

CYBER SECURITY TIPS #72

CHATGPT  
**E CYBER SECURITY:
QUALI I RISCHI?**

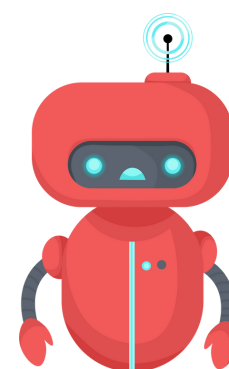
LEGGI SUBITO LE NOSTRE TIPS!



1. COS'È CHATGPT?

ChatGPT è un Bot di intelligenza artificiale sviluppato da OpenAI.

Quello che lo distingue da altre AI è l'accuratezza e la naturalezza con cui è in grado di rispondere alle domande.



2. CHE RISCHI COMPORTA PER LA SICUREZZA?

ChatGPT ha aperto un mondo di possibilità: al Bot possiamo chiedere praticamente tutto.

La domanda che sorge però è questa: può essere usato anche per svolgere attività criminali?



3. CHATGPT PUÒ COMPIERE ATTIVITÀ ILLEGALI?

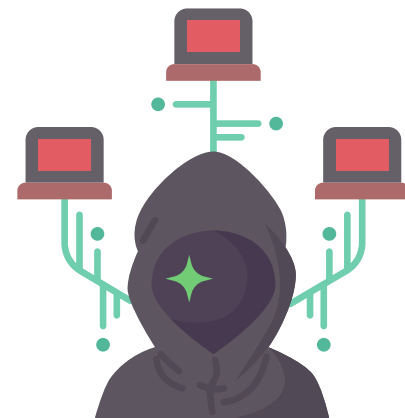
La risposta è no,
è programmato per non farlo.

Non è però così difficile aggirarne i sistemi di controllo: esistono già alcuni metodi e programmi realizzati apposta. Inoltre, in molti casi è sufficiente non dichiarare apertamente le proprie intenzioni al Bot.



4. GENERAZIONE AUTOMATICA DI MALWARE.

Qualsiasi criminale con scarse competenze tecniche potrebbe, per esempio, chiedere a ChatGPT di generare solo alcune parti di codice di un software malevolo per poi assemblarle in un file a parte.



5. TRUFFE VIA EMAIL.

L'AI può essere impiegata anche per generare messaggi di Phishing convincenti in maniera massiva.



6. UN'ALTRA QUESTIONE: LA PROTEZIONE DEI DATI.

Tutto quello che carichiamo nei Chat Bot resta nei database delle organizzazioni che li gestiscono.



Chiediamoci sempre:

- Che fine faranno questi dati?
- Saranno conservati in maniera sicura?
- Il database a cui attinge la AI è difeso da potenziali Breach?

7. COME PROTEGGERCI?

1. Cyber Security Awareness



Continua ad aggiornarti sulle minacce e sii consapevole del fatto che le truffe saranno sempre più numerose e difficili da individuare.

2. Segui le regole base di sicurezza

Usa sempre la dovuta cautela, soprattutto quando maneggi denaro o dati sensibili online. Se ti servono consigli a riguardo leggi anche la caption! ←

8. COME PROTEGGERCI?

3. Tutela i tuoi dati

Evita di fornire dati sensibili alle intelligenze artificiali come:

- indirizzi
- dati bancari
- immagini
- documenti
- ecc...



TI È STATO UTILE QUESTO POST?



Faccelo sapere
con un like!

lumit.it