

## **Achtung, Betrugsfall! Falscher BKA-Direktor fragt nach vertraulichen Daten!**

BKA warnt vor Betrugsmails im Namen von Direktor Holzer. Tipps zur Erkennung und Abwehr von Phishing-Attacken.



**Wien, Österreich** - Das Bundeskriminalamt (BKA) warnt vor einer neuen Betrugsmasche, die potentielle Opfer in Österreich betrifft. Betrüger geben sich als der BKA-Direktor Andreas Holzer aus und versenden gefälschte Nachrichten, die eine vertrauliche Rückmeldung anfordern. Diese Nachrichten beginnen oft mit „Hallo xxx, Wie geht es dir?“ und fordern die Empfänger auf, umgehend zu antworten, wobei eine russische E-Mail-Adresse als Indiz für den Betrug dient. In Wirklichkeit hat der echte BKA-Direktor eine österreichische E-Mail-Adresse, wie **5min.at** berichtet.

Zusätzlich sind auch gefälschte offizielle Schreiben im Umlauf, die an dutzende Österreicher versendet werden. Diese

Dokumente, die mit Logos des Innenministeriums, der Polizei und Europol sowie einem Stempel der Stadt Wien versehen sind, erwecken den Eindruck von Authentizität. In diesen Schreiben wird den Empfängern unterstellt, in Aktivitäten wie Kinderpornographie oder Exhibitionismus verwickelt zu sein und sie werden aufgefordert, innerhalb von 48 Stunden eine Stellungnahme an eine gmail.com-Adresse zu senden. Dies deutet laut Experten auf einen Betrugsversuch hin, da das BKA keine Gmail-Adressen verwendet, wie **heute.at** erklärt.

## **Ratschläge zur Vermeidung von Betrug**

Gerald Sakoparnig, der Leiter der Abteilung Betrug beim LKA Oberösterreich, rät dringend davon ab, auf diese Nachrichten zu reagieren. Nachdem eine Stellungnahme abgegeben wurde, erhalten die Opfer oft ein weiteres Schreiben, in dem sie zur Zahlung von mehreren Tausend Euro in Bitcoin aufgefordert werden. Da solche Drohungen, die auf Angst basieren, häufig von Cyberkriminellen eingesetzt werden, gilt es, Ruhe zu bewahren.

Die Zahl der IT-Sicherheitsvorfälle im Zusammenhang mit Phishing hat im Jahr 2023 um mehr als 13 Prozent zugenommen. Cyberkriminelle haben die Qualität ihrer Betrugsversuche, einschließlich E-Mails, SMS und Messenger-Nachrichten, erheblich verbessert, was das Erkennen gefährlicher Nachrichten erschwert. Laut der Initiative Deutschland sicher im Netz (DSiN) sind Phishing-Attacken nach wie vor eine der größten Cyberbedrohungen, wie **G DATA** feststellt.

## **Wichtige Schutzmaßnahmen**

Um sich vor solchen Betrugsversuchen zu schützen, sollten die Empfänger immer die Absenderadresse überprüfen und skeptisch gegenüber Nachrichten sein, die Dringlichkeit oder Vertraulichkeit suggerieren. Es ist ratsam, verdächtige Nachrichten über alternative Kommunikationswege zu überprüfen, bevor man darauf reagiert. Außerdem sollten

Empfänger bei Erhalt solcher Nachrichten nicht zurückschreiben oder persönliche Informationen preisgeben, sondern die E-Mails sofort löschen und im besten Fall den Vorfall melden.

Details	
<b>Vorfall</b>	Betrug
<b>Ort</b>	Wien, Österreich
<b>Quellen</b>	<ul style="list-style-type: none"><li>• <a href="http://www.5min.at">www.5min.at</a></li><li>• <a href="http://www.heute.at">www.heute.at</a></li><li>• <a href="http://www.gdata.de">www.gdata.de</a></li></ul>

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