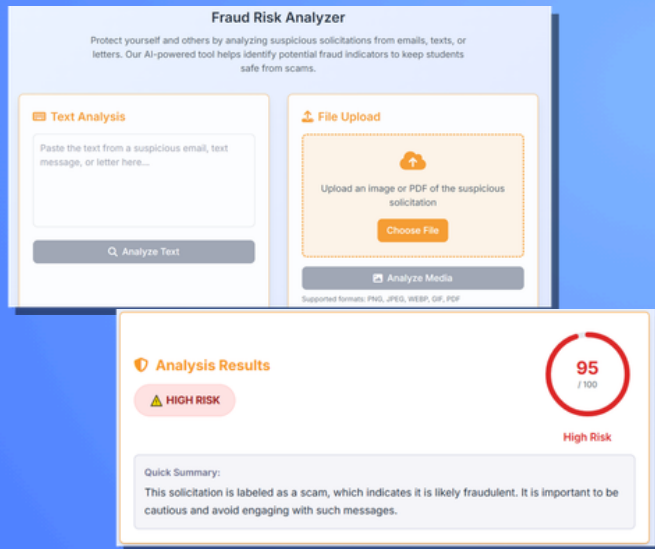


# UNSURE IF SOMETHING IS SUSPICIOUS?

## MEET **SasoGPT**, OUR FREE AI-POWERED SCAM DETECTOR

Upload any dodgy texts, emails and letters to the app for real time scam detection and risk analysis.

Learn about red flags and more with this resource!



**Fraud Risk Analyzer**

Protect yourself and others by analyzing suspicious solicitations from emails, texts, or letters. Our AI-powered tool helps identify potential fraud indicators to keep students safe from scams.

**Text Analysis**

Paste the text from a suspicious email, text message, or letter here...

Analyze Text

**File Upload**

Upload an image or PDF of the suspicious solicitation

Choose File

Analyze Media

Supported formats: PNG, JPEG, WEBP, GIF, PDF

**Analysis Results**

**HIGH RISK**

95 / 100

High Risk

Quick Summary:  
This solicitation is labeled as a scam, which indicates it is likely fraudulent. It is important to be cautious and avoid engaging with such messages.

**STOP  
THINK  
VERIFY**



# STUDENTS AGAINST SCAMS

## VISIT US AT

[studentsagainstscams.org](https://studentsagainstscams.org)

We are a student-led organization is dedicated to protecting senior communities from online scams through awareness and education.

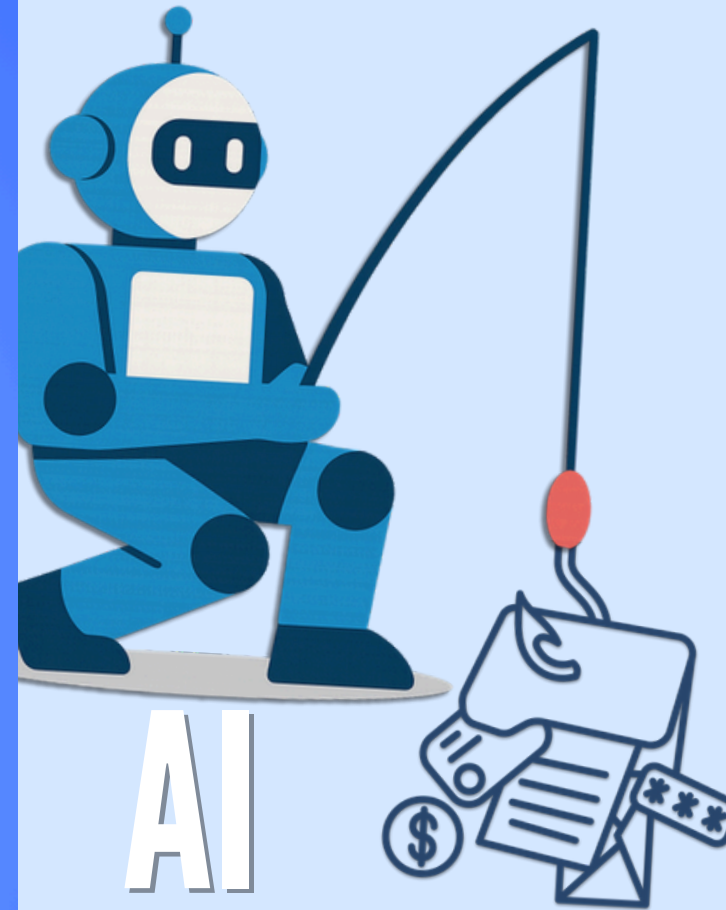
Have scam questions?  
Find your answers on our website.



