

REPUBLIC OF KENYA
IN THE COURT OF APPEAL AT NAIROBI
CIVIL APPLICATION NO. 102 OF 2020

LAW SOCIETY OF KENYA.....APPLICANT

VERSUS

THE BLOGGERS ASSOCIATION OF KENYA.....1ST RESPONDENT
THE HON. ATTORNEY GENERAL.....2ND RESPONDENT
THE NATIONAL ASSEMBLY.....3RD RESPONDENT
THE DIRECTOR OF PUBLIC PROSECUTIONS.....4TH RESPONDENT
THE INSPECTOR GENERAL OF THE
NATIONAL POLICE SERVICE.....5TH RESPONDENT
ARTICLE 19 EAST AFRICA.....6TH RESPONDENT
KENYA UNION OF JOURNALISTS.....7TH RESPONDENT

(Being an Application for conservatory orders pending appeal from the judgment and orders of the High Court at Nairobi (Makau J) given on 20th February, 2020 in Petition No. 206 of 2018)

2ND & 5TH RESPONDENTS' REPLYING AFFIDAVIT.

I, **HILARY NZIOKI MUTYAMBAI, MGH, nsc (AU).**, the Inspector General, the National Police Service of the Republic of Kenya and of Post Office Box Number 44249 – 00100, Nairobi do hereby make an oath and state as follows:-

1. **THAT** I am the 5th Respondent conversant with the facts of this matter and I am therefore competent to swear this Affidavit.
2. **THAT** I have read and where necessary had explained to me by the 2nd and 5th Respondents' Advocates on record, Messrs. V.A. Nyamodi and Company Advocates, the contents of the Applicant's Notice of Motion Application and the

Supporting Affidavit thereof sworn by Mercy Wambua both dated 20th April, 2020.
I swear this Affidavit in response to the same.

3. **THAT** I understand the Application as one seeking conservatory orders suspending the enforcement of Sections 5, 16, 17, 22, 23, 24, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 48, 49, 50, 51, 52 & 53 of the Computer Misuse and Cybercrime Act, 2018. In the alternative, the Applicant seeks conservatory orders suspending the enforcement of Section 22 (False publication) and Section 23 (Publication of false information) of the Computer Misuse and Cybercrime Act, 2018 ('hereinafter the Act') pending the hearing and determination of the intended Appeal.
4. **THAT** I wish to first point out the delay by the Applicant in filing this Application. The impugned Judgment by the High Court upholding the enactment of the Act was delivered on 20th February, 2020. The Application seeking conservatory orders suspending the implementation of the Act was filed on 20th April, 2020, long after the Act has been implemented following the said Judgment.
5. **THAT** moreover, the Applicant has not made a formal application to the Deputy Registrar of the High Court for the supply of certified copies of the proceedings, a certified copy of the Judgement and a Decree for purposes of filing the Record of Appeal. It is thus clear that the Applicant has failed to exercise all due diligence in pursuit of this Appeal by intentionally delaying the filing and hearing of the Appeal.
6. **THAT** I am advised by Counsel on record for the 2nd and 5th Respondents which advise I believe to be sound that the Applicants have inordinately delayed the filing and service of the Appeal and the instant Application, this Honourable Court ought not to exercise its discretion in the Applicant's favour. The Applicant is undeserving of the conservatory orders sought in the Application.

7. **THAT** it is also important to bring to this Honourable Court's attention the fact that the 1st Respondent herein, the Bloggers Association of Kenya, had filed a similar Application under **Rule 5 (2)(b) of the Court of Appeal Rules** seeking similar orders as those sought in this Application (Civil Application No. 79 of 2020). No orders were granted in that Application.
8. **THAT** without prejudice to the foregoing, I wish to respond to the Application as follows –
9. **THAT** it is vital that I briefly set out the sections of the Act which the Applicants wish to have suspended –
- Section 5 – Composition of the National Computer and Cybercrimes Co-Ordination Committee.
- Offences
- Section 16 – Unauthorised interference
 - Section 17 – Unauthorised interception
 - Section 21 – Cyber espionage
 - Section 22 – False publications
 - Section 23 - Publication of false information
 - Section 24 – Child Pornography
 - Section 27 – Cyber Harassment
 - Section 28 – Cybersquatting
 - Section 31 – interception of electronic messaged or money transfers
 - Section 32 – Wilful misdirection of electronic messaged
 - Section 33 – Cyber terrorism
 - Section 34 – Inducement to deliver electronic message
 - Section 35 – intentionally withholding message delivered erroneously
 - Section 36 – unlawful destruction of electronic messages

