

13. Oktober 2026

## **ÖGK rät zu Vorsicht: Erneut Betrugsversuche im Namen der ÖGK im Umlauf**

### **Betrügerische Nachrichten und Anrufe zielen auf sensible Daten von Versicherten ab**

Erneut häufen sich derzeit betrügerische E-Mails, SMS und Anrufe, die vorgeben, von der ÖGK zu stammen. Ab Mitte Oktober rückt die ÖGK das Thema Phishing in den Fokus und informiert dazu auf der Website und Social Media. Die ÖGK ist außerdem Teil der Awareness-Kampagne [#10TageGegenPhishing](#), die über die gängigsten Internet-Betrugsmaschen informiert.

#### **Aktuelle Betrugsmaschen im Namen der ÖGK**

In den aktuellen Phishing-E-Mails wird den Empfänger\*innen eine angeblich ausstehende Leistungsauszahlung in Aussicht gestellt. Die Nachrichten fordern die Empfänger\*innen dazu auf, ihre Bankdaten zu aktualisieren, um eine Gutschrift zu erhalten. Auch per SMS versuchen Betrüger\*innen derzeit, an persönliche Daten zu gelangen. Die Empfänger\*innen werden darin aufgefordert, ihre Daten über einen in der Nachricht enthaltenen Link zu aktualisieren. Mit einer gefälschten E-Mail oder SMS wollen Betrüger\*innen an die Konto- und Anmeldedaten der Versicherten kommen. Werden die Anweisungen befolgt, gibt es nicht das versprochene Geld retour. Stattdessen gibt man sensible Kontodaten preis und riskiert, dass diese Daten missbraucht werden.

Ein weiterer Betrugsversuch, der momentan wieder vermehrt auftritt, ist ein Anruf einer meist weiblichen Person, die sich auf die ÖGK bezieht und im Rahmen eines Hausbesuches das Ausprobieren einer kostenlosen Lichttherapie anbietet. Die ÖGK rät dringend davon ab, auf ein solches Angebot einzugehen oder persönliche Daten bekannt zu geben.

#### **Typische Merkmale von Phishing-Nachrichten**

Empfänger\*innen müssen besonders vorsichtig sein, vor allem bei Nachrichten die eine unpersönliche Anrede wie beispielsweise „Sehr geehrter Kunde!“ und eine unseriöse Absenderadresse sowie Betreffzeile enthalten. Auch kurze Fristen, wie die Aufforderung, einen Vorgang innerhalb weniger Tage abzuschließen sollen Zeitdruck erzeugen und zu einem unüberlegten Klick verleiten.

**Wichtig:**

- Die ÖGK fordert niemals per E-Mail oder SMS dazu auf, sensible Daten über einen Direktlink oder Button zu ändern
- Kein Klicken auf Links oder Buttons – diese führen auf betrügerische Seiten
- Keine Weitergabe von persönlichen Daten, Passwörtern und PINs
- Für Änderungen sollte ausschließlich die offizielle Meine ÖGK-App oder die Webadresse durch direktes Eintippen in den Browser genutzt werden
- Für einen sicheren Austausch von Daten sollte am besten das [Serviceportal Meine ÖGK](#) mit dem ID-Austria-Login genutzt werden

**Phishing Versuche melden**

Auf der ÖGK-Website unter [Betrugswarnungen der ÖGK](#) gibt es detaillierte Hinweise zu aktuellen Betrugswarnungen und die Möglichkeit, einen Betrugsversuch zu melden. Im Vergleich zum Vorjahr konnte 2026 ein deutlicher Rückgang der gemeldeten Phishing-Fälle verzeichnet werden. Die aktuell wieder vermehrt auftretenden Nachrichten zeigen jedoch, dass weiterhin Vorsicht geboten ist.

**Rückfragehinweis:**

Österreichische Gesundheitskasse

[presse@oegk.at](mailto:presse@oegk.at)

[www.oegk.at](http://www.oegk.at)