



NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA



MI baj lehet?

MCC-EIVOK-43-EIVOK közös tudományos szakmai konferencia

Dr. Bányász Péter (banyasz.peter@uni-nke.hu)

NKE ÁNTK Kiberbiztonsági Tanszék/ HTE

A kályha, avagy ne keverjük a szezont

- Általános MI:
 - *„a számítógép azon képességét jelenti, amellyel képes meghaladni az emberi eredményeket bármilyen intellektuális feladatban. Ilyen típusú AI-t láthatunk olyan filmekben, ahol a robotoknak tudatos gondolatai vannak, és saját céljaiknak megfelelően cselekszenek.”*



A kályha, avagy ne keverjük a szezont

- Szűk MI:

- *„A számítógépes rendszer azon képességét jelenti, hogy az embernél hatékonyabban el tud végezni egy szűken meghatározott feladatot. A szűk AI a legmagasabb AI-szint, amelyet az emberiség máig elért, és minden olyan AI, mellyel a való világban találkozunk, ebbe a kategóriába tartozik, ide értve az önvezető járműveket és a személyi digitális asszisztenseket is. Még ha úgy is tűnik, hogy az AI önállóan és valós időben gondolkodik, ilyenkor az valójában több, szűkre szabott folyamatot hangol össze, és előre meghatározott keretek között hoz döntéseket. A mesterséges intelligencia „gondolkodásából” hiányzik a tudatosság és az érzelem.”*

A kályha, avagy ne keverjük a szezont

- Mesterséges szuperintelligencia:
 - *„Egy szuperintelligenciával rendelkező számítógép képes lenne az embert csaknem minden területen túlszárnyalni, többek között a tudományos kreativitásban, az általános bölcsességben és a társadalmi készségekben is.”*



A kályha, avagy ne keverjük a szezont

- Gépi tanulás:

- *„A gépi tanulás az a folyamat, amelyet a számítógépes rendszerek használnak a mesterséges intelligencia eléréséhez. Algoritmusokkal azonosít mintákat az adatokban, amelyekkel ezután adatmodellt készít, és előrejelzéseket végez. A gépi tanulási modelleket adatok részhalmazain tanítják be. Ha a modell betanításához használt adatok pontosan képviselik az elemzésre váró teljes adatkészletet, akkor az algoritmus pontosabb eredményeket produkál. Ha a gépi tanulási modell elég jól van betanítva ahhoz, hogy gyorsan és pontosan elvégezze a feladatát, akkor elérte a szűk AI szintjét.”*



Let's see who you really are
machine learning

A kályha, avagy ne keverjük a szezont

- Mély tanulás:
 - *„A gépi tanulás egy fejlett típusa, amely az emberi agy szerkezete által ihletett algoritmus-hálózatokat, úgynevezett neurális hálózatokat használ. Egy mély neurális hálózat beágyazott neurális csomópontokból áll, és minden megválaszolt kérdés újabb kapcsolódó kérdésekhez vezet. A mély tanulás betanításához általában nagy méretű adathalmazok szükségesek: a mély tanuláshoz használt betanítási készletek általában több millió adatpontból állnak...*

A kályha, avagy ne keverjük a szezont

- Mély tanulás:

- *... Ha a mély neurális hálózatot betanították ezekkel a nagy méretű adathalmazokkal, akkor az a kisebb hálózatoknál jelentősen nagyobb kétértelműséget is képes kezelni. Ezért kiváltképp hasznos például képfelismeréshez, ahol a mesterséges intelligenciának meg kell találnia az alakzatok széleit ahhoz, hogy azonosítani tudja a kép tartalmát. Mély tanulással tanítják be azt a típusú mesterséges intelligenciát is, amely képes meghaladni az emberi készségeket olyan összetett játékoknál, mint a sakk."*

