

Checkliste / Verhaltensweisen zur Prävention von Reputations-schäden im Internet

1. Lesen Sie die Allgemeinen Geschäftsbedingungen und Bestimmungen zum Datenschutz des betreffenden Anbieters, um den Schutz Ihrer persönlichen Daten zu gewährleisten.
2. Kommunizieren Sie unter einem Pseudonym.
3. Seien Sie zurückhaltend mit der Veröffentlichung von privaten Informationen, Texten, Bildern und anderen Inhalten. Geben Sie auf keinen Fall reale Anschriften, Adressen und Erreichbarkeiten preis.
4. Stellen Sie sicher, dass Sie die angebotenen Privatisierungseinstellungen auf Facebook und anderen Seiten nutzen.
5. Wählen Sie sichere Passwörter für Ihre Social Media Accounts, E-Mail Adressen, Online-Banking und weiter wichtige Accounts. Integrieren Sie Zahlen, Gross-/ Kleinschreibung, Sonderzeichen wenn möglich, um die Sicherheit Ihrer Passwörter zu erhöhen.
6. Bei der Auswahl des Netzwerkes sollten Sie auf seriöse Betreuung und Führung der Online-Community achten.
7. Wenn Sie erfahrene Nutzer kennen, profitieren Sie von deren Wissen.
8. Wenn Sie Daten veröffentlichen, tun Sie dies auf Websites, die Ihre Daten schützen und auf denen Sie entscheiden können, welche Daten veröffentlicht und von welchen Personen gesehen werden.
9. Suchen Sie regelmässig nach Ihrem eigenen Namen im Internet, auf verschiedenen Netzwerken, Suchmaschinen und Social Media Sites.
10. Lehnen Sie die Anwendungen von Cookies ab.
11. Lehnen Sie Apps ab, die Zugriff auf persönliche Informationen (z.Bsp. Zugriff auf Ihren Messenger, etc.) benötigen.
12. Seien Sie skeptisch und zurückhaltend, wenn Sie Kontaktanfragen von Ihnen unbekannten Personen bekommen.
13. Zögern Sie nicht, aufdringliche Kontakte dem Netzbetreiber zu melden.
14. Seien Sie misstrauisch, wenn Sie von Online-Bekannten um Leistungen oder Geld gebeten werden.
15. Wenn Sie einen Blog oder in Online-Foren schreiben oder an Diskussionen teilnehmen, halten Sie sich zurück mit dem Posten von extremen Ansichten und Meinungen, etc.
16. Lassen Sie Ihr Handy / Mobile Device nicht ungesperrt unbeaufsichtigt.
17. Schützen Sie alle Ihre Devices mit Passwort.