

BLEIBEN SIE ACHTSAM!

Es gibt nur einen einzigen wirksamen Schutz vor Social Engineering: gesundes Misstrauen, verbunden mit dem strikten Einhalten vereinbarter Regeln zur Datenweitergabe! **Behalten Sie deshalb die Risiken immer im Blick!**



RISIKO SOCIAL NETWORKS

Ihr Profil und andere Daten in sozialen Netzwerken bieten Social Engineers vielfältige Angriffsmöglichkeiten!



RISIKO LAUSCHANGRIFF

Lauschangriffe finden überall statt! Ob im Büro am PC, unterwegs am mobilen Endgerät oder durch Mithören eines Gesprächs!



RISIKO TELEFON

Anrufer können mit falschen Angaben versuchen, an interne Informationen zu gelangen!



RISIKO USB-STICK

Fremde USB-Sticks bieten Kriminellen eine Möglichkeit, Ihre Daten auszulesen oder sogar Ihren PC fernzusteuern!



RISIKO INNENTÄTER

Sensible Daten dürfen selbst unter Kollegen nur an autorisierte Personen weitergegeben werden!