

# AI Scam Report

by RealCall



# **Background**

The rise of Artificial Intelligence (AI) has brought about a new wave of possibilities and conveniences, which is especially true when OpenAI released ChatGPT. However, as with any innovation, there comes a darker side. In RealCall's recent survey aiming at unveiling the prevalence and impact of AI-driven scams, insights have emerged.

The results not only shed light on the scale of this emerging threat but also present a roadmap for individuals to safeguard against these malicious activities. As we delve into the findings of the survey, we uncover patterns, trends, and crucial takeaways that can reshape the strategies of institutions in the ongoing battle against AI scams.



# **Key Takeaways**



Compared with traditional scams, Al scams help scammers reduce costs and increase "success" rates. So, Al scams are much riskier than ordinary scams.



Race and ethinity minorities like American Indians and American Asians are in the greatest risk of Al scams, 9 times more than those in Non-hispanic Whites.



People of all age groups can be vulnerable to Al scams and no specifically vulnerable group is protruding.



The impact of AI scams on various age groups and occupations and offers insights into the potential expansion of AI scams, highlighting the need for increased awareness and vigilance.

# Introduction

Al scams, also known as artificial intelligence scams, involve the use of Al and related technologies to deceive individuals or manipulate them into providing sensitive information, money, or other valuable assets to scammers. These scams leverage the capabilities of Al, such as generating realistic content, mimicking trusted sources, and automating communication, to make their fraudulent activities more convincing and effective. Here are a few common types of Al scams like impersonation scams, romance scams, tech support scams, voice cloning scams, deepfake scams, phishing attacks, social media scams, investment scams, emergency scams, etc.

The underlying principle of AI scams is to leverage technology to create content that seems authentic and trustworthy, making it difficult for victims to differentiate between legitimate communication and fraudulent attempts. As AI technology continues to advance, it's likely that scammers will find new and creative ways to exploit its capabilities for their malicious purposes.



# Characteristics of AI Scams

Al scams have common features with other types of scams and the characteristics of Al scams here refer to the essential features different from other types of scams.

#### & High Believability and Authenticity

Al-generated content can closely mimic trusted sources like banks, social media platforms, friends, and family. This increases the chances of victims falling for scams, as the communication appears genuine. Scammers are able to use Al technology to generate someone's fake voice, images or even videos. All the fake content generated by Al tools is so alike that it's quite difficult to identify it. According to Microsoft, a new text-to-speech Al model called VALL-E that can closely simulate a person's voice when given a 3-second audio sample.

#### Cost-Effectiveness

Al-powered tools enable scammers to automate processes and create convincing content at a fraction of the cost compared to traditional scams. This drives scammers to increasingly adopt Al-based tactics. Due to the Al tools available on the market, it's quite handy to produce millions of scam texts within seconds. In other words, Al technology makes it easier for scammers to implement scams and to "make it".

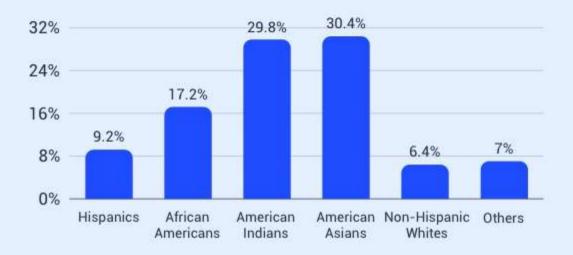
For example, as the keyword "Al voice cloning tool" is entered in Google, numerous recommendations are listed among the search results most of which are free to use.

# **Vulnerable Demographics**

Some people are more likely to become victims of fraud than others. The study found that race or ethnicity was associated with the likelihood of being a victim of fraud.

#### **Racial and Ethnic Minorities**

The survey found that members of several racial and ethnic minorities were much more likely to be victims of AI scams than non-Hispanic whites. Of non-Hispanic whites, 6.4 percent had been victims of one or more of the frauds covered by the survey. However, those who are American Indians and American Asians were at greatest risk: almost 60.2 percent of survey participants in these two groups had been victims of one or more of the frauds covered by the survey – more than 9 times the percentage of victims among non-Hispanic whites.

