Nex Follow
Hacker. Security Researcher. Activist.
Feb 14 · 13 min read

Operation Kingphish: Uncovering a Campaign of Cyber Attacks against Civil Society in Qatar and Nepal

Over the course of 2016—and particularly intensifying towards the end of the year—several individuals known to Amnesty International were approached via email and through social media by "*Safeena Malik*", seemingly an enthusiastic activist with a strong interest in human rights. What lied beneath this facade was a well-engineered campaign of phishing attacks designed to steal credentials and spy on the activity of dozens of journalists, human rights defenders, trade unions and labour rights activists, many of whom are seemingly involved in the issue of migrants' rights in Qatar and Nepal.

Our investigation of the attacks didn't yield any evidence that would indicate the conclusive responsibility of a particular government, although we suspect these attacks might have been orchestrated by a state-affiliated actor. We refer to this campaign and the associated actor as **Operation Kingphish** ("*Malik",* in one of its written forms in Arabic, translates to "*King*").

It is worth noting that in December 2016, Amnesty International published an investigation into another social engineering campaign perpetrated by a seemingly fake human rights organization known as Voiceless Victims, which targeted international human rights and labour rights organizations campaigning on migrant workers' rights in Qatar. While there is a clear alignment of interests, we have found no evidence to suggest these two campaigns are directly connected.

· · ·

Migrants' rights in Qatar

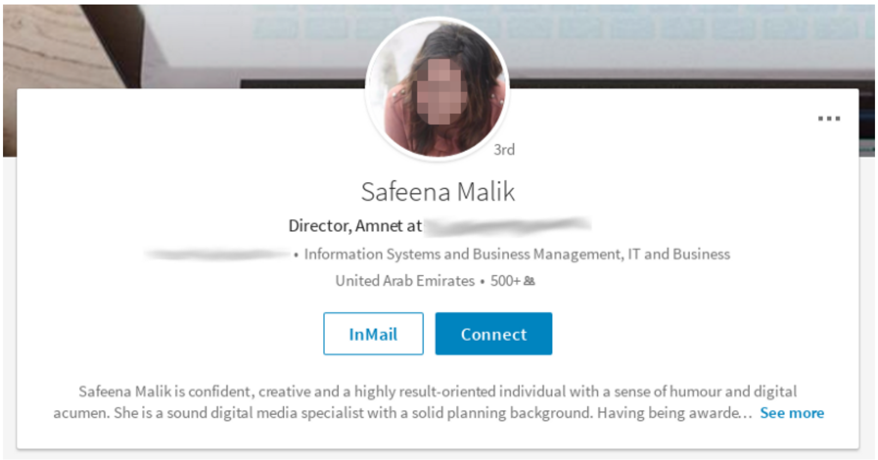
Migrant workers, mainly from South Asia, comprise more than 90% of Qatar's workforce, with Nepalis being one of the largest nationalities. The exploitation of migrant workers in Qatar, particularly in the construction sector, has been widely reported on since Qatar won the right to host the 2022 World Cup. The sponsorship system, which ties migrant workers to their employers has been widely criticized as being a major driver of exploitation.

YouTube

As Amnesty International reported, recent changes to laws governing the migrant labour system in Qatar barely scratch the surface of the problem and continue to leave migrant workers, including those building stadiums and infrastructure for the World Cup, at the mercy of exploitative bosses and at risk of serious human rights abuses including forced labour. Workers still require exit permits to leave the country, which can still be blocked by their employer, and employers can now legally keep hold of their workers' passports under a new loophole which can be easily exploited.

. . .

“Safeena Malik” phishing expedition



3rd

Safeena Malik

Director, Amnet at [redacted]

[redacted] • Information Systems and Business Management, IT and Business

United Arab Emirates • 500+

InMail Connect

Safeena Malik is confident, creative and a highly result-oriented individual with a sense of humour and digital acumen. She is a sound digital media specialist with a solid planning background. Having being awarde… See more

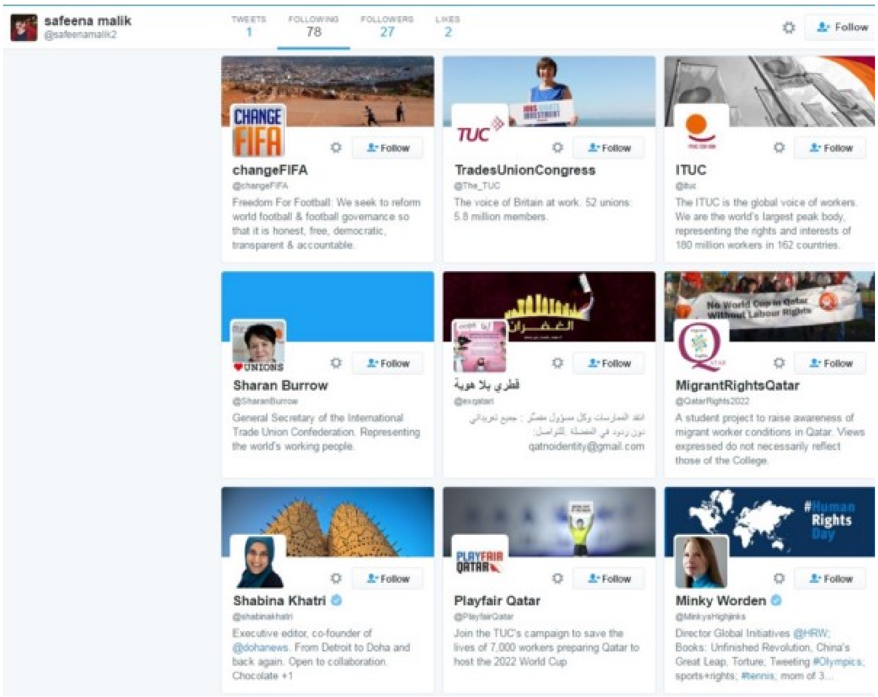
Note: throughout the report we have redacted, where necessary, names and email addresses of individuals and organizations targeted in order to protect their identity and safety. We have also obscured wherever possible the pictures utilized by the attackers on the fake social media profiles, as they have been likely stolen from people with no involvement in these attacks.

Our investigation revealed that unidentified attackers have purposefully created and maintained what appears to be a fake online persona, named "**Safeena Malik**", in order to regularly engage in conversations with the selected targets, and at different times and with different pretenses try to lure them into giving away their credentials to their Gmail account through the use of *phishing* attacks.

