Happy Monday!
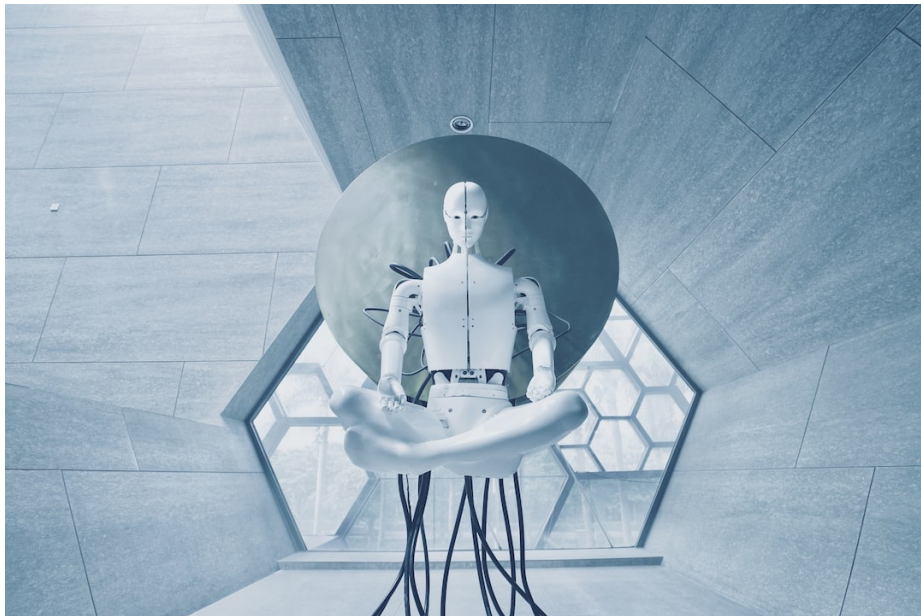
Welcome to the 22nd issue of CyberSec Weekly.
Here is a quick rundown of this week's stories:

Chat-GPT cyber-criminals on the rise

14 cybersecurity best practices for end-users

New phishing attack targeting cybersecurity professionals

Cybercriminals Build Malware And Plot Fake Girl Bots With Chat-GPT

Cybercriminals have started using OpenAI's artificially intelligent chatbot ChatGPT to quickly build hacking tools, cybersecurity researchers warned on Friday. Scammers are also testing ChatGPT's ability to build other chatbots designed to impersonate young females to ensnare targets, one expert monitoring criminal forums told Forbes.

Many early ChatGPT users had raised the alarm that the app, which went viral in the days after its launch in December, could code malicious software capable of spying on users' keyboard strokes or create ransomware.

Underground criminal forums have finally caught on.

To read the full story…

New Phishing Campaign Impersonates Flipper Zero

Several social media accounts and fake websites are pretending to sell the sought-after hacking tool Flipper Zero to lure cybersecurity professionals into making cryptocurrency transactions.

This new campaign of angler phishing – a type of social media phishing that involves impersonating corporate social media accounts to interact with their customers – was first uncovered by security researcher Dominic Alvieri on December 2, 2022.

To read the full story...

Click Here

What did the programmer call their AI girlfriend

Databae.

14 Cybersecurity Best Practices to Instill In Your End-Users

1. Enforce password policy compliance
2. Use MFA
3. Don't leave information unprotected
4. Use a password manager
5. All hardware should be sourced from the correct procedures
6. Mobile devices should be properly protected
7. Shut down/lock devices
8. Don't disable built in protections
9. No personal data storage
10. Discourage USBs
11. Beware of suspicious emails
12. Avoid printing things with company data
13. Be wary of downloads
14. MFA on external software

To read the full story...

Call to action