

Würdest du auf diesen Sparkassen-Link klicken?

<https://www.berliner-sparkasse.de-login-account.de/home/online-banking.html>

Mit täuschend echten Links versuchen Cyberkriminelle,
dich auf ihre gefälschten Websites zu locken.

Lass dich nicht linken!

So erkennst du, wann du zweimal hinschauen solltest! ↓

Eine E-Mail oder Nachricht ist verdächtig, wenn...

du nicht exakt so mit ihr gerechnet hast UND du aufgefordert wirst, sensible Daten einzugeben, auf einen Link oder Button zu klicken oder einen Anhang herunterzuladen.

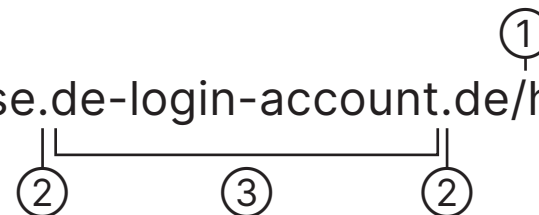
Oft geben betrügerische Nachrichten vor, von großen Unternehmen oder einer mit dir verbundenen Person oder Organisation zu stammen. Meist vermitteln sie eine gewisse Dringlichkeit (drohende Kontosperrung, Abmahnung,...), um dich zu unüberlegtem Handeln zu verleiten.

So erkennst du, wer wirklich hinter einem Link steckt

Grundsätzlich folgen alle Internetadressen einem einheitlichen Schema. Wem eine Seite gehört, kannst du meist in drei Schritten ermitteln:

- ① Den dritten Slash (/) der Webadresse suchen
- ② Die nächsten zwei Punkte finden, die vor diesem Slash stehen
- ③ Zwischen diesen Punkten steht, zu wem die Webadresse gehört

https://www.berliner-sparkasse.de-login-account.de/home/online-banking.html



Wenn du dir nicht sicher bist, zeige den Link einer Person, die für IT-Fragen zuständig ist.



i

Angefixt?

Der kulturBigital-HelpDesk steht dir zur Seite, wenn du IT-Sicherheit und Datenschutz in deiner Institution oder deinem Kollektiv erhöhen möchtest.

Mehr Infos unter:

<https://www.kultur-b-digital.de/helpdesk/>