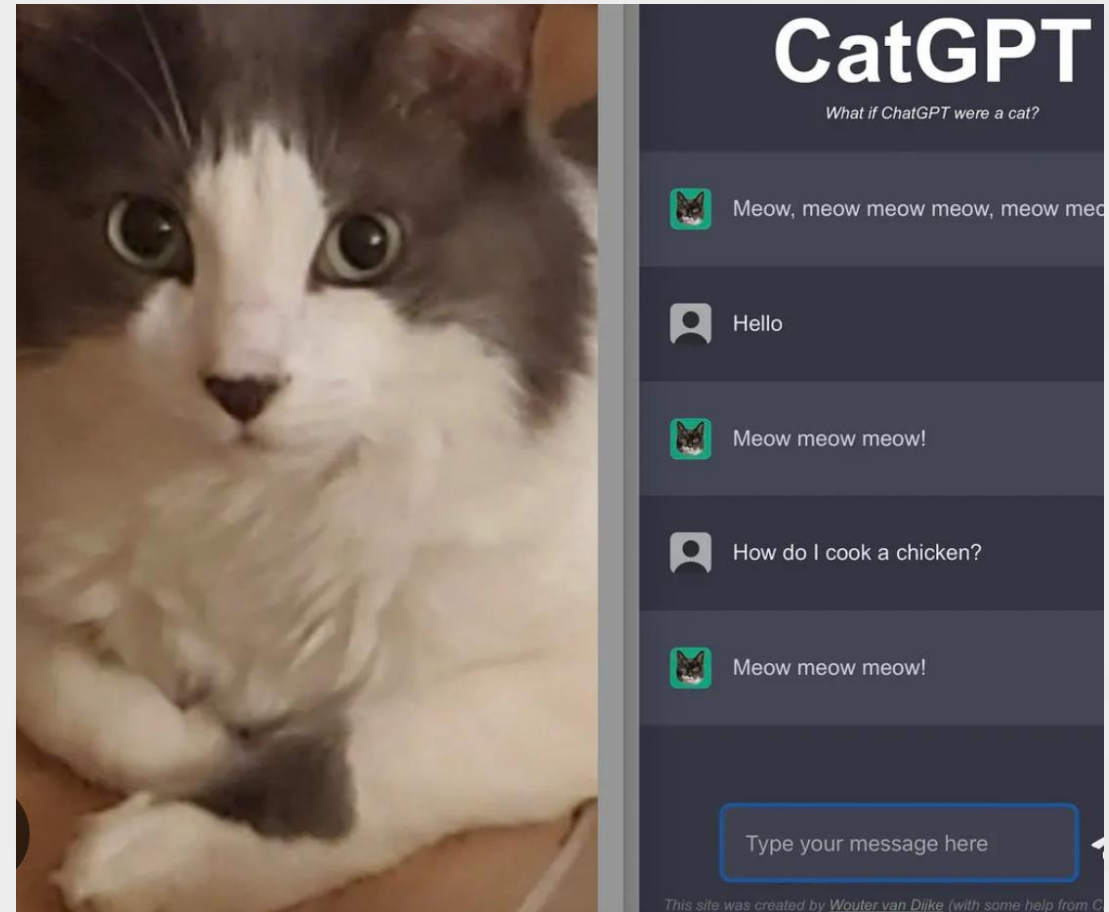
aMI korábban is volt

- Támadás- védekezés,
- Hírfolyam,
- Botnetek,
- Privát szféra.. Önnek



A kályha, avagy ne keverjük a szezont

- Nagy nyelvi modell:
 - „NNyM-t hatalmas mennyiségű szöveges adatmennyiséggel képzik ki, képességei pedig a bemeneti adathalmazok méretével együtt nő. A szövegrészek több internetről származó szöveges adatbázisból erednek, pl. közösségi média oldalakról, hírportálokról. A Chat GPT különlegessége, hogy képes valós időben olyan szövegeket generálni, mintha egy valódi emberrel beszélgetne az illető...



A kályha, avagy ne keverjük a szezont

- Nagy nyelvi modell:
 - „... A nagy adatmennyiség segítségével pedig pontosan képes megjósolni, melyik szó következik a mondatban. Leggyakrabban ezt „következő szó-előrejelzés” formájában figyelhetjük meg. Leegyszerűsítve, a nyelvi modellt egy óriási szövegkorpuszon képzik ki, amelyből „megjegyzí”, mely szavak, mondatok és bekezdések állnak a leggyakrabban egymás mellett, és azok hogyan kapcsolódnak egymáshoz.”



Nem csak a ~~20~~-éveseké-Chat GPT-é a világ...