Phishing is a hacking technique that often consists of mimicking popular online services (such as Google, Facebook, Twitter, and Linkedin) and credibly replicating their login pages, with the goal of stealing usernames and passwords from the designated victims by luring them into mistakenly authenticating through such pages.

This type of attack is extremely popular, and often used against members of civil society. It is relatively easy and cheap to orchestrate, and if successful it grants the attackers access to victims' personal and professional email accounts, which can obviously reveal very sensitive information. For example, having an activist's email account phished might lead to the reconstruction of their network, exposure of sources' identities, as well as abuse of their accounts for impersonation. By comparison, phishing attacks are likely significantly more common than malware attacks.

Phishing attacks are normally delivered through emails soliciting the target to open a link and login to, for example, a Google-like page. The strategies used to make this solicitation credible can vary. Often, for example, the email would falsely inform the victim that their account has been hacked, urgently requiring a password reset.



safeena malik
@safeenamalik2

changeFIFA
@changeFIFA
Freedom For Football: We seek to reform world football & football governance so that it is honest, free, democratic, transparent & accountable.

TradesUnionCongress
@The_TUC
The voice of Britain at work. 52 unions: 5.8 million members.

ITUC
@ituc
The ITUC is the global voice of workers. We are the world's largest peak body, representing the rights and interests of 180 million workers in 162 countries.

Sharan Burrow
@SharanBurrow
General Secretary of the International Trade Union Confederation. Representing the world's working people.

قطري بلا هوية
@exqatari
انقد الممارسات وكل مسؤول مقصّر : جميع تغريداتي
دون ردود في المفضلة. للتواصل:
qatnoidentity@gmail.com

MigrantRightsQatar
@QatarRights2022
A student project to raise awareness of migrant worker conditions in Qatar. Views expressed do not necessarily reflect those of the College.

Shabina Khatri
@shabinakhatri
Executive editor, co-founder of @dohanews. From Detroit to Doha and back again. Open to collaboration. Chocolate +1

Playfair Qatar
@PlayfairQatar
Join the TUC's campaign to save the lives of 7,000 workers preparing Qatar to host the 2022 World Cup

Minky Worden
@MinkysHighjinks
Director Global Initiatives @HRW; Books: Unfinished Revolution, China's Great Leap, Torture; Tweeting #Olympics; sports+rights; #tennis; mom of 3...

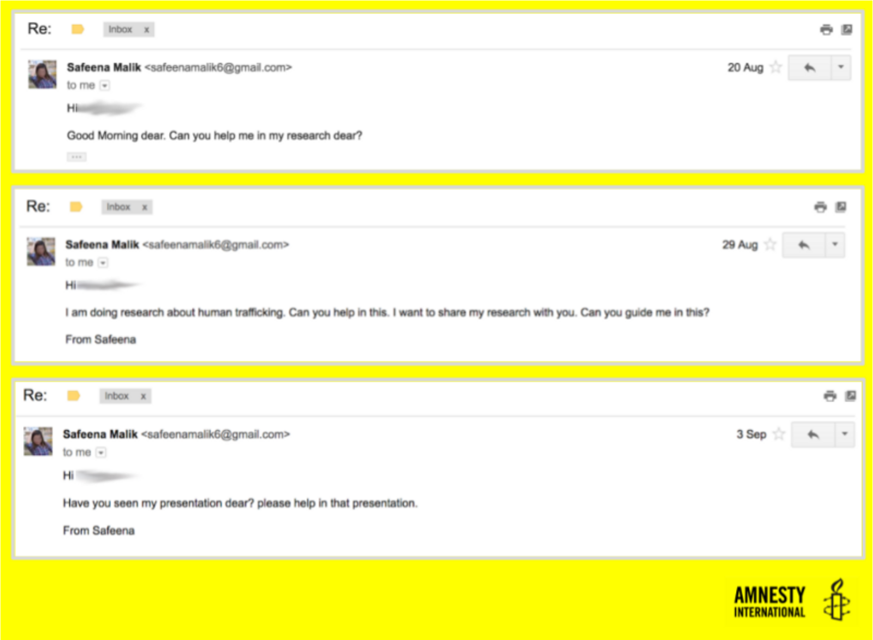
"Safeena Malik" has a full presence on social media but her twitter account, created in December 2014 has only one visible tweet, dating from 23 December 2014, a simple "hi". We believe it is possible that the operators of Operation Kingphish might have acquired a set of pre-registered (or stolen) social media profiles online. The accounts "Safeena Malik" follows show a clear pattern: a large number of Middle East-based journalists for international publications, staff of international human rights organizations and trade unions, and various campaigns for migrants' rights in Qatar.

Their Facebook account appears to be more active, and their LinkedIn profile, has 500+ connections.

The various social media accounts communicated regularly with several of the victims we identified, often for many months. It appears that the attackers may have impersonated the identity of a real young woman and stole her pictures to construct the fake profile, along with a professional biography also stolen from yet another person. The emails and messages sent by the fake "Safeena Malik" would normally be timed around—before, and following—the delivery of yet another attempt at phishing the credentials of the designated victims.

Case 1: Fake Google, real Google

For example, in the exchange below, "Safeena" tried to lure the target by purporting to be seeking help on some important research on human trafficking.



Re: Inbox x

Safeena Malik <safeenamalik6@gmail.com> 20 Aug
to me

Hi [redacted]

Good Morning dear. Can you help me in my research dear?

Re: Inbox x

Safeena Malik <safeenamalik6@gmail.com> 29 Aug
to me

Hi [redacted]

I am doing research about human trafficking. Can you help in this. I want to share my research with you. Can you guide me in this?

From Safeena

Re: Inbox x

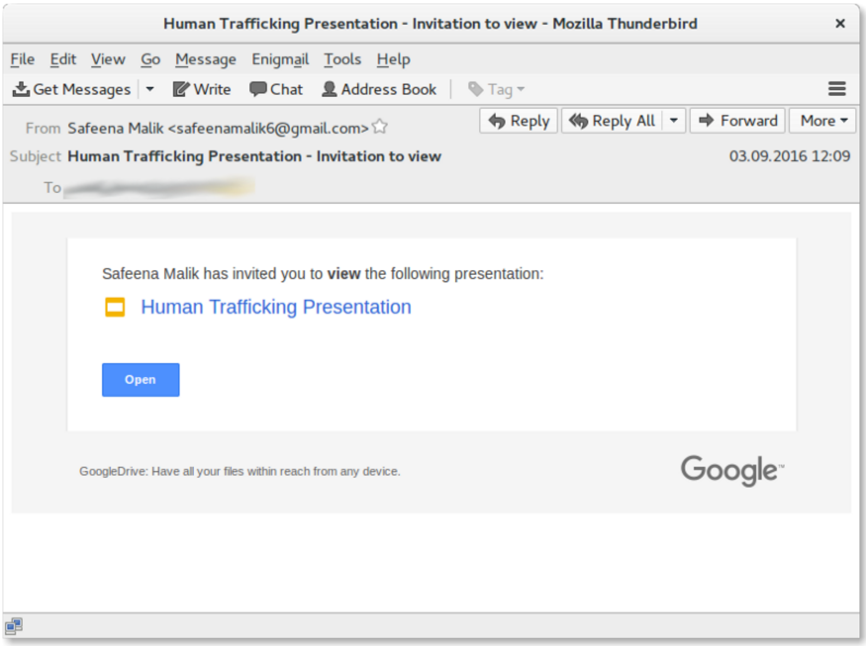
Safeena Malik <safeenamalik6@gmail.com> 3 Sep
to me

