Phishing attacks using third-party applications against Egyptian civil society organizations

A new Amnesty International investigation found a new wave of digital attacks that likely originated from government-backed bodies starting from early January 2019 and involving multiple attempts to gain access to the email accounts of several prominent Egyptian human rights defenders, media and civil society organizations' staff. The attacks appear to be part of a wider strategy, occurring amid an unprecedented crackdown on the same groups in what have turned Egypt into an "open-air" prison for critics. Because of the identities of the targets we have identified, the timing of these attacks, their apparent coordination and the notifications of state-sponsored attacks sent from Google, we conclude that these attacks were most likely carried out by, or on behalf of, the Egyptian authorities.

In recent years, the Egyptian authorities have been harassing civil society and undermining freedom of association and expression through an ongoing criminal investigation into NGOs and a repressive NGO law. The authorities have been investigating dozens of human rights defenders and NGO staff for "receiving foreign funding". Many of them could face prison if convicted. The investigative judges have also ordered a travel ban against at least 31 NGO staff, and asset freezes of 10 individuals and seven organizations. Meanwhile, the authorities have also closed El Nadeem Center for Rehabilitation of Victims of Violence and continue to detain human rights defenders Ezzat Ghoniem and Hisham Gaafar, directors of the Egyptian Coordination for Rights and Freedoms and Mada for media studies, respectively.

The list of individuals and organizations targeted in this campaign of phishing attacks has significant overlaps with those targeted in an older phishing attack wave, known as Nile Phish, disclosed in 2017 by the Citizen Lab and the Egyptian Initiative for Personal Rights (EIPR).

Amnesty International is deeply concerned that these phishing attacks represent yet another attempt by the authorities to stifle Egyptian civil society and calls on the Egyptian authorities to end these attacks on human rights defenders, and the crackdown on civil society, including by dropping the foreign funding case and repealing the NGO law.

A new year and a new wave of attacks

Since January 2019 several human rights defenders and civil society organizations from Egypt started forwarding dozens of suspicious emails to Amnesty International. Through the course of our investigation we discovered that these emails were attempts to access the email accounts of their targets through a particularly insidious form of phishing known as OAuth Phishing (which we explain in detail below). We estimate the total number of targeted individuals to be in the order of several hundreds.

These coincided with a number of important events that took place in the country. In the run-up to the eighth anniversary of Egypt's 25 January uprising, which ended with the removal of former president Hosni Mubarak, after 30 years in power, we recorded 11 phishing attacks against NGOs and media collectives. We saw another burst of attacks during French President Emmanuel Macron's visit to Cairo to meet with President Abdelfatah al-Sisi on 28 and 29 January. The attacks peaked on 29 January, the day that President Macron met with human rights defenders from four prominent Egyptian NGOs. Later, in the first week of February, several media organizations were targeted as part of this campaign of digital attacks; they were reporting on the process of amending the Egyptian Constitution that the parliament had just officially started.

The attacks all bear the same hallmarks and appear to be part of a coordinated campaign to spy on, harass and intimidate their targets. While definitive attribution is difficult, the selective targeting of human rights defenders from Egypt, particularly in concomitance with specific political events, suggests this current wave of digital attacks is politically, rather than financially, motivated.

Additionally, we learned that multiple targets of this campaign received an official warning from Google alerting that *"government-backed attackers are trying to steal your password"*.

Caption: Google warning to one of the targets - 19 January 2019

These elements reinforce the suspicion that a state-sponsored group might be behind this campaign, further contributing to the chilling effect on Egyptian civil society and silencing those who voice criticism of the government.

What an OAuth phishing attack looks like: Step by step

Traditional phishing attacks attempt to deceive the targets into providing their passwords by creating a fake clone of, for example, Google's or Facebook's login page. If the target is successfully lured into entering their password, the attacker then "steals" their credentials and can reuse these to access their email account. Typically, this kind of phishing attack can be prevented through the use of two-step verification procedures such as those provided by most mainstream platforms these days, or by authenticator apps, or even better, security keys.

