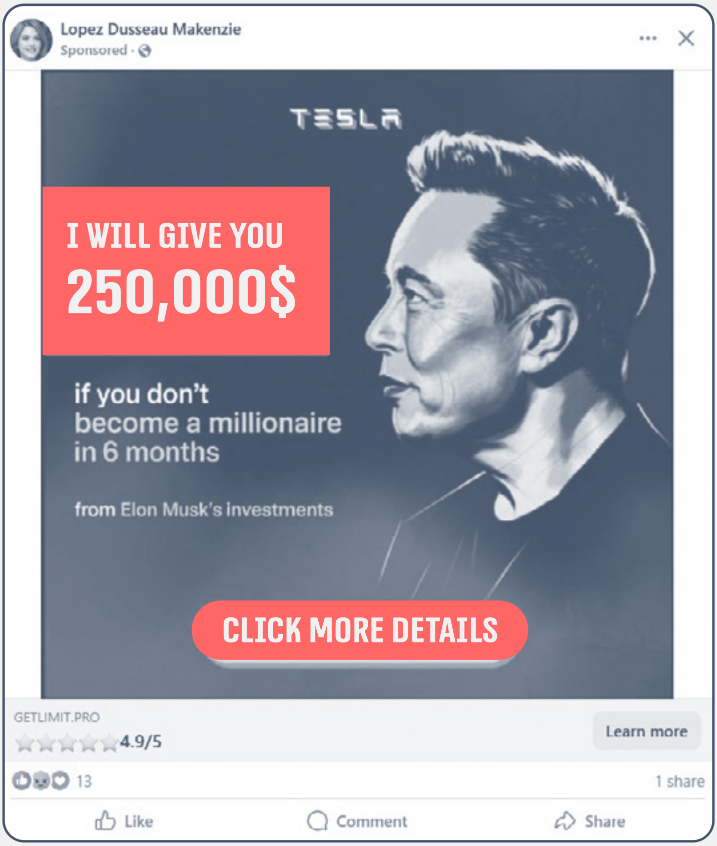
ISRAEL
INTERNET
ASSOCIATION
ISOC-IL

ALGORITHMIC SCAMS: SOCIAL MEDIA AND ARTIFICIAL INTELLIGENCE AS INSTRUMENTS OF FINANCIAL FRAUD

CYBER THREAT REVIEW – THE INTERNET SAFETY HOTLINE



Lopez Dusseau Makenzie
Sponsored ·

TESLA

I WILL GIVE YOU 250,000$

if you don't become a millionaire in 6 months

from Elon Musk's investments

GETLIMIT.PRO
4.9/5

JULY 2025

The Israel Internet Association (ISOC-IL) is a non-profit organization that has been operating since the early 1990s to promote the use of the Internet for the benefit of the public in Israel. It operates critical internet infrastructure in Israel: the national domain name registries ".il" and "ישראל.", and the Israel Internet Exchange (IIX). ISOC-IL's professional knowledge and experience in research, development, and operation of Internet technologies for the Israeli public serve as the foundation for research, policy activity, and community empowerment carried out by ISOC-IL. This includes the operation of the Internet Safety Hotline and the Block.org.il initiative, both of which provide the general public with assistance, knowledge, and tools for improving online safety and security; various initiatives and activities aimed at reducing digital gaps and promoting internet skills and literacy in Israeli society; the data.isoc.org.il initiative, which collects and makes accessible quantitative-statistical data about the Israeli internet and its users; and the publication of professional policy research intended to inform and improve the Israeli and global internet arenas at the various intersections of law and technology.

Authors: Nitsan Yasur and Narkis Moshe
Research and Data Collection: Yonatan Ben Horin
Editing and Supervision: Edan Ring
Review: Yarden Amir
Graphic Design: Studio Lee&Tamar

The Internet Safety Hotline – www.safe.org.il
Israel Internet Association (ISOC-IL) – www.en.isoc.org.il
For further information and contact – info@isoc.org.il

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document describes a new wave of sophisticated global online fraud that has gained momentum in recent years and is impacting Israeli citizens across all sectors of the population. This new wave of online fraud is characterized by the rapid and advanced adoption of new artificial intelligence technologies and sophisticated digital advertising and distribution tools, in order to reach target audiences more effectively and deceive them. In contrast to more basic and traditional forms of online fraud, the new wave leverages artificial intelligence (AI) technologies and social media platforms to precisely target segmented audiences, engage in impersonation and identity fabrication, generate a variety of content and marketing messages, and effectively exploit paid advertising and promotion tools within various platforms and social networks that were once considered a safer and more protected space for users. The combination of generative AI tools for creating images and deepfake videos and their distribution via advertisement mechanisms and sponsored promotion on various platforms enables real-time customization of the fraud campaign's content and messages to different target audiences. This increases both the opportunity and capability of fraudsters to expand the number of victims and the extent of harm caused to them. This review documents, maps, and analyzes these new online fraud schemes based on hundreds of ads and campaigns of this kind, collected and documented by ISOC-IL's Internet Safety Hotline team between 2023 and 2025.

A. INTRODUCTION – THE NEW WAVE OF ONLINE FRAUD

Fraud on social networks has in recent years become a serious global phenomenon affecting individuals, groups, corporations and companies, as well as democratic processes and institutions worldwide. Fraudsters and criminal entities exploit advanced communication and digital technologies to create fake, manipulative, and persuasive content, using the targeted distribution and advertising capabilities of various platforms and social networks to locate and focus on potential audiences and victims. The rapid development of generative artificial intelligence (AI) tools and the ability to create high-quality content such as images or deepfake videos[1] makes online fraud easier to orchestrate, cheaper, and more effective than ever before. The economic model of social platforms, based on sponsored ads and sophisticated targeting systems, allows fraud schemes to thrive under the protection of algorithms – sometimes without being identified in time and without sufficient response or supervision from the platforms or law enforcement authorities.