Hi [redacted]

Have you seen my presentation dear? please help in that presentation.

From Safeena

In the course of this email correspondence, the attacker—"Safeena" —then sent what appeared to be invitations to access several documents on Google Drive.



Human Trafficking Presentation - Invitation to view - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help
Get Messages Write Chat Address Book Tag
Reply Reply All Forward More

From Safeena Malik <safeenamalik6@gmail.com>
Subject Human Trafficking Presentation - Invitation to view 03.09.2016 12:09
To [redacted]

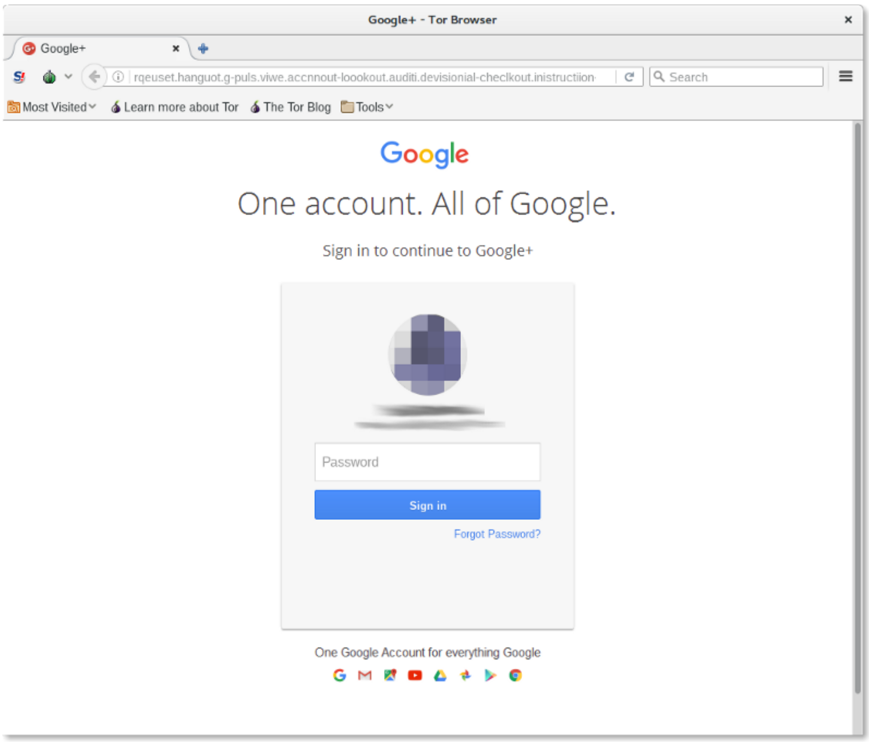
Safeena Malik has invited you to **view** the following presentation:

Human Trafficking Presentation

Open

GoogleDrive: Have all your files within reach from any device.

The links and buttons contained in the emails would direct the victim to a webpage that looked something like this:



Google+ - Tor Browser

Google+

rqeuset.hanguot.g-puls.viwe.accnnout-loookout.auditi.devisionial-checlkout.inistructiion

Google

One account. All of Google.

Sign in to continue to Google+

[redacted]

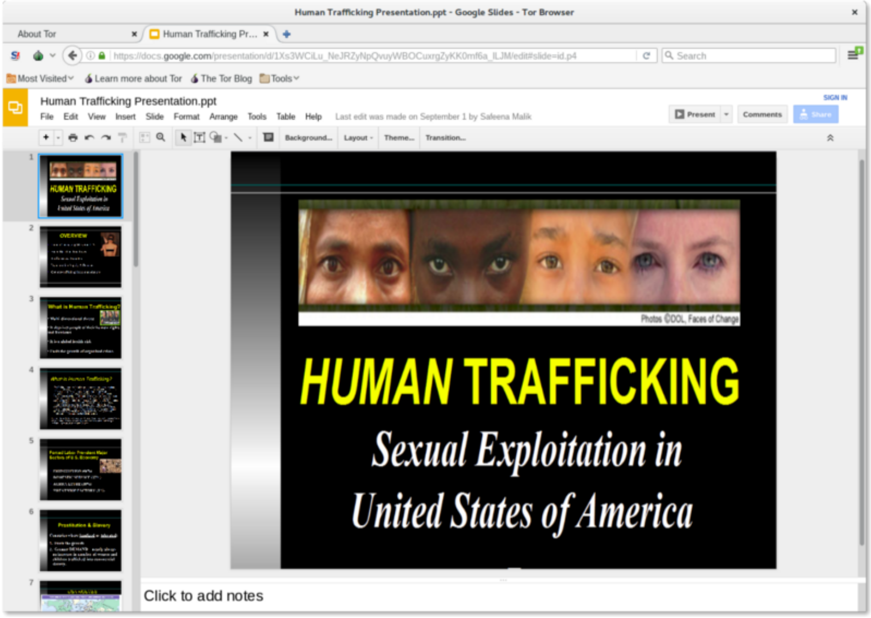
One Google Account for everything Google

Note: the profile picture has been manipulated to protect the identity of the target.

The page is designed to mimic a standard Google login page, with a high degree of accuracy. While most common phishing pages would only provide an empty form to enter an email address and password, this one instead is configured to display the profile picture, the account name, and the email address of the victim. This is obscured in the above screenshot to protect the privacy of the victim.

This design effectively replicates a real Google login page, which would similarly display the same information if you had previously logged into your account from a computer. The attackers were meticulous in making their phishing page as credible as possible.