- Section 37 – wrongful distribution of obscene or intimate images
- Section 38 – Fraudulent use of electronic data
- Section 39 – Issuance of false e-instructions
- Section 40 – Reporting of cyber threat
- Section 41 – Employee responsibility to relinquish access codes

Investigation procedures

- Section 48 – Search and seizure of stored computer data
- Section 49 – Record of and access to seized data
- Section 50 – Production order
- Section 51 – Expedited preservation and partial disclosure of traffic data
- Section 52 – Real time collection of traffic data
- Section 53 – interception of content data

10. **THAT** I wish to state that the criminalization of the acts stated hereinbefore is in the exercise of the State's duty of care to its citizenry. Increased access to the internet and exposure to online risks and insecurity associated with the cyberspace is a pressing concern, not just in Kenya, but the world over. Such phenomenal growth in access to information and connectivity has on the one hand empowered the citizenry and on the other posed new challenges, not just to Governments and law enforcement but also to administrators of cyberspace.

11. **THAT** cyber security is an issue of critical importance with profound implications for Kenya's economic development and national security. Given the growing threats to cyber assets, countries around the world are engaged in actions aimed at ensuring the security of their cyber space. The borderless nature of the cyber space calls for a strategic approach requiring multi-dimensional and multi-layered initiatives and responses in dealing with offences related to the internet and computer systems.

12. **THAT** key amongst these initiatives is the enactment of an act of Parliament to provide for offences relating to computer systems; to enable timely and effective

detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes; to facilitate international co-operation in dealing with computer and cybercrime matters.

13. **THAT** central to the purpose of the Act is to enable the State to effectively combat cybercrime by ensuring its citizens remain protected against the constant threats of computer misuse offences and cybercrime. At the same time, the Act enables the State to fulfill its international obligations in dealing with computer and cybercrime matters especially as relates to the Budapest Convention on Cybercrime which seeks to address internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques and increasing cooperation among nations.
14. **THAT** the suspension of the aforesaid sections of the Act will therefore grossly offend not only Kenya's national security but also its international obligations. The absence of an adequate cybercrime legal framework will result in an undesirable situation where cybercrimes go unpunished, the State is unable to protect its citizens from computer related offences such as terrorism and the State is unable to cooperate with its international partners in the fight against computer misuse and cybercrimes.
15. **THAT** it is important to note that the Act was enacted at the behest of various government institutions including the National Police Service, corporate entities, the civil society and private individuals.
16. **THAT** the National Police Service was involved in the conception, drafting and discussion before and after publication of the various drafts of the Bill which was eventually adopted. Further, various government agencies, Kenyan institutions of higher learning, experts, including the Applicants herein were involved in the process of drafting the Act.

17. **THAT** therefore, all the offences created are matters that are of concern in combating cybercrime using the law enforcement approach and in recognition of the constitutional obligation to protect its citizens.

18. **THAT** in support of the Application, the Applicants have advanced the following grounds for the suspension of various sections of the Act –

- The arrest and prosecution of bloggers for COVID-19 related posts.
- The arguability of the intended Appeal –
 - Disregard of pleadings and submissions on record.
 - Upholding limitation of freedom of expression under the State without conducting the mandatory three-part test in Article 24 of the Constitution.
- Nugatory effect of a successful appeal sans conservatory orders.
- Public interest.

19. **THAT** I wish to respond to the issues raised as below –

The arrest and prosecution of bloggers for COVID-19 related posts

20. **THAT** Sections 22 and 23 of the Act criminalize false publication and publication of false information respectively. The criminalization of these offences is in cognizance of the State's primary obligation to exhibit neutrality toward the content of the opinions and information disseminated by the citizens, while at the same time protecting its citizens against misinformation that is likely to cause cataclysm.

21. **THAT** indeed, the COVID-19 pandemic has created a new reality in the cyber space. There has been an increased reliance in technology in all spheres of life,

including in communication, thereby amplifying the use of social media in the publication of information relating to COVID-19.

