// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

KI-Phishing erkennen: Leitfaden für KMU in Österreich

KI-Phishing trifft österreichische KMU hart. Erkennungsmerkmale, Schutzmaßnahmen und NIS2-Pflichten — praxisnah erklärt.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
29. Mai 2026

ONLINE LESEN
https://wissen.strukturaflow.it.com/ki-phishing-erkennen-kmu-oesterreich/

Eine E-Mail vom „Steuerberater“ trifft ein: perfektes Deutsch, korrekte Signatur, der richtige Ansprechpartner. Alles stimmt — außer dass die Mail nicht vom Steuerberater stammt. KI-generierte Phishing-Mails enthalten keine klassischen Warnsignale mehr: kein gebrochenes Deutsch, keine generischen Anreden, keine verdächtigen Absenderadressen auf den ersten Blick.

Das Problem für österreichische KMU: Wer keine eigene IT-Abteilung hat, verlässt sich auf die Aufmerksamkeit der Mitarbeiterinnen und Mitarbeiter. Und genau dort greift KI-Phishing an — mit personalisierten Nachrichten, die aus Firmenbuch-Daten, LinkedIn-Profilen und der eigenen Firmenwebsite zusammengebaut werden.

Dieser Leitfaden erklärt, woran Sie KI-Phishing 2025 noch erkennen, welche Schutzmaßnahmen mit kleinem Budget sofort umsetzbar sind — und was NIS2 konkret für Ihr Unternehmen bedeutet.

Was KI-Phishing von klassischem Phishing unterscheidet

Klassisches Phishing war ein Mengenspiel: Millionen identische Mails, schlechtes Deutsch, generische Anreden. KI-generiertes Phishing funktioniert anders. Angreifer nutzen Large Language Models — teils speziell für kriminelle Zwecke angepasste Varianten wie WormGPT oder FraudGPT — um maßgeschneiderte Nachrichten in Sekunden zu erzeugen.

Was sich konkret verändert hat:

MERKMAL	KLASSISCHES PHISHING	KI-PHISHING
Sprachqualität	Oft fehlerhaft, generisch	Fehlerfrei, kontextuell korrekt
Personalisierung	Name + Anrede, mehr nicht	Firmenname, Projekte, Ansprechpartner, aktuelle Ereignisse
Erkennbarkeit	Hoch — bei aufmerksamer Lektüre	Gering — ohne Kontextprüfung kaum erkennbar
Angriffstempo	Massenversand, wenig Vorbereitung	Gezielt, datenbasiert vorbereitet
Zielgruppe	Breite Bevölkerung	Spezifische Personen in spezifischen Unternehmen

Laut CERT.at sind in Österreich besonders folgende Branchen im Visier: Handel, Steuerberatung/Wirtschaftsprüfung, Baugewerbe und Gastronomie. Nicht weil diese Branchen technisch unbedarfter wären, sondern weil sie häufig als Schnittstellen zu größeren Auftraggebern oder Finanzsystemen fungieren.

Spear-Phishing auf Österreichisch – wie das konkret aussieht

Szenario 1 — Gefälschte FinanzOnline-Benachrichtigung: Eine GmbH erhält eine Mail mit Betreff „Rückstandsausweis — Handlungsbedarf bis Freitag". Absender-Anzeigename: „FinanzOnline Service". Die Mail enthält die korrekte Steuernummer des Unternehmens (öffentlich über das Firmenbuch abrufbar), nennt den Geschäftsführer mit vollem Namen und verweist auf eine täuschend echte Login-Seite. Ziel: Zugangsdaten zu FinanzOnline.

Szenario 2 — Angebliche WKO-Abmahnung: Eine Handels-KG erhält eine formale Abmahnung wegen angeblicher Datenschutzverstöße. Briefkopf, Firmenbuchnummer, Geschäftsführernennung — alles korrekt. Angehängt ist ein .docx-Dokument mit aktivierten Makros. Der einzige Hinweis: Die Absender-Domain lautet wko-service.at statt wko.at.

