ISRAEL INTERNET ASSOCIATION
ISOC-IL

Author:
Yonatan Ben Horin,
Director of the Internet Safety Hotline

Editor and Supervisor:
Edan Ring,
Director of Community Affairs

Cyber Threat Report – February 2023

Hijacking and Blocking of Business User Profiles on Meta Platforms

The Internet Safety Hotline at the Israel Internet Association www.safe.org.il

Hijacking and Blocking of Business User Profiles on Meta Platforms

Background and Purpose

This paper sets out to describe a new model of online hijacking and fraud that emerged from complaints submitted to the Israel Internet Association's Internet Safety Hotline by users of Meta platforms (Facebook, Instagram, WhatsApp) over the course of 2022. This model was especially prominent among reports from small business owners who manage Business pages on these platforms. The information in this paper is based on the collection and analysis of hundreds of complaints that were submitted over the course of 2022 to the Safety Hotline, as well as numerous reports and posts found in groups and various social media channels dedicated to providing cyber assistance and support to users and businesses in Israel. The purpose of the paper is to bring this phenomenon to light, to describe it and the damage it wreaks, and to point to the urgent need for more optimal and efficient solutions for Israel's internet users, Israeli users of Meta networks in particular. This paper describes a hijacking and blocking technique that recurred in the vast majority of complaints of this kind, and presents representative personal testimonies of real-life victims who contacted the hotline for support. The paper goes on to recommend steps that can be taken by the powers that be at Meta and by state authorities to combat and control this hazardous phenomenon.

Mode of Attack

The Internet Safety Hotline at the Israel Internet Association has received approximately 170 different complaints since September 2021 describing a similar pattern in which Facebook Business accounts are hijacked and pedophilic or pro-terror materials are used maliciously and manipulatively to have the victim automatically banned from Meta's three principal platforms (Facebook, Instagram and WhatsApp). The objective of the attacker is to obtain exclusive control over the victim's digital property, most importantly over the Ad accounts linked to his or her credit cards.

The hacking of Meta accounts is a well-known and common occurrence, but the hijacking technique described here differs in the singularity of its method as well as in the extent of the damage and repercussions it inflicts upon the platform's users in Israel—and, based on foreign media reports, in other countries around the globe as well. Furthermore, this phenomenon is unique in that there is not yet any built-in service response or technical support offered within the platform to assist the victims of this type of attack, and the only way to recover from it is to gain access to a human representative within the company who can assess each case on an individual basis. This is extremely difficult to achieve as Meta offers no active customer service in Israel – in Hebrew or English. This sophisticated method of operation maliciously exploits the platform's automated moderation (content censorship) mechanism, which was designed to protect its users, but in practice makes it very difficult for victims to report and flag the attack in order to receive assistance, since they are automatically identified as offenders and are immediately blocked.

The vast majority of complaints submitted to the Hotline since September 2021 depict a recurring pattern of hijacking and abuse and are characterized by a nearly identical storyline:

01 The attackers obtain access to a user's private Facebook account, apparently using leaked, stolen or weak passwords, and break into it with the intent of hijacking the account and its assets and causing the account owner to be blocked so that the case will not be treated promptly. The vast majority of victims did not have two-factor verification enabled. In most cases, the attackers' motives appear to be financially driven.

02 The attackers' preferred targets are Facebook users who currently hold—or have held in the past—a paid advertising account or an active Facebook Business page.
A few complaints were received by users who fell victim to this kind of attack even after setting up active protective measures, like two-factor verification.

03 After hijacking the victim's Facebook account, the attackers try to attain access to the advertising account and/or to administrator authority over the victim's Business page, unbeknownst to the page owner. They then add themselves or someone working on their behalf as an additional Admin on the advertising page linked to the victim's credit card.

04 In the next phase, the attackers publish pedophilic or pro-terror content on the victim's personal profile page (usually in a story or post) in order to activate the automatic recognition of the malicious content by the moderation system and, as a result, the immediate blocking of the personal profile in accordance with community standards.

05 At this point, with the personal profile blocked, the hijackers have exclusive Admin authority over the Business page and/or Ad account. Once the victim has been blocked, the attackers begin to commit credit card fraud using the victim's Ad account and/or Business pages – most often using the hacked account to finance advertising campaigns for third-parties in remote locations outside the country.

06 If the victim's credit card or PayPal account is linked to the hacked Facebook account, the attackers use it to run ads and to advertise various products—possibly on behalf of third parties who are entirely unaware of the nature of the payment's source.

07 Since the attackers do not have access to the actual credit card information saved in the system, they secure exclusive control over the proxy authorized to operate the credit card saved in its profile. Many of the victims who turned to the Hotline confirmed that their credit cards were used to finance ads in distant locations like Southeast Asia.

08 If the victim's credit card or PayPal account is not linked to the hacked Facebook account, the attackers use other stolen credit cards to perform the ad fraud while using the victim's Ad account or Business pages.

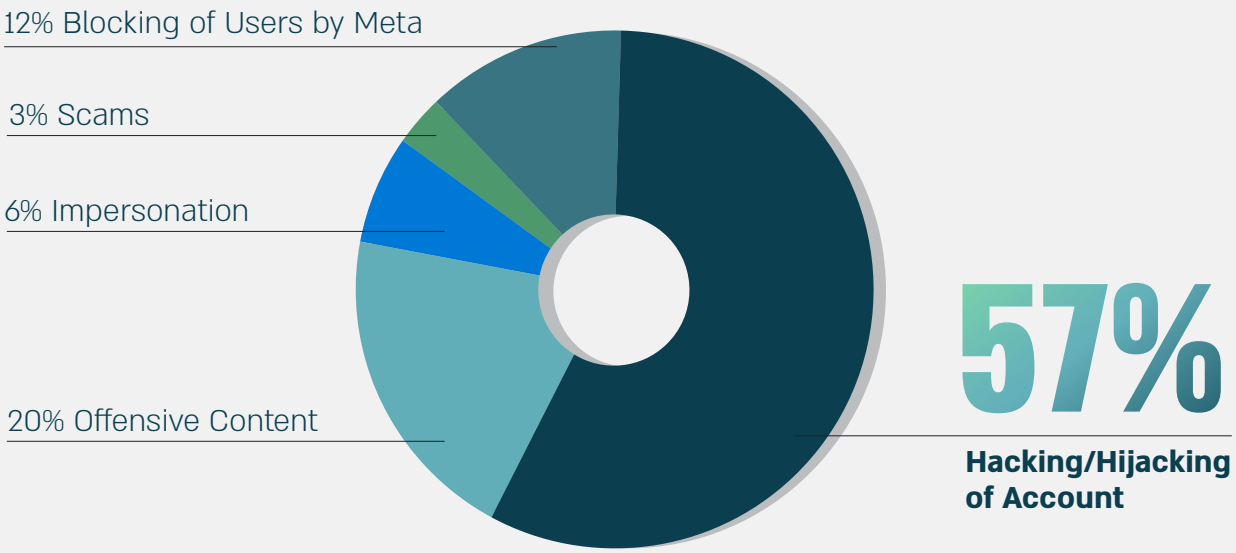
09 These attacks can also harm Facebook users without a Business page or Ad account, but they were a small minority among the complaints we received. The objective in those cases was usually to shut down their personal profiles in order to hurt them for political, nationalistic or other reasons. Approximately 90% of the victims of the phenomenon discussed in this paper reported having an active or inactive Business page or Ad account.

10 Additionally, it is important to note that even when the victims succeed in reclaiming control over their personal Facebook and Instagram accounts after they were hacked, they are unable to reclaim their ownership of the Ad accounts and Business pages that were once associated with their accounts.

11 In cases where the attack interfered with the victim's access to his or her WhatsApp account, it very often remains blocked even after the other accounts have been restored. Attempts to contact and receive assistance from WhatsApp's technical support are fruitless. There is scarce to no support for WhatsApp users in Israel.

