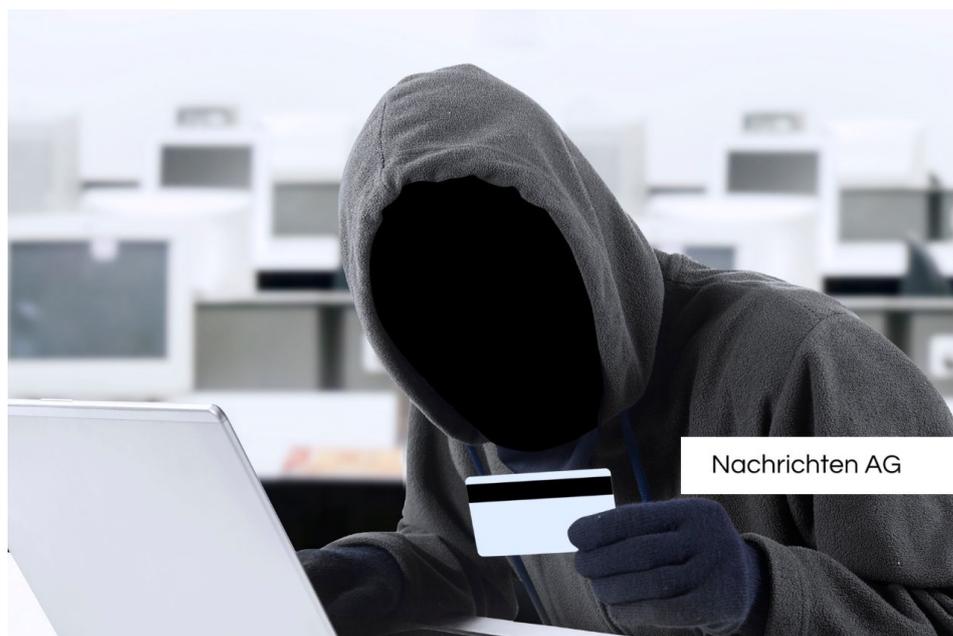


## Achtung! Neue Whatsapp-Betrugsmasche gefährdet Ihre Daten!

Neue Betrugsmasche auf WhatsApp: Cyberkriminelle täuschen Identitäten vor und stehlen persönliche Daten. Vorsicht beim Klicken!



Die Gefahren im digitalen Raum nehmen gefährlich zu, denn Schlüssel zu ungewolltem Zugriff auf persönliche Daten werden zunehmend über das beliebte Kommunikationsmittel WhatsApp geöffnet. Aktuell kursiert eine perfide Betrugsmasche, die zahlreiche Nutzer erschreckt und in die Irre führt. Nutzer erhalten Nachrichten, in denen behauptet wird, dass ihr Konto wegen „illegaler Vorgänge“ gesperrt werden soll. Um dies zu verhindern, wird dazu aufgefordert, einem Link zu folgen, der zu einer vermeintlichen Sicherheitsüberprüfung führt, wie **Berlin Live** berichtet.

### Die Masche des Spoofings

Diese Betrugsversuche, auch als „Spoofing“ bekannt, sind besonders trügerisch, da die Nachrichten von echten WhatsApp-Bestätigungsnummern versendet werden. Dadurch gelangen die Nutzer in die Falle, die Nachricht für echt zu halten. Auf die gefälschte Webseite gelockt, werden die User von einem Chatbot dazu gedrängt, ihre Rufnummer einzugeben und die WHATSAPP-App entsprechend zu manipulieren. Danach erhalten sie einen Sicherheitscode, der es den Cyberkriminellen ermöglicht, den Account zu übernehmen und unbemerkt alle Chats auszulesen oder Nachrichten zu versenden. Deshalb ist es wichtig, bei solchen Anfragen stets skeptisch zu bleiben und keine persönlichen Daten preiszugeben.

Die Gefahren lauern jedoch nicht nur in diesen betrügerischen Nachrichten, sondern auch in der allgemeinen Nutzung von WhatsApp. Um Sicherheitsrisiken zu minimieren, sollten Nutzer regelmäßig die Einstellungen im Menü „Verknüpfte Geräte“ überprüfen. Auf diese Weise kann festgestellt werden, ob unautorisierte Verbindungen zu ihrem Account bestehen. Der Artikel von **Spiegel** verweist darauf, dass Sicherheitsüberprüfungen aus heiterem Himmel häufig auf Phishing-Methoden hindeuten. Wenn eine Nachricht unter dem Namen „WhatsApp“ auftaucht und seltsam erscheint, sollte sofort Misstrauen wachgerufen werden, denn die Absenderkennung kann leicht gefälscht werden.

#### Details

#### Quellen

- [www.berlin-live.de](http://www.berlin-live.de)
- [www.spiegel.de](http://www.spiegel.de)

**Besuchen Sie uns auf: [n-ag.de](http://n-ag.de)**