In Israel, as in the rest of the world, this form of fraud is widespread, exploiting regulatory weaknesses and the absence of adequate enforcement mechanisms, enabling fraudsters to operate with almost no disruption and to reach a significant number of victims and profits. In recent years, online fraud campaigns that used to rely on SMS or email distribution (such as phishing attempts to steal credit card details) are gradually shifting to closed, algorithmic platforms and social networks such as Facebook, Instagram, TikTok, and YouTube. There, they are distributed through sponsored ads using targeted advertising techniques based on user preferences, interests, and personal data collected about them, tailoring the fraud campaign to user

[1] The term Deepfake is based on a combination of the terms Deep Learning and Fake, and refers to artificial intelligence-based technology that enables the modification or processing of image or video content in a way that makes it difficult to detect that the content has been fabricated. Source: www.isoc.org.il/public-action/deepfake

behavior in real time. Thus, they manage to reach focused audiences, tailor more specific fraud schemes to them, and direct them to interfaces where they are asked to provide personal information, account details, and various assets, or to deposit money under the false pretense of a financial investment. The advertising and sponsored promotion mechanisms of social media platforms — which are powerful targeting and advertising tools that allow advertisers to reach target audiences with maximum precision and generate high rates of interaction with their ads — have become, in the hands of fraudsters and malicious actors, a sophisticated and effective digital fraud machine.

ISOC-IL's Internet Safety Hotline (www.safe.org.il) has been in operation since 2013 and provides assistance, guidance, information, and tools to internet and social media users in Israel. The Hotline's mission is to provide support in the battle against a wide range of online threats and harms. As an officially recognized reporting body (Trusted Flagger) by a number of leading global platforms, the Hotline receives hundreds of reports monthly, tracks and analyzes patterns and trends that emerge, and escalates malicious indicators (IOCs) and signals to other NGOs and stakeholders for further action and coordinated response to problematic phenomena. The present report is based on data extracted from reports submitted to the Internet Safety Hotline from 2023 to 2025 and **presents a comprehensive analysis of hundreds of ads and content pieces pointing to the increasing and targeted use of AI technologies, deepfake, and sponsored promotion on social media** for the purpose of financial fraud in Israel. This document presents the scope of the phenomenon, the operational mechanisms used by fraudsters, and the failures of platforms and authorities in detecting, preventing, and addressing AI and deepfake fraud against Israelis on social networks.

The present review reveals and analyzes a growing trend that began in 2023 and has since intensified, in which fraudsters create deepfake videos featuring familiar public figures - such as politicians, celebrities, and businesspeople - seemingly recommending fake investment opportunities or other products and services. The people falsely portrayed in the videos are shown in realistic and convincing scenarios, using cultural and linguistic adaptation and exploiting the public trust in them. These ads lead users to landing pages posing as financial services or other products, where they are asked to provide personal information and transfer funds or payment. The final section of the review presents recommended methods of coping with the current trend of digital fraud and similar phenomena in the future, including technological, regulatory, and educational solutions, alongside collaborations between platforms, enforcement authorities, and civil society.

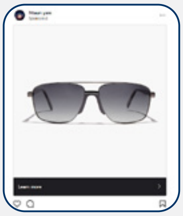
B. DESCRIPTION OF THE STAGES AND COMPONENTS OF AI FRAUD CAMPAIGNS ON ALGORITHMIC SOCIAL MEDIA PLATFORMS

AI-driven fraud campaigns on social media platforms follow a personalized and structured ”marketing funnel” approach to engage and manipulate users. These schemes are designed to build trust, elicit personal information through fraudulent websites, and ultimately convince victims to transfer funds to the scammers.

The setup, built in stages, includes initial exposure to personalized marketing ads on various social media platforms, redirection to external websites or fake trading platforms, and sometimes even personal contact and conversation with a human representative. Below is a description of the various stages the user goes through until the goal of the scam is achieved.

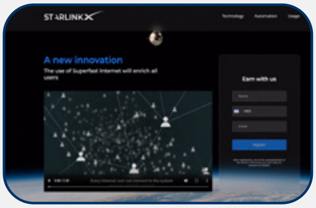
FROM A FACEBOOK AD TO CREDIT CARD HARVESTING

EXAMPLE OF A FRAUD CAMPAIGN "MARKETING FUNNEL" — AS REPORTED TO THE INTERNET SAFETY HOTLINE



1

Social Media Advertisement
(in this case, a cloaked ad)

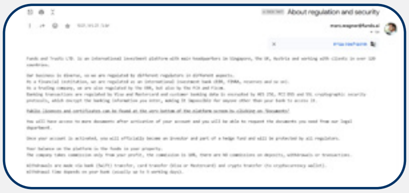


A new innovation

The use of Superfast internet will enrich all users

2

Redirect to External Landing Page
featuring the Starlink logo and a promotional video promoting the investment platform



marc.wagner@funds.ai

Funds and Trusts LTD. is an international investment platform with main headquarters in Singapore, the UK, Austria and working with clients in over 120 countries.