12 Some victims, who contacted Meta Israel's legal department and informed them that they planned to take legal action, reported receiving a relatively quick solution that released their Facebook and Instagram accounts from captivity, but not their WhatsApp accounts.

Incidents Reported by Meta Users to the Hotline in 2022



Damages Sustained by Hijacking Attack Victims

01 Consequent to the attack and posting of the offensive content, users describe an immediate response by Meta in which the platform shuts down the Facebook and Instagram accounts in their possession. These shut-downs severely disrupt their ability to manage their businesses, to communicate with customers and suppliers and with their social circles. They also cause aggravation and severe personal distress to the victims.

02 Many times the victims sustain a financial blow as the result of irreversible credit card charges, and must spend valuable time and effort cancelling and restoring their credit cards, social media pages and Ad accounts.

03 The hacking and usurping of digital assets and the discontinuation of communication with customers tarnishes the affected business's reputation, impedes its ability to provide customer service, and damages its customers' trust regarding future transactions.

04 If victims are unsuccessful in restoring their Business pages and the rest of their digital assets, they also stand to lose marketing materials, customer databases, correspondences, documentation of transactions and more. The reconstruction of all of these materials takes vast amounts of time and effort.

05 Users are allowed 30 days to appeal the decision, after which their account is permanently deleted. The users often appeal in vain, and receive a message that the decision by Meta to shut down the account is final.

06 Approximately 70% of victims report that their WhatsApp account was blocked as well, not immediately, but rather one to two weeks later. The blocking of a WhatsApp account is permanent with no option to appeal the decision.

07 **The damages incurred by these victims, who are left without their Facebook, Instagram and WhatsApp accounts, are at once financial, social and personal.**

Personal Testimonies from Victims of Hijack-and-Block Attacks

"A few days ago my accounts were hacked (Facebook, Instagram, WhatsApp).
Meta responded by immediately blocking the accounts. I was asked to submit documents to verify my account and I cooperated, but they, in turn, blocked my accounts permanently with no opportunity to appeal. My business was hit hard since all of my recommendations appear on Facebook, and all of my advertising content (into which extraordinary resources were invested) redirects to Facebook, Instagram and WhatsApp. I feel completely helpless, haven't been able to sleep for days and am having trouble functioning,
I fear the financial consequences for my family."

M, owner of a pain-treatment business in central Israel, December 2022

"My Facebook account was hacked …. after which my Facebook and Instagram accounts were blocked (my Instagram is linked to my Facebook sign-in). Facebook claims that my accounts were blocked due to the posting of offensive content (pedophilic material posted in my name, according to a friend who saw it) and violation of the Terms of Use. My accounts have still not been unblocked in spite of the objection I submitted along with all the required documents.

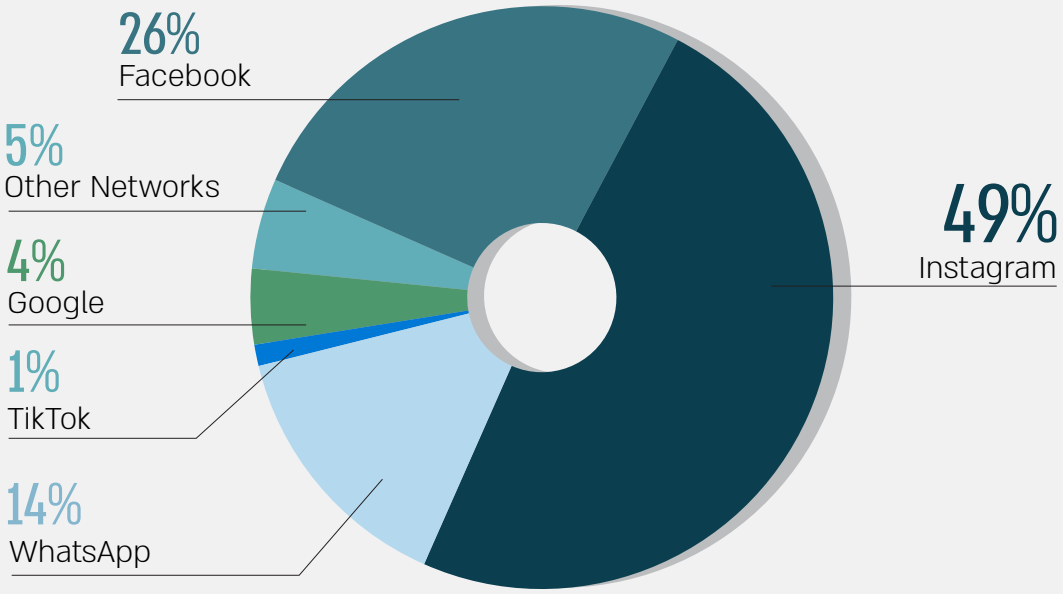
Two weeks after the above incident, WhatsApp notified me that my account had been suspended. When I tried to reach WhatsApp's customer service I received a terse response that my account had violated the Terms of Use and had been the subject of numerous complaints. I have not been able to reach anyone who can restore my accounts. WhatsApp is especially sensitive due to the large amount of information and correspondence that I had stored in it."