22. **THAT** this creates the need for a regulatory framework to ensure the public is protected from both the pandemic and an “infodemic” whereby excessive misinformation, disinformation and rumours are spread during a health emergency such as the COVID-19 pandemic. The Computer Misuse and Cybercrime Act, 2018 is the only existing regulatory framework in place to protect against such crime.
23. **THAT** it is the responsibility of the State to ensure that only verifiable and accurate information on the pandemic is conveyed to its citizens through the proper and official government channels. The dissemination of accurate information on the pandemic is a significant tool in combating the virus and it is only the State, which is equipped with the necessary tools and resources to ensure the accuracy of this information, that can do so.
24. **THAT** cyber-criminals are exploiting interest in the global epidemic to spread fake news and malicious information relating to the outbreak of the virus. This information is alarming, unverified and misleading, often emanating from non-experts, thereby potentially causing panic and tension among citizens resulting in loss of life. Unfortunately, in view of the nature of the internet and the speed with which information is disseminated, the fake news could spread faster than the virus.
25. **THAT** indeed, on 15th February 2020 the Director-General of the World Health Organisation (WHO) raised this concern in his address to the Munich Security Conference on COVID-19 where he stated that if nation states do not tackle the spread of fake news and misinformation on the virus, the world will be headed down a dark path that leads to division and disharmony.

Annexed hereto and marked “HNM-01” is the press statement by the Director-General of the World Health Organisation at the Munich Security Conference on 15th February 2020

26. **THAT** in the case of COVID-19, the spread of fake news offers unique challenges and dangers to the public. It is the sole responsibility of the State to provide detailed, clear and transparent information on the pandemic.
27. **THAT** to complement the efforts by government to combat the spread of misinformation and disinformation on the pandemic, various social media platforms have implemented programs that are aimed at limiting the spread of COVID-19 hoaxes and misinformation.

Annexed hereto and marked “HNM-02” are press statement by Facebook®, Instagram® and WhatsApp® on Combating COVID-19 Misinformation Across those social media platforms.

28. **THAT** publication of false information takes various forms and is not exclusive only to the form the Applicant demonstrates. For instance, there are ongoing investigations of instances where a cyber criminal impersonates a government official on a social media platform (contrary to Section 29 of the Act) and publishes false information on the pandemic that is likely to cause chaos and panic (contrary to Section 23 of the Act). The suspension of these provisions of the Act will result in a situation where false, alarming and unconfirmed information about the COVID-19 pandemic under the purported hand of a government official is published, thereby causing fear and panic amongst Kenyans.
29. **THAT** in addition to the increase in the creation of fake news, there has been publication of false contacts of Ministry of Health officials for criminal purposes, creation of fake websites with false information on the pandemic for exploitative purposes, among other offences. The suspension of the provisions of the Act will

result in a lacuna in the law on the prosecution of these offences, giving cyber criminals a free hand to do/say as they please.

30. **THAT** the arrest and prosecution of persons who have violated **Section 23 of the Act** by spreading information on the COVID-19 pandemic which information is false and calculated to cause fear and panic among the citizens of Kenya is therefore justified and in the public interest. The spread of false information in technology-mediated mediums such as the internet and social media is dangerous as it can cause the recipients of such information to make the wrong decisions, including decisions that endanger themselves or others.
31. **THAT** the persons charged and mentioned in the Application were properly charged for issuing alarming, unconfirmed, unverified, misleading information that can cause panic. They are not experts in epidemics.
32. **THAT** moreover, I am aware that there are sufficient constitutional and statutory safeguards on protection of the rights of accused persons, including those charged with computer misuse and cyber crimes under the Act.
33. **THAT** the Act does not exist in isolation. It should be considered within the context of other statutes such as the Data Protection Act, 2019 which safeguards the rights of data subject and provides for the regulation of the processing of personal data.
34. **THAT** further, in a joint advisory issued on 8th April, 2020 by the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) on exploitation by cyber criminals and advanced persistent threat (APT) groups of the current COVID-19 global pandemic, it was noted that there has been an increase in the number of malicious cyber actors exploiting the current COVID-19 pandemic for their own objectives.

