

## Vorsicht: Betrügerische WKO-Mails bedrohen die Unternehmenssicherheit!

Warnung vor Phishing: Betrüger nutzen WKO-E-Mails, um sensible Unternehmensdaten zu stehlen. Informieren Sie sich über Sicherheitsmaßnahmen.



**Österreich** - Eine neue Phishing-Welle verunsichert derzeit Unternehmen in Österreich. Kriminelle nutzen das Vertrauen in die Wirtschaftskammer Österreich (WKO) aus, um durch gefälschte E-Mails sensible Daten zu stehlen. Diese Mails erscheinen professionell gestaltet und bringen viele Empfänger in die Bredouille, da sie zur Beantragung einer angeblichen staatlichen Innovationsförderung auffordern. Laut **Gaital Journal** stammen die ersten Informationen von der Plattform Watchlist Internet.

Die gefälschten E-Mails fluten derzeit die Postfächer zahlreicher Unternehmen. Absenderadressen, die täuschend echt wirken, wie „Service@wko.vH.at“ oder „service@wko.qn.at“, verstärken

den Eindruck der Seriosität. Betrüger versuchen, durch Links, die zu schadhafter Software führen, das Vertrauen der Empfänger zu gewinnen und deren persönliche Daten, wie Bank- und Zugangsdaten, zu erlangen. Die **Österreichische Nachrichten** berichten, dass die WKO in diesem Zusammenhang betont, sie sende keine derartigen Mails aus.

## **Risiken und Schutzmaßnahmen**

Die Gefahren einer solchen Phishing-Attacke sind gravierend. Die E-Mails enthalten oft Aufforderungen zum schnellen Handeln und wirken durch ihren offiziellen Aufbau besonders glaubwürdig. Empfänger sollten daher äußerst vorsichtig sein. WKO empfiehlt, solche Nachrichten zu ignorieren und keine Links zu öffnen. Wer auf einen Link geklickt hat, sollte umgehend seine Zugangsdaten ändern, Banken oder Kreditkarteninstitute informieren sowie das eigene Gerät auf Viren prüfen. Laut **Gaital Journal** sollten Betroffene auch Anzeige erstatten, um anderen zu helfen und die Ermittlungen zu unterstützen.

Experten des **Bundesamts für Sicherheit in der Informationstechnik (BSI)** raten dazu, stets die Adressleiste im Browser zu überprüfen und keine vertraulichen Daten über verdächtige E-Mails einzureichen. Unternehmen sollten wichtige Webseiten direkt über die Startseite ansteuern und keine Links aus unbekanntem E-Mails verwenden. Sicherheitstipps, wie regelmäßige Updates der Software und der Einsatz von Antivirus-Programmen, werden ebenfalls dringend empfohlen.

## **Fazit**

Die aktuelle Phishing-Welle verdeutlicht einmal mehr die Notwendigkeit für Unternehmen, wachsam zu bleiben und sich über potenzielle Cyberrisiken zu informieren. Vor allem gilt es, das eigene Wissen über Phishing-Methoden kontinuierlich zu erweitern und Sicherheitsmaßnahmen konsequent umzusetzen, um im Ernstfall angemessen reagieren zu können.

Details	
<b>Vorfall</b>	Betrug
<b>Ursache</b>	Cyberkriminalität
<b>Ort</b>	Österreich
<b>Quellen</b>	<ul style="list-style-type: none"><li>• <a href="http://gailtal-journal.at">gailtal-journal.at</a></li><li>• <a href="http://www.oe24.at">www.oe24.at</a></li><li>• <a href="http://www.bsi.bund.de">www.bsi.bund.de</a></li></ul>

**Besuchen Sie uns auf: [die-nachrichten.at](http://die-nachrichten.at)**