

# Evolving Phishing Attacks Targeting Journalists and Human Rights Defenders from the Middle-East and North Africa

16 August 2019, 09:00 UTC

In December 2018, Amnesty International documented widespread targeted phishing attacks against human rights defenders (HRDs) in the Middle-East and North Africa, in the report ["When Best Practice Isn't Good Enough"](#). That report documented how attackers had specifically developed techniques to target HRDs who had taken extra steps to secure their online accounts, such as by using more secure, privacy-respecting email providers, or enabling two-factor authentication on their online accounts.

Following this, in July 2019, HRDs again shared with Amnesty International numerous new malicious emails they had received, that revealed a renewed campaign of targeted phishing we believe to be orchestrated by the same attackers or by a closely related group.

## What is phishing?

Credentials phishing (or “Password-Stealing Phishing”) consists in the creation of a website that imitates the login prompt of a given online service, such as Gmail or Facebook, with the objective of luring a victim into visiting the malicious page and entering their username and passwords, thereby transmitting these credentials to the attackers.

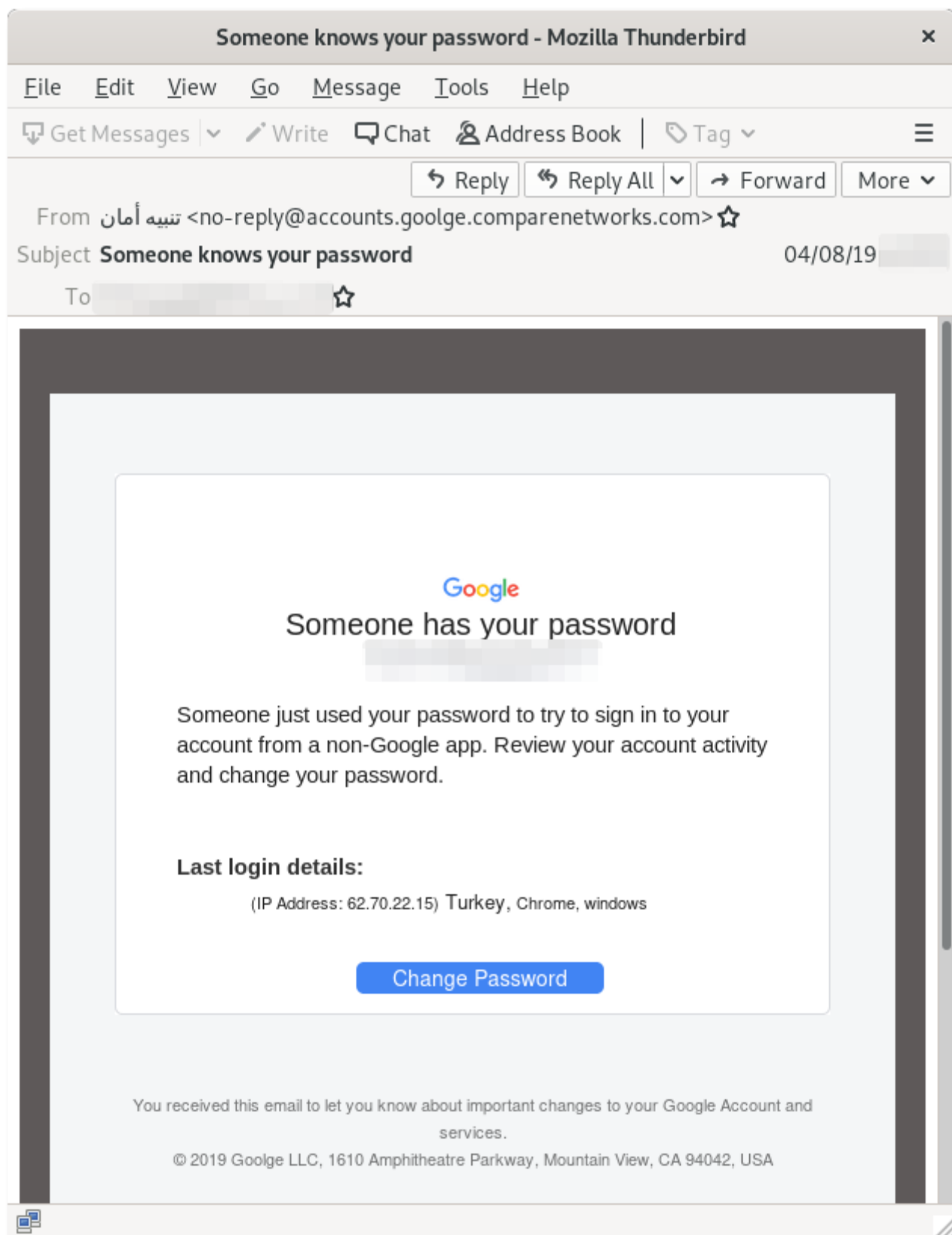
Credentials phishing remains a critical threat to HRDs online. Because of its simplicity and relatively low economic cost, phishing is a favorite tactic among attackers, and we regularly observe targets in the hundreds if not thousands. However, credential phishing is not always simple, and these new attacks - like those we documented previously - have taken novel steps to overcome security measures that targets take. As credentials phishing schemes evolve and improve, mitigations as well as security education need to improve too.

In this report we describe the improved techniques utilized by the attackers, which once more demonstrate their ability to adapt to changes in the technological landscape, and respond to the latest online accounts authentication and security best practices by developing workarounds.

## **First Tactic - Good old "Reset your Password" revisited**

Among the most popular social engineering tricks used in credentials phishing campaigns, the "Reset your Password" bait is an evergreen. In this latest campaign, for example, the attackers sent out emails to their targets impersonating Google and pretending to alert them of unsuccessful suspicious login attempts, and offering to secure the accounts. These emails play on urgency and fear, and their aim is to lure the targets into giving away their credentials, believing their passwords are instead being reset by Google.

In this latest campaign, the attackers took extra care to make sure both the malicious emails and the phishing pages appear as credible as possible. Indeed, these attacks can be very difficult to recognize.