Annexed hereto and marked “HNМ-03” is the joint advisory from the United Kingdom’s National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)

35. **THAT** the threats observed by the NCSC, the DHS and CISA include –

- Phishing, using the subject of coronavirus or COVID-19 as a lure
- Malware distribution using coronavirus or COVID-19 themed lures
- Registration of new domain names containing coronavirus or COVID-19 related wording
- Attacks against newly (and often rapidly) deployed remote access or remote working infrastructure.

36. **THAT** the suspension of the provisions of the Act in the context of the COVID-19 pandemic offends the public interest and the need to protect the wider public from both the pandemic and the infodemic. The interest of the public to receive accurate information on the pandemic ranks higher than the private desires of the private citizens mentioned in the Application to spread unverifiable information.

The arguability of the intended Appeal –

37. **THAT** in support of the assertion that the intended appeal is arguable, it is the Applicant’s averment that in its Judgment, the High Court disregarded pleadings and submissions on record.

38. **THAT** I am advised by my Counsel on record which advise I believe to be sound that the structure of a Judgment ought not to form a ground of appeal. It was well within the discretion of the High Court Judge to decide what to write and how to structure the Judgment.

39. **THAT** the Judgment delivered on 20th February, 2020 in this matter was the Honourable Judge's statement of the conclusions that flow from the application of the governing law to the facts before him during the trial. The Applicants have not demonstrated either an error of fact or an error of law in the form of the Judgment.
40. **THAT** in further support of the assertion that the intended appeal is arguable, the Applicants aver that the Honourable Judge erred in law in upholding the limitation of freedom of expression under the State without conducting the mandatory three-part test in Article 24 of the Constitution.
41. **THAT** I state in response thereto that the existence of threat of violation of rights and freedoms ought to be determined on merits. It does not warrant the grant of conservatory orders at this stage.
42. **THAT** I am advised by my counsel on record which advise I believe to be true that the Applicants have not demonstrated that the Honourable High Court Judge acted on the wrong principles or misapprehended the evidence in any manner so as to warrant the interference by this Honourable Court with that Court's findings of fact.
43. **THAT** the High Court made definitive findings as to the constitutionality of the Act and the challenge thereto, now raised in the Application were distinctly adjudicated.

Nugatory effect of a successful appeal sans conservatory orders.

44. **THAT** I am advised by my counsel on record, which advice I verily believe to be sound, that dismissing this Application will not render the intended Appeal nugatory. In this regard, I note that the grounds cited in support of the Application are based on a distortion of relevant fact for the sole benefit of a small group of private individuals for their private interests.

45. **THAT** on the other hand, the grant of the conservatory orders suspending the Act will result in an ill-fated situation where conduct which the Kenyan people have determined as undesirable and criminal, is perpetrated.
46. **THAT** the situation is further exacerbated with the current COVID-19 pandemic where the grant of the conservatory orders sought by the Applicants will result in the spread of falsehoods related to the pandemic which can easily gain traction that negates the efforts by the State to manage this pandemic thereby posing a real threat to the lives of millions of Kenyans.
47. **THAT** in addition, the rights of any person charged under any provision of the Act are guaranteed by **Article 49 & 50 of the Constitution** as well as the Criminal Procedure Code. In the event the intended appeal is successful, these constitutional and statutory safeguards ensure the protection of the rights of the accused persons.

Public interest

48. **THAT** I am advised by my counsel on record which advise I believe to be sound that a statute or a provision thereof is constitutional until declared unconstitutional, granting a conservatory order at this stage will be unconscionable and will occasion injustice to the millions of Kenyans whose rights and freedoms are safeguarded by this Act.
49. **THAT** imminent danger lies in the inability of the Respondents to ensure national security in view of the cybercrimes and computer misuse offences, especially in the context of the COVID-19 pandemic. Consequently, the need to protect the wider public from the dangers in the cyber space outweighs the grant of the orders sought in the Application.
50. **THAT** in view of the foregoing, I verily believe that the Application herein has no merit and the same ought to be dismissed with costs to the Respondents.

51. **THAT** what is deponed herein is true to the best of my knowledge, information and belief save as to matters deponed to on information sources whereof have been disclosed and matters deponed to on belief grounds whereof have been given.

