

Sicher durchs Internet – wichtige Hinweise!









1. Nicht alles glauben, was im Internet steht

So erkennen Sie verlässliche Seiten:

- ✓ Klare Sprache ohne Rechtschreibfehler
- ✓ Autor oder Quelle wird genannt
- ✓ Kein Druck zur Dateneingabe oder Anmeldung
- ✓ Am besten: Inhalte von Behörden, Krankenkassen, Verbraucherschutz oder bekannten Medien

2. Google, Bing, ChatGPT und verschiedene Plattformen und Systeme nutzen Künstliche Intelligenz (KI / AI), um Fragen schnell zu beantworten oder andere Leistungen zu erbringen.

Aber seien Sie sich bewusst:

- ✓ KI kann sich irren oder Dinge "erfinden"
- ✓ Immer auf Quellen achten. Je nach persönlichem Stellenwert Ihrer Anfrage und System fordern Sie die KI stets auf, ihre Quellen zu nennen, da dies nicht (immer) automatisch ersichtlich ist.
- ✓ Infos lieber nochmal gegenprüfen z. B. bei der Verbraucherzentrale

3. Betrüger wollen Ihre Daten – nicht Ihre Meinung.

Vorsicht bei:

- ✓ Gewinnspielen oder "dringenden Nachrichten"
- ✓ Mails mit Anhängen von unbekannten Absendern
- ✓ Seiten, die IBAN, Ausweis oder Passwörter verlangen

Tipp: Prüfen Sie Webseiten z. B. mit ScamAdviser.com.

Hinterfragen Sie den Inhalt bei unbekanntem E-Mail-Absender: "Bin ich überhaupt Kunde bei dieser Firma?", "Kenne ich diese Person im echten Leben?", "Ist es glaubwürdig, dass diese Institution mich kontaktiert?".

Verdacht auf Internet-Betrug? Nicht schweigen, Hilfe holen!

Es kann jedem passieren – wichtig ist, schnell zu handeln:

- ✓ Nicht schämen! Betrüger sind oft sehr geschickt reden Sie mit jemandem, dem Sie vertrauen.
- ✓ Keine Zahlungen leisten oder bestätigen.
- ✓ Bank oder Sparkasse sofort informieren, wenn Sie Kontodaten eingegeben haben.
- ✓ **Gerät nicht weiter benutzen,** wenn Sie etwas Verdächtiges heruntergeladen haben holen Sie sich Hilfe von Angehörigen oder Fachleuten.
- ✓ Polizei verständigen: Wählen Sie die 110, wenn Sie sich bedroht fühlen.

Gefördert von:

Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen





