



# Die Schattenseiten des Internets

Wie Cyberkriminelle soziale Medien und digitale Kanäle nutzen, um uns auszuspionieren, zu manipulieren und finanziell auszubeuten.

Erstellt von / Tipps von: [DenkRadar.de](https://denkradar.de)

**DenkRadar**  
Zukunft gestalten mit Weitblick



# Die Verlockung des Digitalen

## 24/7 Erreichbarkeit

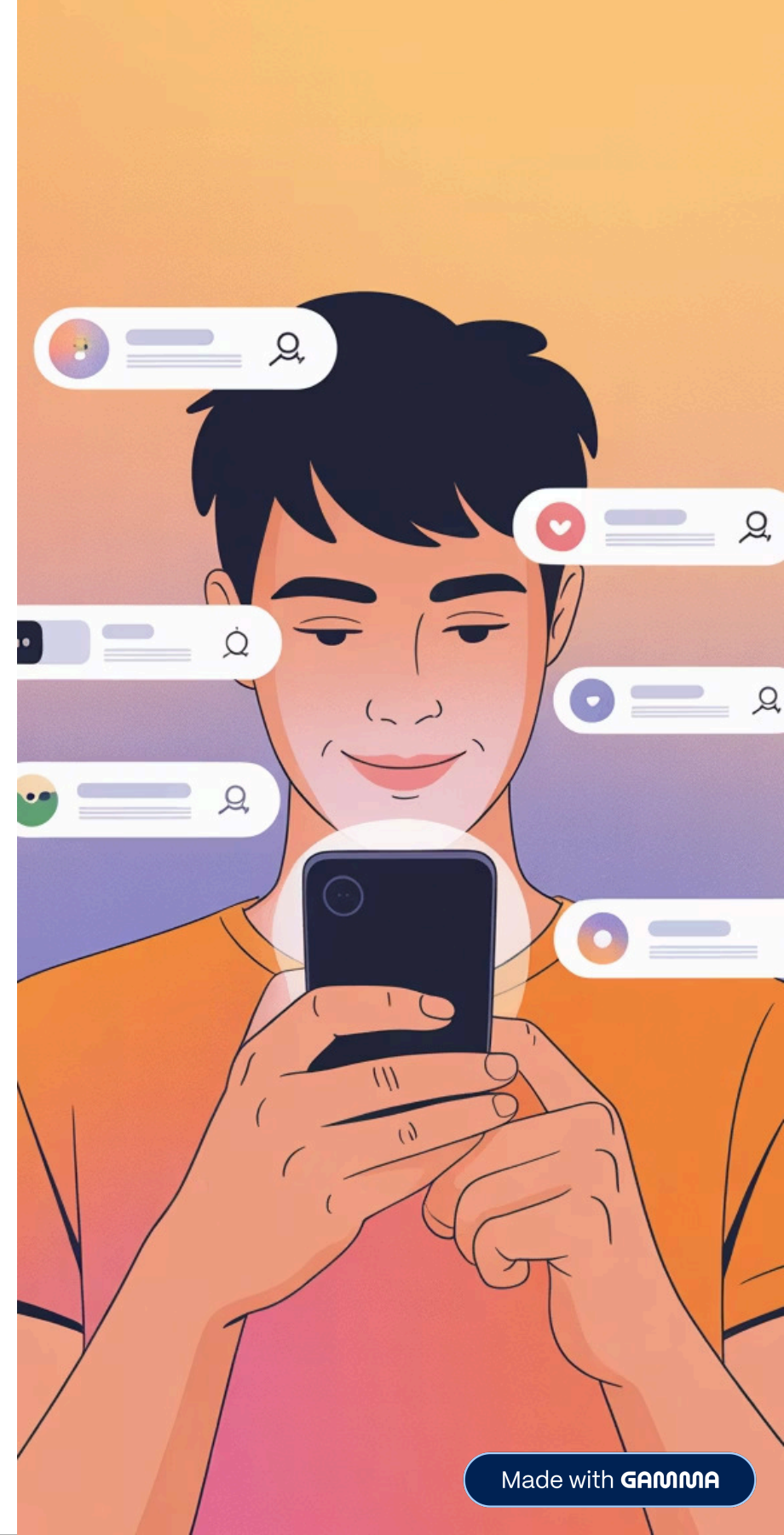
Wir sind ständig online – und damit ständig angreifbar. Kriminelle schlafen nicht.