SWORN at NAIROBI by the said]

HILARY NZIOKI MUTYAMBAI]

This 29th day of MAY 2020]

BEFORE ME]



COMMISSIONER FOR OATHS]

DEPONENT

DRAWN AND FILED BY:

V.A. NYAMODI & COMPANY
ADVOCATES
HSE NO 7 DUPLEX APARTMENTS,
LOWERHILL ROAD, UPPERHILL
P.O BOX 51431-00200

NAIROBI.

P105/3707/98

nyamodipaul@gmail.com

0722514224

TO BE SERVED UPON:

OCHIEL DUDLEY, ADVOCATE
C/O KATIBA INSTITUTE
HOUSE NO. 5, THE CRESENT, OFF PARKLANDS ROAD
P.O.BOX 26586-00100

NAIROBI.

ochieljd@katibainstitute.org

0731740766/0700149469

NZILI AND SUMBI ADVOCATES
MAISONETTE 1, KIRICHTWA/NGONG ROAD JUNCTION
P.O. BOX 2580-00202

NAIROBI.

mercy@mercymutemisumbi.com
0737061138

NATIONAL ASSEMBLY
5TH FLOOR, PROTECTION HOUSE
PARLIAMENT ROAD
P.O. BOX 41842-00100

NAIROBI.

clerk@nationalassembly.go.ke
254 2 2221291

DIRECTOR OF PUBLIC PROSECUTIONS
ODPP HOUSE
RAGATI ROAD, UPPERHILL
P.O. BOX 30701-00100

NAIROBI.

info@odpp.go.ke
0723202880

ARTICLE 19 – EASTERN AFRICA
2ND FLOOR, ACS PLAZA
LENANA ROAD
P.O. BOX 2653-00100

NAIROBI.

Kenya@article19.org
0727862230

KENYA UNION OF JOURNALISTS
DELAMERE FLATS, OPP INTEGRITY CENTRE
P.O. BOX 47035-00100

NAIROBI.

info@kenyaunionofjournalists.org
0721230016



THIS IS THE EXHIBIT MARKED "HNm-01"
REFERRED TO IN THE ANNEXED AFFIDAVIT
/DECLARATION OF HILARY NZIOKI MUYAMBAI
SWORN/DECLARED BEFORE ME ON THIS
29th DAY OF MAY 2020 AT
NAIROBI IN THE REPUBLIC OF KENYA
COMMISSIONER FOR OATHS

Munich Security Conference

15 February 2020

Excellencies, distinguished guests, dear colleagues and friends,

Thank you for the opportunity to address you today. And especially my appreciation to my friend Ambassador Ischinger.

Yesterday I was in Kinshasa, in the Democratic of the Congo, meeting with the President and other senior ministers to review progress against the Ebola outbreak and work together on a plan to strengthen DRC's health system so that it never sees another outbreak like this again.

I'd like to thank the President for his leadership, and for his vision of a healthier and safer DRC.

We are finally starting to see the possibility of ending this outbreak, after more than 18 months and the loss of 2,249 lives. In the past week there has been just 1 case of Ebola, compared with 120 cases a week at the peak in April.

This epidemic stands in stark contrast to the previous Ebola outbreak in the western part of DRC in 2018, an area that is relatively stable and peaceful. That outbreak was controlled in just three months.

This experience illustrates a key lesson of history: disease and insecurity are old friends.

It was no coincidence that the 1918 flu pandemic erupted in the middle of the First World War, and killed more people than the First World War itself.

It's no coincidence that the final frontier for eradicating polio is in the most insecure regions of Pakistan and Afghanistan.

It's no coincidence that Ebola has spread in the most insecure region of the DRC.

Without peace, health can be an unattainable dream.

But the opposite can also be true: epidemics have the potential to cause severe political, economic and social instability and insecurity.

Health security is therefore not just the health sector's business. It's everybody's business.

There are three main scenarios in which a coordinated response between the health and security sectors is essential:

First, high-impact epidemics in situations of conflict and insecurity, such as Ebola. In the last few years, 80% of outbreaks requiring an international response have occurred in countries affected by fragility, conflict and insecurity.

Second, the emergence of a pathogen with pandemic potential, moving rapidly from country to country and requiring an immediate and large-scale response in countries.

And third, the deliberate or accidental release of biological agents – a hopefully rare event for which we must nonetheless be prepared.

