

31. Mai 2022

## **Betrugsmasche: Achtung vor gefälschten PayPal-Mails**

Wer aktuell eine vermeintliche Mail von PayPal erhält, in der es heißt, dass mit dem PayPal-Konto Zahlungen auf einer Glücksspielseite getätigt wurden, sollte diese keinesfalls öffnen bzw. auf den dort enthaltenen Link klicken. Angeblich könne man die Zahlung noch stoppen, wenn man sich über den enthaltenen Link bei PayPal anmelde, so heißt es in den Mails. Mit dieser aktuellen Masche versuchen Betrüger, die Zugangsdaten und Kreditkarteninformationen von PayPal-Nutzern abzugreifen.

### **Mails verlinken auf gefälschte PayPal-Website**

In den gefakten Mails heißt es beispielsweise: „Wir haben eine Anfrage zur Einzahlung in einem Online-Glücksspielladen mit Ihrer mit Ihrem PayPal-Konto verknüpften Karte erhalten.“ Der in den Mails enthaltene Link leitet die Nutzer auf eine gefälschte PayPal-Seite. Diese ist sehr gut nachgebaut, lässt sich aber anhand der URL „payphelpcenter370172755.info“ als Fälschung identifizieren.

In der Vergangenheit waren bereits ähnliche Mails im Umlauf, die angeblich vor einer vorübergehenden Kontosperrung warnten. PayPal-Nutzer sollten grundsätzlich bei solchen E-Mails vorsichtig sein. Nachrichten, die auf Kontosperrungen oder dubiose Transaktionen verweisen, sind häufig gefälscht. Die darin enthaltenen Links sind Phishing-Versuche, um die Kontodaten der Nutzer abzugreifen.

### **So schützen Sie sich vor Phishing-Angriffen**

Um sicherzugehen, dass es mit dem eigenen Konto keine Probleme gibt, sollte man sich – anstatt über solche Links – auf gewohntem Wege bei PayPal anmelden und prüfen, ob es ungewöhnliche

Kontoaktivitäten gibt. Eine weitere Sicherheitsmaßnahme ist dabei, die Internetadresse von Hand in den Browser einzugeben oder die Seite über eine Suchmaschine zu suchen.

PayPal-Nutzer, die auf die Betrugsmasche hereingefallen sind, sollten schnellstmöglich ihr PayPal-Passwort ändern und die für die hinterlegte Zahlungsmethode zuständige Bank über den Vorfall informieren. PayPal bietet zudem die vergleichsweise sichere Zwei-Faktor-Authentifizierung an, bei der zusätzlich zum Passwort entweder über eine spezielle App oder über die Handynummer des Nutzers die Identität bestätigt wird. So lässt sich verhindern, dass sich Betrüger, die Benutzernamen und Passwörter abgegriffen haben, auf dem Konto anmelden können.

Solche Phishing-Mails gibt es nicht nur in Bezug auf PayPal. Oft lassen sie sich aber bereits anhand der enthaltenen Rechtschreib- und Grammatikfehler als Fake identifizieren. Verbraucher, die doch auf eine solche Betrugsmasche hereingefallen, können etwaige bereits abgebuchte Beträge oft noch von der Bank bzw. dem Zahlungsdienstleister zurückbuchen lassen. Wichtig ist hier, schnell zu reagieren. In unserer Kanzlei kennen wir uns mit solchen Betrugsmaschen bestens aus und wissen, wie schnell und effektiv Gegenmaßnahmen zur Schadensbegrenzung einzuleiten sind. Sollten auch Sie Opfer einer Phishing-Attacke geworden sein, vereinbaren Sie zeitnah einen Termin für eine kostenlose Erstberatung bei uns.

[Guido Lenné](#)

Rechtsanwalt aus der Anwaltskanzlei Lenné.

Rechtsanwalt Lenné ist auch Fachanwalt für Bank- und Kapitalmarktrecht.

Wir helfen Ihnen gerne! [Kontaktieren](#) Sie uns. Oder vereinbaren Sie [hier online einen Termin](#) für eine telefonische kostenfreie Erstberatung.

- [Facebook](#)
- [Twitter](#)
- [WhatsApp](#)

- [E-mail](#)

[Zurück](#)