

GEFÄLSCHTE BANK-WEBSEITEN

Bank Phishing E-Mails enthalten in der Regel Links, die Sie zu einer gefälschten Bank-Webseite führen, auf der Sie aufgefordert werden, Ihre finanziellen und persönlichen Daten einzugeben.



WAS SIND DIE ANZEICHEN?

Gefälschte Bank-Webseiten sehen nahezu identisch wie die Original-Webseiten aus. Solche Webseiten verfügen häufig über Popup-Fenster, die Sie auffordern, Ihre Bankdaten einzugeben. Echte Banken benutzen keine Popup-Fenster.

Diese Webseiten beinhalten normalerweise Folgendes:

Dringlichkeit: Sie werden keine solchen Nachrichten auf legitimen Webseiten finden.

Schlechtes Design: Seien Sie vorsichtig mit Webseiten, die Fehler in Design oder Rechtschreibung und Grammatik enthalten.



Popup-Fenster: Sie werden häufig verwendet, um sensible Informationen von Ihnen zu sammeln. Klicken Sie nicht darauf und vermeiden Sie es, persönliche Daten über solche Fenster zu übermitteln.

WAS KÖNNEN SIE TUN?



Klicken Sie nie auf Links, die in E-Mails enthalten sind und die (angeblich) zur Webseite Ihrer Bank führen.



Geben Sie Links immer manuell ein oder verwenden Sie einen vorhandenen Link aus Ihrer Favoritenliste.



Verwenden Sie einen Browser, mit dem Sie **Popup-Fenster blockieren können.**



Über wichtige Ereignisse oder Themen werden Sie von Ihrer Bank informiert, **wenn Sie auf Ihren Online-Account zugreifen.**