The second of these three scenarios is what we are seeing now with the outbreak of COVID-19.

Although PHEIC (Public Health Emergency of International Concern) is declared, with 99% of cases in China, this is still very much an emergency for that country. Because in the rest of the world we only have 505 cases and in China we have more than 66,000 cases.

Let me be clear: it is impossible to predict which direction this epidemic will take.

What I can tell you is what encourages us, and what concerns us.

We are encouraged that the steps China has taken to contain the outbreak at its source appear to have bought the world time, even though those steps have come at greater cost to China itself. But it's slowing the spread to the rest of the world.

We're encouraged that outside China, we have not yet seen widespread community transmission.

We're encouraged that the global research community has come together to identify and accelerate the most urgent research needs for diagnostics, treatments and vaccines.

We're encouraged that we have been able to ship diagnostic kits, as well as supplies of masks, gloves, gowns and other personal protective equipment to some of the countries that need it most.

We're encouraged that an international team of experts is now on the ground in China, working closely with their Chinese counterparts to understand the outbreak, and to inform the next steps in the global response.

But we also have concerns.

We're concerned by the continued increase in the number of cases in China.

We're concerned by reports from China yesterday of the number of health workers who have been infected or have died.

We're concerned by the lack of urgency in funding the response from the international community.

We're concerned about the severe disruption in the market for personal protective equipment, which is putting front line health workers and carers at risk.

We're concerned about the levels of rumours and misinformation that are hampering the response.

And most of all, we're concerned about the potential havoc this virus could wreak in countries with weaker health systems.

The outbreaks of Ebola and COVID-19 underscore once again the vital importance for all countries to invest in preparedness and not panic.

Two years ago, WHO and the World Bank founded the Global Preparedness Monitoring Board, an independent body to assess the state of the world's readiness for a pandemic. My sister Gro Bruntland, the co-chair of the Board, is actually here.

Last year the board published its first report, which concluded the world remains badly prepared.

For too long, the world has operated on a cycle of panic and neglect. We throw money at an outbreak, and when it's over, we forget about it and do nothing to prevent the next one.

The world spends billions of dollars preparing for a terrorist attack, but relatively little preparing for the attack of a virus, which could be far more deadly and far more damaging economically, politically and socially.

This is frankly difficult to understand, and dangerously short-sighted.

===

Today, I have three requests for the international community.

First, we must use the window of opportunity we have to intensify our preparedness.

China has bought the world time. We don't know how much time.

All countries must be prepared for the arrival of cases, to treat patients with dignity and compassion, to prevent onward transmission, and to protect health workers.

WHO is working with manufacturers and distributors of personal protective equipment to ensure a reliable supply of the tools health workers need to do their job safely and effectively.

But we're not just fighting an epidemic; we're fighting an infodemic.

Fake news spreads faster and more easily than this virus, and is just as dangerous.

That's why we're also working with search and media companies like Facebook, Google, Pinterest, Tencent, Twitter, TikTok, YouTube and others to counter the spread of rumours and misinformation.

We call on all governments, companies and news organizations to work with us to sound the appropriate level of alarm, without fanning the flames of hysteria.

Second, this is not a job for health ministers alone. It takes a whole-of-government approach.

But that approach must be coherent and coordinated, guided by evidence and public health priorities.

In many countries, measures have been taken by one part of government without appropriate consultation with the health ministry, or consideration of the impact of these measures.

Now more than ever is the time for us to let science and evidence lead policy.

If we don't, we are headed down a dark path that leads nowhere but division and disharmony.

And third, we must be guided by solidarity, not stigma. I repeat this: we must be guided by solidarity, not stigma.

The greatest enemy we face is not the virus itself; it's the stigma that turns us against each other. We must stop stigma and hate!

[Applause]

Much has been written and said about my praise for China.

I have given credit where it's due, and I will continue to do that, as I would and I did for any country that fights an outbreak aggressively at its source to protect its own people and the people of the world, even at great cost to itself.

It's easy to blame. It's easy to politicize. It's harder to tackle a problem together, and find solutions together.

We will all learn lessons from this outbreak. But now is not the time for recriminations or politicization.

We have a choice. Can we come together to face a common and dangerous enemy? Or will we allow fear, suspicion and irrationality to distract and divide us?