Our business is diverse, so we are regulated by different regulators in different aspects.
As a financial institution, we are regulated as an international investment bank ([illegible], FINRA, [illegible] and so on).
As a trading company, we are also regulated by the [illegible], but also by the FCA and [illegible].
Banking transactions are regulated by Visa and Mastercard and customer banking data is encrypted by AES 256, PCI DSS and SSL cryptographic security protocols, which encrypt the banking information you enter, making it impossible for anyone other than your bank to access it.

Public licenses and certificates can be found at the very bottom of the platform screen by clicking on 'Documents'

You will have access to more documents after activation of your account and you will be able to request the documents you need from our legal department.

Once your account is activated, you will officially become an investor and part of a hedge fund and will be protected by all regulators.

Your balance on the platform is the funds in your property.
The company takes commission only from your profit, the commission is 10%, there are NO commissions on deposits, withdrawals or transactions.

Withdrawals are made via bank (Swift) transfer, card transfer (Visa or Mastercard) and crypto transfer (to cryptocurrency wallet).
Withdrawal time depends on your bank (usually up to 5 working days).

3

The Agent Sends an Email to the Victim
with a username and password to the "innovative trading site" and fake documents aimed at reassuring the victim that they are in good hands

4

The Victim Begins Depositing Funds on the Platform
and is shown fictitious profits that can not be withdrawn

1. FAKE SOCIAL MEDIA PAGES AND HIJACKED ACCOUNTS

First, the fraudsters either create a fake or impostor Facebook (or Instagram) page. Sometimes they pose as an existing individual (usually a public figure) or organization, in other cases they hijack an existing social media account belonging to a real person or organization, and sometimes they generate a fake visual identity using AI, along with a fake name, in order to avoid Facebook's facial recognition mechanism. They thereby create a platform for dissemination of their scam that both appears trustworthy and whose deception is difficult to detect. At times, they prefer to take over an existing account in order to use an identity with an established presence on the platform.

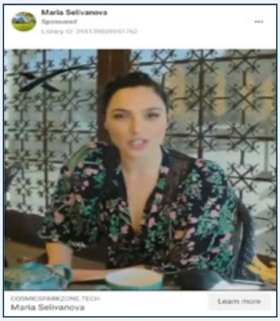
The process of creating a fake page or taking over an existing account usually involves the use of profile pictures and titles that imitate reliable entities such as government bodies or media outlets, by generating and adding fake images and screenshots using basic generative artificial intelligence tools. The content on the pages promoting the fraud scheme draws on current popular trends and topics – for example, investments in ventures associated with Elon Musk, whose name and image are prominent in public discourse, or in stocks related to AI technologies or fake investment avenues on social media platforms. In some cases the fake pages initially publish content that appears common and legitimate, in order to strengthen the page's credibility and appearance in the eyes of users.

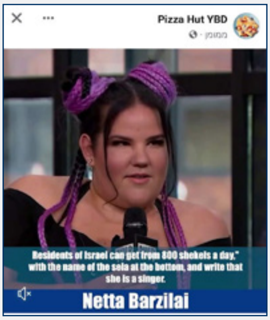
2. PERSONALIZED DEEPFAKE (AI) VIDEOS TAILORED TO FIT TARGET AUDIENCES

Deepfake videos and synthetic AI images are central tools for promoting this type of fraud, as they allow fraudsters to produce highly persuasive and up-to-date visual content and messaging. In the process of creating the video or visual, existing photos and footage of well-known and authoritative figures – such as public officials, government representatives, public experts, and celebrities – are used and manipulated. The fraudsters alter the authentic video to suit the promotion of their scheme, leveraging the reputation of the familiar figures for their own benefit. For example, the fraudsters manipulate the presenters' facial expressions and lip movements using AI tools to match the content and marketing messages promoting the scheme, persuading the target audience to invest in it or purchase it. The goal is to create content that appears as real and credible as possible and grounded in reality, so that it seems as if the featured individual is truly endorsing the fake investment or product with their own voice – something that might appear plausible to the targeted audience.

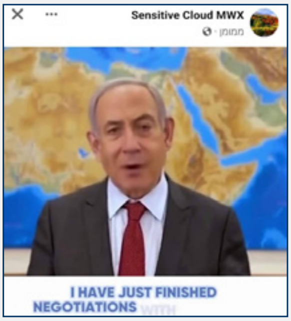
To increase the effectiveness of the fraudulent promotional videos, each video is carefully tailored to different target audiences. Thus, the fraudsters produce dozens of different versions of the fraudulent video featuring various famous "presenters," so that the ads are personally customized to different target population groups based on their interests and preferences. The fraudsters precisely match the presenters, language, visual style, and marketing messages to maximize their appeal to the users. At times, the video content is updated in line with trends, events, and current public discourse to create Real Time Marketing (RTM), which increases the relevance and effectiveness of the fake videos in the eyes of the victims and makes the forgery harder to detect.

For example, novice investors will be shown videos emphasizing quick profits, featuring a well-known financial figure (such as an investment expert who frequently appears on television or social media) or a politician they support (such as the Minister of Finance). Older users will be targeted with videos and messages focusing on financial security and stability featuring trustworthy and familiar figures (such as the President of Israel or the Governor of the Bank of Israel). Younger audiences will be targeted with videos featuring tech-related figures (such as Elon Musk or Mark Zuckerberg) or celebrities and local pop culture icons (for example Israeli singers Eyal Golan or Netta Barzilai). In addition, the use of a wide variety of graphic elements, fake statistics, and fabricated testimonials strengthens the false credibility of the videos and makes it more difficult for viewers to detect the scam.