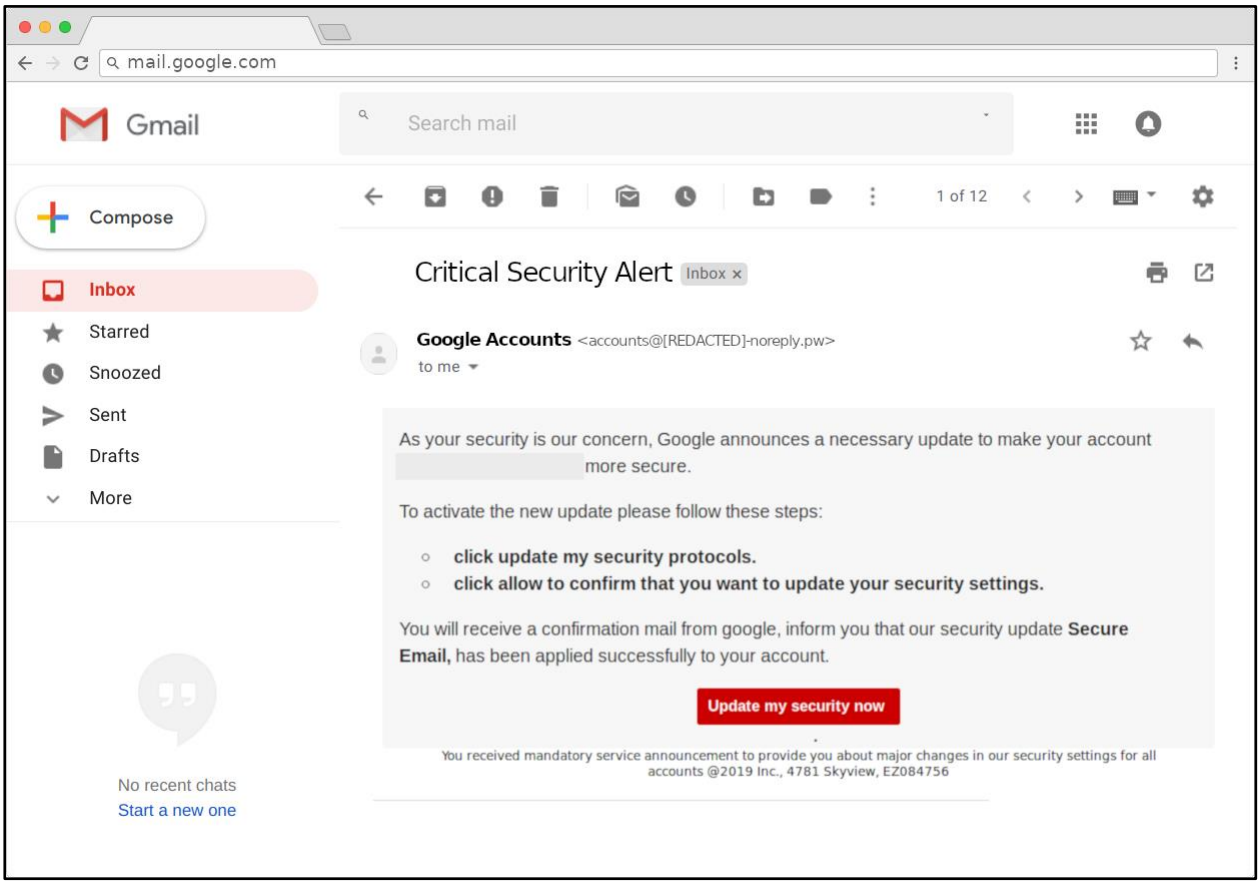
However, in this phishing campaign we have documented in Egypt, the attackers instead leverage a simple but less known technique generally called OAuth Phishing. Rather than cloning a legitimate login prompt that aims to trick targets into entering their password on a dubious-looking site, OAuth Phishing abuses a legitimate feature of many online service providers, including Google, that allows third-party applications to gain direct access to an account. For example, a legitimate external calendar application might request access to a user's email account in order to automatically identify and add upcoming events or flight reservations.

With OAuth Phishing, attackers craft malicious third-party applications that are disguised not to raise suspicion with the victims. (More information on this functionality is available on Google Support in English or Arabic).

Here we provide a step by step look at the ways in which these attacks work, and we follow on below with some concrete ways that people can better protect themselves from these kinds of attacks.

