

## Phishing mit KI – So nutzen Angreifer KI und so können sich Unternehmen schützen

*Phishing ist eine der häufigsten und gefährlichsten Betrugsformen im Internet. Die Tricks und Herangehensweisen der Cyberkriminellen werden auch dank künstlicher Intelligenz immer raffinierter.*

*Das Wissensnugget „Phishing mit KI – So nutzen Angreifer KI und so können sich Unternehmen schützen“ zeigt, wie Händler:innen solche Angriffe erkennen können, und auch, wie sie KI sie dabei unterstützen kann, solche Angriffe zu verhindern.*

### Einleitung

Phishing ist eine der häufigsten und gefährlichsten Betrugsformen im Internet. Dabei versuchen Kriminelle, über gefälschte E-Mails, Webseiten oder Nachrichten an vertrauliche Daten zu gelangen – zum Beispiel an Kreditkartennummern oder Zugangsdaten.

Mit dem Einsatz von **künstlicher Intelligenz (KI)** hat sich das Phishing deutlich verändert. KI ermöglicht es Angreifern, täuschend echte Nachrichten zu erstellen – oft fehlerfrei, glaubwürdig und spezifisch auf bestimmte Personen oder Firmen zugeschnitten. Besonders für Handelsunternehmen, die täglich mit vielen E-Mails, Kundendaten und Bestellinformationen arbeiten, entsteht dadurch ein erhöhtes Risiko.

### Wie nutzen Angreifer KI beim Phishing?

Cyberkriminelle verwenden KI, um ihre Angriffe realistischer, gezielter und effizienter zu gestalten. Typische Methoden sind:

- **Automatische Textgenerierung:** KI-Tools schreiben perfekte E-Mails ohne Tippfehler oder sprachliche Auffälligkeiten.
- **Personalisierung:** KI analysiert öffentlich verfügbare Informationen (z. B. aus sozialen Netzwerken) und passt den Inhalt an das Zielunternehmen an.

Gefördert durch:



Mittelstand-  
Digital



- **Imitation realer Personen:** Stimmen, Schreibstile oder Logos werden täuschend echt nachgebildet.
- **Massenangriffe:** KI kann in kurzer Zeit tausende individuelle Mails verschicken – jede leicht angepasst an das jeweilige Opfer.

So entstehen Mails, die auf den ersten Blick echt wirken – etwa eine angebliche Rechnung, eine Lieferbestätigung oder ein Kundenhinweis.

### Wie kann KI beim Schutz helfen?

Zum Glück wird KI auch auf der Seite der Verteidigung eingesetzt. Moderne Sicherheitssysteme erkennen verdächtige Muster, ungewöhnliche Sprache oder schädliche Links automatisch.

### Beispiele für KI-basierte Schutzmaßnahmen:

- **E-Mail-Scanner:** erkennen betrügerische Absender, fehlerhafte Links und bekannte Angriffsmuster.
- **Anomalieerkennung:** KI bemerkt, wenn ungewöhnlich viele Mails mit ähnlichem Inhalt auftreten.
- **Automatische Warnungen:** Verdächtige Nachrichten werden markiert oder in Quarantäne verschoben.

Diese Systeme sind wertvolle Helfer, aber sie können nur unterstützen. Entscheidend bleibt, dass Mitarbeitende aufmerksam bleiben und Warnzeichen erkennen.

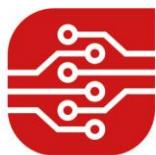
### Praxistipps – So schützen sich Unternehmen

1. **Absender prüfen:** Schau dir die vollständige E-Mail-Adresse an, nicht nur den angezeigten Namen.
2. **Links testen:** Fahre mit der Maus über einen Link, bevor du klickst – stimmt die angezeigte Adresse?

Gefördert durch:



Mittelstand-  
Digital



3. **Achtung bei Anhängen:** Öffne nur Dateien, die du erwartest.
4. **Vorsicht bei Zeitdruck:** E-Mails mit Formulierungen wie „sofort handeln“ sind verdächtig.
5. **Sicherheitssoftware nutzen:** Aktuelle Viren- und Spamfilter aktivieren und regelmäßig aktualisieren.
6. **Melden statt Schweigen:** Verdächtige Mails sofort an die IT oder verantwortliche Personen weiterleiten.

## Fazit

Phishing-Angriffe werden durch KI immer raffinierter – aber auch der Schutz wird intelligenter. Die beste Verteidigung ist die Kombination aus **technischem Schutz** und **bewusster Aufmerksamkeit**.

Gerade im Handel, wo täglich unzählige E-Mails mit Kund:innen und Lieferanten ausgetauscht werden, kann ein einziger Klick auf einen falschen Link großen Schaden anrichten.

**Merke:** KI kann helfen, Gefahren zu erkennen – aber dein wachsames Auge bleibt der entscheidende Faktor.

Gefördert durch:



Mittelstand-  
Digital