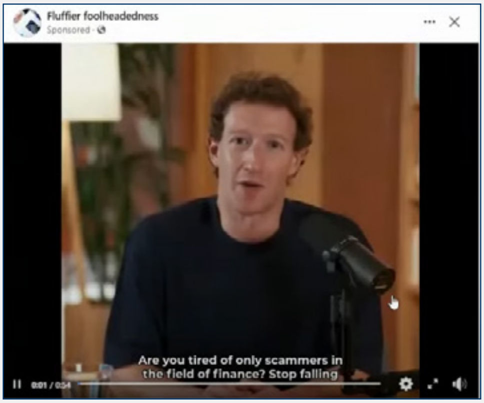
Residents of Israel can get from 800 shekels a day."
with the name of the sela at the bottom, and write that
she is a singer.



I HAVE JUST FINISHED
NEGOTIATIONS WITH

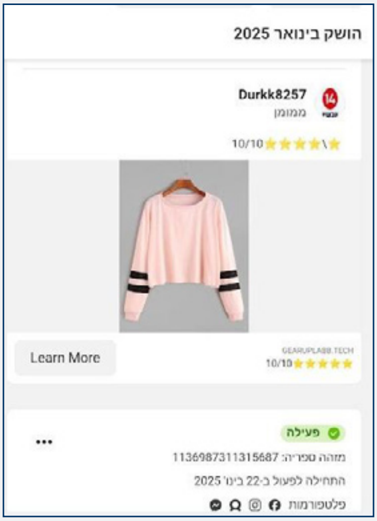
3. FAKE ADS ARE DISTRIBUTED TO PROMOTE THE FRAUD CAMPAIGN ON SOCIAL MEDIA PLATFORMS

The distribution of fake ads from hijacked or impostor pages is carried out through paid promotion using the various deepfake videos or visuals – and as mentioned, each version is designed to match its intended target audience and demographics, as supplied to advertisers by social media platforms. The platforms' sponsored promotion mechanisms are powerful targeting and advertising tools that enable advertisers to reach the right user, with the right ad, at the optimal time – in order to entice the user to interact with the ad and tempt them to enter the designated website created for the fraud scheme. The fraudsters can easily reach precise vulnerable users with personalized ads, taking full advantage of the platforms' powerful marketing systems.



Are you tired of only scammers in
the field of finance? Stop falling

In addition, the platforms' advertising tools offer advanced options that allow the fraudsters to disguise the fraudulent videos in order to conceal them from the platforms' algorithms. The cloaking tools available to advertisers make it easy for fraudsters to exploit the platforms for malicious purposes. For example, tools like ”Dynamic Ads” and ”A/B Testing” allow them to display a legitimate-looking ad in the platform's ad library, while showing the target user a different ad promoting a fake financial product. These advanced tools and the allowance for anonymity are leveraged by the fraudsters to distribute the fake content under the radar of the safety and protection systems of the social media platforms.



הושק בינואר 2025

Durkk8257
ממומן

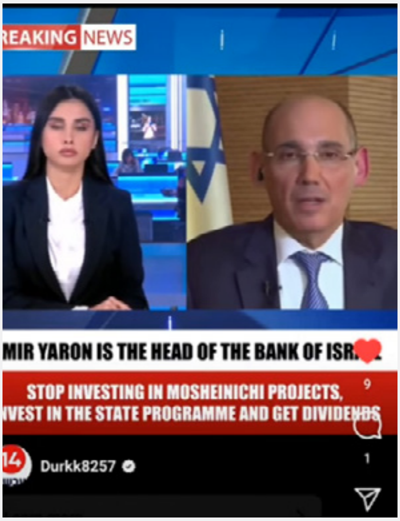
10/10★★★★\★

GEARUPLABB.TECH
10/10★★★★★

מזהה ספריה: 1136987311315687

התחילה לפעול ב-22 בינו' 2025

פלטפורמות



MIR YARON IS THE HEAD OF THE BANK OF ISR

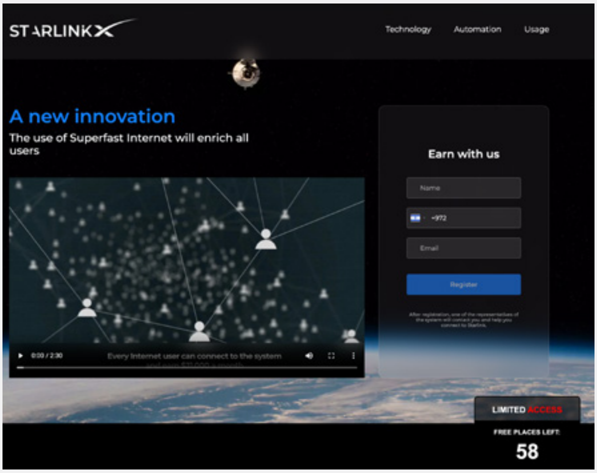
STOP INVESTING IN MOSHEINICHI PROJECTS,
NVEST IN THE STATE PROGRAMME AND GET DIVIDENDS

Ad Cloaking: A seemingly generic and legitimate image of a textile product (left) is displayed in the fraudster's Meta ad library. Meanwhile, the same ad is displayed differently to users in various Meta platform feeds as a deepfake video of a Channel 14 news anchor interviewing Amir Yaron, Governor of the Bank of Israel (right). Both versions of the ad lead to the same malicious landing page.