## Soziale Medien als Jagdgrund

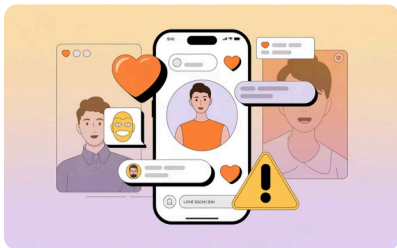
Facebook, Instagram, WhatsApp – jede Plattform bietet Angriffsfläche für Täter.

## Ablenkung macht anfällig

Benachrichtigungen, Likes und Nachrichten lenken uns ab – genau das nutzen Betrüger aus.



# Raffinierte Betrugsmaschen



## Love Scamming

Gefälschte Identitäten bauen über Wochen echte Gefühle auf. Plötzliche „Notfälle“ münden in Geldüberweisungen.



## „Pig Butchering“

Beziehungsaufbau über Dating-Apps, gefolgt von gefälschten Krypto-Plattformen. Erst kleine Gewinne – dann verschwinden die Täter mit dem großen Geld.



## Smishing

Betrügerische SMS mit Fake-Links: „Ihr Paket wartet“ oder „Konto gesperrt“. Ein Klick reicht – Zugangsdaten sind weg.

# Weitere perfide Methoden

## PayPal & Friends Betrug

Zahlung ohne Käuferschutz – Ware wird nie geliefert, Geld unwiederbringlich verloren.

## Deep Fakes im Anlagebetrug

KI-generierte Videos imitieren Prominente, um für unseriöse Investments zu werben.

## Phishing-E-Mails

Gefälschte Bank- oder Shop-Mails fordern zur Dateneingabe auf gefälschten Login-Seiten auf.



# Die psychologischen Tricks der Cybermafia



## Emotionen ausnutzen

Liebe, Gier, Angst und Hilfsbereitschaft – Betrüger spielen gezielt auf der menschlichen Gefühlsskala.



## Druck & Dringlichkeit

Künstliche Knappheit und Zeitdruck verhindern rationales Nachdenken beim Opfer.