G, self-employed in the field of computing, February 2022

"Today I received numerous emails from Facebook reporting that my account had been accessed by various email addresses and a request had been received to reset the password. I responded to these messages by clicking on the appropriate links to confirm that I had not submitted this request. That evening I received notifications that my Facebook and Instagram accounts had been suspended due to noncompliance with their policy.
At the same time I received an email with the message "Your ad has been approved," though I hadn't posted any ad.
I have no access to my accounts and Facebook's and Instagram's responses say they don't have enough staff to examine my request. This is my personal account, under which I have a number of Business pages that are of utmost importance to me and my livelihood."

D, owner of a small productions company, October 2022

Cyber Incidents Reported to Hotline in 2022 – by Platform



Inadequate Support from Meta

In spite of numerous entreaties to Meta representatives by both the victims and the Israel Internet Association's Hotline representatives regarding the blocking of the victims' pages, the phenomenon persists, with no proper and effective response from Meta.

The Hotline is recognized as a "Trusted Partner" of Facebook and Instagram, allowing it to report "Safety"-related incidents using a direct communication channel designated solely for this purpose. The Hotline used this channel to report incidents and directly alerted policy managers at Facebook-Instagram and at WhatsApp (separate entities) about the phenomenon over the course of 2022, but received no suitable response. This phenomenon is categorized as "Security"-related which means that it does not merit response and treatment by the direct reporting channel dedicated to "Safety"-related incidents associated with "real-world harm" (real danger to human lives).
According to the company's representatives, financially or commercially-based cyber incidents do not meet the qualifications that would allow the company's Trust and Safety representatives to handle them effectively. And so an impossible situation is created, in which the blocked victims have no way to complain and receive assistance from the platform's representatives, and even organizations and entities recognized as official reporters (or Trusted Partners) are denied permission to report or to receive any response that could help the victims in this type of case. The final outcome is the outright neglect of these victims, the majority of whom are not only the platform's users, but also its paying customers, using it to manage their businesses and paid advertising—and nevertheless are refused support as they contend with this unacceptable phenomenon that has affected a great number of victims in the past year.

Summary and Conclusions

The complaints received and our analysis of the phenomenon they describe reflect severe abuse to users' rights to safety and freedom to function on both personal and business levels on Meta platforms, platforms that today play a central role in the management of many small businesses and digital assets in Israel. The attackers exploit the fact that countless Israeli users rely on Meta platforms as a central channel in the operation of small businesses and communication with their customers and business contacts.

The majority of complaints that reached the Israel Internet Association's Safety Hotline over the past year paint a clear picture in which business owners and users of the networks are stricken on two fronts: first, their freedom to function and manage their business affairs with respect to their customers, and second, their trust in—and receipt of help from—the platform paid to serve as their advertising channel. All this is compounded by the lack of response and treatment by the authorities and police in Israel, who do not offer assistance in this type of cyber abuse and fraud.