Step 1
We identified a few variants of the phishing emails received by the human rights defenders who shared these with Amnesty International. In the most common case pictured below, the email imitates

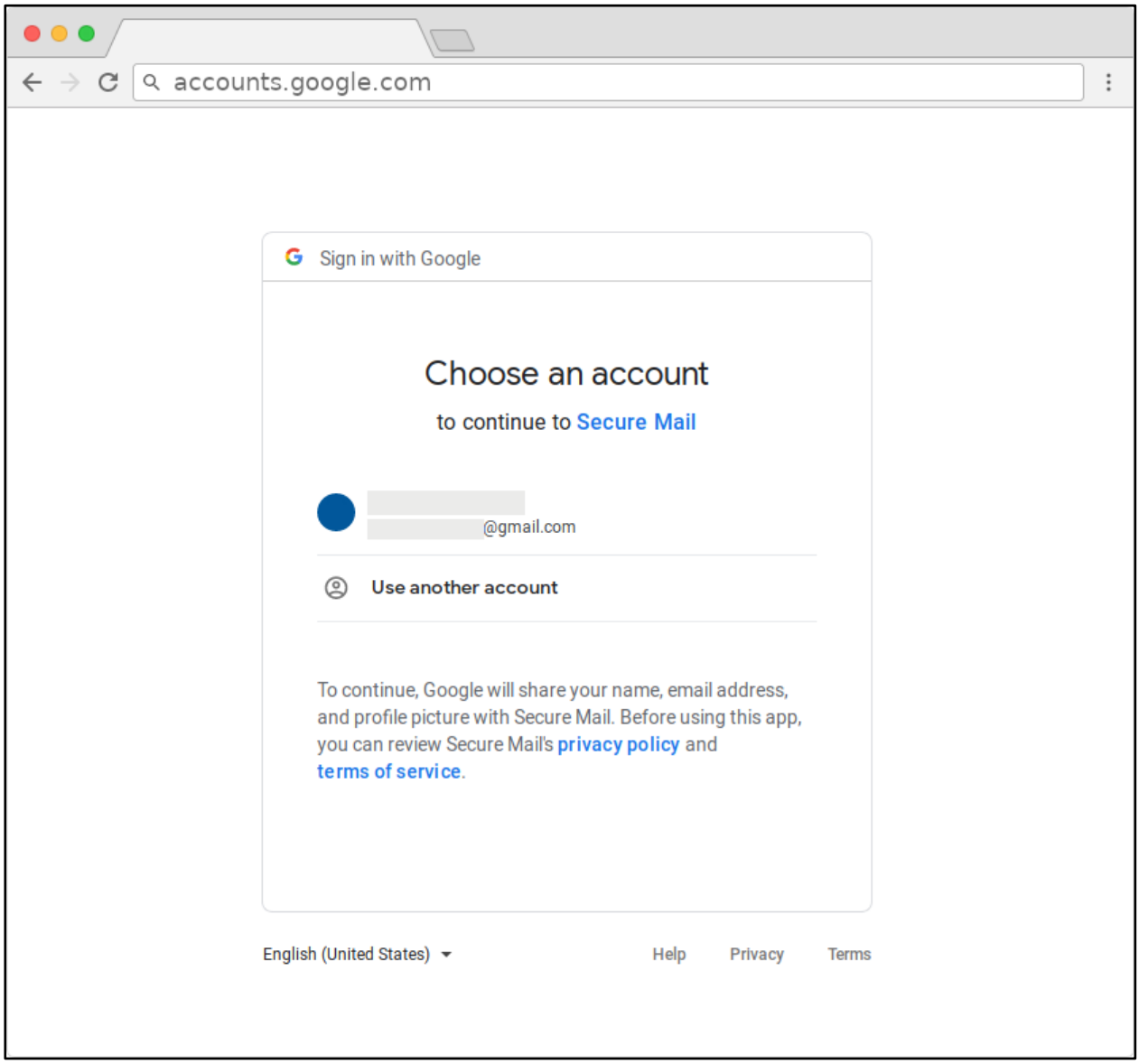
a security warning from Google and solicits the target to apply a “Secure Email” security update to their Google account.



