

Informationen zu verdächtigen Nachrichten und Betrug

Es ist unsere oberste Priorität, einen sicheren Raum für unsere Benutzer*innen zu schaffen, in dem sie miteinander kommunizieren können. Daher arbeiten wir unablässig daran, Spam oder unerwünschte Nachrichten, die über WhatsApp gesendet werden, zu reduzieren. Es ist jedoch genau wie auch bei SMS oder Telefonanrufen möglich, dass du von anderen WhatsApp-Benutzer*innen, die deine Telefonnummer in ihrem Telefon gespeichert haben, kontaktiert wirst. Möglicherweise hast du diese Personen in deinen Kontakten gespeichert, vielleicht aber auch nicht.

Manche Personen senden dir möglicherweise Nachrichten, um dich dazu zu verleiten, persönliche oder finanzielle Informationen mit ihnen zu teilen, oder weil sie Fehlinformationen verbreiten möchten. Scams können überall passieren und alle betreffen. Du kannst dein Konto jedoch schützen, wenn du weißt, wonach du Ausschau halten musst.

Verdächtige Nachrichten erkennen

Es gibt bestimmte Anhaltspunkte, an denen du verdächtige Nachrichten erkennen kannst oder die darauf hindeuten, dass der*die Absender*in nicht vertrauenswürdig ist. Halte nach diesen Anzeichen Ausschau:

- Die Nachricht enthält Rechtschreib- oder Grammatikfehler.
- Du wirst aufgefordert, einen Link zu öffnen, über einen Link neue Funktionen zu aktivieren oder eine App herunterzuladen.
- Du wirst gebeten, persönliche Informationen zu teilen, beispielsweise Kreditkarten- oder Kontonummern, dein Geburtsdatum oder Passwörter.
- Du sollst eine Nachricht weiterleiten.
- Du wirst um Geld gebeten oder es wird behauptet, dass du für die Nutzung von WhatsApp zahlen musst.
- Der*Die Betrüger*in behauptet, mit dir bekannt zu sein.
- In der Nachricht geht es um eine Lotterie, ein Glücksspiel, einen Job, eine Investition oder einen Kredit.

- Die Person beginnt eine Unterhaltung mit dir, um dein Vertrauen zu gewinnen, bevor sie dich nach persönlichen Informationen fragt.

Wenn du zum ersten Mal eine Nachricht von einer Person erhältst, die nicht in deinen Kontakten gespeichert ist, zeigen wir dir in der Nachricht Details, anhand derer du über deine weitere Vorgehensweise entscheiden kannst. Mithilfe dieser Details kannst du feststellen, ob ihr gemeinsame Gruppen habt und ob die Telefonnummer der Person in einem anderen Land registriert ist. Mit diesem Wissen kannst du entscheiden, ob du antwortest, die Person als Kontakt hinzufügst oder sie blockierst bzw. meldest.

In einigen Situationen zeigen wir dir möglicherweise zusätzliche Informationen an, wenn du jemanden zum ersten Mal kontaktierst. Wir zeigen diese Tools an, wenn du zum ersten Mal mit jemandem chattest, der nicht in deinen Kontakten gespeichert ist und den du möglicherweise nicht kennst. In diesem Fall stellen wir dir zusätzliche Details zur Verfügung, ob ihr gemeinsame Gruppen habt und ob die Telefonnummer der Person in einem anderen Land registriert ist. Du kannst dann eine fundierte Entscheidung treffen, ob du den Chat fortsetzen oder abbrechen möchtest.

Hinweis: WhatsApp ist eine kostenlose App. Du musst also nichts bezahlen, um sie zu nutzen. Wenn jemand eine Zahlung für die Nutzung von WhatsApp verlangt oder anbietet, den Ausschluss deines WhatsApp-Kontos gegen Bezahlung aufzuheben, geht es dieser Person wahrscheinlich um deine finanziellen oder personenbezogenen Informationen.

Best Practices bei verdächtigen Nachrichten

Setze auf diese Best Practices, um dich zu schützen:

- Wenn eine Nachricht dir verdächtig oder „zu schön, um wahr zu sein“ vorkommt, tippe nicht darauf, teile sie nicht und leite sie nicht weiter. Wenn du eine verdächtige Nachricht identifizierst, erfährst du [hier](#) mehr darüber, wie du dich schützen kannst.
- Als Best Practice hat sich bewährt: Wenn du nicht sicher bist, ob etwas wahr ist, oder du nicht weißt, wer die Nachricht verfasst hat, leite sie nicht weiter. Mehr zur Vermeidung von Fehlinformationen erfährst du [hier](#).
- Sieh dir einen Link bzw. eine Datei genau an, bevor du ihn bzw. sie öffnest. Auf den ersten Blick mögen Links und Dateien seriös wirken, sie können jedoch schädlich sein. Erfahre mehr über verdächtige Dateien und Links in [diesem Artikel](#).
- Wenn du an der Identität eines unbekannten Kontakts zweifelst, stelle persönliche Fragen, um seine Identität

zu bestätigen. Du kannst auch einen Sprach- oder Videoanruf tätigen, um die Identität der Person zu bestätigen.

- Alternativ kannst du die Nachricht melden, die Person blockieren und die Nachricht löschen. Mehr zum Blockieren und Melden von Kontakten oder unbekannten Nummern erfährst du in [diesem Artikel](#).

Wenn du eine verdächtige Nachricht von einem bekannten Kontakt erhältst, könnte sein Konto gehackt worden sein.

Mehr über gehackte Konten erfährst du in [diesem Artikel](#).

Gängige Beispiele für Betrug

Wenn du gängige Betrugsmaschen kennst, kannst du Betrüger*innen leichter erkennen und dich schützen. Jemand, der versucht, dich zu betrügen, könnte dir eine Nachricht senden, dich anrufen oder dich einer Gruppe hinzufügen. Nachfolgend findest du einige gängige Betrugstaktiken:

Romantik- oder Beziehungsbetrug: Manche Betrüger*innen geben vor, eine Beziehung oder emotionale Verbindung zu dir aufzubauen, und bitten dich dann um Geld oder ein Darlehen. Sie könnten auch Pläne für ein Treffen machen und diese dann kurzfristig absagen.

Beschäftigungsbetrug: Du könntest auch gefälschte Stellenangebote von Betrüger*innen erhalten. Jemand könnte sich als Personalvermittler*in eines bekannten Unternehmens ausgeben, um dich dazu zu bringen, persönliche Informationen preiszugeben, oder im Rahmen einer Bewerbung um Geld bitten. Dazu gehören oft gut bezahlte Stellenangebote und Arbeitsmöglichkeiten im Homeoffice.

Anlagebetrug: Ein*e Betrüger*in könnte dir eine gefälschte Investitionsmöglichkeit mit dem Versprechen eines geringen Risikos und hoher Renditen anbieten, um dich dazu zu ermutigen, persönliche Informationen oder Geld weiterzugeben. Diese Arten von Betrug konzentrieren sich in der Regel auf Kryptowährungen, Aktien, Anleihen, Güter und Immobilien. Mehr über Online-Anlagebetrug erfährst du [hier](#).

Betrug durch Nachahmung: Betrüger*innen geben sich häufig als Freund*innen oder Familienmitglieder aus, um dich dazu zu bringen, Geld oder persönliche Informationen weiterzugeben. Sie könnten auch vorgeben, eine berühmte Person oder ein bekanntes Unternehmen zu sein.