Wumbel®

Soziale Medien

DR. BITTNER GROUP

Täglich entstehen unzählige Fotos, Kommentare und Beiträge in sozialen Netzwerken. Für viele ist das längst Routine: ein Urlaubsfoto auf Instagram, ein kurzer Kommentar auf LinkedIn, ein Beitrag bei Facebook. Doch was vielen nicht bewusst ist, **jede dieser Aktionen hinterlässt digitale Spuren.** Diese Daten werden gespeichert, ausgewertet und können in falsche Hände geraten. Soziale Medien sind kein rein privater Raum mehr, sondern eine gigantische Datensammelstelle. **Wer unbedacht teilt, gibt mehr preis, als er ahnt.**

Was sind soziale Medien?

Unter sozialen Medien versteht man Plattformen wie **Facebook, Instagram, LinkedIn, XING, TikTok, YouTube oder Blogs**. Sie ermöglichen, Fotos, Videos, Meinungen und Erfahrungen mit einem großen, **teils unbekannten Publikum** zu teilen .

Typische Risiken sind:

1. Oversharing: Zu viele persönliche oder vertrauliche Informationen werden öffentlich gemacht. Vor allem sogenannte „Influencer“ geben ihren kompletten Alltag preis, was zwar sehr unterhaltsam sein kann, aber fremden Personen reichlich Informationen für Profiling gibt und Straftaten eventuell vereinfacht werden.

2. Vermischung von privat und beruflich: Eine Äußerung über das berufliche Umfeld in einem privaten Profil kann leicht als Unternehmensmeinung verstanden werden. Auch sollte ein privater Account nicht mit der Unternehmens-E-Mail-Adresse registriert werden.

3. Rechtsverletzungen: Das Veröffentlichen fremder Fotos ohne Einwilligung könnte als Urheberrechtsverstoß verstanden werden. Das Veröffentlichen von selbst erstellten Fotos ohne Einwilligung der Abgebildeten könnte das allgemeine Persönlichkeitsrecht verletzen.

4. Datenmissbrauch: Plattformbetreiber und Dritte nutzen Daten für Werbung, Betrug oder Social Engineering.

5.Geotagging: Fotos können Aufenthaltsorte oder persönliche Details verraten, da unter anderem Standorte in den Metadaten des Fotos gespeichert sind. Diese sind heutzutage leicht auszuwerten. Noch einfacher machen es Nutzer durch die eigene Bereitstellung des Standorts.

Darum ist Social Media riskant für Ihre Daten

1. Inhalte verbreiten sich blitzschnell und lassen sich kaum kontrollieren!

2. Schon kleine Details im Hintergrund eines Fotos können sensible Informationen zeigen. (z.B. QR-Codes auf Tickets für Veranstaltungen).

3. „Das Internet vergisst nicht“: Selbst gelöschte Inhalte bleiben oft auffindbar oder tauchen durch Verbreitung wieder auf.

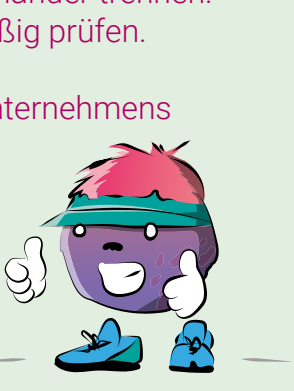
So handeln Sie sicher in sozialen Medien

Vermeiden Sie:

- Bilder von Kollegen, ohne deren Einverständnis zu veröffentlichen.
- sensible Daten (z. B. Passwörter, Kundendaten) über Messenger **oder** soziale Netzwerke zu verschicken.
- Inhalte zu posten, die Urheber- und weitere Rechte verletzen.
- private Accounts für Aussagen über das Unternehmen zu nutzen.
- Informationen zu teilen, deren Quelle oder Wahrheitsgehalt unklar ist.

Machen Sie es besser, indem Sie:

- vor jeder Veröffentlichung das Einverständnis aller erkennbaren Personen einholen.
- Kommentare stets sachlich und respektvoll formulieren.
- private und berufliche Social-Media-Auftritte klar voneinander trennen.
- die Privatsphäre-Einstellungen Ihrer Accounts regelmäßig prüfen.
- Quellen und Urheber korrekt angeben.
- klarstellen, dass Ihre Meinung nicht die Haltung des Unternehmens widerspiegelt.



Tipps für den Berufsalltag

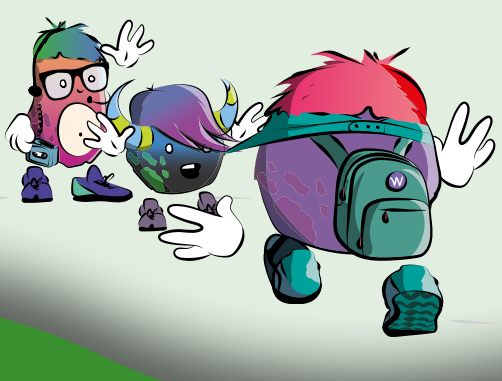
1. Respektieren Sie fremde Rechte: Holen Sie Einverständnisse ein und beachten Sie Urheberrecht, Markenrecht und das Recht am eigenen Bild.
2. Bleiben Sie respektvoll: Keine Beleidigungen, obszöne oder irreführenden Äußerungen posten.
3. Gehen Sie diskret mit Informationen um: Vertrauliche Firmeninformationen gehören nicht ins Internet.
4. Separate Zugangsdaten: Nutzen Sie getrennte Passwörter und aktivieren Sie die Mehrfaktor-Authentifizierung.
5. Regelmäßige Schulungen: Informieren Sie sich regelmäßig über Risiken im Social-Media-Bereich und halten Sie den Datenschutz ein.
6. Geodaten deaktivieren: Standortinformationen in Fotos und Posts ausschalten.

Was sagt Wumbel zur Datensicherheit?

Plattformen sind „kostenlos“, weil sie mit Ihren Daten arbeiten. Jede Interaktion (Likes, Nachrichten, Kontakte) wird durch den Betreiber analysiert, um gezielt Werbung zu platzieren. Mit jedem Kauf verdient auch der Plattformbetreiber. Auch private Nachrichten können mitgelesen werden. Hackerangriffe auf soziale Netzwerke sind keine Ausnahme. Deshalb gehören Passwörter, vertrauliche Dokumente und persönliche Geheimnisse niemals in Messenger oder Chats.

Bewusst handeln und sich auf die sichere Seite stellen

Soziale Medien bringen Chancen, aber auch Risiken. **Datenschutz beginnt bei Ihnen:** Entscheiden Sie bewusst, was Sie teilen, wie Sie es formulieren und welche Grenzen Sie ziehen. Wer **private und berufliche** Rollen trennt, **respektvoll** kommuniziert und **sensible Informationen schützt**, verhindert **Missverständnisse, Datenverlust** und **Imageschäden**. Achtsamkeit im Internet schützt Privates und Berufliches gleichermaßen.



Wumbel

Dr. Bittner Consulting GmbH & Co. KG
Podbielskistraße 386
30659 Hannover
Servicenummer: 0800 88446688
E-Mail: office@drbg.de

DR. BITTNER GROUP