NACHRICHTEN AG

18. März 2025

Achtung, Commerzbank-Kunden! Phishing-Mails gefährden Ihr Geld!

Commerzbank-Kunden aufgepasst: Phishing-Mails warnen vor Konto-Einschränkungen. Tipps zum Schutz vor Betrug und Datenverlust.

Deutschland - Commerzbank-Kunden sind derzeit einem besorgniserregenden Phishing-Angriff ausgesetzt. In letzter Zeit erhalten Kunden vermehrt betrügerische E-Mails, die ein angebliches Update zur Vermeidung von Konto-Einschränkungen fordern. Die Verbraucherzentrale hat am 14. März vor diesen gefährlichen Nachrichten gewarnt und empfiehlt, solche Mails in den Spam-Ordner zu verschieben und nicht darauf zu reagieren. Ein weiterer Klick auf den Button „Konto jetzt aktualisieren“ könnte zu einem finanziellen Verlust führen, da der Link in der E-Mail wahrscheinlich zu einer manipulierten Website führt. Diese Informationen stammen von **Ruhr24**.

Die Mails sind oft unpersönlich verfasst und adressieren ihre Empfänger nicht mit Namen – ein häufiges Merkmal von Phishing-Versuchen. Kriminelle können persönliche Daten aus dem Internet beschaffen und diese nutzen, um gefälschte Nachrichten zu konstruieren, die echt wirken. Im Grunde genommen sollten Links in E-Mails oder SMS nur angeklickt werden, wenn die Quelle verifiziert werden kann, wie etwa die offizielle Seite der Commerzbank. Klickt man auf solche gefälschten Links, wird man oft auf Webseiten weitergeleitet, die zwar ähnlich aussehen, jedoch nicht mit der Commerzbank verbunden sind. Diese Informationen sind auch im Bericht von **Biallo** nachzulesen.

Risiken und Schutzmaßnahmen

Die Eingabe von Daten auf gefälschten Seiten kann schwerwiegende Folgen haben, da die Informationen nicht an die Commerzbank, sondern an unbekannte Dritte gesendet werden. Gestohlene Daten könnten für weitere Straftaten verwendet werden. Kunden sind dringend geraten, Login-Daten auf keinen Fall auf diesen Fake-Seiten einzugeben. Zudem wird empfohlen, persönliche Angaben nicht über den Browser am Smartphone einzugeben. Besser ist es, die Banking-App der Commerzbank zu nutzen, um sicherer zu agieren.

Ein weiteres Risiko besteht in den gefährlichen Anhängen von E-Mails. Diese können Viren, Trojaner und Schadsoftware enthalten, was zum Aktivieren schädlicher Programme führen kann. Virenscanner sind wichtig, jedoch erkennen sie neue Phishing-Angriffe oft erst nach einer gewissen Zeit. Regelmäßige Updates für Betriebssysteme und Apps sind daher unabdingbar.

Verhaltensregeln im Netz

Das BSI rät dazu, niemals vertrauliche Informationen per E-Mail anzufordern. Nutzer sollten immer die Adressleiste im Browser überprüfen und häufig besuchte Login-Seiten in der Favoritenliste speichern. Wenn eine E-Mail verdächtig erscheint, sollte der direkte Kontakt mit dem Anbieter aufgenommen werden, um deren Echtheit zu verifizieren.

- Klicken Sie nicht auf Links in dubiosen E-Mails.
- Geben Sie persönliche Daten nur auf vertrauenswürdigen Webseiten ein.
- Beenden Sie Online-Sessions durch regulären Log-out.

Bei Unsicherheiten ist es ratsam, sofort zu handeln und die Bank über vertrauenswürdige Kommunikationsmethoden zu kontaktieren. Für weitere Informationen über den Schutz gegen Phishing können Verbraucher im Sicherheitskompass der Polizei und des BSI nachlesen, wie in **dieser Quelle** empfohlen.

Details	
Vorfall	Phishing
Ort	Deutschland
Quellen	• **www.ruhr24.de** • **www.biallo.de** • **www.bsi.bund.de**