Interestingly, after the victims would have entered their Google account credentials, they would be redirected to an actual document hosted on Google Drive, effectively recreating a normal browsing experience in order to avoid suspicion. In the example below, the target would have been redirected to a PowerPoint presentation on human trafficking. Amnesty has identified that this presentation had also been stolen from another source.



Human Trafficking Presentation.ppt - Google Slides - Tor Browser

https://docs.google.com/presentation/d/1Xs3WCiLu_NeJRZyNpQvuyWBOCuxrgZyKK0mf6a_ILJM/edit#slide=id.p4

Human Trafficking Presentation.ppt

Last edit was made on September 1 by Safeena Malik

HUMAN TRAFFICKING

Sexual Exploitation in United States of America

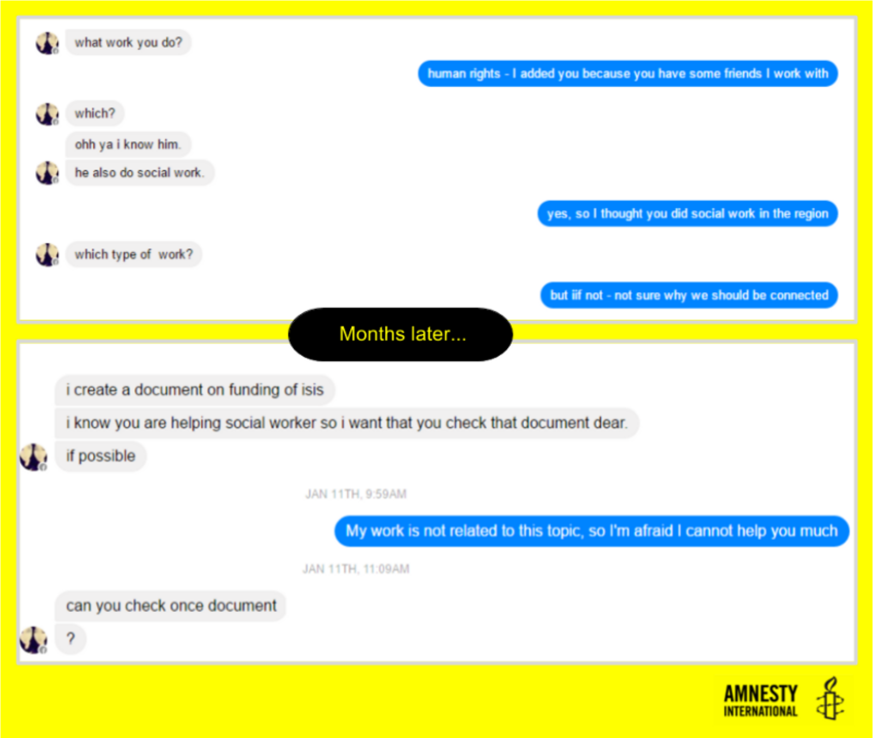
Photos ©DOL, Faces of Change

Click to add notes

Case 2: Making friends and connections

Among the targets of this campaign is the **International Trade Union Confederation** (ITUC). ITUC is a trade union federation based in Brussels and among the largest in the world, counting over 170 million members. ITUC has been very outspoken in recent years about migrant labour rights in Qatar, and is behind the "Re-Run the Vote!" campaign against the award of the organization of the 2022 FIFA World Cup to Qatar.

Both in the attacks against ITUC and in other occasions, the attackers approached selected targets over social media, prominently Facebook, and engaged in chat conversations with them on and off, sometimes over a period of several months. At times the attackers behind the profile would just have a short casual conversation, while at others they attempted an attack. Possibly in order to identify further targets, "Safeena Malik" found her way into several Facebook groups dealing with migrant workers and forced labour.



what work you do?

human rights - I added you because you have some friends I work with

which?

ohh ya i know him.

he also do social work.

yes, so I thought you did social work in the region

which type of work?

but iif not - not sure why we should be connected

Months later...

i create a document on funding of isis

i know you are helping social worker so i want that you check that document dear.

if possible

JAN 11TH, 9:59AM

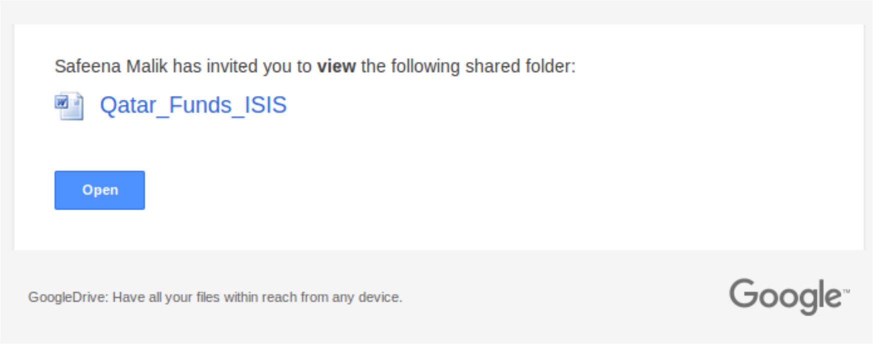
My work is not related to this topic, so I'm afraid I cannot help you much

JAN 11TH, 11:09AM

can you check once document

?

Similarly to attempts described previously, in this case the attackers also invited the targets to open a document seemingly shared on Google Drive. This time the document purported to be about the involvement of the Emir of Qatar in funding ISIS, which was seemingly copied from a website critical of Qatar.

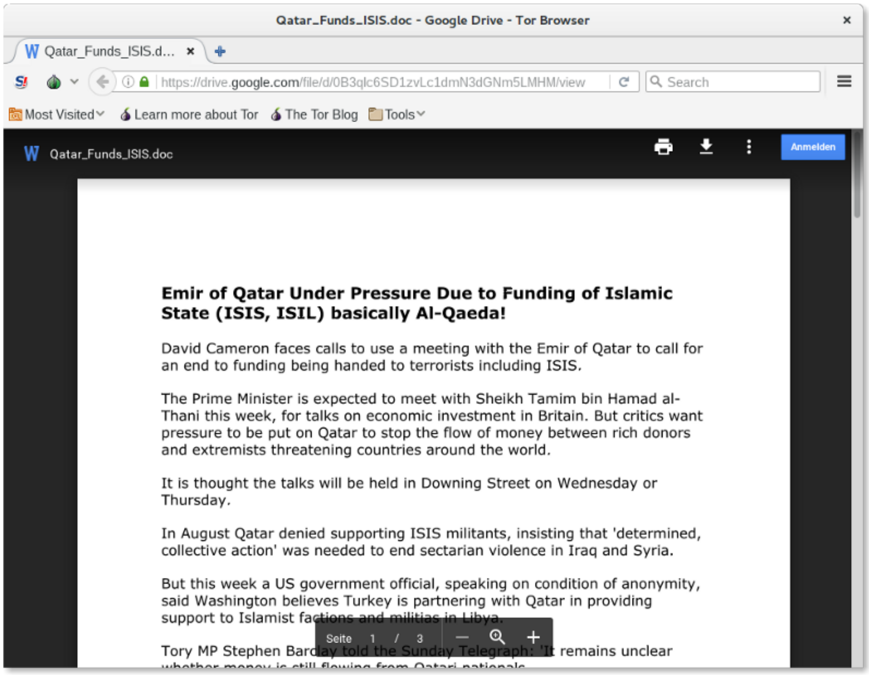


Safeena Malik has invited you to **view** the following shared folder:

Qatar_Funds_ISIS

GoogleDrive: Have all your files within reach from any device.