4. REDIRECTING TO A FRAUDULENT EXTERNAL LANDING PAGE AND COLLECTING PERSONAL AND FINANCIAL INFORMATION

When the user clicks on the ad shown to them on social media, containing the fake content and video, they are redirected to an external website or landing page that visually appears credible, professional, and polished. These external service or produce sites presents the investment or purchase opportunity offered to the potential victim. Typically, this involves enticing financial services or opportunities that reflect public trends and demand. For example, a website offering a fake AI application that promises the user smart and continuous monitoring of stock market performance and recommendations for the most profitable investments. The many websites established to carry out the fraud schemes present a range of content and simulations designed to give the user a sense of trustworthiness and professionalism.

For instance, just like the fake ads presented on social media platforms, the websites contain fake AI promotional videos based on real images and video clips taken out of context; fabricated endorsements from celebrities, experts, or public figures promoting the financial product that promises high returns; and colorful, impressive graphic simulations of dashboards and various financial applications.



A new innovation

The use of Superfast Internet will enrich all users

Every Internet user can connect to the system

Earn with us

Name

+972

Email

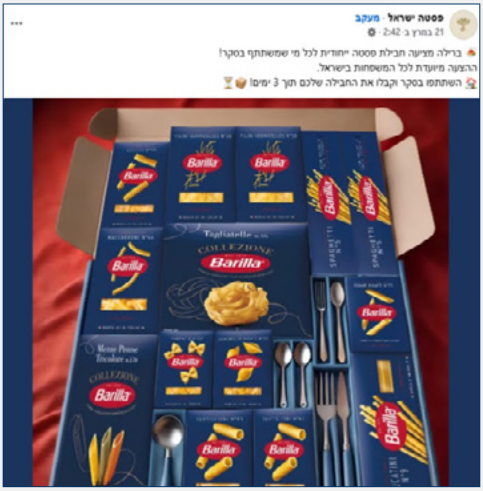
After registration, one of the representatives of the system will contact you and help you connect to Starlink.

FREE PLACES LEFT:

58

COLLECTION OF PERSONAL INFORMATION

After gaining access to the fraud scheme's designated landing page, the user is asked to register on the page (or for the service being offered) and to input personal information and contact details such as name, email address, and phone number. In some cases, a representative implicit in the scheme initiates private and direct contact with the user via phone call or email and provides them with access details to a fake investment platform, in order to create the false impression of a legitimate financial product. There have also been documented cases of malicious use of spoofing techniques, including foreign phone numbers posing as local Israeli numbers. In fact, when attempting to call back the number, the call leads either to a disconnected line or to a person with no connection to the fraud scheme. In certain cases, the fraud mechanism concludes at this stage – after collecting credit card or bank account details, the fraudsters attempt to withdraws funds from the victim's financial account. In other cases – which will be detailed in the following sections – there is an attempt to draw the victims into a more prolonged and complex scam, including direct communication and ongoing manipulation.

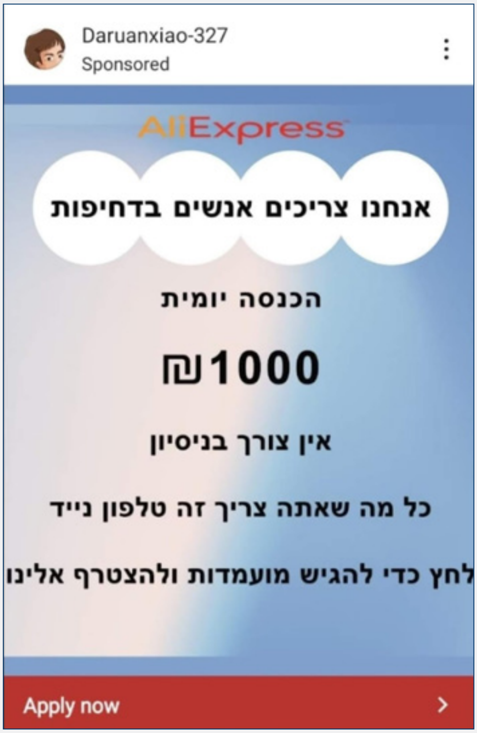


פסטה ישראל · מעקב

21 במרץ ב 2:42 · ⚙

ברילה מציעה חבילת פסטה ייחודית לכל מי שמשתתף בסקר!
ההצעה מיועדת לכל המשפחות בישראל.
השתתפו בסקר וקבלו את החבילה שלכם תוך 3 ימים! 📦⏳

A fake Facebook ad offering a free luxurious package of Barilla pasta products. In reality, the user is asked to input credit card details to pay a "shipping fee," but receives nothing – and the credit card information is sent to the fraudsters.



Daruanxiao-327
Sponsored

AliExpress

אנחנו צריכים אנשים בדחיפות

הכנסה יומית

₪1000

אין צורך בניסיון

כל מה שאתה צריך זה טלפון נייד

לחץ כדי להגיש מועמדות ולהצטרף אלינו

A sponsored ad allegedly recruiting for a job in collaboration with AliExpress to "promote products" and receive a commission. The victim performs "simple tasks" on a site that appears legitimate, including viewing products and "encouraging purchases," and sees a display of fake earnings. Later, the victim is required to deposit funds in order to "benefit from higher commissions." In reality, this is a fraudulent site – the platform is fake, the money cannot be withdrawn, and the profits are not real.