The phenomenon described in this report attests to the ever-growing complexity of online civilian cyber abuse. Meta classifies these attacks as security-related, assuming that their repercussions are primarily financial and commercial, and thereby justify their failure to intervene. However even by Meta's standards, this type of abuse certainly warrants a response, since there is a real safety issue here as well, involving personal and emotional harm, along with the clear danger of impersonation and serious privacy violations.

Since Israel is a relatively small market with a small number of business owners in comparison to other countries around the world, there is concern that the global Meta corporation is not devoting sufficient effort to examination of the phenomenon, to finding technological solutions to it and to the provision of help and service in response to these complaints and instances of abuse.

In many cases, left with no other choice, the complainants considered taking legal action and only after the threat of a law suit did Meta find a way to solve the problem and remove the block preventing the users from managing their pages. Even contacting state authorities and law enforcement officials did nothing to resolve the problem.

Principal Recommendations

Though the pattern described is highly complex and sophisticated, we are certain that there are several important measures that can be taken by the Meta company, other social media corporations, and Israeli state authorities, that would diminish and even thwart this serious phenomenon within a short time frame, thereby alleviating the suffering and abuse experienced by users of the network in Israel. We have divided these recommendations into four categories—Technology, Customer Service, Public Advocacy and Education, and Policy.

01 Technology

It is incumbent upon Meta to devote research and development resources to the study of the pattern that characterizes this type of attack, and the company must act to identify and prevent exploitation of its automated content censorship mechanisms as instruments of attack rather than protection. The company must develop tools that can distinguish between systematic, deliberate publication of offensive and destructive content (such as pornography or terrorism), and the publication of damaging content on hijacked, innocent profiles for the purpose of blocking those profiles' owners.

02 Customer Service and Assistance

Meta must act to improve the responsiveness and treatment it affords Business page owners hurt by cyber attacks, account takeovers and fraud within a reasonable time frame, and in the Hebrew language.

This would combat the phenomena of account hijacking and wrongful blocking in general, and in particular the malicious phenomenon described in the current report. The company needs to establish customer service that responds to Business account owners wronged by hacking and fraud, without first being threatened with legal action.

03 Public Advocacy and Education

Social media corporations that are active in Israel and act as a central and significant instrument for small business owners (like Meta) need to take more proactive, widespread and effective action encouraging their Business clients to ensure that their property is optimally protected.

To do this the platforms can use technological tools that they have at their disposal, by providing information and reminders in Hebrew on their apps and by encouraging users to fortify the active protection around their digital assets. They can also use public advertising outlets to raise awareness and encourage the use of safety measures like two-factor verification, strengthening password security and adding alternative trusted administrators to accounts.

05 Investigation and Policing

A response must be established by state authorities to provide appropriate assistance to small business owners hurt by attack, fraud, impersonation and harassment affecting their digital property on social media platforms. Attacks on small business owners' digital property must be treated with the same gravity as other forms of fraudulent or criminal activity.

04 Policy

State and official authorities also have an important role to play in the protection of business users' rights on social platforms and the advancement of protective action on their end. State authorities need to hold the platforms accountable and ensure that they are advocating and increasing awareness on this topic, while advancing similar advocacy themselves using the state's own resources—the National Cyber Directorate, for instance, and other relevant authorities.

ISRAEL INTERNET ASSOCIATION
ISOC-IL

Cyber Threat Report – February 2023

Hijacking and Blocking of Business User Profiles on Meta Platforms

A Report by the Internet Safety Hotline - ISOC-Il

safe@isoc.org.il

www.safe.org.il

Block - Cyber Civil Security Center
https://block.org.il

Author: Yonatan Ben Horin,
Director of the Internet Safety Hotline

Editor and Supervisor: Edan Ring,
Director of Community Affairs

Safety Hotline Consultation: Orna Heilinger,
Director of the Netica Center

Translation: Nina Mishraky

Graphic Design: Tali Gilad

The Internet Safety Hotline -
Israel Internet Association

https://en.isoc.org.il/netica

The Israel Internet Association (ISOC-IL)

www.isoc.org.il

https://www.facebook.com/ISOC.ORG.IL

https://twitter.com/ISOCIL