

# Vorsicht Manipulation: Betrugsmaschen am Telefon

Verbraucher Cybersicherheit



Tanja Beller

Immer wieder kommt es zu den verschiedensten Betrugsversuchen per Telefon. Von Schockanrufen (siehe **Enkeltrick**), über aufgedrängte Vertragsabschlüsse bis zu vermeintlichen „Serviceanrufen“. Häufig geht es den Kriminellen darum, an sensible Informationen wie die Bankverbindung zu kommen.

„Ihr Konto wurde aus Sicherheitsgründen geblockt.“ Oder: „Es gibt ein Problem mit Ihrem Computer.“ Die Betrüger geben sich beispielsweise als Bankangestellte aus, als Mitarbeiter der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), als Ermittler von Europol oder Interpol, oder aber sie behaupten, sie seien vom technischen Support eines Softwareunternehmens. Die Masche ist bekannt: Seriöse Unternehmen dienen als Einstieg in ein Telefonat, das nur darauf abzielt, Ihr Vertrauen zu gewinnen oder Sie unter Druck zu setzen.

Aus „Sicherheitsgründen“ oder um angeblich die Online-Banking-Funktionen wieder herzustellen, sollen dabei die Kontodaten oder andere persönliche Daten, wie die Adresse, „abgeglichen“ werden. Alternativ wird auch „Hilfe“ bei der Umstellung auf ein anderes TAN-Verfahren angeboten. In einigen Fällen versuchen Kriminellen, über eine Fernwartungssoftware Zugang zum Computer zu erhalten. Ziel ist es, das Opfer so zu manipulieren, dass es unbeabsichtigt eine Zahlung per TAN freigibt.

## Vorsicht vor manipulierten Telefonnummern

Auf dem Display des Telefons erscheint vermeintlich die Nummer einer Bank oder des Kundenservices eines Softwareunternehmens. Tatsächlich ist diese Rufnummernanzeige manipuliert. Lassen Sie sich von der Anzeige der Telefonnummer nicht in die Irre führen. Fragen Sie den Anrufer nach seinem Namen, sagen Sie ihm, dass Sie sich melden werden, und legen Sie vorsichtshalber auf.

Recherchieren Sie selbst auf der korrekten Unternehmenswebseite. Nutzen Sie für den Rückruf nicht die am Telefon genannte oder die im Display angezeigte Telefonnummer, weil Sie dann wieder direkt bei den Betrügern landen können

## Fremde nicht auf den Rechner zugreifen lassen

Spätestens, wenn der Anrufer einen vermeintlichen Fehler auf Ihrem Computer beheben oder das geblockte Konto „entsperren“ will und Ihnen dabei ankündigt, dass er auf Ihren Computer von extern zugreifen muss, sollten bei Ihnen alle Alarmglocken schrillen! Vordergründig geht es um Hilfe, tatsächlich aber um die Übernahme Ihres Computers.

Besonders vertrauenswürdig wirkt die Betrugsmethode, wenn Sie bereits einige Tage zuvor eine Mail mit einem Link angeblich von Ihrer Bank, erhalten haben (Phishing-Mail). Ruft Sie nun noch jemand als angeblicher Bankmitarbeiter an, erzeugt dieses Zusammenspiel von Mail und Telefonat oftmals den Eindruck einer scheinbaren Seriosität. Das Opfer der Kriminellen ist eher geneigt, dem Anrufer zu vertrauen.

Im Laufe des Gesprächs gibt es dann eine Aufforderung, den Link

aus der Mail anzuklicken. Eine beispielhafte Redewendung hierfür ist: „Sie können natürlich auch zu uns in die Filiale kommen. Aber wenn Sie möchten, kann ich auch gleich von hier den Fehler korrigieren.“

Auch hier gilt: Folgen Sie keinem Link und laden Sie sich kein Programm herunter, selbst wenn der Anrufer auf Sie einen sehr sympathischen und vertrauenserweckenden Eindruck macht.

## Nicht unter Druck setzen lassen

Egal, welche Szenarien der Anrufer schildert: Wichtig ist, dass Sie ruhig und besonnen bleiben und sich nicht unter Druck setzen lassen. Der Kriminelle wird möglicherweise alle Register ziehen: Er könnte beispielsweise behaupten, dass Ihnen eine Kontosperrung drohe, dass Sie finanzielle Einbußen erleiden würden. Aber auch wenn er Ihnen mit einem Rechtsanwalt, einem Inkassobüro oder mit strafrechtlichen Konsequenzen droht: Lassen Sie sich nicht einschüchtern!

Er könnte aber genauso gut an Ihr Verantwortungsgefühl appellieren, indem er Sie um Mithilfe bei der Verbrechensbekämpfung oder Ähnliches bittet.

Auch eine sehr freundliche und vertrauensvolle Atmosphäre sollte Sie nicht verleiten, aktiv zu werden. Ziel ist zu jeder Zeit, Sie zum Handeln zu bewegen: dem Link zu folgen, Ihre Daten einzugeben, eine Fernwartungssoftware herunterzuladen oder auf anderem Wege an Ihre persönlichen Daten zu gelangen. Legen Sie im Zweifel einfach auf. Und falls Sie sich unsicher sind, ob doch etwas an der Geschichte wahr sein könnte, können Sie immer

selbst Ihre Bank oder die angegebene Polizeidienststelle zurückrufen und den Sachverhalt klären.