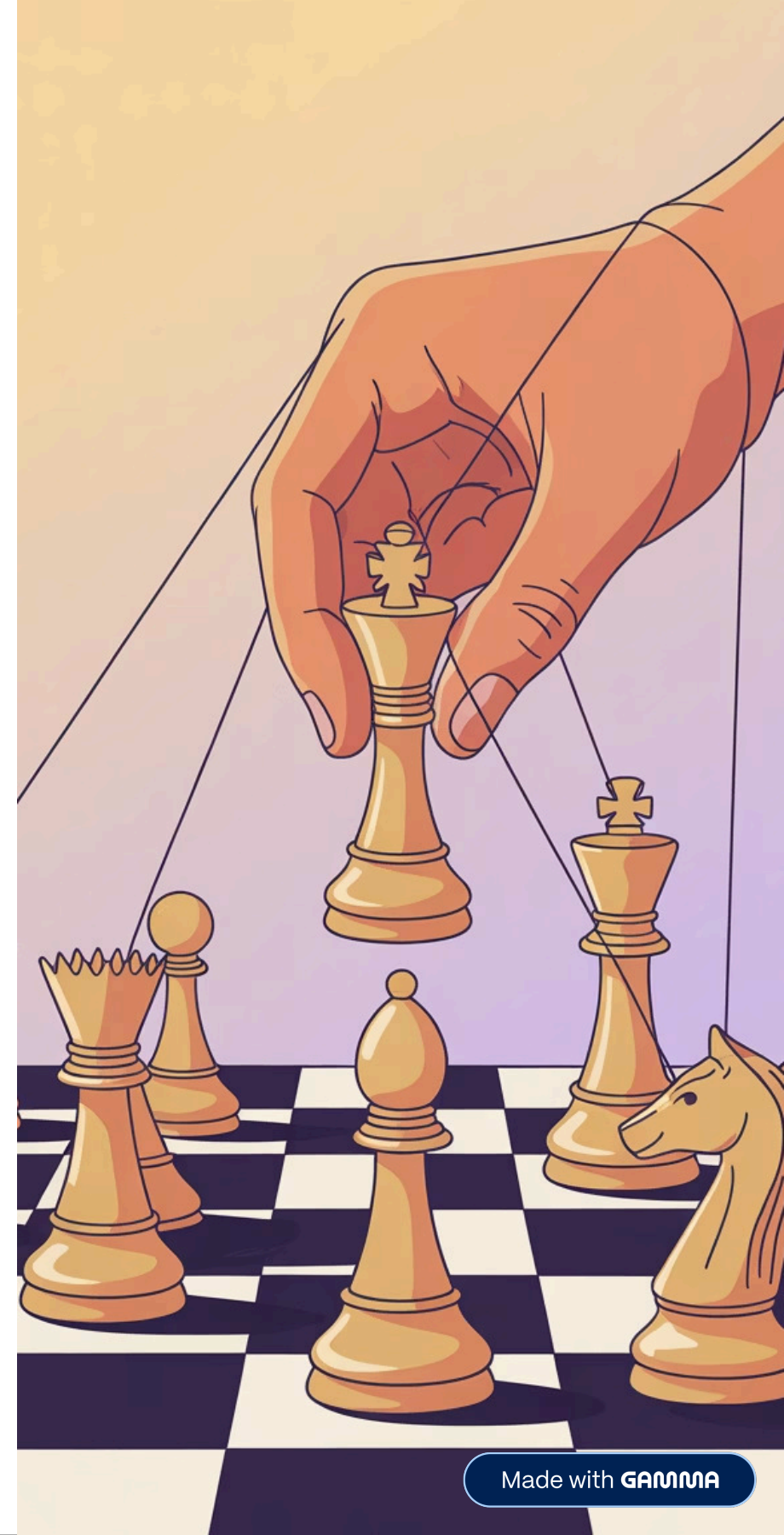
## Vertrauensaufbau

Wochen- oder monatelange Beziehungspflege senkt die Hemmschwelle erheblich.



## Täuschung & Nachahmung

Bekannte Marken, Logos und Persönlichkeiten werden imitiert, um Seriosität vorzuspiegeln.



# Wie Sie sich schützen können

## → Gesunder Menschenverstand

Skeptisch bleiben bei unerwarteten Kontakten, Angeboten oder Geldforderungen.

## → Links & Absender prüfen

Verdächtige SMS und E-Mails ignorieren – Absenderadresse genau kontrollieren.

## → Keine sensiblen Daten weitergeben

Niemals Passwörter, Bankdaten oder persönliche Infos an Unbekannte übermitteln.

## → 2-Faktor-Authentifizierung & Updates

Starke Passwörter, 2FA und aktuelle Software schließen viele Sicherheitslücken.

 **Im Zweifel:** Melden Sie verdächtige Aktivitäten sofort bei der Polizei.

# Fazit: Wachsamkeit ist Ihre beste Verteidigung

## Cyberkriminalität entwickelt sich weiter

Täter passen ihre Methoden ständig an neue Plattformen und Technologien an.

## Informiert bleiben

Wer die Maschen kennt, erkennt sie rechtzeitig – Wissen schützt besser als jede Software.

Sie sind der entscheidende Faktor

**Schützen Sie Ihr Geld und Ihre Daten – kritisches Denken ist Ihre stärkste Waffe!**

Erstellt von / Tipps von: [DenkRadar.de](https://denkradar.de)

**DenkRadar**  
Zukunft gestalten mit Weitblick



Made with GAMMA