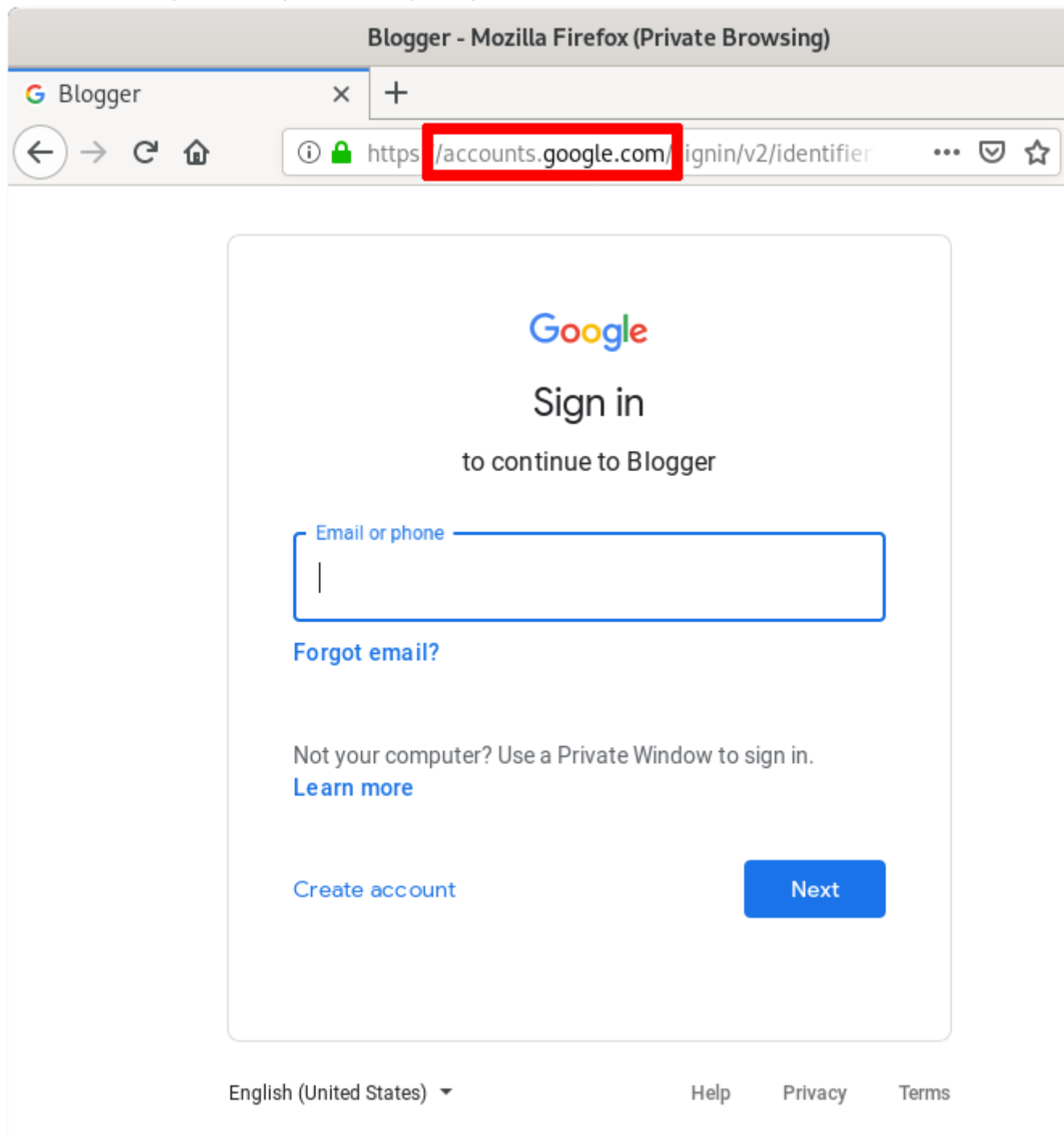


*Example of a phishing email shared with Amnesty International.*

In fact, the button that some of these malicious emails solicit the target to click points to a legitimate Google domain, **accounts.google.com**:

[https://accounts.google.com/Login?service=blogger&hl=en\\_US&continue=https://script.google.com/macros/s/\[REDACTED\]/exec?z=\[REDACTED\]](https://accounts.google.com/Login?service=blogger&hl=en_US&continue=https://script.google.com/macros/s/[REDACTED]/exec?z=[REDACTED])

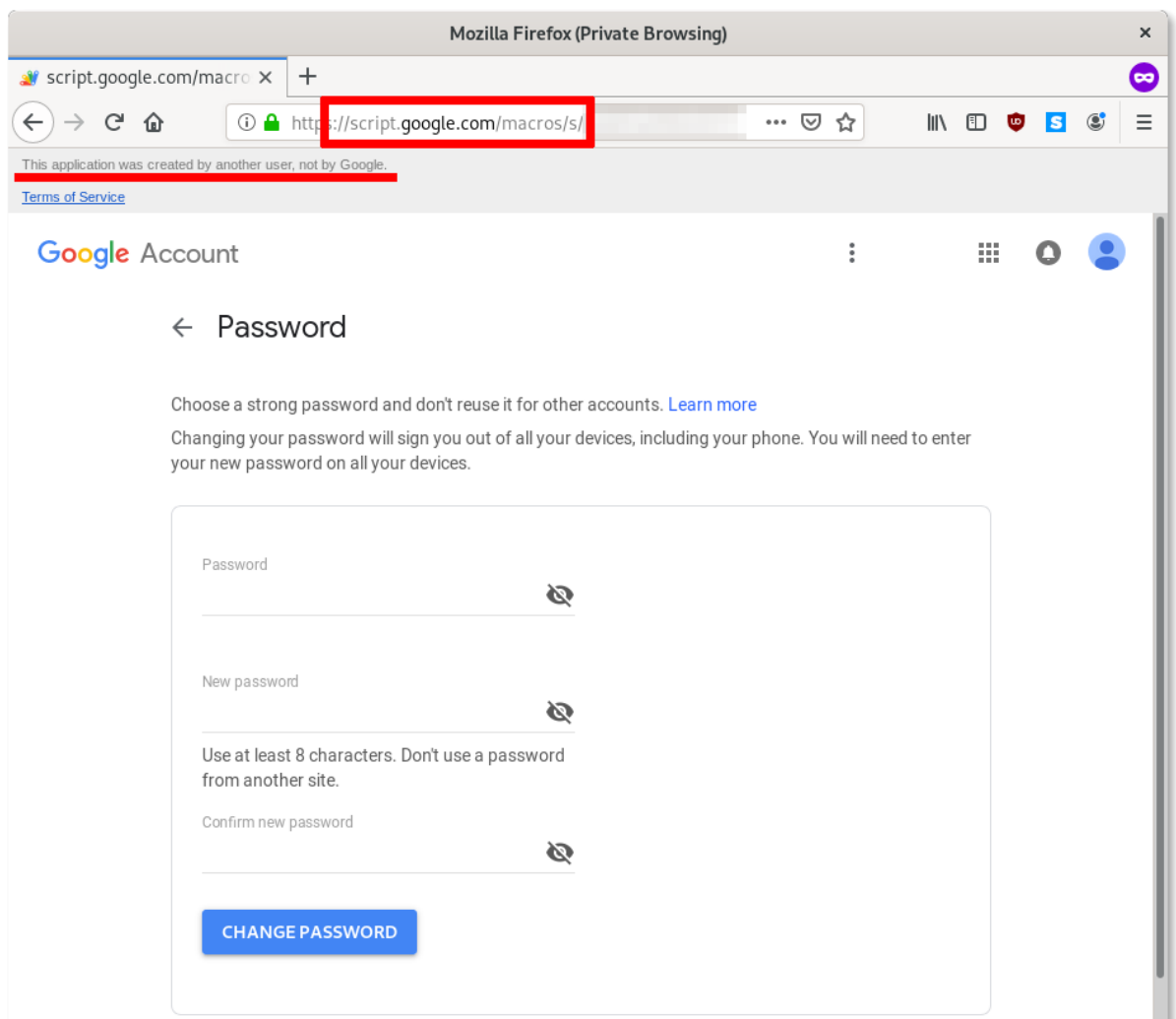
Here, the attackers are abusing a redirection procedure used by Google in order to first direct the targets to a legitimate Google page.



*Screenshot of the legitimate Google login page used as a decoy, which then redirects to the actual phishing page.*

This is in fact the original Google login prompt and it serves no other function to the attacker, other than to make the link in the email appear legitimate and make the procedure more credible. After having logged in (if the target wasn't logged in already), the target is subsequently redirected to the fake password change form that, if filled, will grant the attackers access to the victim's account.

Another technique the attackers used in this case is to present the phishing pages directly on legitimate Google infrastructure. For example, we can see in the screenshot below that the fake password change form is hosted at **script.google.com**.



*Screenshot of the phishing page displaying a fake password reset form.*

On other occasions, the attackers have hosted the malicious page on **site.google.com**. These two legitimate Google services (**script.google.com** and **site.google.com**) allow Google users to create and host web content and applications. Here the attackers are abusing this service to load phishing pages impersonating Google. Tech-savvy targets, who perhaps received security trainings, might be suspicious of domain names in the browser's address bar that do not look legitimate. By using this trick, even these relatively security-conscious targets may be fooled into believing the phishing pages are legitimate.

As highlighted in the screenshot above, the only visible warning this page is fake (other than the domain itself not being **accounts.google.com** or **myaccount.google.com**, but **script.google.com**) is the message Google displays at the top "This application was created by another user, not by Google."

Similarly to the attacks described in our [report from December 2018](#), this particular phishing system is also capable of verifying the login credentials and phishing for two-factor verification codes as well.

In this case, using [Security Keys](#) would help mitigate the attacks where other forms of two-factor authentication generally would not.

## **Second Tactic - Outlook Phishing Using Malicious Third-Party Applications**

Instead of creating fake login pages or fake password reset forms and grabbing the credentials to the targets' accounts, attackers sometimes make use of what is commonly referred to as "OAuth Phishing".

[OAuth](#) is a Web standard used to allow authentication over third-party services without the need of sharing passwords. It is commonly used by legitimate applications developer to permit the connection between their software to existing online accounts. For example, a calendar application might want to be able to automatically extract your hotel and flights booking from your Outlook account. Or, an email client (as we will see later) might want to allow you to connect to your Gmail account.

