CYBEREADY

Gli strumenti di intelligenza artificiale stanno cambiando le regole del gioco per gli hacker.

Sei pronto?

In passato...

Gli attacchi altamente ingannevoli richiedevano molto tempo e lavoro e potevano essere creati solo da hacker esperti.

Di conseguenza, **la maggior parte dei tentativi di phishing avveniva con poca esperienza** (ad esempio, con errori di ortografia, design sospetti, linguaggio scorretto e così via), quindi individuare un messaggio falso risultava piuttosto facile.

Al giorno d'oggi...

Gli strumenti di intelligenza artificiale consentono agli hacker di creare in modo semplice e veloce e-mail e contenuti dall'aspetto altamente professionale.

Per questo motivo, **gli attacchi più sofisticati hanno iniziato a raggiungere le nostre caselle di posta.** Questi attacchi altamente ingannevoli sono più difficili da identificare come minacce e fanno aumentare il rischio di caderci.

Come puoi riconoscere il phishing ora?

- Nelle e-mail, assicurati che l'**indirizzo del mittente** appaia esattamente come previsto. Gli hacker non possono falsificare questo dettaglio.

- Passa il mouse sui **link** prima di fare clic per assicurarti che siano legittimi. Gli hacker possono imitare i design di aziende famose, ma non possono utilizzare i loro domini originali.

Cosa non è più un segno affidabile di autenticità?

- Design professionali
- Testo ben scritto
- Registrazione vocale di qualcuno che conosci
- Video di alta qualità

CYBERREADY

Ricorda: La nostra sicurezza è nelle nostre mani.

Prendi l'abitudine di esaminare ogni e-mail prima di fare clic su qualsiasi link e non controllare mai le e-mail quando sei distratto.