AEDIAEVUM LEITFADENREIHE

Phishing erkennen: Die neuen KI-Maschen 2026

Warum alte Erkennungsregeln nicht mehr ausreichen

Für alle, die Phishing-Versuche zuverlässig erkennen wollen

Herausgegeben von der aediaevum Stiftung · Mühltal · Juni 2026

„Achte auf Rechtschreibfehler“ — dieser Ratschlag war jahrelang die wichtigste Phishing-Regel. 2026 ist er weitgehend wirkungslos geworden. Dieser Leitfaden erklärt, warum sich Phishing grundlegend verändert hat.

---

1. Was sich verändert hat

Künstliche Intelligenz hat die Spielregeln verschoben. Weit über 80 Prozent aller Phishing-E-Mails werden inzwischen mit KI-Unterstützung erstellt. Das bedeutet konkret: keine Rechtschreibfehler mehr, keine holprige Anrede, täuschend echte Logos und Layouts.

Die wichtigste Erkenntnis

• Sie können sich nicht mehr darauf verlassen, „schlechte“ Nachrichten zu erkennen.

• Entscheidend ist: WIE eine Nachricht Sie unter Druck setzt — nicht WIE GUT sie geschrieben ist.

• 61 % der Internetnutzer in Deutschland waren 2025 von Cyberkriminalität betroffen (Bitkom Research).

2. Die vier aktuellen Betrugsmaschen

Stimmklon-Anrufe („Hallo Mama, hallo Papa“)

Drei Sekunden Audiomaterial reichen für ein überzeugendes Stimmmodell. Der vermeintliche Sohn oder die Enkelin bittet um dringende finanzielle Hilfe. Schutz: Familien-Codewort vereinbaren, bei

Geldforderungen immer zurückrufen.

Quishing (Phishing per QR-Code)

QR-Codes auf Plakaten oder in E-Mails führen auf gefälschte Seiten. Schutz: keine QR-Codes aus unaufgeforderten E-Mails scannen, auf Aufkleber über Original-Codes achten.

Phishing über Messenger-Dienste

Betrüger geben sich als Support aus und fordern Sicherheitscodes. Schutz: niemals einen per SMS oder Messenger erhaltenen Code weitergeben.

Gefälschte Behörden- und Bank-Mails

Vermeintliche Steuerrückerstattungen oder Mahnungen mit täuschend echten Login-Seiten. Schutz: Behörden fordern nie per E-Mail zur Eingabe von Zugangsdaten auf.

3. Die drei Warnsignale, die immer noch funktionieren

Künstliche Dringlichkeit	Formulierungen wie „innerhalb 24 Stunden handeln“ sind fast immer ein Alarmzeichen.
Unpassende Absenderadresse	Angezeigter Name wirkt seriös, die echte Adresse dahinter nicht.
Forderung nach Codes	Kein seriöser Anbieter verlangt 2FA-Codes per Telefon oder Chat.

4. Soforthilfe: Was tun im Verdachtsfall?

Bei einer verdächtigen Nachricht:

- Nicht klicken, nicht antworten
- Beim E-Mail-Anbieter oder Phishing-Radar der Verbraucherzentrale melden
- Im Zweifel über eine offiziell bekannte Telefonnummer nachfragen

5. Ihre Phishing-Checkliste

■	Ich öffne keine Links aus unerwarteten E-Mails oder SMS.
■	Ich prüfe immer die tatsächliche Absenderadresse.
■	Ich gebe niemals einen 2FA-Code am Telefon weiter.
■	Meine Familie hat ein Codewort für Notfälle vereinbart.
■	Ich melde verdächtige Nachrichten aktiv.

aediaevum Stiftung · In der Röde 5 · 64367 Mühltal · Gemeinnützige Stiftung zur Förderung der Kriminalprävention
Stiftungsaufsicht: Regierungspräsidium Darmstadt · Stand: 21.06.2026 · Dieses Dokument darf kostenlos ausgedruckt und weitergegeben werden.