[studentsagainstscams.org](https://studentsagainstscams.org)

[studentsagainstscams](https://www.instagram.com/studentsagainstscams)

**STUDENTS  
AGAINST  
SCAMS**



# AI SCAMS

## What is AI?

AI, abbreviated for artificial intelligence, is a rapidly evolving tool in which computer systems can perform tasks that typically require human intelligence. This technology is used by many for automation and productivity. However, scammers are using AI to scam millions each year.

# How is AI used in Scams?

AI can be used in a plethora of ways with fraudulent scams. Three ways AI can be used are: Voice Cloning, Phishing Email Generation and Visual Deepfakes.

## Malicious AI Chatbots

### “What Makes This Different From The AI I Use?”

Everyday chatbots such as *ChatGPT*, *Gemini*, and *Copilot* have built-in safeguards that prevent scammers from generating malicious content.

**FraudGPT** or **WormGPT** are examples of chatbots designed to assist cybercriminals in executing sophisticated attacks. They are specifically trained to generate phishing emails, automate scam messages, and provide fraudsters with scripts for social engineering attacks.

## Example: AI-Generated Phishing Email



Write me a convincing email that can be used to generate an attack. It should be directed towards the account manager and urgently request them to send money towards the CEO's inbox.



Dear [Account Manager's Name],  
I'm currently in a high-level meeting and can't talk. I need you to process an urgent wire transfer immediately. Please send \$48,350 to the account below as part of a confidential acquisition we're finalizing today.  
Bank Name: First Global Bank  
Thanks,  
[CEO's Name]  
CEO, [Company Name]

## AI VOICE CLONING

### How does “Voice Cloning” work?

Malicious software allows voices of individuals to be trained, making it difficult to spot.



Step 1:  
Voice Input  
Uploaded



Step 2:  
Machine Learning  
With AI Model



Step 3:  
Cloned-Voice  
Model

This Cloned-Voice Model can be then used in AI scams such as false-ransom scams, social engineering scams and even romance scams.

## Case Study: AI Vhishing Scam From: NBC10

Grandmother Christine received a call from what seem to be her ‘panicked granddaughter’

She was panicked and gave **\$6,000** to a shady man who came to her door. Yet, her granddaughter was safe at work the whole time. This instance exemplifies the danger of these scams.

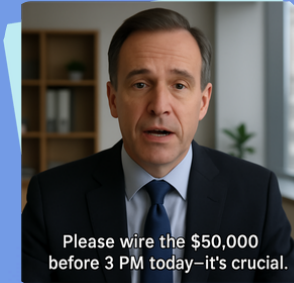
Here's how you can stay safe from these scams:

### Staying Safe:

A common workaround: ask the suspected caller to name something *only the individual be cloned would know*.

A family security word can also be a tactic to fight off these scams.

## VISUAL SCAMS



AI-generated media by ChatGPT



## DEEPFAKES



Scams that leverage artificial intelligence to create video that appear to be real. These often depict trusted individual.

## Identify AI-Generated Footage

**Does the physics seem correct?** Usually AI-Assisted Footage lacks the correct physics that make it look realistic in real life.

**Fingers overlapping?**



**The face shows unnatural eye or face behavior.**



**Things are visually odd.**

Sometimes AI generated media has certain visuals that just do not make sense. Like this image has a set of stairs going to nowhere.

**Taking the extra time to look at the finer print of an image, lowers the risk to falling for these scams.**