(Caption: Screenshot of an example of phishing email used by the attackers)

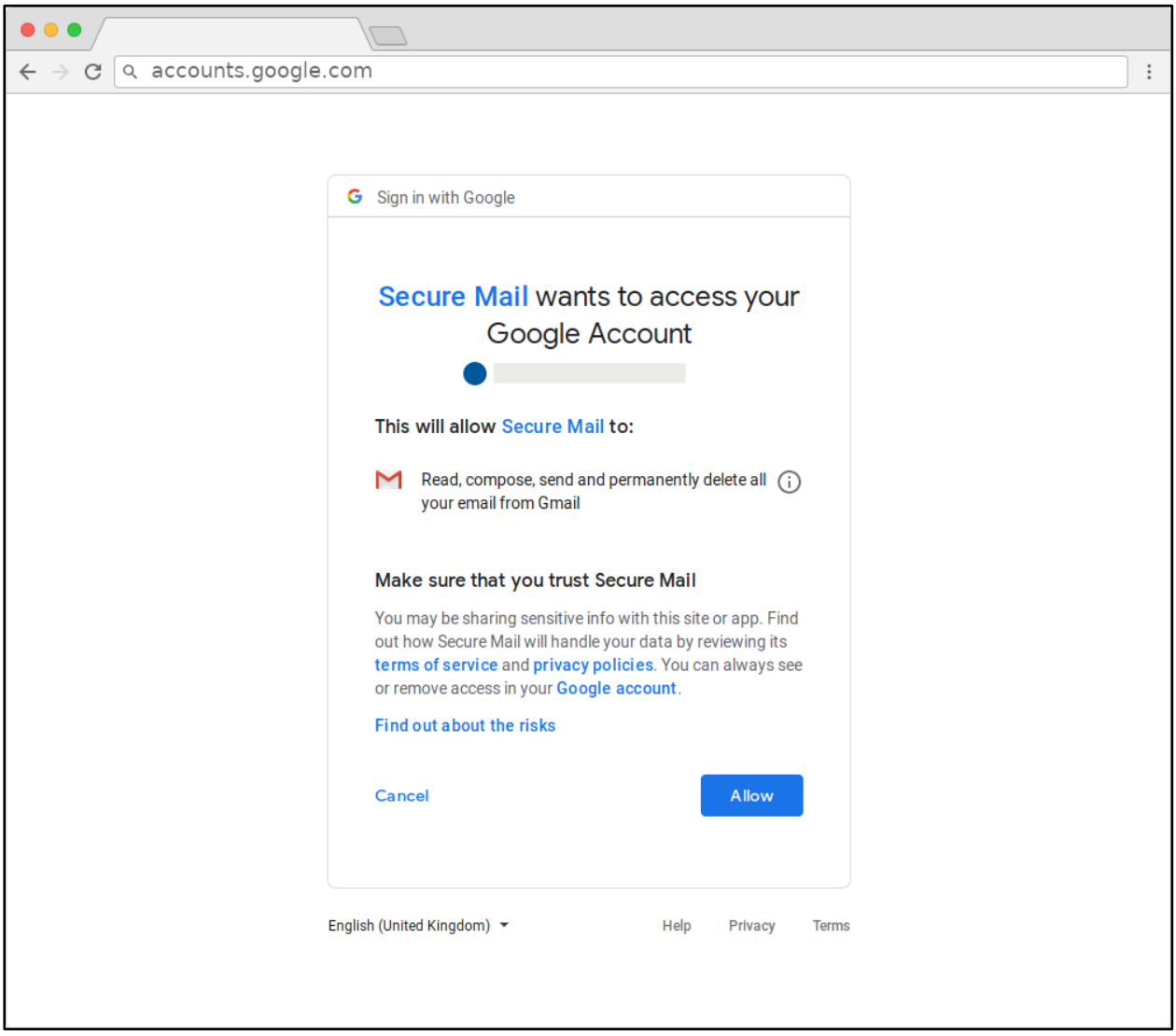
Step 2
Clicking the "Update my security now" button directs to a page that initiates the OAuth authorization process of the malicious third-party application named by the attackers as “Secure Mail”.

Step 3
At this point the target is requested to log into Google or choose an existing logged in account.



(Caption: Screenshot of Google's login prompt requesting authorization to the malicious app)

Step 4
Now the target is asked to explicitly authorize the malicious “Secure Email” third-party application to be granted access to their email account. While this authorization prompt does contain a warning from Google, it may be overlooked as the user has been directed from what appeared to be a legitimate email from Google.



(Caption: Screenshot of the confirmation to authorize the malicious app to the victim's Google account)

Step 5
Once the "Allow" button is clicked, the malicious “Secure Email” application is granted access to the target’s email account. The attackers are immediately able to read the email’s content, and the victims are directed to the real Google account settings page, which further reduces any suspicion on the part of the target that they have been victim of a fraudulent attack.

