



Checkliste Surfen in sozialen Netzwerken

Soziale Netzwerke bieten die Möglichkeit, miteinander zu interagieren und Informationen austauschen. Die meist kostenlosen Angebote haben jedoch einen hohen Preis: unsere persönlichen Daten. Wir geben 10 Tipps zum sicheren Surfen in sozialen Netzwerken.

1. Für Profile in sozialen Netzwerken gilt immer: Seien Sie sparsam mit persönlichen Daten!
2. Verwenden Sie für verschiedene soziale Netzwerke unterschiedliche und sichere Passwörter!
3. Prüfen Sie in den Profil-Einstellungen, welche Daten Sie mit wem teilen und wer Einblick in Ihr Profil haben soll.
4. Schauen Sie sich die Voreinstellungen zum Datenschutz an und grenzen Sie bestimmte Rechte ein – beispielsweise personalisierte Werbung.
5. Wählen Sie als Profilbild einen Platzhalter oder ein neutrales Foto, das Ihnen auch später einmal nicht peinlich ist.
6. Bevor Sie Inhalte ins Internet hochladen, überlegen Sie, ob und mit wem Sie den Inhalt teilen wollen. Möchten Sie, dass ein Bild oder ein Statusbericht für immer im Netz auffindbar ist?
7. Hinterfragen Sie stets Kontaktanfragen. Ist der Absender echt und vertrauenswürdig? Tipp: Seien Sie besonders aufmerksam, wenn sich jemand als Bekannte:r bzw. Familienmitglied ausgibt und Sie um Geld oder persönliche Daten wie die Mobilfunknummer bittet.
8. Melden Sie Personen, die Sie oder andere belästigen („Cyberstalker“ und „Trolle“) an das jeweilige soziale Netzwerk – beispielsweise, wenn diese unaufgefordert und dauerhaft versuchen, mit Ihnen Kontakt aufzunehmen.
9. Dokumentieren und melden Sie Texte, Bilder, Videos oder Kommentare, die Sie als Beleidigung und als Hetze gegen bestimmte Menschengruppen empfinden. Zum Beispiel hier: meldestelle-respect.de und hateaid.org.
10. Klicken Sie nicht wahllos auf Links. Soziale Netzwerke werden verstärkt dazu genutzt, um an Ihre persönlichen Daten und Zugänge zu Online-Konten zu gelangen (Phishing).

Wie Sie Fake News erkennen

Wenn Sie Nachrichten in sozialen Netzwerken konsumieren oder teilen, fragen Sie sich immer: Kann das wirklich stimmen?

- Von wem stammt die Nachricht? Gibt es eine Quelle?

Tipp: Bei Verlinkungen auf externe Nachrichtenportale hilft ein Blick in das Impressum des Portals. Laut deutschen Gesetzen muss auf Webseiten aus Deutschland ein Impressum vorhanden sein. Das Impressum wird häufig ganz unten auf einer Website verlinkt.

- Wie wurde die Nachricht verfasst? Reißerische Texte mit spektakulären Bildern, gepaart mit vielen Ausrufe- und Fragezeichen, können ein erstes Indiz sein.
- Wer hat die Nachricht verfasst? Was ist über die Person bekannt?
- Haben andere seriöse Quellen und verlässliche Seiten von Zeitungen oder Nachrichtensendungen bereits über denselben Sachverhalt berichtet?

Tipp: Nutzen Sie Faktenfinder. Auf mimikama.org, tagesschau.de/faktenfinder oder correctiv.org können Sie nachlesen, welche Falschmeldungen aktuell stark verbreitet werden.

- Wo, wann und von wem wurde ein Bild oder Video aufgenommen? Was zeigt es wirklich?

Tipp: Mit der Rückwärtsbildersuche von [Google images.google.de](http://Google.images.google.de) oder Bing können Sie den Ursprung eines Bildes nachverfolgen und herausfinden, in welchem Zusammenhang das Bild bereits verwendet wurde.

- Ist die Nachricht aktuell? Gibt es ein Datum und kann das Datum stimmen?

! Sie sind unsicher? Lassen Sie sich unabhängig beraten! Weitere Informationen erhalten Sie bei Ihrer Verbraucherzentrale. www.verbraucherzentrale.de