien, um wahr zu sein.
- 23 % bemerkten dies, weil der Ton zu allgemein oder roboterhaft war oder nicht zum Kontext des Videos passte.
- 25 % bemerkten dies, weil der Ton nicht mit den Lippenbewegungen synchronisiert war oder der Ton unnatürlich klang.
- 24 % bemerkten dies, weil das Branding von schlechter Qualität war oder nicht zum Inhalt passte.
- 16 % bemerkten dies, weil sie eine Rückwärtssuche durchführten und das Original fanden.

Lösung

- Die Deutschen verbrachten durchschnittlich 1,3 Monate damit, die Probleme zu lösen, die durch das Aufgehen auf einen Online-Betrug entstanden waren. Dies umfasst:
- 23 % verbrachten weniger als einen Tag
- 41 % verbrachten weniger als eine Woche
- 81 % weniger als einen Monat
- 98 % weniger als ein Jahr

- Die durchschnittliche Person in Deutschland verbringt 1,6 Stunden pro Woche damit, zu überprüfen, zu verifizieren oder zu entscheiden, ob eine per Textnachricht, E-Mail oder über soziale Medien gesendete Nachricht echt oder gefälscht ist. Das sind 83,2 Stunden pro Jahr.

Umfragemethodik

Die Umfrage, die sich auf das Thema Deepfakes, betrügerische Text- und E-Mail-Nachrichten und die Auswirkungen dieser Betrugsversuche auf Verbraucher konzentrierte, wurde im Dezember 2024 online durchgeführt. 5.000 Erwachsene ab 18 Jahren in 7 Ländern (USA, Deutschland, Großbritannien, Frankreich, Deutschland, Japan) nahmen an der Studie teil.