5. THE USER GAINS ACCESS TO THE SCAM PLATFORM

Using the login credentials received from the scam representative, the user connects to a platform that appears professional and trustworthy. For example, the platform displays a dashboard and graphs of activity in the capital market, and an interface posing as a legitimate trading platform, even displaying a "Withdrawal" button to give the user the impression that they can expect to earn money through use of the product and will be able to withdraw profits at a later time. To begin the trading and investment process, the user is asked to deposit an initial amount.

6. USER'S SENSITIVE FINANCIAL INFORMATION IS COLLECTED

In order to ”continue trading and earn additional profits,” the platform prompts the user to deposit larger amounts and provide bank account details, ID card information, and other personal financial data. At this stage, the user is already emotionally and financially invested in the process and the platform, making it harder for them to question the situation and understand that they are being exploited and falling victim to fraud. The fraudsters use social engineering techniques to manipulate the user into investing more funds and create a sense of urgency and false trust through personal conversations, presentation of fake graphs, and fabricated data.

7. USER IS PROMPTED TO CONTINUE DEPOSITS AND SUBMISSION OF SENSITIVE INFORMATION

The cycle of communication and financial deposits repeats until the user attempts to withdraw the funds, or the fake platform shows the user that they have in fact lost all the money they deposited. When the victims try to make contact or file a complaint, they encounter complete unresponsiveness – after having lost their assets.

C. TAILORING THE CHARACTERISTICS OF THE SCAM TO THE TARGET AUDIENCE AND LOCAL CONTEXT IN ISRAEL

The current new wave of social media fraud using deepfake technologies and sponsored ads, as described in this document, is a global, broad-scale phenomenon and is not limited to Israel alone. However, the phenomenon differs from country to country, and in Israel it exhibits several unique characteristics that are tailored to the local audience and discourse:

- **Use of Familiar Israeli Figures and Entities**

  AI-based scams in Israel often focus on local public figures such as politicians, public personalities, media figures, and popular Israeli celebrities. The use of these figures is intended to enhance the sense of credibility and attract the attention of the Israeli target audience. For example, in one video, Prime Minister Benjamin Netanyahu is seen declaring that he asked Elon Musk to launch an investment platform for Israeli use. Other examples can be seen in fake videos of El Al Airlines, i24 News, Channel 14, singer Noa Kirel, Rotem Sela, and Yaron Amir, the Governor of the Bank of Israel, who is shown recommending false investments.

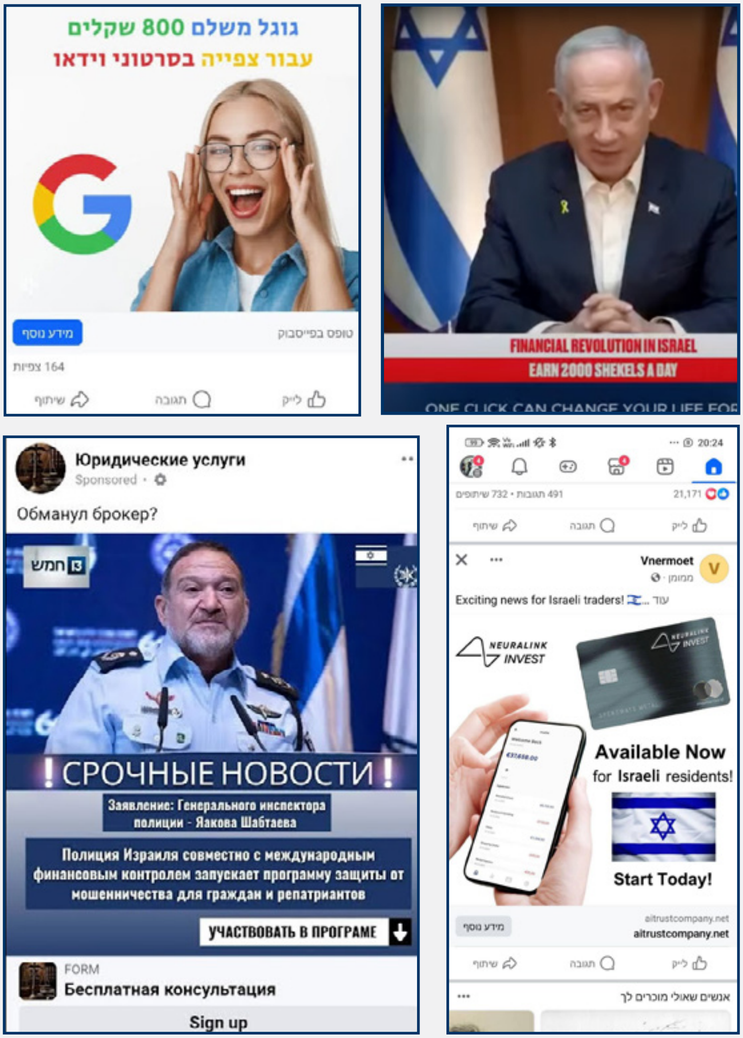
- **Use of Local Currency**

  Many fraudulent offers in Israel are phrased with reference to the local currency. For example, promises of high profits in shekels or investment offers tied to the local capital market. This element increases the perceived authenticity of the content among potential victims. Campaigns have also been observed promoting investments in an Israeli digital currency that does not yet exist, mirroring current events in Israel and exploiting actual public statements about the development of such a currency.

Cultural and Linguistic Adaptation

In contrast to previous similar scams, the content of these fraud schemes is precisely adapted to Israeli culture and language. These adaptations, which include the use of local expressions and references to current events, make the scam harder to detect and increase its persuasive power over the local public. Videos featuring familiar Israeli figures sometimes contain subtitles in languages common in Israel, such as Russian, and are tailored to the local context, enabling precise targeting and a false sense of the ads’ credibility among Russian-speaking Israelis. These adaptations are made possible by new AI tools that have made drafting and generating localized texts and content easier and more accessible for fraudsters.