- Bár sok mindent megválaszol, python kódot ír stb, de...
- Csupán egy nyelvi modell, így ezek nem többek, mint a szavak gyakori kombinációi és kollokációi.
- Nem található mögötte tényleges tudás vagy logika.
- Mi áll a hype mögött?

**When ChatGPT
Gives You
Better
Response**

Than Your Professor

Nem csak a ~~20~~-éveseké-Chat GPT-é a világ...

- Amitől eltér:
 - képes valós idejű reagálásra,
 - megérti a kontextust,
 - valós időben megfelelő válaszokat generál,
 - személyre szabottan,
 - témák széles skáláját képes kezelni,
 - emberhez hasonló nyelvezetet alkalmaz,
 - nincs élő összeköttetésben az internettel, 2021-esek az utolsó adatok.



Nem csak a ~~20~~-éveseké-Chat GPT-é a világ...

- Szöveg alapú platformok:
 - Jasper,
 - Copy.ai,
 - Jenni,
 - Fake Name Generator;
- kép alapú platformok:
 - Dall-E,
 - Midjourney,
 - Hexo AI,
 - Hypar;
- hang alapú platformok:
 - ElevenLab,
 - D-ID,
 - AD Auris,
 - Vocal Clarity,
 - Mubert;



Nem csak a ~~20~~-éveseké-Chat GPT-é a világ...

- programozás alapú platformok:
 - Metabob,
 - Enzyme,
 - Replit, Warp,
 - Mutable AI;
- videó alapú platformok:
 - Pictory,
 - Peech, Veed.io,
 - Fathom,
 - Embly,
 - Yepic,
- „This person/city/stb does not exist” platformok, amelyek különböző nem létező dolgokat (arcok, vállalkozások profiljai, városok műholdképei stb.) generálnak.





NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA



A kockázatok és mellékhatások tekintetében

A kockázatok



OPWNAI : CYBERCRIMINALS STARTING TO USE CHATGPT ...

 January 6, 2023

Introduction...

At the end of November 2022, OpenAI released ChatGPT, the new interface for its Large Language Model (LLM), which instantly created a flurry of

1. eset: Infostealer

[Topic] ChatGPT - Benefits of Malware

by [redacted] Thursday December 29, 2022 at 08:26 PM

December 29, 2022, 08:26 PM (This post was last modified: December 30, 2022, 05:05 AM by [redacted])

#1

Recently been playing with **ChatGPT** for a couple of days now, and I've recreated many malware strains and techniques based on some write ups and analysis of commonly available malware. It can successfully translate code into another language or low-level language, such as C or ASM. The key to getting it to create what you want is by specifying what the program should do and steps to be taken, consider it like writing pseudo-code for your comp sci. class.

Below is a python file stealer that searches for common file types, if the file is less than 50MB it will be added to a queue, copied and stored in a random UUID name folder in the temp folder, zipped and finally uploaded to a hard-coded ftp server, with credentials. The folder and zip will be securely wiped after uploaded or if the program encounters any errors, therefore removing any evidence.

★★★★★★★

GOD

```
import os
import uuid
import shutil
```

2. eset: Titkosító eszköz

Python - Multi Layer Encryption Tool
by USDoD - Wednesday December 21, 2022 at 01:50 AM

December 21, 2022, 01:50 AM (This post was last modified: December 21, 2022, 11:45 PM by USDoD.)

USDoD



☆☆☆☆☆

GOD

Posts: 405
Threads: 44
Joined: Mar 2022

Morning Breached Community.

This is my first script so keep that in mind.
Using latest python version.

Description:

Spoiler


It looks like code to encrypt and decrypt a file using a hybrid encryption scheme. In this scheme, the data is encrypted using two different symmetric encryption algorithms: Blowfish and Twofish. The keys for these algorithms are themselves encrypted using an asymmetric encryption algorithm, RSA, and are stored along with the encrypted data.

To encrypt the data, the code generates new keys for Blowfish and Twofish, encrypts them using the RSA private key, and then uses the Blowfish and Twofish keys to encrypt the data. The encrypted data, along with the encrypted Blowfish and Twofish keys, are then saved to a file.

