Phishing im Zeitalter von KI – wie KI Angriffe perfektioniert

Lukas Fässler
lic.iur.Rechtsanwalt[1,2], Informatikexperte
faessler@fsdz.ch

Zugerstrasse 76b
CH-6340 Baar
Tel.: +41 41 727 60 80
www.fsdz.ch
sekretariat@fsdz.ch
UID: CHE-349.787.199 MWST

Quelle: Studium publizierter Artikel zu «Phising und KI» (BornCity, Microsoft, BSI, Security-Insider, KeeperSecurity, Kapersky)

Author: Elena Martin

Datum: 30. April 2026

Phishing gehört seit Jahren zu den erfolgreichsten Methoden von Cyberkriminellen. Doch mit dem Einzug generativer künstlicher Intelligenz (KI) verändert sich die Bedrohungslage grundlegend. **Angriffe werden glaubwürdiger, schneller, skalierbarer – und für viele Menschen kaum noch zu erkennen**. Die im Artikel zusammengeführten Analysen von Sicherheitsfirmen, Forschungseinrichtungen und Behörden zeichnen ein klares Bild: **KI macht Phishing so gefährlich wie nie zuvor.**

Mehrere Quellen betonen, dass KI Phishing professionalisiert und automatisiert. Generative KI Modelle ermöglichen hyperpersonalisierte Nachrichten, perfekte Grammatik, täuschend echte Tonalität und automatisierte Erstellung in Sekunden. **KI-Phishing ist deshalb so gefährlich sei, weil Nachrichten «menschlich, fehlerfrei und personalisiert» wirken** und sich Inhalte sogar in Echtzeit anpassen können. Damit verschwinden klassische Warnsignale wie schlechte Sprache oder untypische Formulierungen. KI erzeugt fehlerfreie Phishing-Nachrichten, **wodurch traditionelle Erkennungsmerkmale nicht mehr greifen**.

KI ist in der Lage, riesige Datenmengen aus sozialen Netzwerken, beruflichen Profilen oder E-Mail-Verläufen zu analysieren. Eine neuere Angriffswelle nutzt KI-generierte, vollständig personalisierte E-Mails, die Rollen wie Einkauf oder Buchhaltung imitieren. Solche Angriffe nutzen dynamische Gerätecodes, Browser-in-Browser-Techniken und umgehen sogar MFA-Mechanismen. Das Ergebnis: **Phishing wird massgeschneidert – und damit extrem überzeugend.**

---

[1] Mitglied des Schweizerischen Anwaltsverbandes
[2] Eingetragen im Anwaltsregister des Kantons Zug

Ein weiterer Trend ist **die Nutzung von KI zur Imitation realer Personen**. Mit Deepfake-Stimmen, gefälschten Gesichtern und Chatbots, wird über Wochen Vertrauen aufgebaut. KI generiert automatisch erzeugte Fake-Websites und täuschend echte Landing Pages. Damit wird «CEO-Fraud» – etwa gefälschte Zahlungsanweisungen – noch glaubwürdiger. Auch Romance-Scams oder politische Manipulationen profitieren von dieser Entwicklung.

Die Kommerzialisierung von KI-Tools senkt die Einstiegshürden dramatisch. Mit **Phishing-as-a-Service (PhaaS)** ermöglicht es selbst technisch unerfahrenen Personen professionelle Angriffe durchzuführen. KI übernimmt Recherche, Textgenerierung, Design und sogar die Erstellung von Fake-Webseiten.

⇒ **Phishing wird damit zu einer globalen Industrie.** Laut IBM beginnt „jede siebte Datenpanne mit Phishing", die durchschnittlichen Kosten pro Vorfall liegen bei 4,9 Millionen Euro.

Die Zahlen sind alarmierend. Publizierte Auswertungen zeigen, dass KI-Phishing-Mails Klickraten von 54 bis 68 % erreichen, während klassische Angriffe bei rund 12 % liegen. Die Gesamtschäden durch KI-gestützte Cyberkriminalität werden auf 200 Milliarden Euro geschätzt. Studien von Security-Experten weisen darauf hin, **dass IT-Führungskräfte einen Anstieg von 51 % KI-basierter Angriffe beobachten**.

KI wird nicht nur für Social Engineering genutzt**. KI kann Sicherheitslücken autonom finden und sogar einfachen Schadcode (Malware) generieren**. Damit verschwimmen die Grenzen zwischen Social Engineering und technischen Angriffen – ein gefährlicher Trend, der Verteidigungsstrategien komplexer macht. Viele der beschriebenen Angriffe umgehen traditionelle Sicherheitsmassnahmen:

- Browser-in-Browser-Angriffe täuschen echte Login-Fenster vor
- Dynamische Codes imitieren MFA-Verfahren
- KI generiert täuschend echte Marken- oder Behördenkommunikation
- Filter erkennen KI-Texte oft nicht mehr zuverlässig

⇒ **Klassische E-Mail-Filter „versagen", weil KI-Inhalte keine typischen Muster mehr aufweisen**.

Wie sich Unternehmen schützen können

Technisch

- MFA mit Hardware-Token statt SMS
- KI-gestützte E-Mail-Filter
- DMARC, DKIM und SPF zur Domain-Absicherung
- Browser-Isolation für kritische Rollen

Organisatorisch

- Regelmässige Awareness-Trainings
- Klare Prozesse für Zahlungsfreigaben
- Vier-Augen-Prinzip bei sensiblen Aktionen
- Notfallkontaktwege ausserhalb von E-Mails

Individuell

- Vorsicht bei Zeitdruck
- Absender immer unabhängig verifizieren
- Keine Links in unerwarteten Nachrichten anklicken
- Keine sensiblen Daten per E-Mail weitergeben

Zusammenfassend: KI verändert Phishing grundlegend und macht Phishing schneller, glaubwürdiger, skalierbarer und schwerer erkennbar. Hyperpersonalisierung, Deepfakes, automatisierte Schwachstellensuche und PhaaS-Modelle führen zu einer Bedrohungslage, die Unternehmen und Privatpersonen gleichermassen betrifft. Unternehmen müssen technische, organisatorische und menschliche Schutzmassnahmen kombinieren

Über uns ….
Wir sind die Spezial-Anwaltskanzlei für digitale Rechtsfragen mit den Schwerpunktgebieten Informatikrecht, IP-Recht (insbesondere Marken-, Lizenz- Urheber- und Patentrecht), Cyberkriminalität, Europäisches und Schweizerisches Datenschutzrecht, Datensicherheit sowie Submissionsrecht im Informatiktechnologiebereich. Ferner sind wir spezialisiert in den Bereichen E-Commerce-Recht Europa für Onlineshops und ICT-Security und Riskmanagement.

Zu unseren Spezialgebieten gehören ebenfalls das Erb- und Immobilienrecht für Schweizer mit Wohnsitz in Frankreich oder für Schweizer, die Immobilien in Frankreich besitzen.

Was tun wir anders ….
Durch klare Spezialisierung erbringen wir qualitativ hochstehende Dienstleistungen ausschliesslich in