Once the target would provide their credentials through the fake Google login page, they would also be automatically redirected to an existing document hosted on the legitimate Google Drive.



Emir of Qatar Under Pressure Due to Funding of Islamic State (ISIS, ISIL) basically Al-Qaeda!

David Cameron faces calls to use a meeting with the Emir of Qatar to call for an end to funding being handed to terrorists including ISIS.

The Prime Minister is expected to meet with Sheikh Tamim bin Hamad al-Thani this week, for talks on economic investment in Britain. But critics want pressure to be put on Qatar to stop the flow of money between rich donors and extremists threatening countries around the world.

It is thought the talks will be held in Downing Street on Wednesday or Thursday.

In August Qatar denied supporting ISIS militants, insisting that 'determined, collective action' was needed to end sectarian violence in Iraq and Syria.

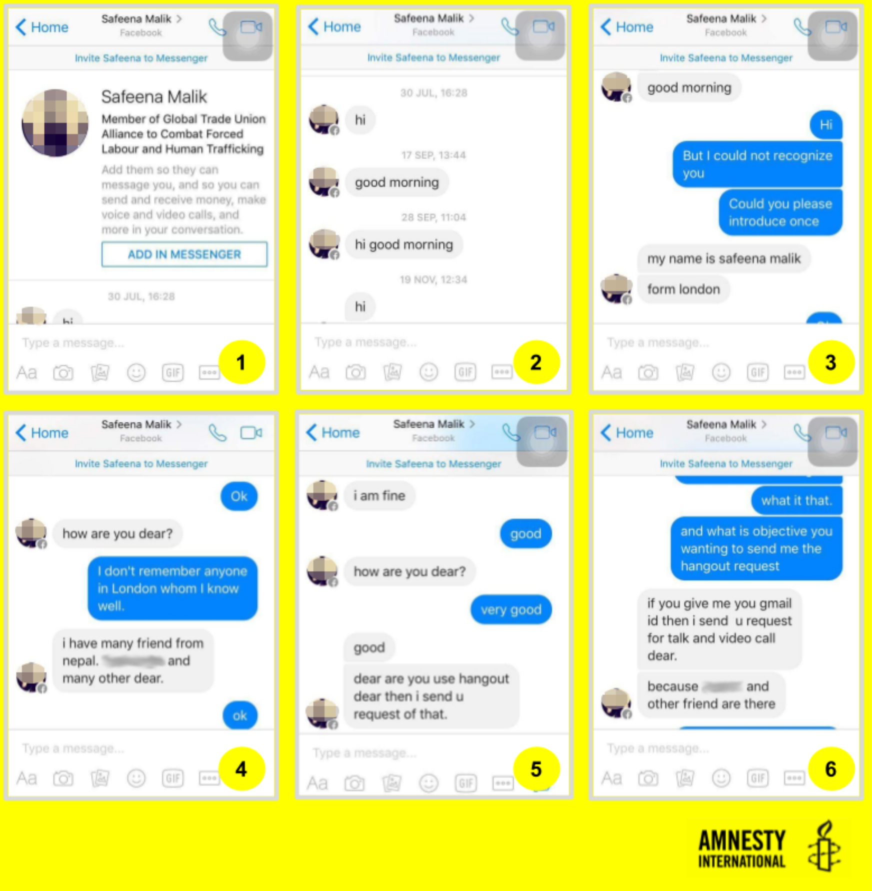
But this week a US government official, speaking on condition of anonymity, said Washington believes Turkey is partnering with Qatar in providing support to Islamist factions and militias in Libya.

Tory MP Stephen Barclay told the Sunday Telegraph: 'It remains unclear whether money is still flowing from Qatari nationals

While it might not appear significant, this attention to detail is what, in our experience, sets apart these phishing attempts from more common ones, as they demonstrate a level of experience and care that is both unusual and remarkable.

Case 3: Hanging out

Similar tactics are exemplified by yet another case we’ve become aware of and portrayed in the picture below, where the fake “Safeena Malik” profile is conversing with a prominent activist from Nepal working on migrant workers issues, soliciting them to give away their Gmail address.



1

Safeena Malik

Member of Global Trade Union Alliance to Combat Forced Labour and Human Trafficking

Add them so they can message you, and so you can send and receive money, make voice and video calls, and more in your conversation.

ADD IN MESSENGER

30 JUL, 16:28

hi

2

30 JUL, 16:28

hi

17 SEP, 13:44

good morning

28 SEP, 11:04

hi good morning

19 NOV, 12:34

hi

3

good morning

Hi

But I could not recognize you

Could you please introduce once

my name is safeena malik

form london

4

Ok

how are you dear?

I don't remember anyone in London whom I know well.

i have many friend from nepal. [redacted] and many other dear.

ok

5

i am fine

good

how are you dear?

very good

good

dear are you use hangout dear then i send u request of that.

6

what it that.