Attackers use the same architecture to instead create malicious third-party applications and attempt to lure the targets into granting the applications access to their accounts. Therefore, with OAuth Phishing, attackers do not need to steal credentials: they simply abuse legitimate functionality that online platforms - such as Google, Microsoft or Facebook - provide. Because the authentication to the account happens on the legitimate site, no form of two-factor authentication - including

Security Keys - can mitigate against this. Targets can only be alert of any clues or warnings visible in the malicious emails or in the service's login procedure. Normally, tech companies would eventually discover the malicious third-party application and disable it.

We have previously encountered and described this technique in our report [Phishing attacks using third-party applications against Egyptian civil society organizations](#) from March 2019, targeting Google users.

In this campaign, the attackers have similarly created malicious third-party applications in order to conduct OAuth Phishing against Microsoft Outlook users instead. As shown in the images below, attackers have crafted malicious emails impersonating Microsoft, falsely warning of suspicious login attempts on the victim's accounts and offering to "secure" them.



Mozilla Thunderbird - لم تقم حتى الان بتأمين حسابك

FileEditViewGoMessageToolsHelp

Get MessagesWriteChatAddress BookTag

ReplyReply AllForwardMore

From security@microsoftstore.com

Subject لم تقم حتى الان بتأمين حسابك

To

03/08/19

Microsoft

على ما يبدو قمت بمحاولة  
لتأمين حسابك ولم تكمل عملية  
التحقق

We detected something unusual about a recent sign-in to the Microsoft account

Sign-in details

Country/region: United Stats

IP address: 198.41.214.162

Date: 8/3/2019 08:47 AM (GMT)

Platform: Windows10

Browser: Chrome

ما زالت هناك محاولات لتخمين كلمة المرور الخاصة بك ، قمنا بمنع عملية الدخول ، يجب  
..تسجيل الدخول وتأمين حسابك فورا لنقوم بحظر جميع هذه المحاولات

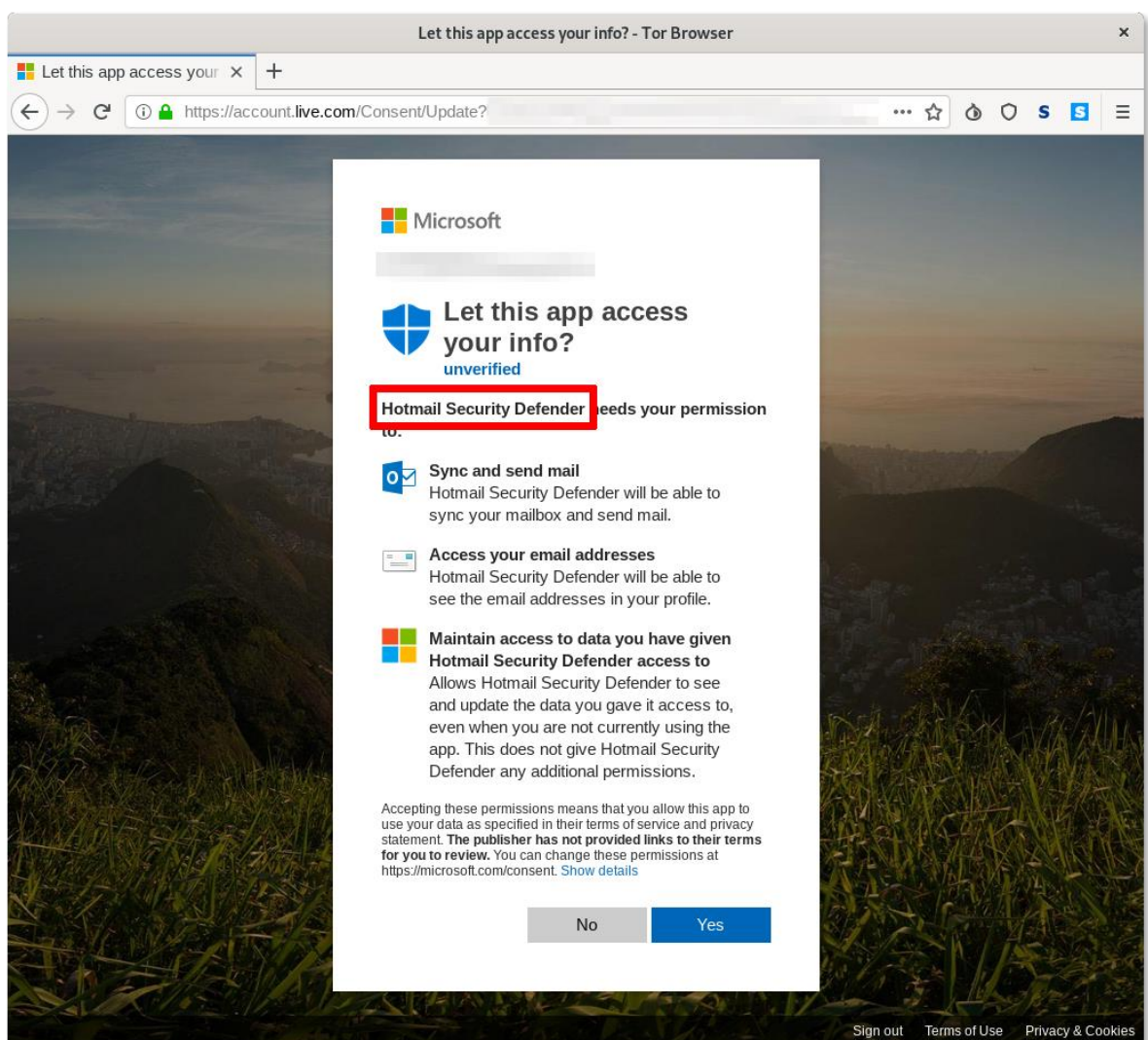
تأمين حسابي

To opt out or change where you receive security notifications, [click here](#).

Thanks,  
The Microsoft account team

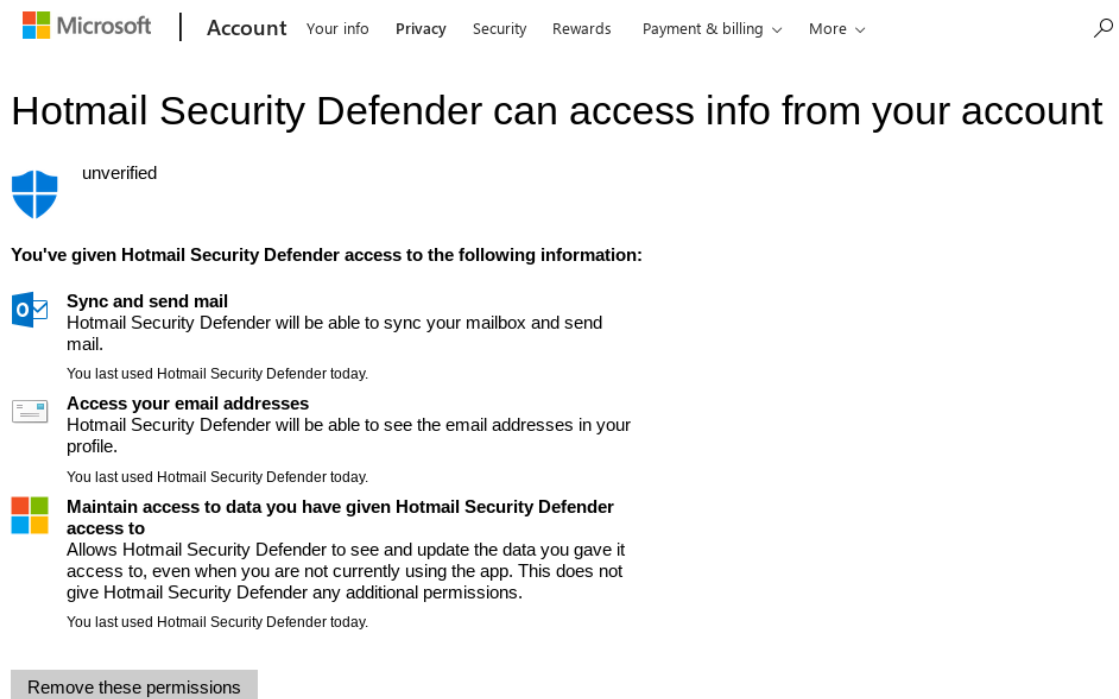
*Example of an Outlook phishing email shared with Amnesty International (note the mis-spelling of “United States” - one of the few visual clues that this is not a legitimate notification).*

Clicking on the link contained in the email would eventually lead to this legitimate Microsoft page asking confirmation for the activation of the third-party app "**Hotmail Security Defender**" on the account, warning that it would be capable of reading all emails and contacts. In other variants of this attack, the third-party app was called "**Outlook Security Defender**".