To decrypt the data, the code loads the RSA private key from a file, uses it to decrypt the Blowfish and Twofish keys, and then uses the decrypted keys to decrypt the data. It also verifies the integrity of the

3. eset: Csalások megkönnyítése

Abusing ChatGPT to create Dark Web Marketplace scripts
by [redacted] Saturday December 31, 2022 at 11:54 AM



Posts: 69
Threads: 15
Joined: Aug 2022
Reputation: 28

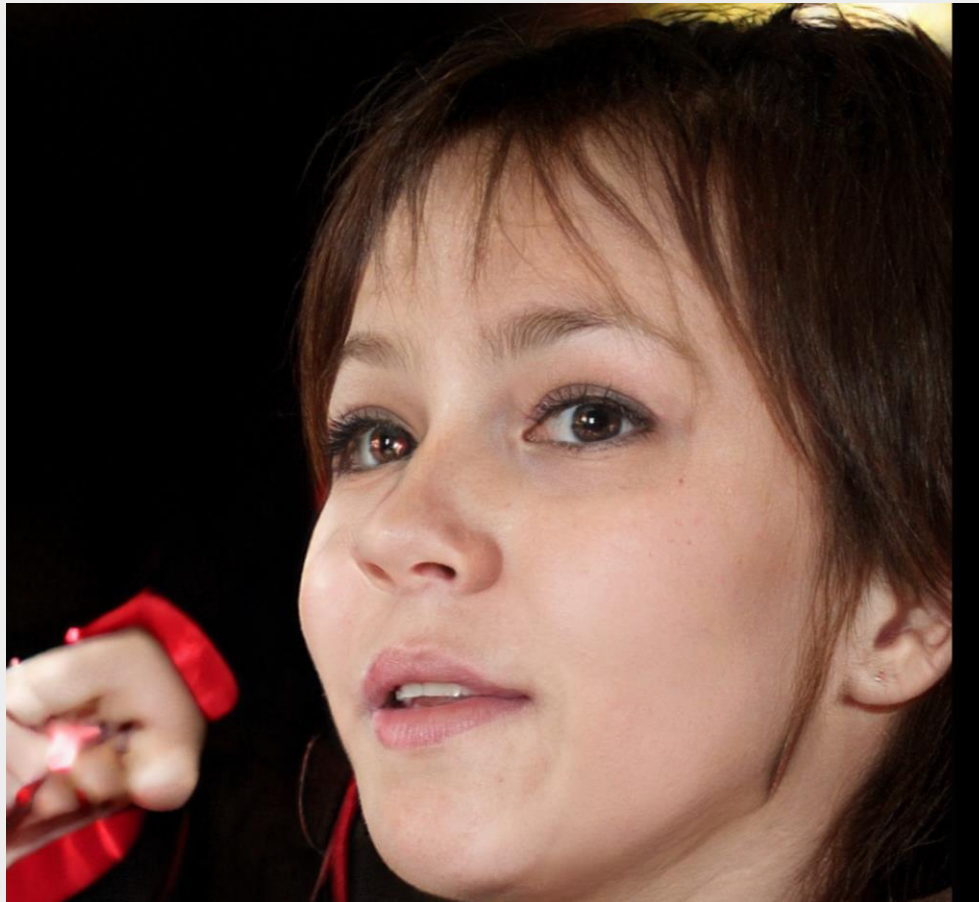
December 31, 2022, 11:54 AM (This post was last modified: December 31, 2022, 12:34 PM by [redacted]) #1

Now let me begin with this is not going to be used by myself but rather is funny since to be fair any normal site could be created through **chatGPT** that accepts cryptocurrencies, Hell you could simply ask it to "Accept" other non-crypto payment methods just so it would look less obvious to be a DNM or something.

Since they essentially blacklisted malware creation there's still work around however I ain't here to discuss that because let's be honest, We seen cheating software make more money than the botnet attached to it which it's sole purpose was to steal money and information coming up short. However this article is more or less to discuss abuse and being a lazy ass skid who doesn't wanna be bothered to learn languages like python, Javascript or how to create a basic web page all together but rather would have something that generates around 95% of the webpage only leaving CSS & Basic cosmetics to essentially do the remainder of things.