## Persönliche Daten nicht preisgeben

Gehen Sie stets verantwortungsvoll und möglichst sparsam mit persönlichen Daten um. Dazu zählen neben Konto- und Kartendaten, PINs und TANs auch die Adresse, Telefonnummern oder das Geburtsdatum. Überlegen Sie stets, ob diese Informationen für den beabsichtigten Vorgang überhaupt benötigt werden. Bei betrügerischen Anrufen kann es auch sein, dass den Kriminellen einige Informationen bekannt sind, aber weitere bestätigt werden sollen. Lassen Sie sich nicht in die Irre führen.

## Rufnummern blockieren

SPAM-Anrufe können Sie blockieren und auch dem Provider und der Bundesnetzagentur melden. Die Bundesnetzagentur nimmt Beschwerden auf ihrer [Website](#) entgegen. Neben belästigenden Anrufen auch zu sogenannten „Ping-Anrufen“, nicht verlangten SMS- oder Nachrichten über Messenger-Diensten, E-Mail-Spam oder Rufnummernmanipulationen.

Bei einem „Ping-Anruf“ wird nach einmaligen Klingeln gleich aufgelegt. Beim Rückruf meldet sich niemand persönlich. Dass man in einer Kostenfalle gelandet ist, zeigt sich dann erst auf der nächsten Telefonrechnung.

## Strafanzeige erstatten

Wichtig: Wenden Sie sich bei jeglichem Missbrauch Ihrer Bankdaten – und auch schon bei einem Verdacht – umgehend an Ihre Bank. Kontaktieren Sie zudem die Polizei und erstatten Sie Strafanzeige. Nur wenn der Betrug angezeigt wurde, kann er auch strafrechtlich verfolgt und den Kriminellen das Handwerk gelegt werden.

## Links

---

[Lexikon Cybersecurity](#)

---

## Ansprechpartnerin



Kontakt

Tanja Beller

Pressesprecherin

+49 (30) 1663 1220

E-Mail senden

---

# Gefälschte Stimmen: Fünf Tipps gegen Betrug mit KI

Digitalisierung Cybersicherheit Verbraucher



Kathleen Altmann

Stellen Sie sich vor, Sie hören die vermeintliche Stimme Ihres Kindes am Telefon: „Mama, ich hatte einen Unfall. Sie lassen mich erst gehen, wenn ich eine Kaution hinterlege. Hilf mir, schnell!“ Der Missbrauch künstlicher Intelligenz kann betrügerische Anrufe auf ein neues Level heben. Die gute Nachricht: Mit ein paar Tipps können Sie sich schützen.

Allerdings wird es mit der Weiterentwicklung der KI-Technologie immer schwieriger, solche betrügerischen Anrufe sofort zu durchschauen. Denn: Die Stimmen von Verwandten oder Freunden können damit täuschend echt imitiert werden. Als Angerufener kann man den Unterschied kaum feststellen. Hinzu kommt der Überraschungseffekt, der das Opfer dazu verleitet, sofort zu handeln und möglicherweise das Geld gleich zu überweisen. Oft bleiben die Opfer auf dem finanziellen Schaden sitzen.

# So kommen die Täter an die Stimmen

An die Stimmen kommen die Kriminellen zum Beispiel durch Schadsoftware, mit der sie sich Zugang zu mobilen Endgeräten verschaffen, um Gespräche aufzuzeichnen.

Diese können sie entweder sofort verwenden oder zum Training von KI-Anwendungen nutzen. Für das Training von KI-Systemen werden nur wenige Minuten Audiomaterial des Originals benötigt.

## Die Zukunft: Betrug bei Videotelefonaten

Eine mögliche Zukunft dieser Betrugsmasche könnten Videoanrufe mit ähnlichem Inhalt sein. Hierbei könnten Kriminelle KI-Technologien nutzen, um neben der Stimme auch Mimik und Gestik zu fälschen, also sogenannte Deep Fakes einsetzen. Dazu werden beispielsweise Videoaufnahmen als Vorlage verwendet und lippensynchron aufbereitet.

## Fünf Tipps für Ihren Schutz

1. Lassen Sie sich am Telefon nicht unter Druck setzen und rufen Sie den vermeintlichen Anrufer unter der Ihnen bekannten Nummer zurück.
2. Achten Sie auf kleine Unstimmigkeiten in der Stimme oder abgehackte Wörter. Achten Sie auch auf die individuellen

Besonderheiten in der Aussprache, beispielweise ein bestimmter Dialekt, ein Akzent oder Wörter, die die Ihnen bekannte Person üblicherweise verwendet, oder eben nicht.

3. Wichtig: Vereinbaren Sie ein Familienpasswort! Das sollte ein Codewort sein, das jedes Familienmitglied kennt und das am Telefon abgefragt werden kann.
4. Alternativ kann am Telefon auch eine Frage gestellt werden, die der Anrufer nur beantworten kann, wenn er tatsächlich das betreffende Familienmitglied ist.
5. Das Wissen um die Möglichkeit eines solchen Angriffs hilft dabei, wachsam zu sein. Sprechen Sie daher mit Ihren Angehörigen und Freunden und informieren Sie sie über diese Betrugsszenarien.

## Links

---

## Lexikon Cybersecurity

---



Kontakt

Kathleen Altmann

Pressesprecherin

+49 (30) 1663 1286

E-Mail senden