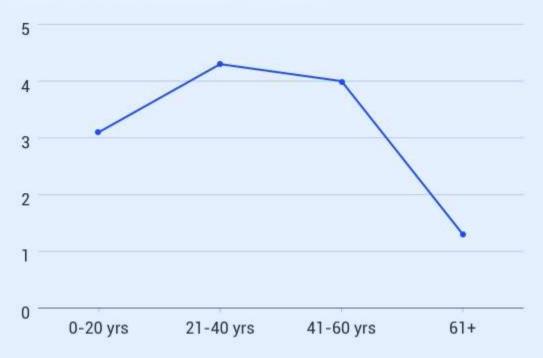


# The Elderly Experience Slightly More AI Scams

Before the survey, it's estimated by RealCall Insights Center that the elderly (61+ yrs) tend to suffer from more AI scams than any other age group. However, the survey result is not that typical.

According to the answers catering to familiarity of AI scams, the age group of 61+ yrs features much lower familiarity than the age groups of 21-40 yrs and 41-60 yrs.

#### Familiarity of AI Scams for Different Age Groups



However, the data difference is not that high when it comes to the vulnerability of AI scams between different age groups.

The data shows that people of different ages are equally at risk of falling for AI scams. Even though older folks may not be as familiar with AI scams, they can still be just as vulnerable as younger generations. Surveys suggest that around one-third of people in each age group—whether they're young, middle-aged, or elderly—are susceptible to AI scams. While we often hear about older individuals being targeted, the risk is pretty much the same for everyone, so anyone could become a victim of AI scams.

#### A familiar bank of References personal financial institutoin information A friend or family Urgent or emergency 0-20 yrs = 21-40 yrs = 41-60 yrs = 61+ member situations 125 50 100 40 30 75 20 50 25 10

61+

Personal Information Providing Possibility

Neutral

Likely Very likely

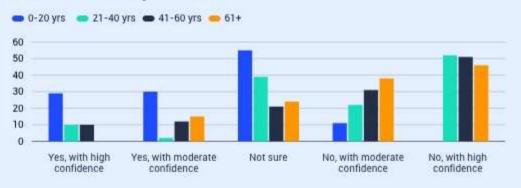
Very unlikely Unlikely

#### Confidence to Identify AI Scams

21-40 yrs 41-60 yrs

0-20 yrs

Personal Information Providing Trigger



### **Emerging Trends and Predictions**

Al scams are an evolving threat that shows no signs of receding. As scammers become more adept at utilizing AI, their potential victim pool expands to include both smart and less tech-savvy individuals. The ubiquity of AI-generated content and its increasing sophistication will likely lead to an escalation in AI phone scams and other forms of digital deception.



#### Conclusion

Al scams have proven to be a formidable and evolving challenge, leveraging technology to deceive individuals from various demographics. The increasing believability of Algenerated content, coupled with its cost-effectiveness, highlights the urgency for individuals to maintain skepticism and vigilance in their digital interactions. Awareness campaigns, education, and improved digital literacy are crucial in the fight against the growing threat of Al scams.

## RealCall AI: Defeat AI with AI

This is how RealCall works on your phone: OpenAI + RealCall Blocklist.

Simply put, the more you use RealCall, the less risk you'll receive spam or scam calls & texts.

Between You and Scammers is RealCall Al as a One-to-One Mobile Communication Guardian.

Based on the AI language model, ChatGPT 4, RealCall can analyze and process language input to identify patterns, sentiments, and intent and sense the trivial malicious intent hidden in the text message ordinary people fail to notice. Plus, with the continuously updated risky number database developed by RealCall team and long-term users' reports, RealCall AI is capable of accurately and quickly identifying scam-likely texts and dealing with them in users' personalized ways.





RealCall is an app that provides spam call blocking and caller ID for global users. Empowered by the vast and ever-evolving database and Al-based modeling, RealCall features top-notch accuracy of blocking. For more information, please visit

ttps://www.realcall.ai

#### Report DISCLAIMER

The content of this document is for general informational purposes only. RealCall makes no representation or warranty whatsoever including as to the accuracy, completeness or adequacy of the information contained in this document. RealCall disclaims all warranties including of accuracy, completeness, merchantability or fitness for a particular purpose with respect to any information contained in this document. RealCall is not acting as your advisor, agent or fiduciary and no legal relationship between you and RealCall shall be created by virtue of the information contained in this document. Any information contained in the document, and anyopinions and estimates by RealCall therein, should be regarded as indicative, preliminary and for illustrative purposes only. Any mark or other intellectual property contained in the document belongs to its respective owner.