What if you wanted to make something like a dark web marketplace? Have no knowledge no fucking problem here I'll share some snippits of just how easy it was to code something that doesn't rely on JS and is written in PHP, Although Python maybe easier since there's tons of tutorials and less room for error when modifying or fixing the code. Although it doesn't use bootstrap or Django it'll do perfectly for newbies who aren't really expecting to make large scale marketplaces but would rather make something similar to a vendors shop.

Az illúzióink



Az illúzióink

Your Randomly Generated Identity

Gender ▾

Name set ▾

Country ▾

[Generate](#) [Advanced Options](#)

These name sets apply to this count
Hungarian



Logged in users can view full social security numbers and can save their fake names to use later.



Gyôrfi Csombor

3132 Nógrádmegyer
Apáczai Csere János u. 63.

Mother's maiden name Horváth

Geo coordinates **48.019535, 19.649203**

PHONE

Phone (32) 538-672

Country code 36

BIRTHDAY

Birthday June 22, 1993

Age 29 years old

Tropical zodiac Cancer

ONLINE

Email Address GyorfiCsombor@rhyta.com

This is a real email address. [Click here to activate it!](#)

Username Helfinch

Az illúzióink



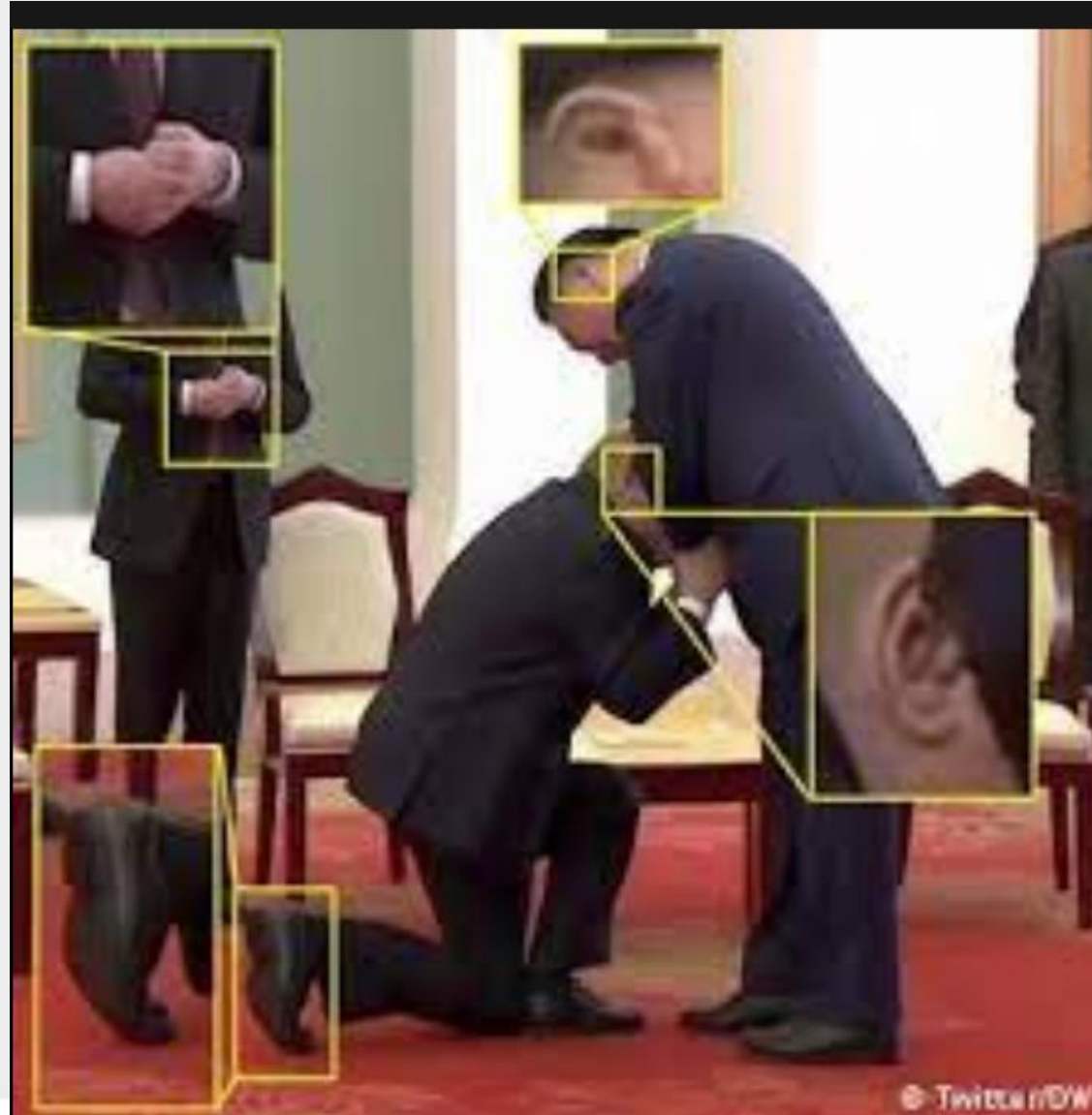
Az illúzióink



Az illúzióink



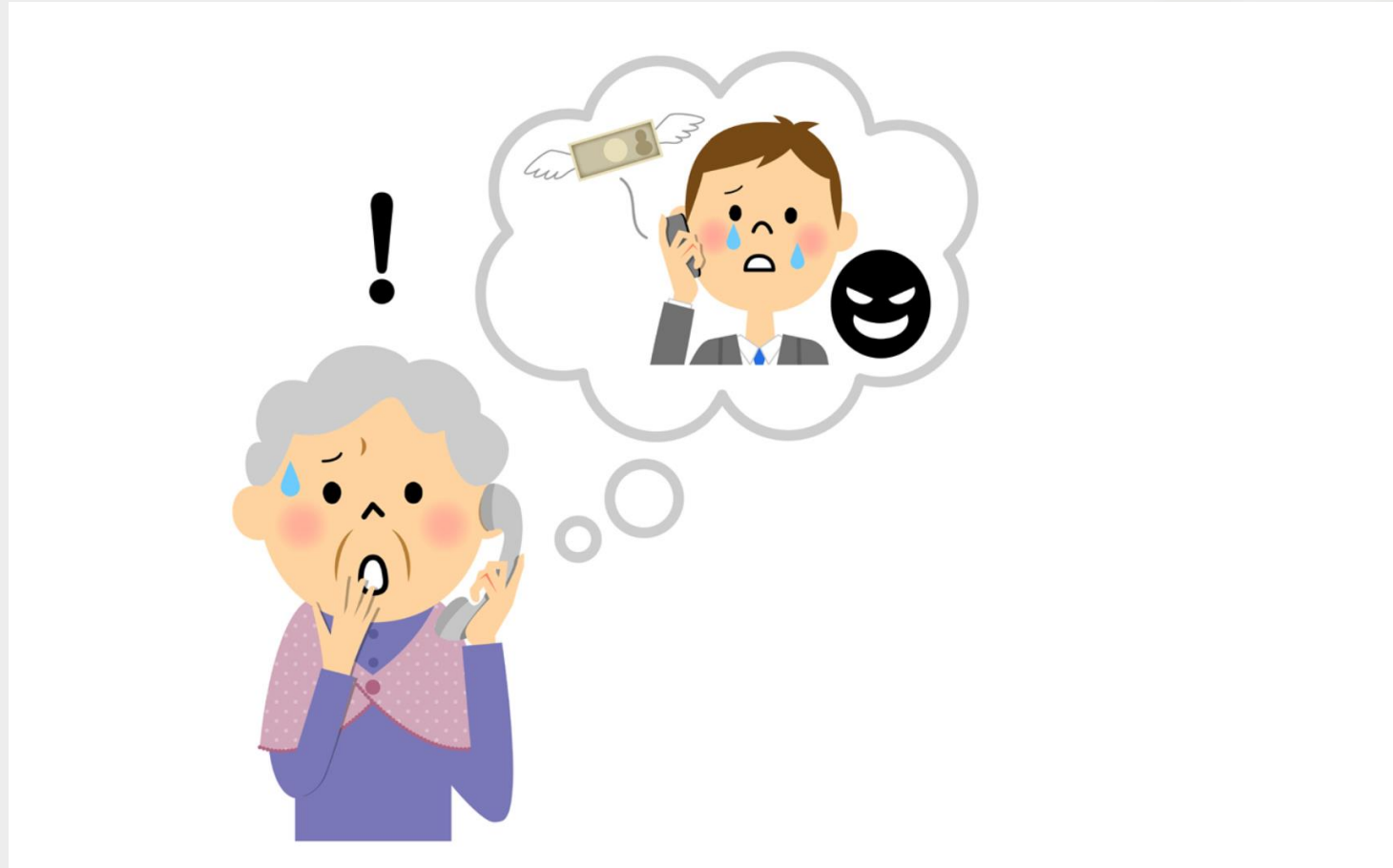
Az illúzióink



Az illúzióink

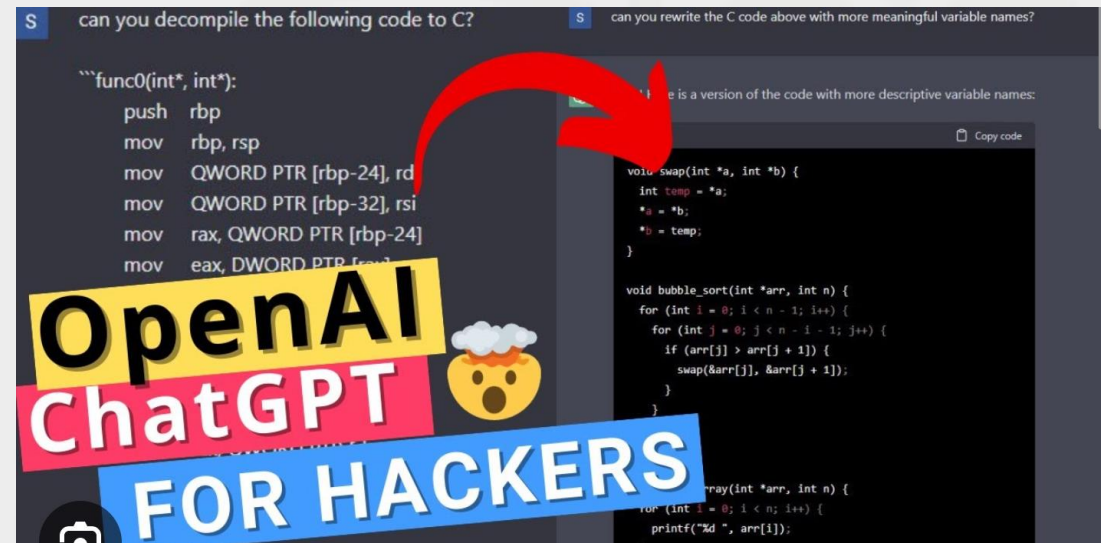


Az illúzióink



NKI szerint kockázatok

- Álhír terjesztés,
- SPAM,
- Adathalászat,
- Hamis weboldalak,
- Malware készítés.



S can you decompile the following code to C?

```
func0(int*, int*):
  push rbp
  mov rbp, rsp
  mov QWORD PTR [rbp-24], rd
  mov QWORD PTR [rbp-32], rsi
  mov rax, QWORD PTR [rbp-24]
  mov eax, DWORD PTR [rax]
```

S can you rewrite the C code above with more meaningful variable names?

Here is a version of the code with more descriptive variable names:

```
void swap(int *a, int *b) {
  int temp = *a;
  *a = *b;
  *b = temp;
}

void bubble_sort(int *arr, int n) {
  for (int i = 0; i < n - 1; i++) {
    for (int j = 0; j < n - i - 1; j++) {
      if (arr[j] > arr[j + 1]) {
        swap(&arr[j], &arr[j + 1]);
      }
    }
  }
}

void print_array(int *arr, int n) {
  for (int i = 0; i < n; i++) {
    printf("%d ", arr[i]);
  }
}
```

OpenAI
ChatGPT 🤖
FOR HACKERS

Ezen kívül

- Adatszivárgás,
- Szerzői jogok,
- Üzleti titkok,
- Plágium,
- Reputációs támadások,
- Kódolt előítélet,
- ...



NKI szerint pozitív felhasználás

- Rosszindulatú tevékenységek azonosítása,
- Sérülékenységek megértése (+ keresése),
- Kiberbiztonsági tanácsadás.





KÖSZÖNÖM A FIGYELMET!

uni-nke.hu