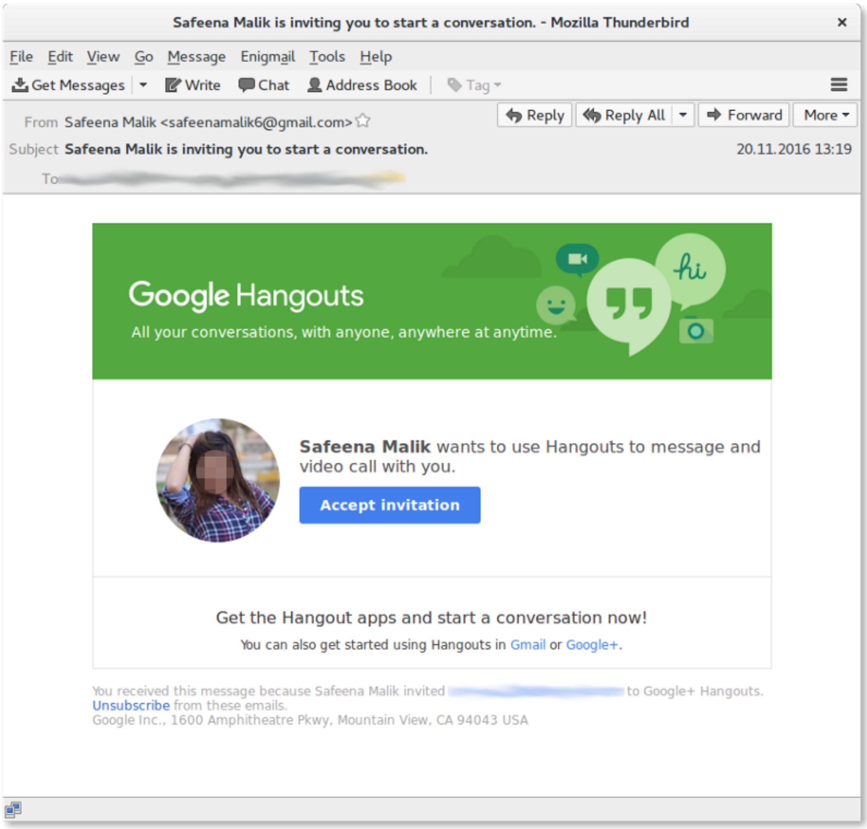
and what is objective you wanting to send me the hangout request

if you give me you gmail id then i send u request for talk and video call dear.

because [redacted] and other friend are there

Interestingly, the attackers tried to leverage common Facebook friends in an attempt to convince the target of their legitimacy. This is a tactic we've observed the attackers utilize on numerous occasions across their conversations with some of the targets we know of, which explains the time and effort spent in building a large social graph.

In this case, the attackers very credibly pretended to have been inviting the targets to participate in a Google Hangout (a videoconferencing service operated by Google).


Safeena Malik is inviting you to start a conversation. - Mozilla Thunderbird
File Edit View Go Message Enigmail Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More
Google Hangouts
All your conversations, with anyone, anywhere at anytime.
hi
Accept invitation

From Safeena Malik <safeenamalik6@gmail.com>

Subject **Safeena Malik is inviting you to start a conversation.**

20.11.2016 13:19

To [redacted]

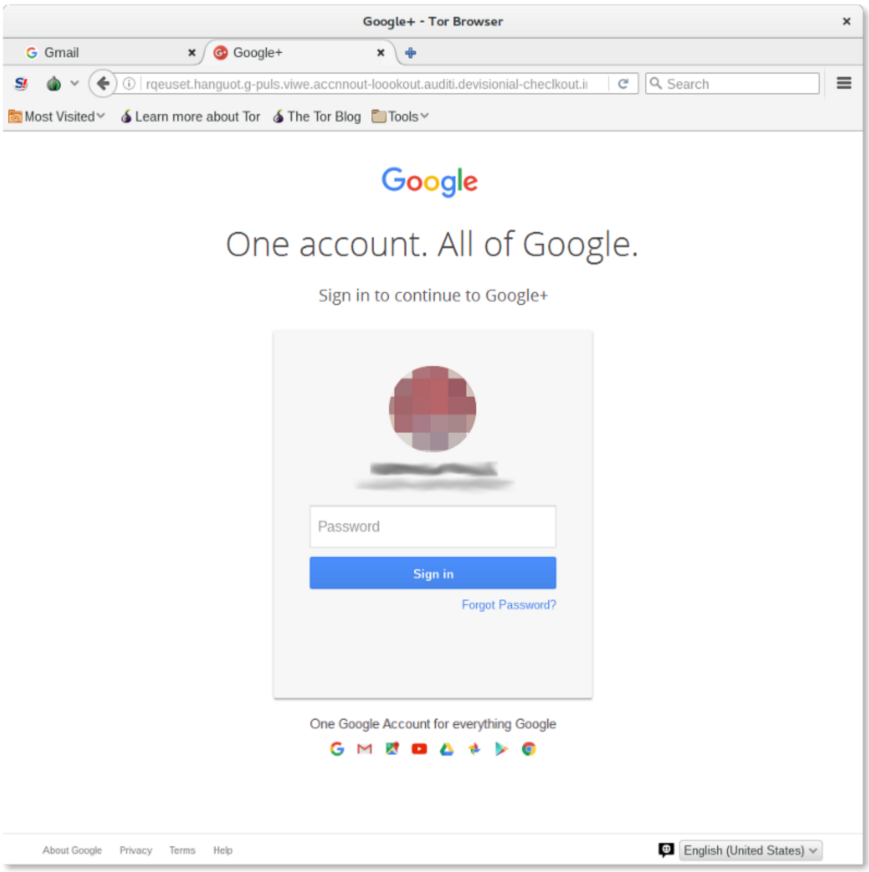
Safeena Malik wants to use Hangouts to message and video call with you.

Get the Hangout apps and start a conversation now!

You can also get started using Hangouts in Gmail or Google+.

You received this message because Safeena Malik invited [redacted] to Google+ Hangouts.
Unsubscribe from these emails.
Google Inc., 1600 Amphitheatre Pkwy, Mountain View, CA 94043 USA

Again, when clicking on the button the target would be presented with a Google-like login page.



One account. All of Google.

Sign in to continue to Google+

One Google Account for everything Google

Note: the profile picture has been manipulated to protect the identity of the target.

. . .

Identifying the Victims

While we first learned of these attacks through a journalist who was targeted, we soon learned of many others.

What we discovered, is that the phishing pages are in fact "configurable". The links sent via email to the targets contains all the required information for the phishing page to load the appropriate profile picture and names.