Szenario 3 — CEO-Fraud mit lokalem Kontext: Die Buchhaltung eines Wiener Betriebs erhält eine interne Mail, scheinbar vom Geschäftsführer: „Schau, ich bin grad beim Kunden draußen in Favoriten — kannst du bitte die Überweisung von 8.400 Euro für die neue Lieferantenrechnung im Anhang noch heute rausmachen? Ich ruf dann nach." Ton, Schreibstil und Formulierungen wurden aus früheren E-Mails imitiert, die über einen kompromittierten Mailaccount abgegriffen wurden.

Die 7 Erkennungsmerkmale, die noch funktionieren

Wenn Sprache und Formatierung nicht mehr reichen, worauf soll man dann achten? Hier sind die Merkmale, die KI-Phishing noch verrät — und die sich trainieren lassen.

1. Absender-Domain exakt prüfen, nicht nur den Anzeigenamen Outlook und Gmail zeigen standardmäßig den Anzeigenamen, nicht die technische Absenderadresse. Wer in Outlook auf den Absendernamen klickt, sieht die echte Adresse. In Gmail öffnet ein Klick auf den Pfeil neben dem Namen das Detail. Konkret: „WKO Service info@wko-service.at" ist keine WKO-Adresse.

2. Ungewöhnlicher Zeitpunkt oder fehlender Kontext Kommt eine Mail ohne Vorgeschichte? Kein laufendes Projekt, kein vorheriger Kontakt, kein Grund für diese Anfrage genau jetzt? KI kann eine überzeugende Mail schreiben, aber keinen echten Kommunikationsverlauf erfinden.

3. Künstliche Dringlichkeit kombiniert mit eingeschränkten Optionen „Bis heute 17:00 Uhr", „Bitte nur über diesen Kanal", „Ruf mich nicht an, bin im Meeting" — diese Kombinationen sollen Nachfragen verhindern. Legitime Anfragen — auch dringende — vertragen eine kurze Rückfrage.

4. Links vor dem Klicken auf Hover prüfen Mauszeiger über den Link halten (nicht klicken): Wohin führt die URL tatsächlich? Bei mobilen Geräten: Link lang antippen, um die vollständige URL anzuzeigen. Achten Sie auf Subdomain-Tricks wie „finanzonline.at.phishingdomain.com" — das ist keine österreichische Behörden-Domain.

5. Ungewöhnliche Dateianhänge Dateiformate wie .iso, .lnk, .html-Archiv (.htm in einem ZIP) oder passwortgeschützte Archive ohne Erklärung sind Warnsignale. Legitime Geschäftspartner versenden selten .iso-Dateien.

6. Inkonsistente Signaturdetails Telefonnummer stimmt nicht mit der Website überein? Adresse veraltet? Fehlt die Durchwahl, die sonst immer dabei ist? KI kann aus öffentlichen Quellen eine Signatur zusammenbauen — aber Inkonsistenzen schleichen sich ein, wenn die Quellen nicht aktuell sind.

7. Bitte um Prozessumgehung „Sag bitte niemandem davon", „Das läuft außerhalb des normalen Bestellprozesses", „Ich erkläre alles später" — jede Anfrage, die etablierte interne Abläufe aushebeln soll, ist ein starkes Warnsignal. Keine legitime Geschäftsanfrage braucht Geheimhaltung gegenüber Kolleginnen und Kollegen.

Diese sieben Punkte sind erlernbar. Sie erfordern keine technischen Kenntnisse, nur Gewohnheit.

Schritt-für-Schritt – So reagieren Sie auf eine verdächtige Mail

Wenn eine Mail Zweifel auslöst, gilt: Reihenfolge einhalten, nicht improvisieren.

Schritt 1: Nicht klicken, nicht antworten Die Mail bleibt unberührt. Kein Link, kein Anhang, keine Antwort. Wer die Mail in einem separaten Ordner verschiebt oder markiert, verhindert versehentliche Interaktion durch andere.

Schritt 2: IT oder Vertrauensperson informieren Falls eine interne IT-Ansprechperson existiert: sofort melden. Falls nicht, direkt weiter zu Schritt 3.

Schritt 3: Absender über einen bekannten, unabhängigen Kanal verifizieren Nicht über „Antworten" — sondern über eine Telefonnummer aus dem eigenen Adressbuch oder von der offiziellen Website. „Ich habe eine Mail von euch bekommen — habt ihr die wirklich geschickt?" dauert 90 Sekunden und ist der zuverlässigste Test.