*Screenshot of Outlook authorization page for the attackers' malicious third-party app.*

In order to verify if you have any unwanted third-party applications enabled, you should visit <https://microsoft.com/consent>. If you fell victim of this particular attack you would have seen something like this:



*Screenshot of a Microsoft account settings page displaying the authorized malicious third-party app.*

We have reported these malicious applications to Microsoft, who promptly removed them.

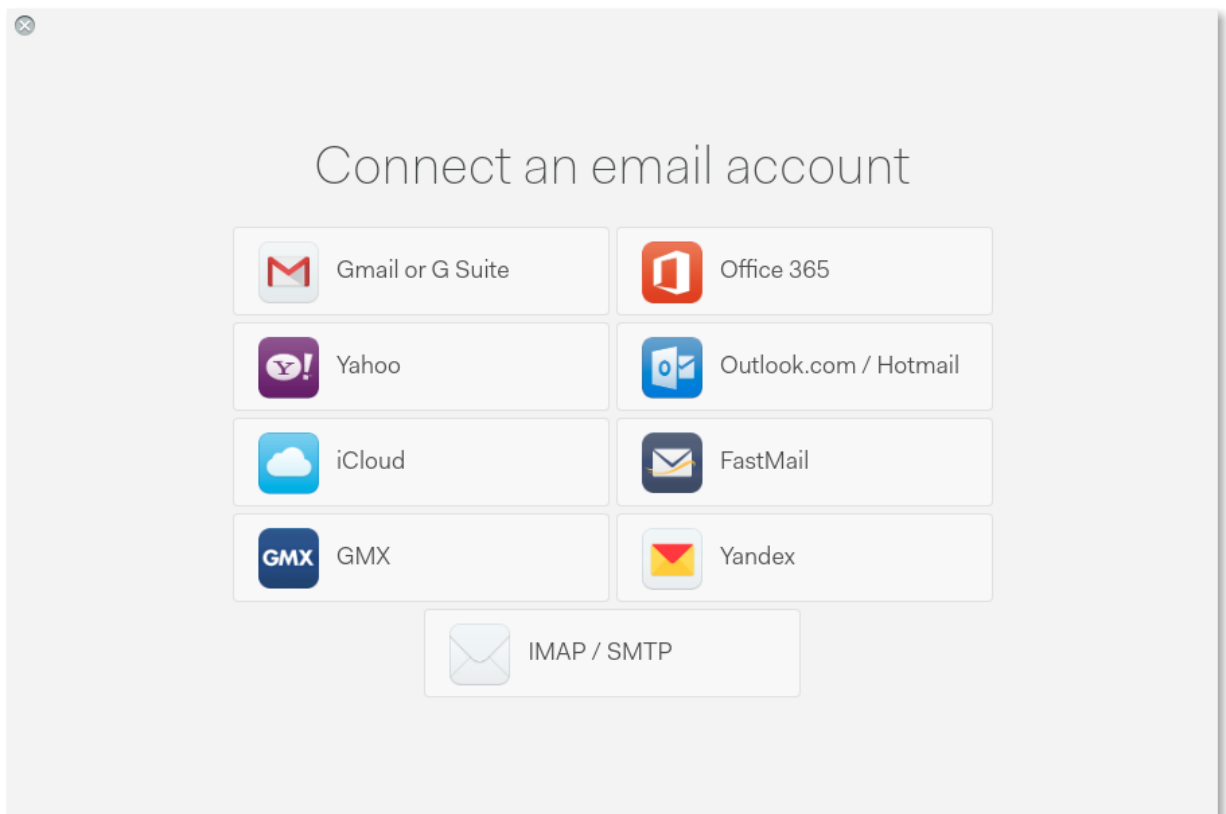
## Third Tactic - Google Phishing Abusing Legitimate Third-Party Applications

Due to the common abuse the abuse of the OAuth web standard, [Google announced in October 2018](#) that it will apply new, stringent policies on the [verification](#) and approval of third-party applications.

Perhaps because of these new policies, the attackers devised a new OAuth Phishing technique that we had not previously observed. While in most OAuth Phishing cases,

as explained, attackers normally create malicious third-party applications designed to steal data (such as emails) from targets' accounts, in this latest campaign, they have, instead, started abusing the authentication procedure employed by legitimate and verified third-party applications. In the attacks we have collected from the Human Rights Defenders who shared the malicious emails with us, the attackers have specifically been abusing a legitimate and popular email client application called [Mailspring](#).

Mailspring supports various email services, including Gmail.



*Screenshot of Mailspring's configuration wizard.*

In order to allow the desktop or mobile apps to connect to a Gmail account, Mailspring also makes use of the OAuth standard. Google [offers four OAuth options](#) to desktop and mobile app developers, and while the Mailspring developers use the recommended one ("Loopback IP address"), the attackers figured out that by abusing another available option ("Manual copy/paste") together with the publicly available Client ID of the Mailspring application account, they could obtain access tokens to victims' accounts (and avoid needing a client secret or an authorized redirect URL).

Following is a break-down of this particular attack.

### **Step 1: "Advanced Protection" as a bait**

The malicious emails we collected carry links to websites controlled by the attackers, such as **srf-google[.]de** , **gmailusercontent[.]site** and **protect-outlook[.]com**.

⌵

Mozilla Thunderbird - يتعرض حسابك لهجمات منتظمة ومتكررة

FileEditViewGoMessageToolsHelp

⬇️ Get Messages ⌵✍️ Write💬 Chat👤 Address Book | 🏷️ Tag ⌵☰

↩️ Reply⌵⌨️ Reply All⌵➡️ ForwardMore ⌵

From VAMS Webservice <alerts@valabs.info> ☆

Subject يتعرض حسابك لهجمات منتظمة ومتكررة20/07/19

To ☆

Google

قم بتنفيذ إجراءات الأمان الجديدة من جوجل

أنت الآن على بعد خطوات قليلة من حماية حسابك للابد وتحسينه ضد الهجمات المتكررة

كيف تقوم بتطبيق إجراءات مستوى الحماية المتقدمة

يقوم تطبيق الأمان من جوجل برفع مستوى الحماية للحد الأقصى ويقوم بإرسال تنبيهات مكثفة حول . أمان حسابك ويعمل على تحسين بريدك ضد الهجمات التي تستهدف التجسس على بياناتك الشخصية

ابدا الآن بتنفيذ تطبيق الأمان من تم قم باستخراج معرف الأمان الخاص بحسابك ومن ثم احفظه في . مكان آمن . يمكن استخدام هذا المعرف عند التواصل مع عملائنا

تطبيق إجراءات الحماية المتقدمة - GET SECURITY KEYS

Wasn't you? Someone may have access to your account. Use the [Security Checkup](#) to look for suspicious account activity.

You received this email to let you know about important changes to your Google Account and services.

