

RATGEBER – SCHUTZ VOR WHATSAPP-BETRUG

"Hallo Papa, ich habe eine neue Nummer. Speichere sie doch bitte", so oder so ähnlich schreiben Kriminelle ihre Opfer über WhatsApp an. Kurze Zeit später fragen sie nach Geld. Mit solchen Betrugsmaschinen entsteht jährlich ein Gesamtschaden in Millionenhöhe mit Betrug über WhatsApp und anderen Messengern.

WhatsApp: So schützen Sie sich vor Betrug

Ein beliebter Trick bei Internet-Kriminellen ist, sich in einer Nachricht als Sohn, Tochter oder Enkel auszugeben und etwa um Geld für eine Autoreparatur zu bitten. Andere versuchen, an die Registrierungsnummer zu kommen, die Sie bei der Einrichtung von WhatsApp erhalten haben, und damit das Konto zu übernehmen. Und wieder andere geben sich als Polizisten aus, um Sie unter Druck zu setzen. Zahlen Sie, ist das Geld mit hoher Wahrscheinlichkeit weg. "Die Ermittlung der Straftäter ist schwierig, da es oft um relativ geringe Beträge und über Landesgrenzen hinweg geht. Umso wichtiger ist, dass sich jeder Einzelne schützt und absichert", erklärt Harald Schmidt, Geschäftsführer der polizeilichen Kriminalprävention der Länder und des Bundes, die seit 2021 mit WhatsApp zusammenarbeitet, um das Sicherheitsbewusstsein der User zu schärfen. Ausländische Strafverfolger treten bei Einzelfällen, bei denen es "nur" um ein paar Tausend Euro geht, selten in Aktion. Und eine Zuordnung mehrerer Opfer zum selben Täter ist schwierig. Daher müssen Sie selbst aktiv werden und sich schützen:

- Verlangt jemand von Ihnen Geld oder private Daten über WhatsApp, lassen Sie sich die Identität bestätigen, etwa durch eine Sprachnachricht, einen Anruf oder einen Videoanruf. Lehnt der Chatpartner das ab, geben Sie weder Geld noch Daten heraus.
- Geben Sie niemals die Registrierungsnummer weiter, die Sie bei der Einrichtung von WhatsApp als SMS erhalten haben. Diese dient nur dazu, Ihr Konto auf einem Gerät zu aktivieren.
- Richten Sie eine PIN für Ihr WhatsApp-Konto ein (siehe unten). Diese dient als Zwei-Faktor-Authentifizierung.
- Geben Sie Ihr Profilbild nur für Kontakte frei.
- Informieren Sie sich über aktuelle Phishing-Maschen.
- Seien Sie bei unbekanntem Nummern skeptisch. Meldet sich jemand und behauptet, er sei Ihr Sohn und habe ein neues Handy, rufen Sie die alte Nummer an. Oft stimmt das gar nicht und der Betrug fliegt so schnell auf.
- Klicken Sie nicht auf Links, von denen Sie nicht wissen, wohin sie führen.
- Ignorieren Sie Kettenbriefe.
- Prüfen Sie, ob Sie eine Antivirus-App auf Ihrem Android- oder iOS-Gerät nutzen wollen. Die bieten oft zusätzlichen Schutz vor Phishing.

WhatsApp: Zwei-Faktor-Authentifizierung einrichten

Mit einer PIN in WhatsApp schützen Sie Ihr Konto vor Fremdzugriffen. Nur wer Ihre Registrierungsnummer und die PIN kennt, kann Ihr WhatsApp-Konto auf einem Gerät aktivieren. Bei der täglichen Nutzung ändert sich für Sie nichts. So richten Sie die Zwei-Faktor-Authentifizierung ein:

1. Öffnen Sie die Einstellungen in WhatsApp.
2. Klicken Sie auf Konto, Verifizierung in zwei Schritten und Aktivieren.
3. Geben Sie eine sechsstellige PIN ein, bestätigen und notieren Sie sie. Sie brauchen diese PIN immer dann, wenn Sie WhatsApp auf ein anderes Gerät übertragen wollen.
4. Geben Sie Ihre E-Mail-Adresse ein und tippen Sie auf Weiter.
5. Bestätigen Sie die E-Mail-Adresse.

Das sollten Sie tun, wenn Sie Opfer von Betrug geworden sind

Die Kriminellen entwickeln ständig neue Tricks und Maschen und jede und jeder kann darauf hereinfallen. Niemand muss sich dafür schämen. Sie sollten dann aber schnell handeln, um weiteren Schaden zu verhindern. So gehen Sie am besten vor:

- Haben Sie Zahlungsdaten oder Kreditkartennummern weitergegeben oder eine Zahlung veranlasst, melden Sie sich schnellstens beim Anbieter. Der kann Karten sperren und manchmal auch Zahlungen zurückbuchen.
- Hat jemand Ihr WhatsApp-Konto übernommen oder das Telefon gestohlen, schreiben Sie an [Meta](#), den Hersteller von WhatsApp, um das Konto zurückzubekommen.
- Informieren Sie auch Ihre Kontakte, dass jemand anderes möglicherweise Nachrichten in Ihrem Namen verschickt.
- Gab es einen finanziellen Schaden, erstatten Sie Anzeige bei der Polizei. Auch wenn die Aufklärungsrate gering ist: Die Polizei kann nur tätig werden, wenn sie Bescheid weiß. Zudem brauchen Sie diese Anzeige gegebenenfalls bei [Identitätsdiebstahl](#).
- Hat der Betrüger Sie ausgefragt, informieren Sie ebenfalls Ihre Kontakte. Mit den Informationen von Ihnen könnte er neue Betrugsversuche starten.

Auch junge Menschen fallen auf Phishing herein

Internet- und WhatsApp-Betrug zielt auf alle Menschen ab, die im Netz unterwegs sind, die Betrüger unterscheiden nicht nach Altersgruppen. Viele mögen zwar denken, dass hauptsächlich Ältere darauf hereinfallen, das stimmt aber nicht. [Studien](#) zeigen, dass vor allem die junge Generation unvorsichtig ist und auf Phishing-Links klickt. Die Kriminellen nutzen immer raffiniertere Tricks und wirklich niemand ist davor komplett geschützt oder erkennt alles sofort als Betrug.