Schritt 4: Vorfall dokumentieren Zeitpunkt, Betreff, Absender-Domain, Screenshot. Diese Dokumentation ist wichtig für DSGVO-Meldepflichten und etwaige Anzeigen. Ein simples E-Mail an sich selbst mit Screenshot reicht als Erstdokumentation.

Schritt 5: Meldung an CERT.at Das österreichische Computer Emergency Response Team nimmt Phishing-Meldungen unter https://www.cert.at/de/meldungen/ entgegen. Eine Meldung ist sinnvoll, wenn die Mail überzeugend gestaltet ist und wahrscheinlich an viele österreichische Empfänger verschickt wurde. CERT.at wertet Meldungen aus und warnt bei systematischen Angriffswellen.

Schritt 6: Bei tatsächlichem Schadensfall — Anzeige erstatten Wurde auf einen Link geklickt, wurden Daten eingegeben, wurde eine Überweisung ausgelöst? Dann ist die Cybercrime-Meldestelle des BMI zuständig. Anzeige unter https://www.bmi.gv.at/ — und parallel sofort Passwörter ändern, betroffene Konten sperren, Bank informieren.

> **Wann ist sofortiges Handeln nötig?**
>
> Verdächtig aber nichts passiert (Mail nur gelesen): Ruhig und strukturiert vorgehen, Schritte 1–5 reichen.
>
> Link geklickt oder Seite geöffnet: Gerät vom Netzwerk trennen, IT informieren, Passwörter von einem anderen Gerät ändern. Auch wenn „nichts passiert zu sein scheint" — Schadcode kann im Hintergrund aktiv sein.
>
> Daten eingegeben oder Überweisung ausgelöst: Sofortmaßnahmen, Anzeige, Bank, DSGVO-Meldung prüfen. Zeit zählt.

Bei einem erfolgreichen Phishing-Angriff werden häufig zuerst Passwörter abgegriffen. Was danach mit diesen Zugangsdaten passiert — und warum schwache Passwort-Hashing-Verfahren das Problem verschärfen — erklärt unser Artikel Der Algorithmus aus 1991, der heute Ihre Passwörter knackt.

NIS2 und KI-Phishing – Was das für österreichische GmbHs bedeutet

Das österreichische NIS2-Umsetzungsgesetz (NISG 2024) ist seit 2024 in Kraft. Wer als „wesentliche" oder „wichtige Einrichtung" eingestuft wird, unterliegt konkreten Anforderungen — darunter Risikomanagement, Incident-Reporting und Mitarbeiterschulungen.

Direkt betroffen sind in Österreich primär Unternehmen ab 50 Mitarbeitern in definierten Sektoren (Energie, Gesundheit, Verkehr, digitale Infrastruktur u. a.). Für viele KMU unter 50 Mitarbeitern gilt: keine direkte NIS2-Pflicht.

Aber — die Lieferketten-Logik greift trotzdem:

Wenn Ihr Unternehmen Dienstleistungen an eine NIS2-pflichtige Organisation erbringt — als Subunternehmer, IT-Dienstleister, Steuerberater, Logistikpartner — dann fordern diese Auftraggeber zunehmend Nachweise über Ihr eigenes Sicherheitsniveau. Ein erfolgreicher Phishing-Angriff auf Ihr KMU kann die Systeme des Auftraggebers gefährden. Das wird in Verträgen und Ausschreibungen zunehmend explizit adressiert.

Mehr zur NIS2-Einordnung für österreichische KMU finden Sie im Artikel NIS2 / NISG 2026: Auch ohne direkte Pflicht relevant für KMU?

Relevant ist auch die DSGVO-Meldepflicht: Wer durch einen Phishing-Angriff personenbezogene Daten verliert oder unbefugt preisgibt, hat nach Artikel 33 DSGVO 72 Stunden Zeit, die Datenschutzbehörde zu informieren. Das gilt unabhängig von der Unternehmensgröße. Bei konkreten Rechtsfragen empfehlen wir die Konsultation eines Datenschutzanwalts — dieser Artikel ersetzt keine Rechtsberatung.