For example, a link would look like this (*please note that the links have been edited to disable any accidental clicks and redacted to protect the victim's privacy*):

```
hxxp://rqeuset.hanguot.g-puls.viwe.accnnout-
loookout.auditi.devisionial-checlkout.inistructiion-
mutuael.halftoine.appliacctiorn-gurad-way.leigacy-fs.termp-
forn.provider-saefe.alvie-valuse.token-
centeir.recollect.label.ping2port[.]info/?ml=
[REDACTED]=&n@e=[REDACTED]&P4t=
[REDACTED]&Re3d=aHR0cDovL3Rpbnl1cmwuY29tL2g5d3h3cDg=&pa=2&gp
=1
```

In the URL there are some encoded values passed to the webpage, which decode to the following:

```
hxxp://rqeuset.hanguot.g-puls.viwe.accnnout-
loookout.auditi.devisionial-checlkout.inistructiion-
mutuael.halftoine.appliacctiorn-gurad-way.leigacy-fs.termp-
forn.provider-saefe.alvie-valuse.token-
centeir.recollect.label.ping2port[.]info/?ml=[REDACTED]&n@e=
[REDACTED]&P4t=//ping2port.info/[REDACTED]/[REDACTED].jpg&Re
3d=http://tinyurl.com/h9wxwp8&pa=2&gp=1
```

The first value is the email address of the target, the second is the account name (most often the full real name of the intended target), the third value is an address pointing to a copy of the target's profile picture pulled from their Google+ or YouTube profile, and the last is a link to which the victim will be redirected after their credentials have been successfully stolen.

The stolen profile pictures would be stored on the server owned by the attackers. Interestingly, their filename and location were predictable as they would be normally saved in a particular folder with a filename that would be a combination of two lower-case letters. For example:

hxxp://ping2port[.]info/[REDACTED]/xx.jpg (*this particular filename is fictional, and the URL has been disabled to prevent misclicks)*.

As we noticed that this pattern was repeated across a couple of attacks that came to our attention, we realized we might be able to identify additional victims by regularly attempting to download all the available profile pictures stored with all the 676 possible combinations of two-letter filenames. Once we obtained new profile pictures, a simple image search online could reveal the identity behind these victims.

Surely enough, it allowed us to identify nearly 30 distinct targets.

Most identified targets were activists, journalists, and labour union members. While some of targets had published critical opinions about Qatar's international affairs, the majority of identified targets were affiliated with organisations supporting migrant workers in Qatar. Interestingly, a significant number of them are from Nepal, which is one of the largest nationalities amongst migrant workers in Qatar, and a country that has featured prominently in the migrant worker narrative on Qatar.

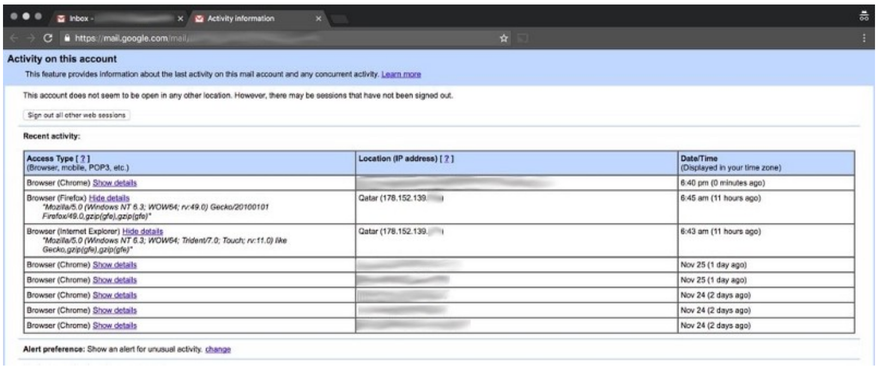
We learned however of several more targets who appeared to not have been configured with a stored profile picture, so it is possible that the number of actual targets was far larger. Through our conversations with identified targets it became clear that "Safeena Malik" often approached members of thematic Facebook groups and asked for information and contact details about further targets we were not originally aware of.

· · ·

Who is behind the attacks?

We don't have conclusive evidence that could implicate any particular government or individual as being responsible for these attacks, but the fact that the campaign specifically targets individuals active on human rights issues in Qatar, makes us believe that it might be a state-sponsored or affiliated actor. We believe it is also possible that these attacks have been orchestrated by contractors. In fact, similar intelligence gathering operations uncovered in other GCC countries, have shown a reliance on outsourcing this work to private firms.

Interestingly, the attackers logged into some of the harvested email accounts from the IP address **178.152.139.XXX** [*last octet redacted*] as these Gmail recent activity records display:


Inbox - [redacted]
Activity information
https://mail.google.com/mail/[redacted]

Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. Learn more

This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

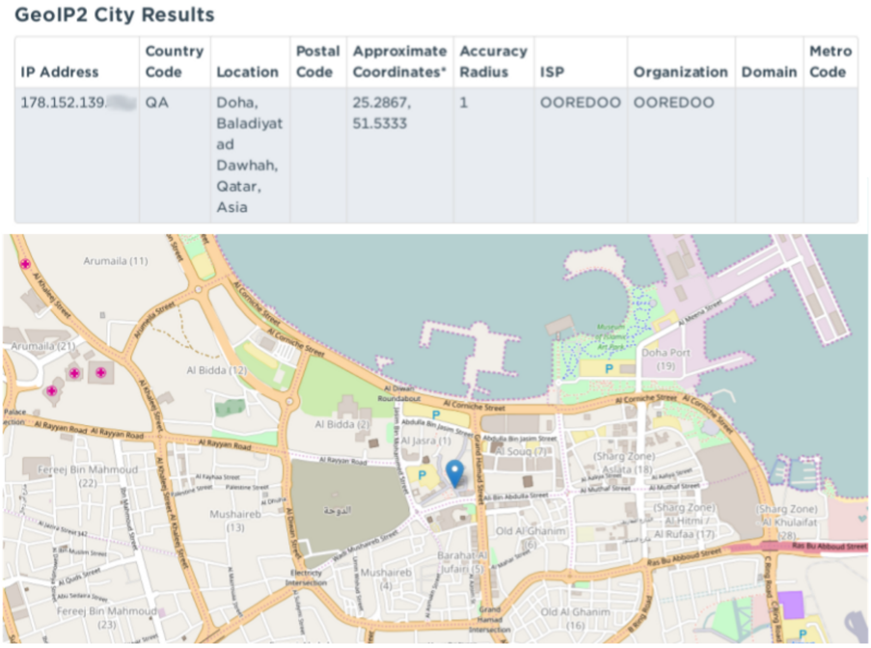
Sign out all other web sessions

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	**Location (IP address) [?]**	**Date/Time** (Displayed in your time zone)
Browser (Chrome) Show details	[redacted]	6:40 pm (0 minutes ago)
Browser (Firefox) Hide details *"Mozilla/5.0 (Windows NT 6.3; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0,gzip(gfe),gzip(gfe)"*	Qatar (178.152.139.[redacted])	6:45 am (11 hours ago)
Browser (Internet Explorer) Hide details *"Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko,gzip(gfe),gzip(gfe)"*	Qatar (178.152.139.[redacted])	6:43 am (11 hours ago)
Browser (Chrome) Show details	[redacted]	Nov 25 (1 day ago)
Browser (Chrome) Show details	[redacted]	Nov 25 (1 day ago)
Browser (Chrome) Show details	[redacted]	Nov 24 (2 days ago)
Browser (Chrome) Show details	[redacted]	Nov 24 (2 days ago)
Browser (Chrome) Show details	[redacted]	Nov 24 (2 days ago)

Alert preference: Show an alert for unusual activity. change

This IP address appears to be an Internet connection provided by Ooredoo, an Internet Service Provider with headquarters in Doha, Qatar.