These unique characteristics highlight the need for locally adapted solutions at the national level, with an emphasis on increasing Israeli awareness and regulation, alongside broad international cooperation.



Examples of ads adapted to the local Israeli context

D. THE ROLE OF PLATFORM FEATURES, VULNERABILITIES AND INACTION IN ENABLING ONLINE FRAUD

Over the past decade – and especially in recent years – fraudsters have rapidly adopted advanced technological tools and used them to carry out sophisticated fraud schemes, while social media platforms have failed to develop effective detection and enforcement mechanisms.

Below are several key failures that turn social media platforms into intelligent, user-friendly, and efficient distribution mechanisms for fraudsters and criminal entities:

- **Use of Advanced Digital Advertising Tools**
  Social media platforms provide advertisers and business users with powerful marketing tools, offering them advertising tools that draw on user data and segmented audience targeting. Fraudsters take advantage of these tools to disguise their scams. For example, dynamic ads allow the advertiser to display different versions of the same ad. A user might see an ad for a simple product like clothing, but upon clicking it, is redirected to different content that lures the user into the fraud scheme. The platforms' content monitoring processes – which are sometimes based on random sampling or automated tools.

- **Protection of Advertisers' Anonymity**
  The high level of anonymity and protection that platforms offer advertisers and malicious actors operating through them makes it difficult to identify and locate those responsible for misleading or harmful content. This hampers the ability of civil society organizations, researchers, and enforcement bodies to operate effectively and trace the origins of the scam – particularly given the lack of cooperation from global platforms, which often do not maintain local offices, provide local support, or offer national authorities adequate transparency about their operations and users.

Approval of Ads Featuring Political Figures Without Disclosure Labels

Though state regulations and the platform’s policies demand that any advertisement featuring political issues or personalities adhere to transparency requirements, fraudsters frequently publish fraudulent ads featuring deepfakes of political figures – without the ads being classified as political advertising. This allows entire campaigns to be launched that seemingly show political figures endorsing suspicious messages or products, without the platforms’ systems identifying the content as sensitive or suspicious.

Difficulty in Monitoring ”Related” Ads

Even when a fake ad is removed, the platforms fail to monitor all other ads by the same advertiser, allowing them to continue running simultaneously. Attackers use techniques such as campaign duplication, subtle wording changes, and decentralized advertising models that enable them to replicate the fraud campaign repeatedly while avoiding detection. The platforms themselves prioritize retaining advertising revenue and therefore have insufficient incentive to invest resources in active enforcement against fraudulent ads.

Redirecting Users to External Fraudulent Websites

The scam process consists of multiple stages, beginning with exposing victims to fake ads, redirecting them to untrustworthy websites, domains and fake services, and sometimes including direct contact with the operators. Every step of this process is monitored and tracked by Meta, who have easy access to this digital trail and coordinated activity. Meanwhile, fake comments by fictitious accounts on the ads contribute to the false credibility of the content.

E. MAJOR FAILURES BY THE PLATFORMS AND AUTHORITIES IN HANDLING FRAUD

Cumulative experience from the field shows the issue of financial fraud and the harm it causes to users is not among social media platforms' top priorities. Moreover, the platforms actually profit from the very same sponsored ads used to promote the fraud schemes. The inadequate handling of fraud on social networks stems in part from the absence of preliminary detection and monitoring tools to block malicious ads, as well as a lack of proper reporting mechanisms and effective policies for handling user reports. Below are the main failures by various platforms in addressing financial fraud threats:

FAILURES IN EARLY DETECTION,PREVENTION, AND ENFORCEMENT OF FRAUD PROMOTION ON PLATFORMS

■ Lack of Effective Mechanism for Early Detection and Identification of Fraud

The platforms are flooded with malicious campaigns and ads that deceive users and extract significant funds from them. These cases could have been avoided using various technological means to identify malicious ads prior to publication based on different parameters – for example, redirection to malicious websites, impersonation of brands and legitimate entities, or ties to known fraud sites and pages already identified in previous incidents.

■ Lack of Early and Effective Detection of Malicious AI Videos

In most of the fraud campaigns reviewed in this document, the promotional ads use generative AI videos featuring familiar figures. Nevertheless, the platforms lack effective mechanisms for identifying and labeling AI-generated impersonation videos – neither in the context of fraud nor in broader contexts.

FAILURE TO ACT ON REPORTS ON FRAUD SCHEMES PROMOTED VIA PLATFORMS

- **Removal of a Single Ad Without Addressing the Fraud System**
  In most cases, even when a fraudulent ad is reported and effectively removed, similar ads by the same fraud perpetrator continue to appear on other pages without disruption.

- **Lack of Sanctions Against Pages that Operate Fraud Schemes**
  Even when a page publishes fraudulent content, it is not blocked or removed, allowing it to continue launching new ads in the future and to replicate the content unhindered.

- **Preservation of the Fraudsters' Digital Infrastructure**
  Without sufficient enforcement, the same actors can continue to use the same pages, profiles, and advertising systems repeatedly, without needing to establish new infrastructure.