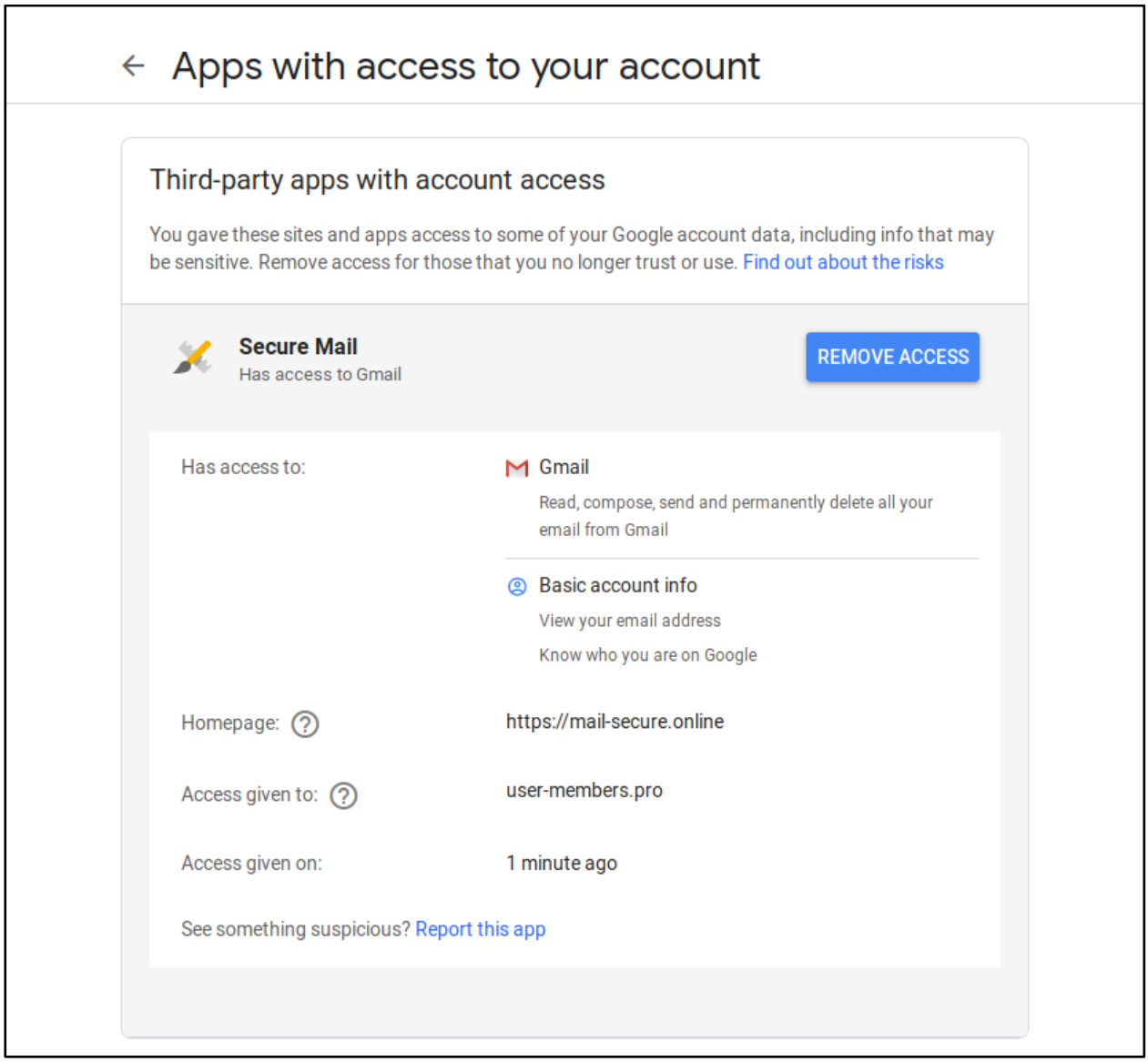
In addition to Google, we observed that the same attackers make use of similar tactics against Yahoo, Outlook and Hotmail users.

Defending Against OAuth Phishing

OAuth Phishing can be tricky to identify. Often, security education for individuals at risk does not include mentions of this particular technique. People are usually trained to respond to phishing by looking for suspicious domains in the browser's address bar and by enabling two-factor verification. While those are very useful and important safety practices to adopt, they would not help with OAuth phishing because victims are in fact authenticating directly through the legitimate site.

