



Phishing wird immer raffinierter: Wie KI Online-Betrug verändert

Haben Sie jemals eine E-Mail-Adresse erhalten, die echt aussah, aber tatsächlich ein Betrugsversuch war? Das nennt sich Phishing — ein Trick, den Cyberkriminelle verwenden, um an Ihre persönlichen Informationen zu gelangen. Mit Hilfe von künstlicher Intelligenz (KI) werden diese Betrugsmaschen jetzt noch überzeugender. Im Folgenden zeigen wir, wie KI Phishing-Angriffe verändert und was Sie tun können, um sich in dieser sich stetig wandelnden digitalen Umgebung zu schützen.



Wie KI es schwieriger macht, Phishing-Versuche zu erkennen

Personalisierte Angriffe

KI kann Social Media-Daten und weitere Informationen aus dem Internet analysieren, relevante Details zusammenstellen und so personalisierte Phishing-Mitteilungen erstellen. Die auf Basis von persönlichen Informationen durch KI erstellten E-Mails sind dann an Sie persönlich adressiert, wodurch diese gefälschten Mitteilungen schwerer zu erkennen sind.

Bessere Formulierungen und Texte

KI kann E-Mails mit weniger Fehlern kreieren, wodurch Nachrichten mit schädlichen Inhalten authentischer wirken.

Sprach- und Video-Tricks

KI kann menschliche Stimmen täuschend echt nachahmen oder Gesichter so realistisch imitieren, dass diese in gefälschten Videos eine oder mehrere Ihnen bekannte Personen zu zeigen scheinen. Sie könnten beispielsweise einen Anruf von einem Freund erhalten, der Sie um Geld bittet. In Wahrheit aber steckt dahinter KI-gestützte Software.

Gezielte und anpassungsfähigere Angriffe

KI erstellt nicht nur überzeugende Phishing-Nachrichten; sie revolutioniert auch die Herangehensweise von Cyberkriminellen bei Betrugsmaschen. Diese KI-gestützten Systeme können:

- Phishing-Ergebnisse in Echtzeit analysieren
- Angriffsstrategien schnell verfeinern
- Perfekt personalisierte Nachrichten für spezifische Ziele erstellen
- Lernen und sich Schritt für Schritt verbessern

Dieser adaptive Ansatz macht KI-gestütztes Phishing für Einzelpersonen und Sicherheitssysteme zunehmend schwieriger zu erkennen. Durch die stetige, rasche Weiterentwicklung werden Angriffe ausgeklügelter, wodurch Schwachstellen besser und schneller ausgenutzt werden können. Das Ergebnis? Eine neue Ära bricht an: Phishing wird schneller, klüger und reaktionsfähiger. Es entwickelt sich kontinuierlich weiter und ist somit klassischen, bewährten Abwehrmaßnahmen stets einen Schritt voraus.



Wie Sie sich schützen können

KI-generierter Inhalt kann folgende Merkmale aufweisen:

- Ungewöhnliche Formulierungen oder abrupte Änderung des Tonfalls
- Plötzliche Änderungen im Schreibstil
- Unpassende Wortwahl
- Unstimmigkeiten bei persönlichen Angaben

Praktische Schritte zur Verbesserung Ihrer Sicherheit:

- Aktivieren Sie die Multi-Faktor-Authentifizierung bei allen Konten
- Verwenden Sie einen Passwort-Manager, um starke, eindeutige Passwörter zu erstellen und zu speichern
- Seien Sie vorsichtig beim Klicken auf Links oder Herunterladen von Anhängen, auch wenn diese von scheinbar vertrauten Quellen stammen
- Überprüfen Sie Anfragen nach sensiblen Daten über einen separaten, vertrauenswürdigen Kanal

Blieben Sie sicher und lassen Sie sich nicht von den Cyberkriminellen erwischen!



Indem Sie wachsam bleiben und gute Gewohnheiten im Bereich der Onlinesicherheit annehmen, können Sie sich bestmöglich vor Betrugsversuchen schützen.

Denken Sie daran: Wenn etwas zu gut klingt, um wahr zu sein, ist es das wahrscheinlich auch. Vertrauen Sie Ihrem Bauchgefühl und gehen Sie immer auf Nummer sicher, bevor Sie persönliche Daten online teilen. Bleiben Sie sicher und lassen Sie sich nicht von den Cyberkriminellen erwischen!