

20.07.2023

# Le banche e gli attacchi informatici basati sull'IA

**Spesso gli istituti finanziari sono presi di mira dai truffatori. Anche per i criminali informatici l'intelligenza artificiale (IA) è estremamente promettente, perché rende gli attacchi sempre più sofisticati.**

«Tutto il gran parlare su ChatGPT stimola la creatività dei cybercriminali», afferma la società statunitense di cibersicurezza Palo Alto Networks. La squadra aziendale d'indagine sulle minacce ha svelato numerosi tentativi di frode. Pubblicando siti Internet contraffatti o spacciandosi per il capo grazie all'IA, i criminali cercano di convincere i collaboratori a effettuare pagamenti urgenti. «Le truffe fatte con ChatGPT sono in aumento», concludono gli esperti.

L'Ufficio federale tedesco per la sicurezza nelle tecnologie dell'informazione (BSI) è preoccupato che in futuro l'IA venga utilizzata in tentativi di inganno basati sull'uso di «voci o video falsificati». Ad esempio, i criminali possono falsificare le voci e lasciare a dipendenti o clienti di una banca messaggi vocali manipolati provenienti da un numero di telefono apparentemente noto. Anche i video registrati si possono falsificare. Per ora l'IA non sarebbe in grado di imitare le conversazioni audio o video in diretta, afferma Nico Leidecker, un hacker che lavora per l'azienda tedesca di sicurezza informatica NVISO. «Ma le cose potrebbero cambiare in futuro, perché la tecnologia si evolverà rapidamente».

Le aziende che impiegano al loro interno sistemi di intelligenza artificiale si trovano ad affrontare nuove vulnerabilità. Nel suo rapporto SONAR 2023, la compagnia di riassicurazioni Swiss Re lancia l'allarme contro questo fenomeno nel capitolo «L'IA viene violata – vulnerabilità sistemiche di una tecnologia in espansione». Gli hacker professionisti non sarebbero solo in grado di manipolare i modelli in modo da generare errori e perdite di dati, ma anche di manipolare i dati, così da falsare i calcoli dei premi, per esempio.

## **Protegetevi così:**

- Comunicate il minor numero possibile di informazioni personali su di voi. Sulle reti sociali, in particolare, è opportuno agire con grande cautela nella pubblicazione di informazioni.
- Siate sospettosi quando ricevete richieste di informazioni via e-mail o al telefono. Anche le e-mail di mittenti conosciuti e le telefonate da numeri noti possono essere falsificate!
- Gestite con grande prudenza gli allegati delle e-mail e dei servizi di messaggistica breve.
- In caso di incertezze o dubbi rivolgetevi al vostro istituto finanziario.