If you are an activist, human rights defender, journalist, or anyone else concerned about being targeted by these kinds of attacks, it is important to be alert whenever you are requested to authorize a third-party application on your accounts.

Occasionally it is a good exercise to review your account's security settings and check for authorized external applications. In the case of this campaign, the malicious Secure Email application will appear authorized as pictured below.



(Caption: Screenshot of the malicious third-party applications used by the attackers as it appears in the Google account settings page)

You might also want to consider revoking access to any other authorized application that you do not recognize or that you might have stopped using.

Google also offers an Advanced Protection Program that in addition to enforcing the authentication with a security key, disables third-party applications on your account. Beware that enabling this configuration introduces some limitations, so make sure it fits your particular requirements before enrolling.

Here you can find instructions on how to check for authorized third-party applications on your Yahoo account instead.

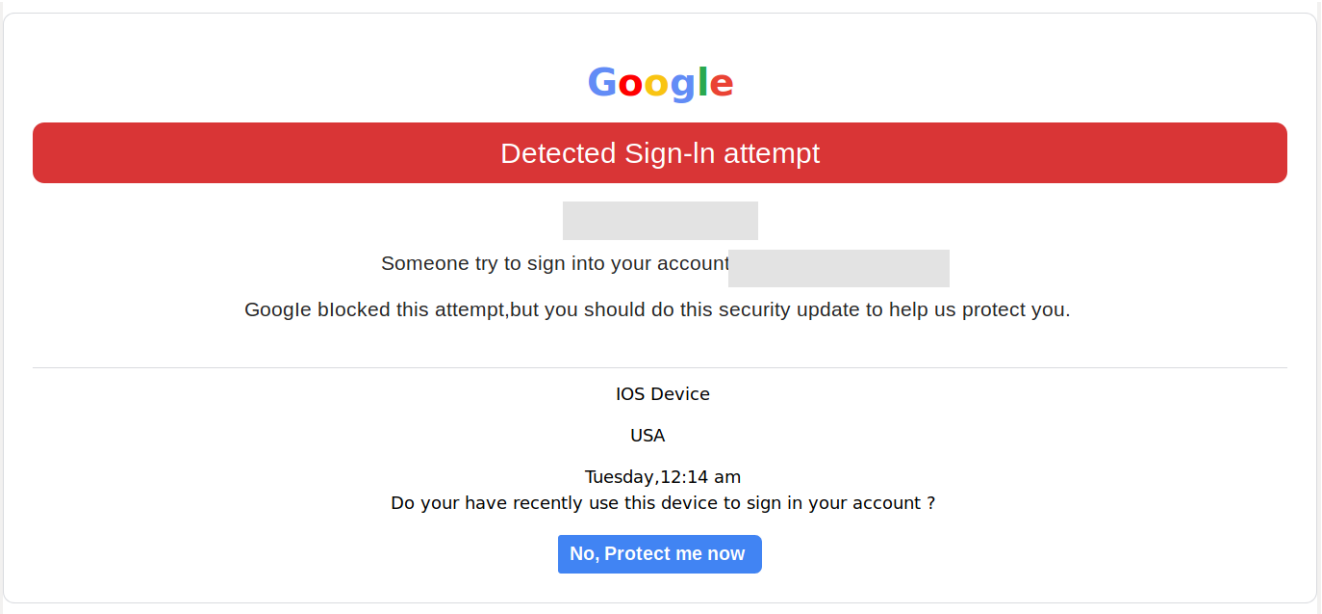
Get in touch

If you received any suspicious email like those we described in this report, or other forms of suspected targeted attack, you can contact us at **share@amnesty.tech**.

Appendix

Indicators of Compromise and attacks Infrastructure available here.

Following are screenshots of other phishing emails used in this same campaign.



Google

Unknown sign-in attempt was detected

Someone just try to sign in to your account.
Google blocked them, but you should check your security setting.

Check activity

Googel

Hi,

Mails team has suspended your account , because of your cancellation request.

if you think you didn't do this request you can try to recover your account, Recover your account now.

Any information related to your account will permanently get deleted after 48 hours, unless successfully appealed.

Regards,

Mails Team

Google

Your account is vulnerable so our team has made a new necessary update to make you more secure, The new update **Secure Email,** is easy to activate and will prevent any suspicious attempt against your account.

Secure my account now

if you ignore this update, the security of your account might be at high risk.