© 2019 Google LLC, 1610 Amphitheatre Parkway, Mountain View, CA 93041, USA

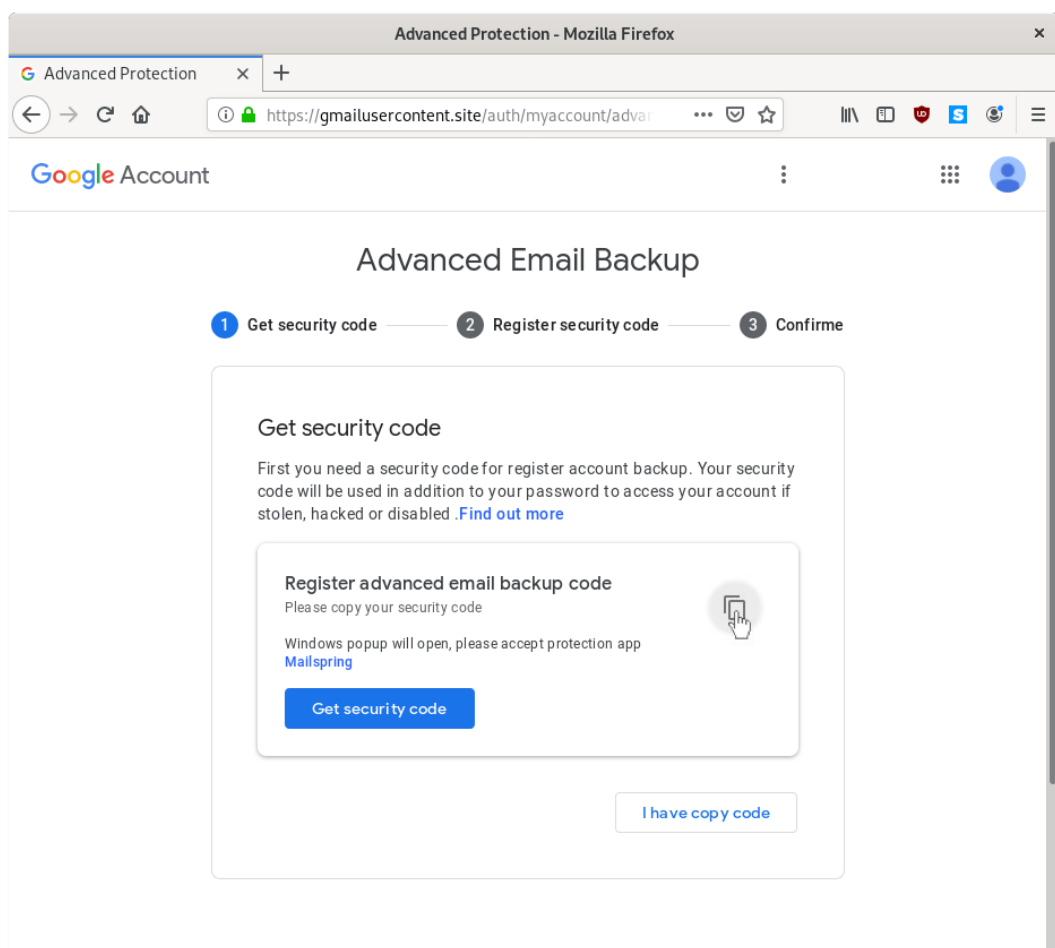
🌐

<https://sites.google.com/site/secauthv1/?id=>

*Screenshot of a phishing email shared with Amnesty International.*

As we previously documented in our report from [December 2018](#), these attackers are particularly dedicated to attacking privacy-conscious users. In this more recent campaign of attacks, the phishing pages are designed to appear as legitimate Google sites, and the bait appears to reference the [Google Advanced Protection](#) program, which is a secure authentication program Google markets particularly to journalists, NGOs and other at-risk individuals.

The page pretends to offer the ability to set up security codes to protect the account. As you can see, the instructions provided in the page specifically solicit the targets to grant access to the "protection app" called Mailspring.



*Screenshot of the phishing page.*

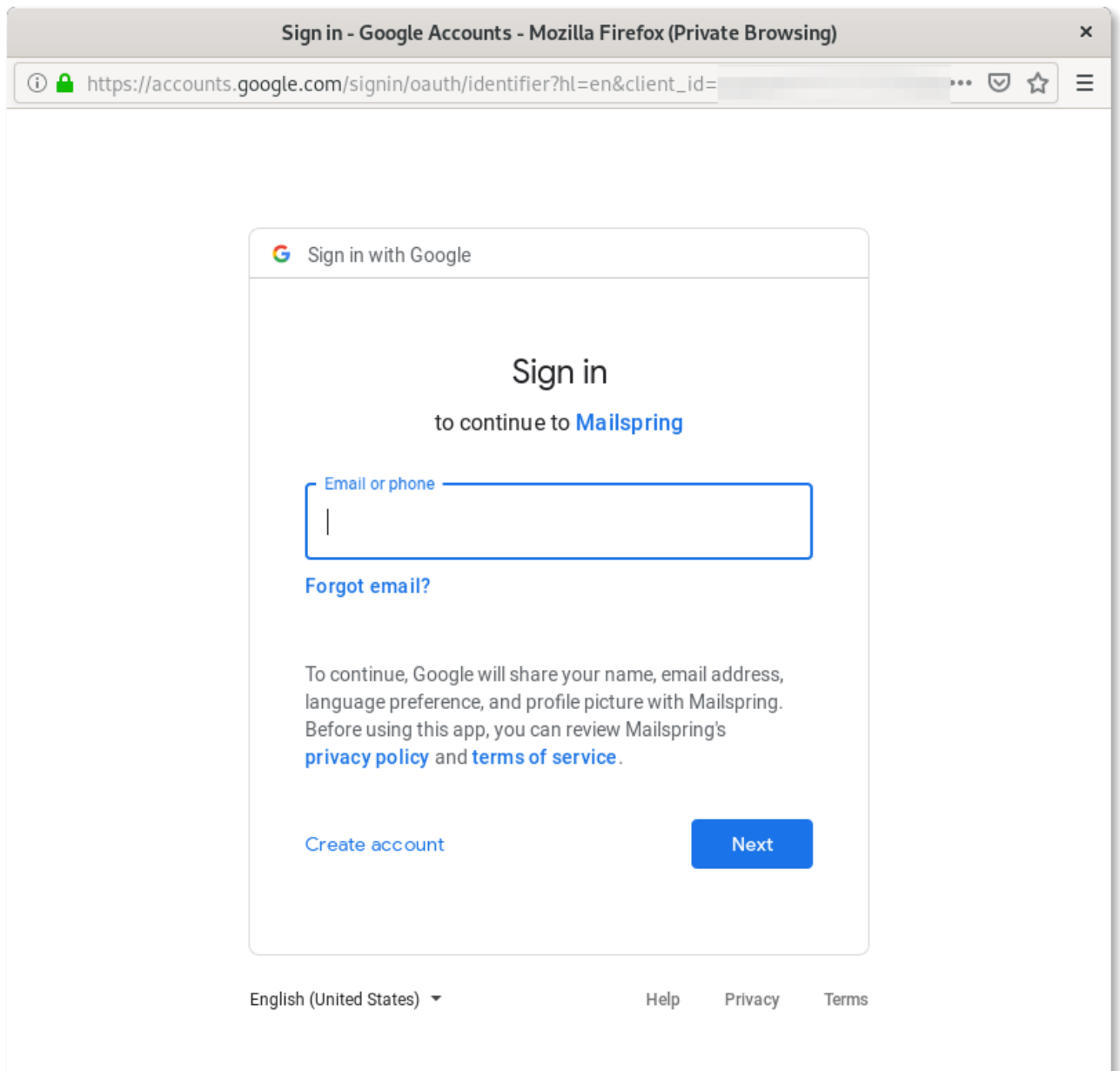
## **Step 2: Login with Mailspring**

The "Get security code" button leads to a valid Google login configured with the "Manual copy/paste" option for Mailspring's OAuth account.

The screenshot shows a web browser window with the title "Google - تسجيل الدخول - حسابات" and the URL "https://accounts.google.com/signin/oauth/identifier?hl=ar&client\_id=". The main content is a Google login form in Arabic. At the top, it says "تسجيل الدخول باستخدام Google". Below that, the heading is "تسجيل الدخول" followed by "المتابعة إلى Mailspring". There is a text input field for "البريد الإلكتروني أو الهاتف" (Email or phone). Below the input field, it asks "هل نسيت البريد الإلكتروني؟" (Forgot email?). A paragraph of text explains that by continuing, the user agrees to Google's terms and conditions, and that Mailspring will use the account information to provide services. At the bottom of the form, there are two buttons: "التالي" (Next) and "إنشاء حساب" (Create account). At the very bottom of the page, there are links for "الشروط" (Terms), "الخصوصية" (Privacy), "تعليمات" (Help), and a language selector for "العربية" (Arabic).

Original screenshot in Arabic of the Google authorization page to enable Mailspring on the account.

