

SICHER UNTERWEGS IM BEREICH SOCIAL MEDIA 10 TIPPS

Die sozialen Medien haben in unserem Leben einen festen Bereich eingenommen. Leider verbergen sich hier auch Risiken, die beachtet werden sollten, damit Cyberkriminelle keine Chance haben.

1. Wenn Sie Ihre **Urlaubsfotos und Urlaubsorte** auf Social Media Kanälen posten, verraten Sie potenziellen Dieben, wann Ihr Arbeitsplatz und Ihr Zuhause leer stehen.
2. **Bilder und Selfies**, die auf dem Arbeitsplatz entstanden sind könnten unter Umständen Informationen enthalten, die für Dritte wertvoll sein könnten (Preise, Adressen, Kundendaten). Prüfen Sie zuvor Ihre Aufnahmen!
3. **Partyfotos** posten oder von Freunden auf Party-Bildern markiert zu können Konsequenzen haben, oder gar Rufschädigend sein. Können auch Geschäftspartner oder gar ihr Arbeitgeber die Bilder sehen?
4. Ist es möglich, dass von Ihrem **Titelbild oder Ihren Postings** Rückschlüsse auf ihre Passwörter gezogen werden können? Kinder,- oder Haustiernamen oder Geburtsjahre?
5. **Karriereportale** wie Xing und LinkedIn liefern Social Hacking Gruppen wertvolle Informationen. Dies kann eine Grundlage für einen zielgerichteten Spear Phishing angriff legen. Seien Sie sparsam mit Ihren Angaben.
6. Geben Sie **keine Informationen an Dritte** weiter. Sie wissen nie, wer am anderen Ende der Leitung sitzt.
7. **Freundschaftsanfragen** nur annehmen, wenn Sie diese Person auch kennen.
8. Kinder haben oft kein oder nur sehr wenig **Sicherheitsbewusstsein**. Denken Sie daran, wenn Sie Ihrem Nachwuchs ein Smartphone oder Laptop aushändigen.
9. **Deaktivieren Sie Standortverläufe** auf Ihrem Smartphone. Google erstellt Bewegungsprofile.
10. Öffentliche W-Lan Netze sind gefährlich. Schnell können hier Log-in-Daten entwendet werden.

Fragen zum Thema IT-Sicherheit? Dann schreibt uns einfach an!

**JETZT ANRUFEN:
0212 659 85-0**

**JETZT MAILEN:
INFO@SICDATA.DE**