Hinweis: Unkontrollierter KI-Einsatz im Unternehmen — sogenannte Shadow AI — vergrößert die Angriffsfläche und ist ebenfalls NIS2-relevant. Wer KI-Tools im Team einsetzt, ohne dass die IT davon weiß, schafft potenzielle Einfallstore, die durch einen Phishing-Angriff ausgenutzt werden können. Mehr dazu im Artikel KI-Workflows mit Unternehmensdaten absichern.

Die WKO stellt unter wko.at/nis2 einen eigenen NIS2-Leitfaden zur Verfügung — empfehlenswert als erste Orientierung.

Schutzmaßnahmen mit KMU-Budget – Was kostet was in Österreich

Kein österreichisches KMU mit 10 Mitarbeitern und 3 Millionen Euro Jahresumsatz braucht eine Enterprise-Security-Plattform für 50.000 Euro im Jahr. Was es braucht: die richtigen Maßnahmen in der richtigen Reihenfolge.

STUFE	MONATLICHE KOSTEN	MASSNAHMEN
Basis	0–50 €	DMARC/DKIM/SPF konfigurieren, Phishing-Filter in Microsoft 365 oder Google Workspace aktivieren, CERT.at-Newsletter abonnieren
Standard	50–200 €	Proofpoint Essentials, Microsoft Defender for Business, Hornetsecurity (österreichischer Anbieter mit DSGVO-Vorteil und deutschsprachigem Support)
Erweitert	200–500 €	Managed Security Service Provider (MSSP) — österreichische Anbieter wie lokale MSPs mit Security-Fokus, Raiffeisen IT, oder spezialisierte IT-Dienstleister mit österreichischem Datenschutzsitz

Hinweis: Dies ist eine Orientierungstabelle, keine Produktempfehlung. Preise können variieren; keine Affiliate-Beziehungen.

Warum österreichische Anbieter bei Sicherheitsprodukten einen echten Vorteil haben: Datenhaltung in der EU (relevant für DSGVO-Compliance), deutschsprachiger Support ohne Wartezeit über internationale Hotlines, und im Schadensfall kürzere Reaktionswege.

Wenn KI-Tools im Unternehmen eingesetzt werden, ist auch der Datenzugriff dieser Systeme abzusichern. Ein erfolgreicher Phishing-Angriff, der Zugangsdaten zu einem KI-Agenten kompromittiert, kann mehrere Systeme gleichzeitig gefährden. Mehr dazu im Artikel KI-Workflows mit Unternehmensdaten absichern.

DMARC, SPF, DKIM – Drei Konfigurationen, die jedes KMU sofort prüfen sollte

Diese drei Protokolle schützen nicht nur eingehende Mails — sie verhindern, dass die eigene Domain für Phishing-Mails an andere missbraucht wird.

SPF (Sender Policy Framework) legt fest, welche Server im Namen Ihrer Domain Mails versenden dürfen. Fehlt ein SPF-Eintrag, kann jeder Server Mails mit Ihrer Absenderadresse verschicken.

DKIM (DomainKeys Identified Mail) signiert ausgehende Mails kryptografisch. Empfänger-Server können prüfen, ob die Mail tatsächlich von Ihrer Domain stammt und unterwegs nicht verändert wurde.

DMARC (Domain-based Message Authentication, Reporting & Conformance) kombiniert SPF und DKIM und legt fest, was mit Mails passiert, die diese Prüfungen nicht bestehen — Ablehnen, Quarantäne oder nur Reporting.

Prüfen Sie den Status Ihrer Domain kostenlos unter MXToolbox. Eingabe: Ihre Domain, Auswahl „DMARC Lookup“. Ein fehlender DMARC-Eintrag bedeutet: Ihre Domain kann für Phishing-Mails missbraucht werden, ohne dass Sie es bemerken.

Mitarbeiterschulung – Wie Sie KI-Phishing-Awareness in Ihrem Team aufbauen

Technische Maßnahmen filtern einen Teil der Angriffe heraus. Den Rest entscheiden Menschen. Laut Branchenstatistiken sind über 80 % erfolgreicher Cyberangriffe auf menschliche Fehler zurückzuführen — und das bleibt auch mit KI-Phishing so, nur die Fehler werden schwerer zu vermeiden.