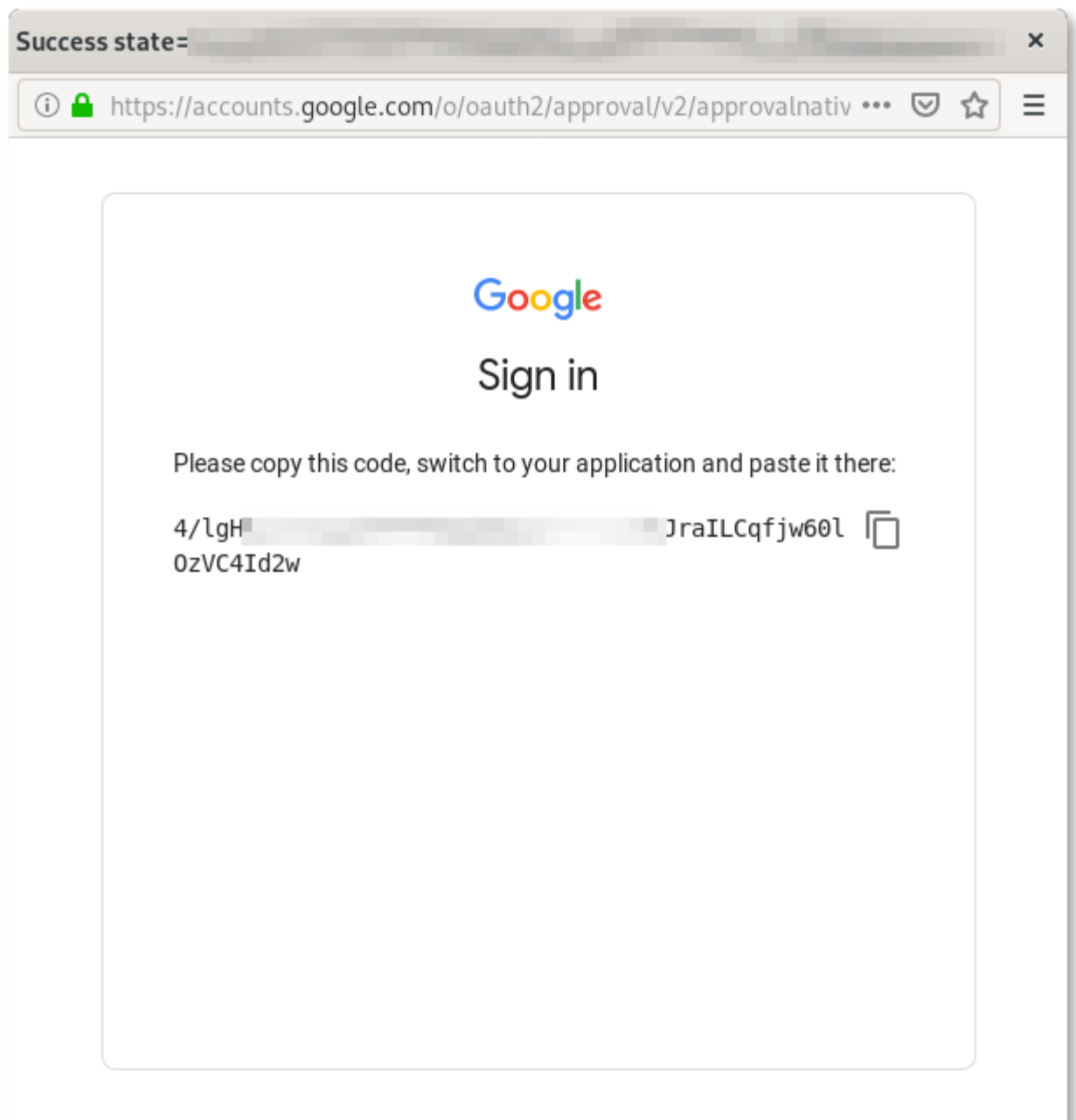




*Same screenshot as above, in English.*

### **Step 3: Obtain the token to copy**

Once authenticated, Google presents a token that can be copied and pasted in the third-party application, which should have been the legitimate Mailspring, but is, instead, the phishing page set up by the attackers.



*Screenshot of the authorization token generated by Google for Mailspring.*

**Step 4: Paste the token in the phishing page**

At this point, the phishing page shows a form that solicits the token that was just generated. If the token is submitted, the attackers will be able to use it to get access to the user's email account and read the content of their emails.

Advanced Protection - Mozilla Firefox

Advanced Protection x Advanced Protection x +

https://protect-outlook.com/auth/myaccount/advanc

Google Account

## Advanced Email Backup

1 Get security code — 2 Register security code — 3 Confirm

Google

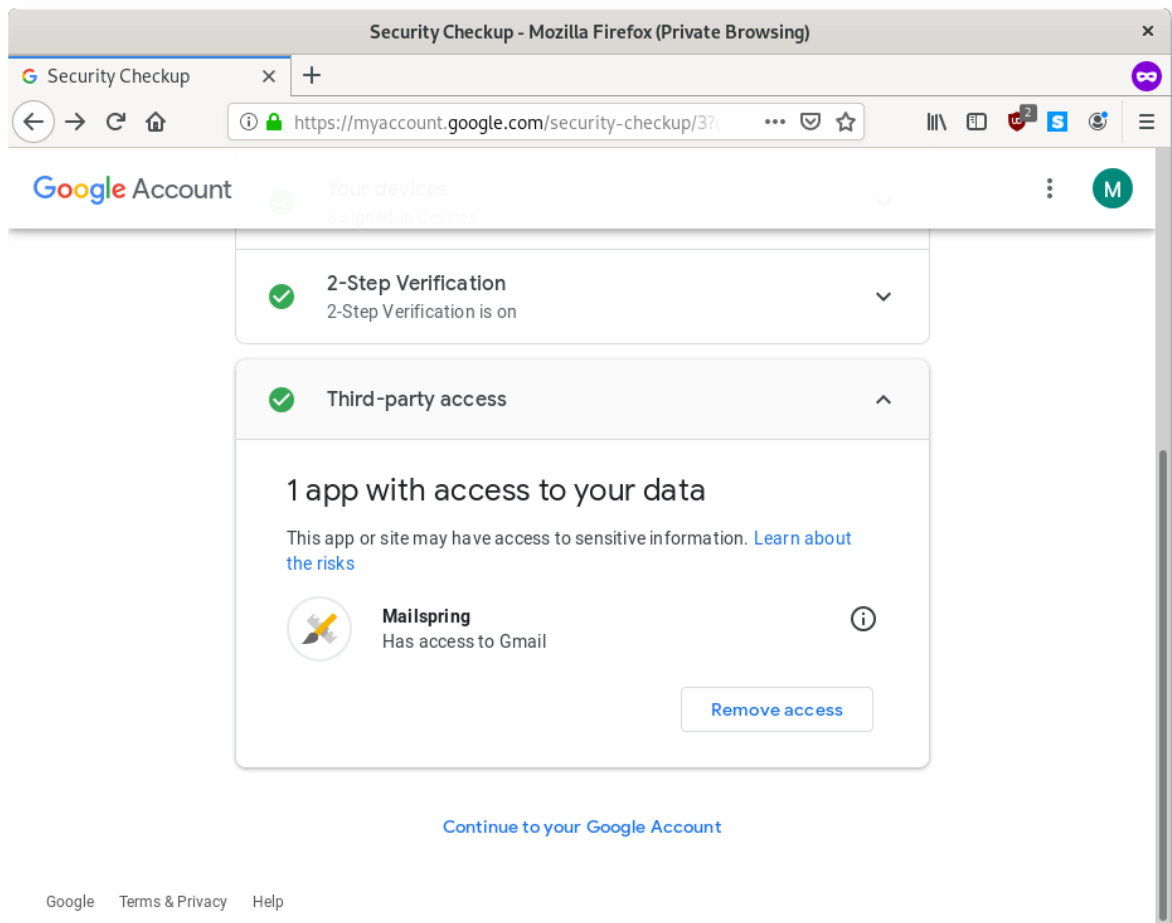
### Advanced Protection

Enter the code displayed on your device

Next

*Form from the phishing page requesting the authorization token.*

Checking the [Security page on your Google account](#) would display any third-party application enabled on it. In this case, Mailspring would appear in the list.



*Screenshot of a Google account settings with Mailspring enabled.*

If you have never been a user of Mailspring before, this might be a sign of compromise. **If you are a current or past Mailspring user, you should see the same record, but it wouldn't be anything to worry about.**

This is the first time we see attackers abuse legitimate third-party applications, and, through their Google accounts, leverage less secure OAuth options to steal authentication tokens and gain access to victims' emails. Obviously, while it is possible for Google to identify and disable malicious third-party applications, they cannot disable legitimate ones. Mailspring, for instance, accounts for tens of thousands of users. Following the discovery of this malicious use, we immediately got in contact with the Mailspring developers who promptly answered and cooperated with us to investigate and try to resolve this attack. We reported these attacks to Google, and the malicious infrastructure is now blocked through SafeBrowsing.

