2. Jänner 2025

Presseaussendung

Österreichische Gesundheitskasse

Vorsicht Betrug!
Falsche Mails und SMS an Versicherte
Betrügerische Meldungen im Namen der Österreichischen Gesundheitskasse im Umlauf

Achtung Betrug: Versicherte der Österreichischen Gesundheitskasse (ÖGK) erhalten erneut Nachrichten über eine angebliche Rückerstattung. Die Nachrichten werden per SMS bzw. e-Mail verschickt. Darin werden die Versicherten aufgefordert, einen Link zu öffnen, um die Rückerstattung online anzufordern.

Achtung! Hände weg!

Bei diesen Nachrichten handelt es sich um einen Betrugsversuch. Die ÖGK fordert ihre Versicherten eindringlich auf, nicht darauf einzugehen. Auf keinen Fall sollte der angegebene Link geöffnet oder persönliche Daten bekanntgegeben werden.

Smishing – Vorsicht vor betrügerischen SMS-Nachrichten

Nicht nur e-Mails sind im Umlauf, sondern auch SMS. Smishing ist eine Form des Phishings, bei dem Cyberkriminelle versuchen, durch gefälschte SMS-Nachrichten die Menschen dazu zu verleiten, persönliche Informationen preiszugeben. Diese Informationen können beispielsweise Bankdaten, Passwörter oder Identitätsdaten sein. Dabei wird die SMS oft so gestaltet, dass sie einen dringenden oder wichtigen Eindruck hinterlässt und dazu auffordert, auf einen Link zu klicken oder eine Telefonnummer anzurufen.

Das Erkennen von Smishing-Nachrichten und Maßnahmen dagegen

- **Dringende Aufforderungen sind verdächtig**: Smishing-Nachrichten enthalten häufig Drohungen oder Versprechungen. Niemals direkt auf Links in verdächtigen SMS-Nachrichten klicken. Die Adresse manuell in den Browser eingeben oder die Telefonnummer direkt auf der offiziellen Website der Organisation anrufen.

- **Falsche Absender bzw. verdächtige Telefonnummern sofort blockieren**: Der Absender bzw. eine Telefonnummer der Nachricht scheint häufig eine vertrauenswürdige Quelle zu sein, wie etwa Banken, Behörden oder bekannte Unternehmen. Banken oder staatliche Stellen versenden normalerweise keine Nachrichten mit dringenden Aufforderungen per SMS. Die Telefonnummern in Smishing-Nachrichten sind häufig an abweichenden Vorwahlen oder Zeichenkombinationen erkennbar.

- **Misstrauen gegenüber dringender Forderungen**: Wenn eine Nachricht auffordert, sofort auf einen Link zu klicken oder sensible Daten einzugeben, ist dies ein eindeutiges Warnzeichen. Seriöse Organisationen fordern nicht auf diese Weise zu einer sofortigen Reaktion auf.

- **Keine persönlichen Daten per SMS oder e-Mail mitteilen**: Niemals persönliche Informationen wie Passwörter, Kreditkartendaten oder PINs per SMS oder über verdächtige Links preisgeben. Um die Sicherheitslücken auf dem Computer bzw. mobilen Geräten zu schließen, ist ein regelmäßiges Softwareupdate durchzuführen

Rückfragehinweis:
Österreichische Gesundheitskasse
presse@oegk.at
www.gesundheitskasse.at