FAILURES IN REPORTING MECHANISMS FOR IMPERSONATION AND FAKE CONTENT

- **Ineffective Reporting Mechanisms**
  Platform users lack advanced and effective tools for reporting content violating platform policy, and surveys by ISOC-IL in recent years show that many users tend not to report abuse and threats they experience on the platforms due to a lack of trust in platform willingness to take action[2]. In many cases, there is also no structured mechanism or option to report scams that are promoted through sponsored content or the ads associated with them.

[2] Survey on Internet Safety in Israel: Analysis and Trends of Violent Discourse, Online Harm, and Responses (2024–2025) – www.isoc.org.il/sts-data/isoc-il-survey-2025-online-violence-and-safety

- **Lack of Adequate Action in Response to Reports from Trusted Flaggers and Partners**

  The platforms operate global programs for cooperation with local civil society bodies in various countries designated as Trusted Flaggers, who report on phenomena, trends, and severe incidents of harm and harmful content. However, in these programs and their corresponding reporting and response mechanisms, fraud and financial abuse reports to the platforms receive limited attention and priority.

- **Absence of Reporting Mechanisms for Coordinated Inauthentic Behavior**

  The lack of a mechanism that allows for reporting coordinated activity by groups of accounts or pages distributing fraudulent content impairs the ability to report, identify, and dismantle fraud networks.

LOW PRIORITY FOR ADDRESSING FINANCIAL FRAUD THREATS ON PLATFORMS

The issue of financial fraud and scams receives relatively low priority in the Trust and Safety policies of most platforms. Social media platforms declare that actions that do not amount to Real World Harm—such as physical space violations—are not a top priority. In practice, it seems that platform policies do not attribute significant damage to this form of financial fraud, although in reality it can ruin users' lives. This phenomenon is even more severe in countries with weaker regulation, where levels of enforcement and platform accountability toward users and enforcement authorities are even lower.

LACK OF NATIONAL REGULATION AND ENFORCEMENT

While in some countries and regions, such as the European Union, the United Kingdom, and Australia, there is advanced regulation requiring, among other things, transparency and oversight of ad usage, in many other countries—including Israel—similar oversight and enforcement mechanisms are lacking under the law. Information shown about ads to users located in the European

Union is much more detailed than what Israeli users receive. Users in Israel are exposed to scams without receiving sufficient information about the ads and advertisers. Moreover, there is currently no regulation or oversight in Israel concerning the creation, publication, and sponsored promotion of synthetic marketing and persuasive content generated through artificial intelligence, which is now at the heart of the global fraud industry.

F. MAIN RECOMMENDATIONS FOR CORRECTING THE SITUATION

RECOMMENDATIONS FOR PLATFORMS — DIGITAL COMMUNICATIONS CORPORATIONS AND SOCIAL MEDIA NETWORKS

- **Oversight, Enforcement, and Transparency in Sponsored Advertising**

  Platforms must require advertisers who benefit from their advanced advertising and targeting mechanisms to provide disclosure and reveal the identity of the sponsoring entity. Any investment of resources and finances in sponsored promotion must be accompanied by full transparency and public accountability.

- **Improvement of Oversight Mechanisms Regarding Redirects to Fraudulent External Sites and Platforms**

  Deactivation of ads and pages that redirect to websites identified as part of active fraud mechanisms.

- **Systematic and Comprehensive Removal of Fraud Infrastructure**

  Comprehensive handling and removal of duplicate scam ads and blocking of pages linked to repeat fraud advertisers.

- **Improvement and Implementation of AI Content Detection Mechanisms (with emphasis on deepfake audio and videos)**

Detection or labeling of misleading and manipulative content prior to its distribution on platforms, especially when using sponsored promotion mechanisms.

- **Development and Improvement of Detection and Prevention Mechanisms for Coordinated and Inauthentic Behavior**

This includes not only political influence campaigns and foreign state interference but also commercial fraud and manipulation.

- **Increasing Resources Dedicated to Local User Safety**

Assigning trained personnel and adapting systems and tools to the local language and culture in smaller countries, including Israel, and providing a direct response to issues concerning user safety and protection.

- **Platforms Must Provide Accessible Reporting Mechanisms and Efficient Ongoing Support for End Users**

Additionally, platforms must provide a comprehensive and effective response for Trusted Flaggers.

STATE-LEVEL RECOMMENDATIONS — LEGISLATORS AND LAW ENFORCEMENT AUTHORITIES

The economic harm posed—both at the individual and public levels—is significant and therefore requires the prioritization and allocation of public resources for locating offenders, assisting victims, and addressing the phenomenon through investigation, enforcement, and raising public awareness. Below are several recommendations for state regulatory and enforcement bodies:

- **Mandatory Legislation for Transparency and Accountability of Digital Platforms**
  Promote regulation in accordance with international standards (such as the DSA in the European Union) for the accountability and oversight of social media conduct, including the imposition of significant sanctions for violations that compromise user safety and protection, including the use of platforms to promote fraud, criminality, impersonation, and financial harm to users in Israel.

- **Improving Digital Investigation and Enforcement Capabilities**
  Strengthening the tools available to enforcement bodies and authorities to address digital crimes, including financial scams on social networks, and improving the interface and information flow between authorities and the platforms.

- **Empowering Dedicated Enforcement Units**
  Upgrading the resources and capabilities of units specializing in handling online fraud, including the training of professional personnel to address complex cyber offenses and provide public-level support in identifying networks and widespread patterns of fraud and financial abuse online.

- **International Cooperation**
  Promoting cooperation between countries and relevant organizations for the monitoring, detection, and response to cross-border digital fraud, including efforts to combat foreign interference in democratic processes and election systems.