## **How to protect yourself from these attacks?**

As this latest campaign demonstrates, it can be very difficult to identify phishing attacks and protect yourself from them. Currently, the most reliable mitigation against phishing are Security Keys. This is further discussed in our previous report [When Best Practice Isn't Good Enough](#).

OAuth Phishing appears to be on the rise, probably in response to the decreasing success rate of other tactics. Unfortunately, two-factor authentication is not really intended as a mitigation against this kind of attack. Always be alert when you receive a request to authorize a third-party application on your account!

If you want to read more about phishing and its countermeasures, please check out Security Without Borders' [Guide to Phishing](#).

If you believe you have been targeted with attacks similar to the ones described here, you can share with us your suspicious messages and links here:

**share@amnesty.tech**

## **Appendix: Screenshots of Phishing Emails**



Mozilla Thunderbird - لم تقم حتى الان بتأمين حسابك

FileEditViewGoMessageToolsHelp

Get MessagesWriteChatAddress BookTag

ReplyReply AllForwardMore

From security@microsoftstore.com

Subject لم تقم حتى الان بتأمين حسابك

To

03/08/19

Microsoft

على ما يبدو قمت بمحاولة  
لتأمين حسابك ولم تكمل عملية  
التحقق

We detected something unusual about a recent sign-in to the Microsoft account

Sign-in details

Country/region: United Stats

IP address: 198.41.214.162

Date: 8/3/2019 08:47 AM (GMT)

Platform: Windows10

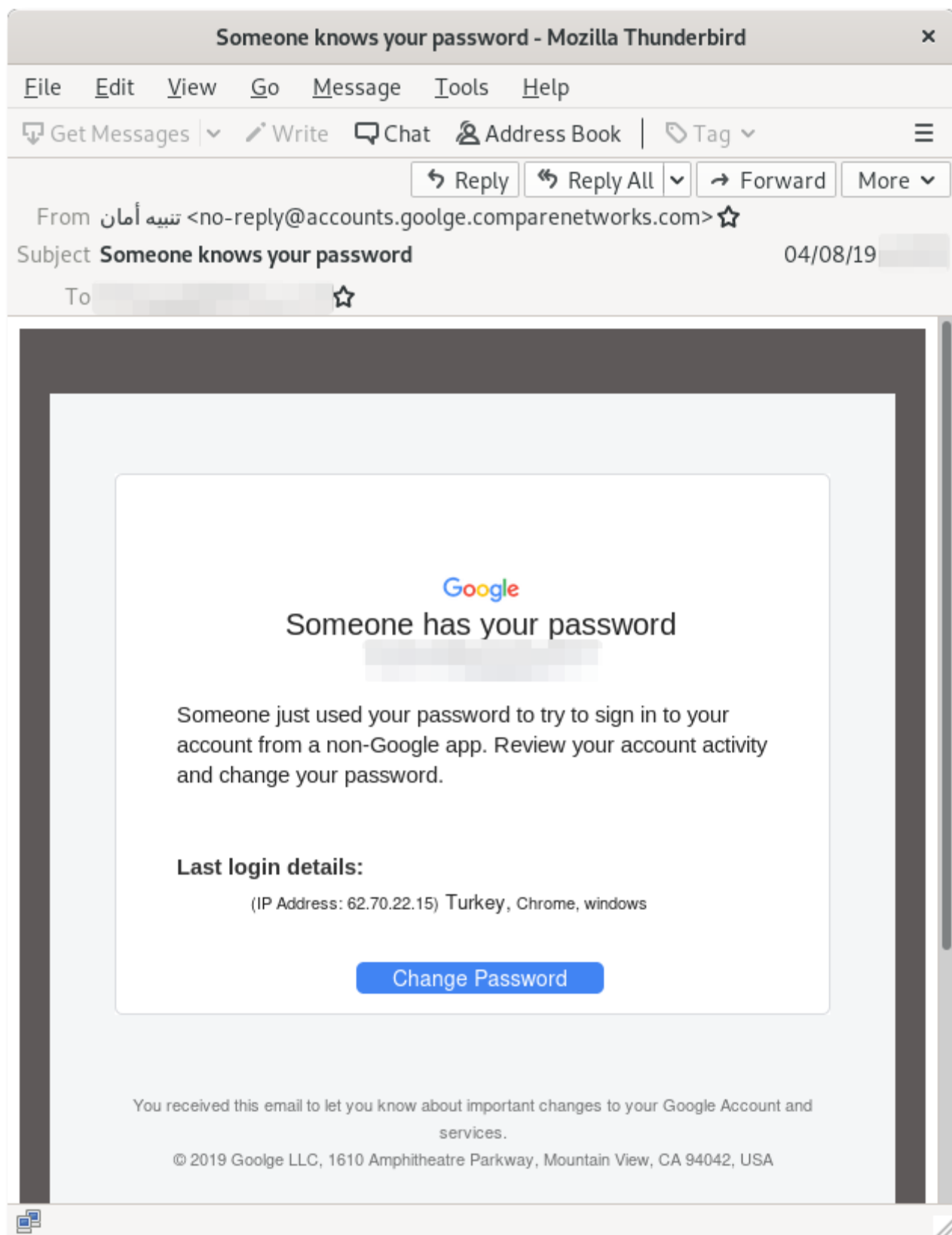
Browser: Chrome

ما زالت هناك محاولات لتخمين كلمة المرور الخاصة بك ، قمنا بمنع عملية الدخول ، يجب  
..تسجيل الدخول وتأمين حسابك فورا لنقوم بحظر جميع هذه المحاولات

تأمين حسابي

To opt out or change where you receive security notifications, [click here](#).

Thanks,  
The Microsoft account team





FileEditViewGoMessageToolsHelp

Get MessagesWriteChatAddress BookTag

ReplyReply AllForwardMore

From VAMS Webservice <alerts@valabs.info>  
Subject يتعرض حسابك لهجمات منتظمة ومتكررة  
To 20/07/19

Google

قم بتنفيذ اجراءات الامان الجديدة من جوجل

انت الآن على بعد خطوات قليلة من حماية حسابك للأبد وتحسينه ضد الهجمات المتكررة

كيف تقوم بتطبيق اجراءات مستوى الحماية المتقدمة

يقوم تطبيق الامان من جوجل برفع مستوى الحماية للحد الاقصى ويقوم بارسال تنبيهات متكررة حول  
امان حسابك ويمثل حلي تحمين بريدك ضد الهجمات التي تستهدف التجسس على بياناتك الشخصية

ابدا الان بتنفيذ تطبيق الامان من ثم قم باستخراج معرف الامان الخاص بحسابك ومن ثم احفظه في  
مكان امن ، يمكن استخدام هذا المعرف عند التواصل مع عملائنا