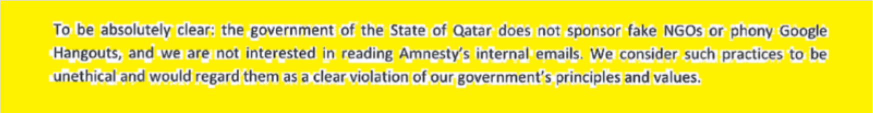


GeoIP2 City Results

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius	ISP	Organization	Domain	Metro Code
178.152.139.[redacted]	QA	Doha, Baladiyat ad Dawhah, Qatar, Asia		25.2867, 51.5333	1	OOREDOO	OOREDOO		

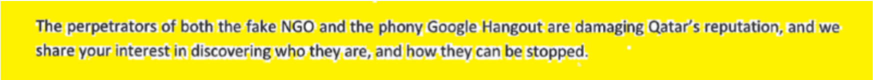
Note: the geographical mapping of an IP address is often very approximate, and while it indicates that the attackers used a connection in Doha, the coordinates, which were provided by the free MaxMind service should not to be considered to be a precise location.

We wrote to the Government of Qatar with information about this phishing campaign and asking about their possible involvement. They responded, vigorously denying any link to the attacks. (We should note that Amnesty International was not one of the targets of this campaign.)



To be absolutely clear: the government of the State of Qatar does not sponsor fake NGOs or phony Google Hangouts, and we are not interested in reading Amnesty's internal emails. We consider such practices to be unethical and would regard them as a clear violation of our government's principles and values.

The Government of Qatar also expressed their interest in stopping the phishing attacks.



The perpetrators of both the fake NGO and the phony Google Hangout are damaging Qatar's reputation, and we share your interest in discovering who they are, and how they can be stopped.

We also wrote to "Safeena Malik" on the Gmail address used to contact targets. We summarized our findings and asked for a response. We similarly contacted the Facebook account used in the attacks. As of publication, we have not received any reply.

While there is a clear underlying Qatar migrant workers theme in this campaign, it is also hypothetically possible that these attacks could have been perpetrated by a malicious actor affiliated to a different government with an interest in damaging the reputation of the State of Qatar.

However, in the absence of clear evidence, trying to identify the entity behind this attack can only be speculative. As such, we cannot make any conclusive attribution.

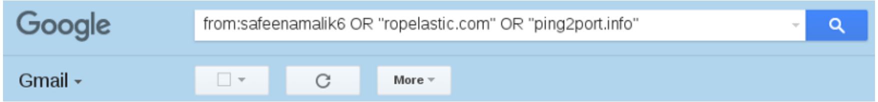
. . .

Have I been targeted too?

Following is a Gmail query to search for specific keywords that we believe are unique to the malicious emails sent by the “Safeena Malik” profile.

```
from:safeenamalik6 OR "ropelastic.com" OR "ping2port.info"
```

You can copy and paste it in the search bar at the top of your Gmail window like so:



from:safeenamalik6 OR "ropelastic.com" OR "ping2port.info"

If you have received any emails related to this campaign, Gmail should filter them from your inbox and highlight them to you.

If you have further information about this campaign or have been targeted, and would like to share information with us, you can write us at tech.reports@amnesty.org or use Amnesty’s secure dropbox https://amlea.org/en/.

Some tips to protect yourself against phishing

Be careful with links: before clicking a link or button on an email check where it is redirecting you to. You can usually do this by hovering your mouse pointer over the link or button; you can also find out by right-clicking and copying the link. If an email tells you it's taking you to Facebook or Gmail but the link doesn't look like like a Facebook or Google address, then there might be something wrong. If you're not sure, type the address yourself and log in.

Enable two-factor authentication: two-factor authentication is an extra step you need to log-in to your account. In most cases, it's very simple and you only need to do it when you use a new device or once every few weeks. Most commonly you will be required to provide a six-digit code delivered through your phone either through an SMS message, or preferably through a mobile app, like Google Authenticator, Authy or Duo Mobile. While it might appear tedious at first, this process makes it a lot harder to hack your online accounts, as your passwords alone wouldn't be sufficient to access them.

Many popular services have two-factor authentication, including Gmail, Outlook, Facebook and Twitter. You can read more details on two-factor authentication here.

Be wary of strangers: if someone you don't know contacts you and starts asking you for personal details, contact details and names of people you know, treat it with suspicion. A simple rule is: if you wouldn't share it on twitter, don't share information with someone you don't know, even if it is someone who appears to have friends on social media in common with you. As we learned from this campaign, attackers do commonly befriend many people to leverage common social connections as a way to appear more credible and legitimate.

. . .

Acknowledgements

This report is the product of investigations by *Claudio Guarnieri*, *Sherif Elsayed-Ali*, *Ashmita Sapkota* and others at Amnesty International, and with the help *Collin Anderson*. We would also like to thank all those targeted who came forward to share information on these attacks.

Security Indicators

Following are details useful for Internet Service Providers and the security community to further research and implement appropriate defenses.

```
ropelastic[.]com

ping2port[.]info

drvie.goo-qle.aconnut.corn.provider-termp.fs-valuse.checlk-
out.appliactiorn.token-loookout-
recomrnendation.deivisional.centeir-halftone.mutuael-
inistructiion.leigacy-auditi.label-recollect.forn-
alive.ropelastic[.]com

rqeuset.hanguot.g-puls.viwe.accnnout-
loookout.auditi.devisionial-checlkout.inistructiion-
mutuael.halftoine.appliacctiorn-gurad-way.leigacy-fs.termp-
forn.provider-saefe.alvie-valuse.token-
centeir.recollect.label.ping2port[.]info

direve.g-co.pohto.shraning.fodler-premissiion.viwe.termp-
recomrnendation.appliacctiorn.loookout.forn-
devisionial.recollect.auditi-
checlkout.inistructiion.halftoine-valuse.provider-
alive.leigacy.gurad-way.saefe-fs.ping2port[.]info
```