Was funktioniert, was nicht:

Ein einmaliger Schulungstag pro Jahr funktioniert nicht. Mitarbeiterinnen und Mitarbeiter vergessen; Angriffsmuster ändern sich. Was funktioniert: kurze, regelmäßige Wiederholung.

Konkrete Maßnahmen:

- **15-Minuten-Briefings monatlich** — kein Frontalvortrag, sondern ein konkretes Beispiel aus der Praxis: „Diese Woche hat eine ähnliche Firma in unserer Branche diesen Angriff erlebt — so hat er ausgesehen."
- **Simulierte Phishing-Tests** — Tools wie KnowBe4 (Free Trial verfügbar) oder das Open-Source-Tool GoPhish erlauben es, intern zu testen, wie viele Mitarbeitende auf eine simulierte Phishing-Mail klicken würden. Wichtig: Das Ziel ist Sensibilisierung, nicht Bestrafung.
- **„Verdächtige Mail melden"-Kultur** — Wer eine Mail meldet, die sich als harmlos herausstellt, hat trotzdem richtig gehandelt. Fehlalarme sind gut. Stille ist gefährlich.
- **Österreich-spezifische Szenarien** — Schulen Sie mit konkreten Beispielen: Finanzamt, SVS, WKO, FinanzOnline, ELDA. Diese Behörden werden von Angreifern gezielt imitiert, weil österreichische KMU mit ihnen regelmäßig zu tun haben.

5-Punkte-Schulungsplan für KMU ohne IT-Abteilung:

1. Einmalige 30-Minuten-Einführung für das gesamte Team: Die 7 Erkennungsmerkmale + Meldeweg intern klären
2. Monatliches 15-Minuten-Briefing mit einem aktuellen Beispiel (CERT.at liefert regelmäßig Warnungen als Vorlage)
3. Simulierten Phishing-Test mit GoPhish oder KnowBe4 Free Trial durchführen
4. Internen Meldeweg schriftlich festhalten und im Team kommunizieren
5. Halbjährliche Überprüfung: Hat sich etwas an Angriffsmustern verändert?

Förderungen: Die AWS Digitalisierungsförderung und das Programm KMU.DIGITAL haben in der Vergangenheit Maßnahmen zur Cybersicherheit mitgefördert. Aktuelle Verfügbarkeit und Konditionen bitte direkt bei der AWS (Arbeitsmarktservice) und der WKO prüfen — Programme werden regelmäßig angepasst. Informationen zur aktuellen KI-Förderungslandschaft in Österreich finden Sie auch im Artikel KI Förderung Österreich 2026: KMU-Leitfaden.

Praxis-Tipp – KI-gestützte Sicherheit richtig einordnen

Wenn KI auf der Angreiferseite eingesetzt wird, liegt der Gedanke nahe: Dann brauchen wir KI auf der Verteidigungsseite. Das stimmt — aber mit Einschränkungen.

KI-basierte E-Mail-Security (etwa in Microsoft 365 Defender oder vergleichbaren Produkten) erkennt Muster: ungewöhnliche Absenderverhalten, abnormale Linkstrukturen, Metadaten-Anomalien. Das ist wertvoller als reine Filter-Regeln.

Das Grundproblem: KI auf der Angreiferseite passt sich an. Was heute als Muster erkannt wird, ist morgen bereits angepasst. Das ist kein Argument gegen KI-gestützte Sicherheitstools — aber es ist ein Argument gegen die Erwartung, dass ein einzelnes Tool ausreicht.

Was tatsächlich funktioniert: das Zusammenspiel aus technischen Maßnahmen (E-Mail-Filter, DMARC/SPF/DKIM, MFA), menschlicher Awareness (Schulung, Prozesse, Meldekultur) und klaren internen Abläufen (wer entscheidet was, wenn eine verdächtige Mail ankommt).