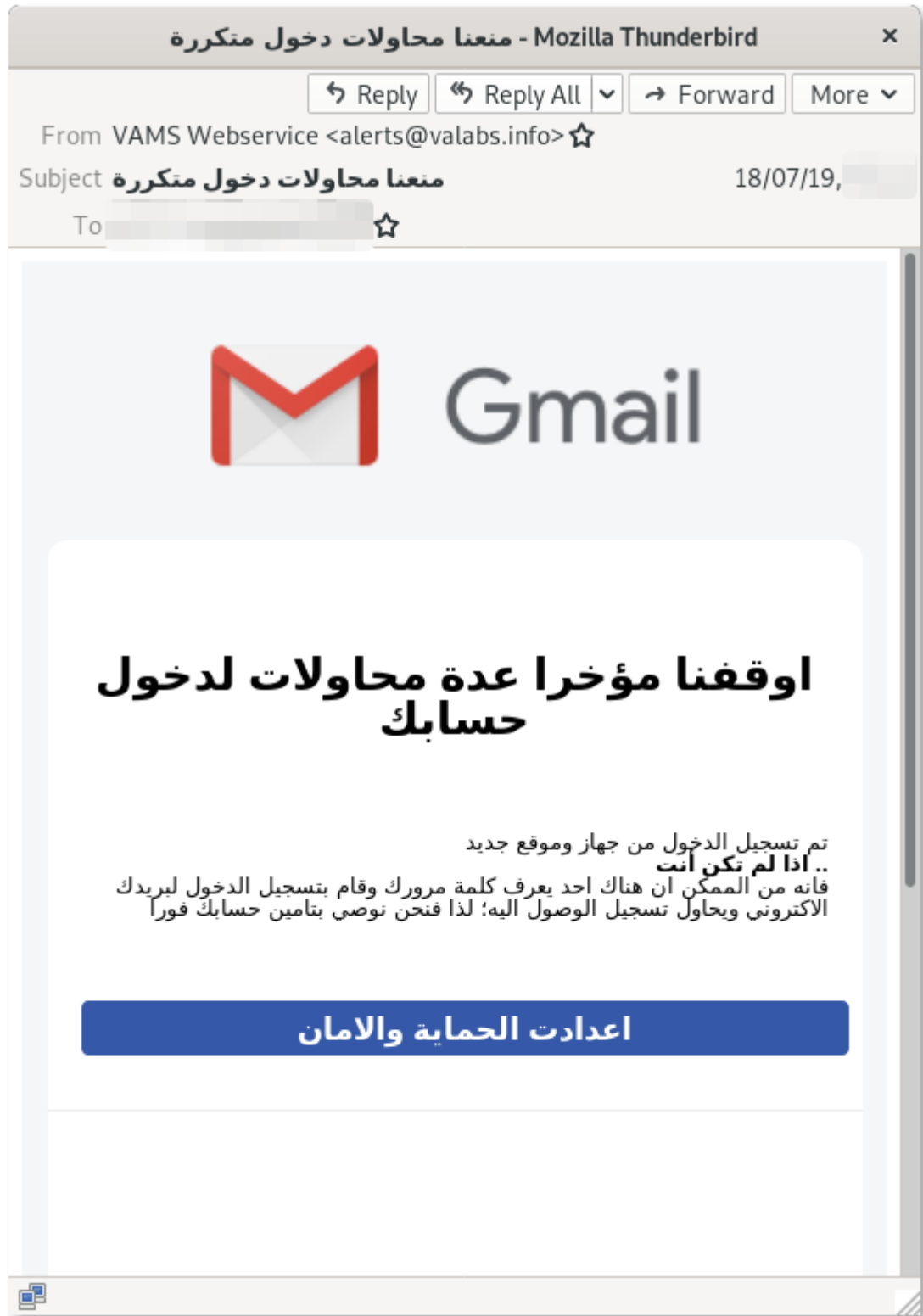
تطبيق اجراءات الحماية المتقدمة - GET SECURITY KEYS

Wasn't you? Someone may have access to your account. Use the [Security Checkup](#) to look for suspicious account activity.

You received this email to let you know about important changes to your Google Account and services.

© 2019 Google LLC, 1610 Amphitheatre Parkway, Mountain View, CA 93041, USA

https://sites.google.com/site/secauthv1/?id=



From **تنبيه أمان** <no-reply@accounts.google.com> ☆Subject **شخص ما يحاول تخمين كلمة مرورك**

04/08/19,

To



Google



## منعنا محاولات جديدة لتخمين كلمة المرور الخاصة بحسابك

هناك من يحاول الوصول الى حسابك ، قام هذا الشخص بمحاولات عديدة لتسجيل الدخول الى حسابك ،

**.. اذا لم تكن انت**

فيعرف الشخص الذي سَجَّل الدخول كلمة المرور لبريدك الالكتروني ويحاول تسجيل الدخول اليه؛ لذا فنحن نوصي بتأمين حسابك فورا

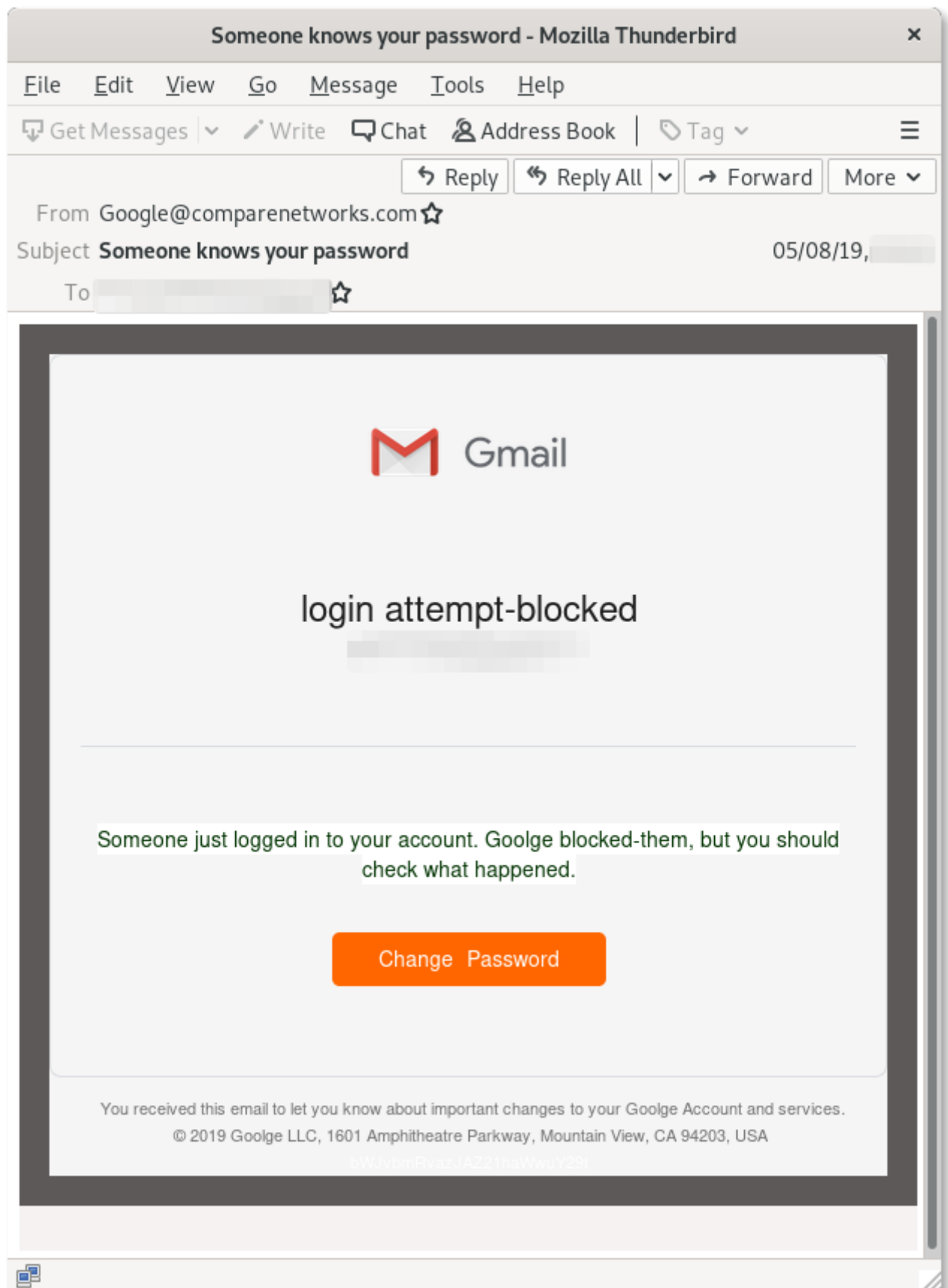
[Take action](#)

Worried about clicking links?

Visit the Security Checkup at <https://myaccount.google.com/security-checkup>

You received this email to let you know about important changes to your Google Account and services.

© 2019 Google LLC, 1610 Amphitheatre Parkway, Mountain View, CA 94143, USA



## Technical Appendix

**Following are the domain names associated with this campaign:**

srf-goolge[.]site

gmailusercontent[.]site

protect-outlook[.]com

**The IP address hosting the malicious infrastructure is:**

**95.217.60[.]161**

**Following are the email addresses used in phishing emails:**

admin[ @]microsoftstore.com

google.com[ @]localhost

google[ @]script

noreply750[ @]mailgoogle.ccm

noreply[ @]gmailusercontent.site

noreply[ @]mailgoogle.ccm

googlecommunityteam-noreply[ @]srf-goolge.site

noreply-accounts[ @]goolge.cm

noreply[ @]accounts-goolge.com

noreply[ @]accounts-goolgeemail.site

accounts-noreply[ @]google.ccm

noreply-accounts[ @]google.ccm

alerts[ @ ]valabs.info

google[ @ ]noreply-accounts.com

no-reply[ @ ]goolge.email