

## **Dringende Warnung: Betrugsmasche gefährdet Telekom-Kunden!**

Achtung Telekom-Kunden: Eine neue Phishing-Mail droht mit Datenklau. Vermeiden Sie Betrug und erkennen Sie Warnzeichen.

**Merkur, Deutschland** - Die Verbraucherzentrale warnt dringlich vor einer neuen betrügerischen E-Mail, die gezielt an Telekom-Kunden gerichtet ist. In der Betreffzeile der Nachricht wird über eine neue Sprachnachricht auf der Mailbox informiert. Diese E-Mail fordert die Empfänger auf, einen Link zu klicken, um die Nachricht abzuhören. Laut **Merkur** ist das Ziel dieser Phishing-Mail, persönliche Daten der Telekom-Kunden zu stehlen. Die Telekom weist darauf hin, dass derartige Informationen über neue Mailbox-Nachrichten niemals per E-Mail kommuniziert werden, sondern ausschließlich über SMS oder die Voicemail-App.

Besonders alarmierend ist, dass bei diesen Betrugsversuchen immer mehr Künstliche Intelligenz eingesetzt wird, was die Erkennung solcher Machenschaften erschwert. Weitere Merkmale, die auf Betrug hindeuten, sind eine unpersönliche Anrede, eine unseriöse Absenderadresse sowie das Fehlen eines offiziellen Logos. Die Verbraucherzentrale rät dazu, derartigen E-Mails zu misstrauen, sie direkt in den Spam-Ordner zu verschieben und auf keinen Fall zu antworten.

### **Gefälschte Domains und persönliche Daten**

Die Sicherheitswarnungen vor diesen Phishing-E-Mails werden durch zusätzliche Informationen ergänzt. Die verlinkte Seite in

der E-Mail ist oft gefälscht und enthält nicht die echte Telekom-Domain. Angreifer haben es auf sensible Daten der Empfänger abgesehen und können durch die Preisgabe dieser Informationen zu unerwünschten Anmeldungen bei teuren Abo-Diensten oder Spam-Services führen. Das **Chip**-Portal rät dazu, auf keine E-Mails zu reagieren und keine persönlichen Daten einzugeben.

Ein wichtiges Sicherheitselement ist das kritische Überprüfen der Adressleiste im Browser. Vertrauenswürdige Anbieter fordern niemals vertrauliche Zugangsdaten per E-Mail an. Nutzer sollten auf keinen Fall Links in dubiosen E-Mails anklicken, sondern die Seite über die Startseite der Organisation erreichen. Weitere empfohlene Maßnahmen sind, keine persönlichen Informationen in unverschlüsselten Webseiten einzugeben und die eigene Antivirus-Software stets aktuell zu halten.

## **Praktische Tipps zum Schutz vor Phishing**

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet fundierte Informationen zum Schutz gegen Phishing. Die enthaltenen Ratschläge umfassen unter anderem:

- Regelmäßige Überprüfung des Bankkontos auf verdächtige Umsätze.
- Keine Eingabe persönlicher Daten auf ungesicherten Webseiten (erkennbar an „http://“ statt „https://“).
- Verdächtige Anhänge nicht öffnen und Downloads nicht direkt aus E-Mails starten.
- Online-Sessions immer regulär über Log-out beenden.

Für weitere Informationen und Unterstützung stehen der Sicherheitskompass der Polizei sowie der Cybersicherheits-Lotse zur Verfügung, um Verbraucher im digitalen Verbraucherschutz zu informieren. Zudem ist es ratsam, bei Unsicherheiten telefonisch beim Anbieter nachzufragen, um etwaige Betrugsversuche zu erkennen und zu melden. Weitere Details zur Thematik sind im BSI verfügbar unter **bsi.de**.

Details	
<b>Vorfall</b>	Betrug
<b>Ursache</b>	Phishing
<b>Ort</b>	Merkur, Deutschland
<b>Quellen</b>	<ul style="list-style-type: none"><li>• <a href="http://www.merkur.de">www.merkur.de</a></li><li>• <a href="http://www.chip.de">www.chip.de</a></li><li>• <a href="http://www.bsi.bund.de">www.bsi.bund.de</a></li></ul>

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