Bei Strukturaflow sehen wir regelmäßig, dass KMU in dieser Reihenfolge stolpern: zuerst wird ein teures Tool gekauft, dann wird festgestellt, dass es falsch konfiguriert ist, und dann fehlt die interne Struktur, um Vorfälle überhaupt zu bemerken. Die sinnvollere Reihenfolge ist umgekehrt: erst Struktur, dann Konfiguration, dann Tools.

FAQ

Woran erkenne ich, ob eine E-Mail mit KI generiert wurde?

In der Praxis nicht zuverlässig. KI-Detektions-Tools für Text haben hohe Fehlerquoten und sind leicht zu umgehen. Was hilft: nicht auf die Sprache achten, sondern auf Kontext und Prozess. Kommt die Mail zu einem unerwarteten Zeitpunkt? Passt die Anfrage nicht zum laufenden Geschäft? Weicht sie von gewohnten Abläufen ab? Das sind die zuverlässigeren Signale.

Bin ich als kleines österreichisches Unternehmen wirklich ein Ziel für KI-Phishing?

Ja — gerade KMU sind für Angreifer interessant, weil sie oft Zugangsdaten zu größeren Partnerunternehmen, Finanzdienstleistern oder Behördensystemen besitzen und dabei weniger Schutz bieten als Konzerne. Ein Subunternehmer mit Zugang zum ERP-System eines Großkunden ist ein attraktiveres Ziel als der Großkunde selbst — weil der Weg dorthin einfacher ist.

Was muss ich bei einem Phishing-Angriff rechtlich melden?

Nach DSGVO (Artikel 33) gilt: Wenn durch den Angriff personenbezogene Daten kompromittiert wurden — also Kundendaten, Mitarbeiterdaten, Gesundheitsdaten — muss die österreichische Datenschutzbehörde (DSB) innerhalb von 72 Stunden informiert werden. Bei hohem Risiko für die betroffenen Personen sind auch diese zu informieren (Artikel 34 DSGVO). Das gilt nach aktueller Rechtslage — bei konkreten Fragen empfiehlt sich die Rücksprache mit einem Datenschutzanwalt.

Nächste Schritte – Was Sie diese Woche noch tun können

Fünf Maßnahmen, die keine IT-Kenntnisse erfordern und zusammen unter zwei Stunden dauern:

1. **DMARC-Status der eigenen Domain prüfen** — MXToolbox öffnen, Domain eingeben, DMARC Lookup. Dauert 5 Minuten. Ergebnis: Sie wissen, ob Ihre Domain aktuell für Phishing missbraucht werden kann.
2. **Team per E-Mail auf die 7 Erkennungsmerkmale hinweisen** — Die Liste aus diesem Artikel direkt kopieren und intern verschicken. Kein Meeting, keine Präsentation notwendig.
3. **CERT.at Newsletter abonnieren** — Kostenlos, österreichischer Kontext, aktuelle Warnmeldungen. Abonnement unter https://www.cert.at/.
4. **Microsoft 365 / Google Workspace Phishing-Filter überprüfen** — Beide Plattformen haben integrierte Phishing-Schutzfunktionen, die oft nicht aktiviert oder nicht korrekt konfiguriert sind. Der jeweilige Admin-Bereich unter „Sicherheit" oder „Spam-Filter" ist der richtige Einstiegspunkt.
5. **Intern klären: Wer ist Ansprechperson bei einer verdächtigen Mail?** — Diese Person muss nicht IT-Kenntnisse haben. Sie muss nur da sein und wissen, was zu tun ist. Wenn diese Frage offen ist, ist das die wichtigste Maßnahme dieser Woche.

Wenn Sie nach diesen Schritten das Gefühl haben, dass Sie zwar die Oberfläche verstehen, aber nicht sicher sind, wo Ihr tatsächlich größtes Risiko liegt — welche Konfigurationen fehlen, welche Maßnahmen für Ihre konkrete Unternehmensgröße und Branche Priorität haben — dann ist ein strukturiertes Beratungsgespräch der sinnvollste nächste Schritt. Im unverbindlichen 30-Minuten-Gespräch analysieren wir gemeinsam Ihre aktuelle Situation und zeigen Ihnen, welche Maßnahmen für Ihre Größe und Ihr Budget tatsächlich sinnvoll sind — ohne Produktverkauf, ohne Verpflichtung.