Phishing
AI POWERED PROTECTION

THREAT AWARENESS

AI + Social Engineering: l'alleanza più pericolosa della cybersecurity

Deepfake, voice cloning e avatar interattivi: le nuove armi dell'inganno che le aziende devono conoscere oggi

A cura di Rosario Mauro Catanzaro

10 gennaio 2025 www.gpiphishing.com

THREAT AWARENESS

Deepfake, voice cloning e avatar interattivi: le nuove armi dell'inganno che le aziende devono conoscere oggi

01 L'intelligenza artificiale ha cambiato le regole

Fino a qualche anno fa, un'e-mail di phishing si riconosceva dagli errori grammaticali, dai loghi sgranati, dall'italiano impreciso. Quei tempi sono finiti. I modelli linguistici avanzati consentono oggi di generare in pochi secondi messaggi perfettamente scritti, personalizzati con informazioni reali sulla vittima, adattati al contesto aziendale specifico.

La combinazione di social engineering e intelligenza artificiale ha prodotto un salto qualitativo nella pericolosità degli attacchi: più credibili, più mirati, più scalabili. Un attaccante può ora colpire migliaia di persone con messaggi ultra-personalizzati a un costo vicino allo zero.

02 Deepfake: quando vedere non significa credere

Le reti neurali generative sono in grado di produrre video in cui il volto di una persona viene sostituito con quello di un impostore in modo indistinguibile dall'originale. Più accessibile ancora è il **voice cloning**: bastano pochi secondi di audio per addestrare un modello che riproduce fedelmente il timbro e l'intonazione di una persona reale.

Nel 2020, un'azienda britannica ha subito una frode da 243.000 dollari dopo che il CFO aveva ricevuto una telefonata con la voce sintetizzata del CEO, che richiedeva un bonifico urgente. Non era un caso isolato: è diventato un vettore d'attacco sistematico, e oggi, con i modelli disponibili online, è alla portata di chiunque.

03 Gli avatar interattivi: la frontiera dell'“avishing”

Questa tecnica, già denominata 'avishing' (Avatar Phishing), rappresenta il prossimo scenario d'attacco su larga scala per le organizzazioni.

> *I messaggi malevoli generati con supporto AI sono fino al 40% più efficaci nel superare i filtri di sicurezza tradizionali e nell'ingannare l'utente finale.*

La frontiera più avanzata è rappresentata dagli avatar interattivi: sistemi che combinano clonazione vocale e manipolazione video in tempo reale, capaci di sostenere conversazioni credibili durante una videoconferenza. Un partecipante a una chiamata di lavoro potrebbe trovarsi di fronte a qualcuno che sembra e parla esattamente come il proprio direttore finanziario — ma non lo è.[1]

04 L'AI come difesa

La buona notizia è che la stessa tecnologia può essere impiegata in senso difensivo. Algoritmi di machine learning analizzano pattern anomali nel traffico e-mail, strumenti di natural language processing identificano testi potenzialmente fraudolenti, soluzioni di deep learning cercano artefatti nei video deepfake. La corsa agli armamenti è simmetrica.

Per le organizzazioni, la risposta non è solo tecnologica: è formare i dipendenti a riconoscere anche i segnali più sottili, a verificare sempre su canali alternativi prima di autorizzare operazioni sensibili, e a non fidarsi mai di una richiesta basata su urgenza improvvisa, anche se la voce sembra familiare.

RIFERIMENTI

1 Il termine “avishing” (Avatar Phishing) è proprietario, definito dall'autore come acronimo coerente con la logica di vishing e smishing.

GPI PHISHING — CYBERSECURITY PLATFORM

Proteggi la tua azienda dalle minacce AI-driven di nuova generazione

Rilevamento avanzato, formazione continua e simulazioni realistiche per proteggere la tua organizzazione.

Phishing
AI POWERED PROTECTION

www.gpiphishing.com