In our fractured and divided world, health is one of the few areas in which international cooperation offers the opportunity for countries to work together for a common cause.

This is a time for facts, not fear.

This is a time for rationality, not rumours.

This is a time for solidarity, not stigma.

I thank you.


Subscribe to the WHO newsletter →

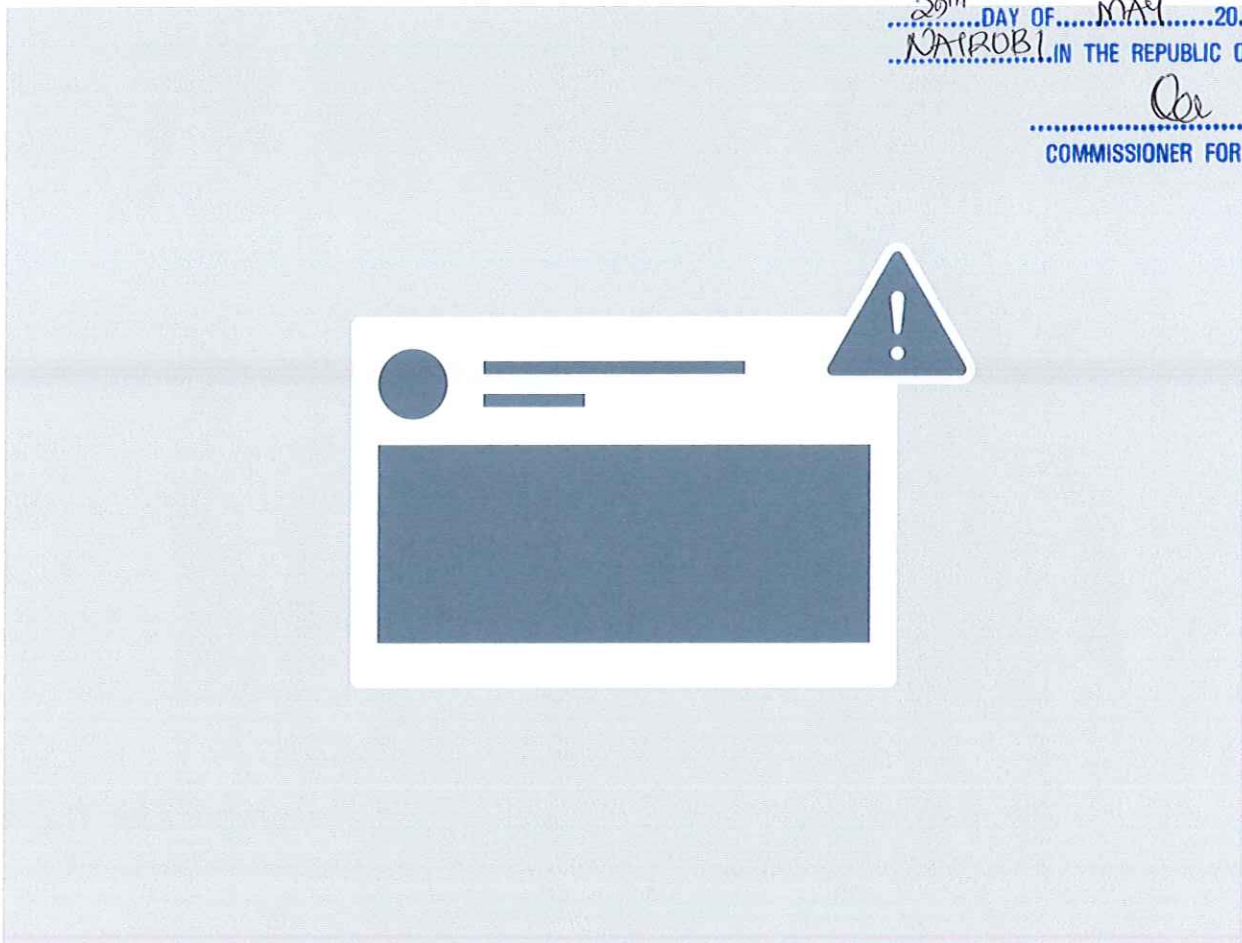
Facebook

Combating COVID-19 Misinformation Across Our Apps

March 25, 2020

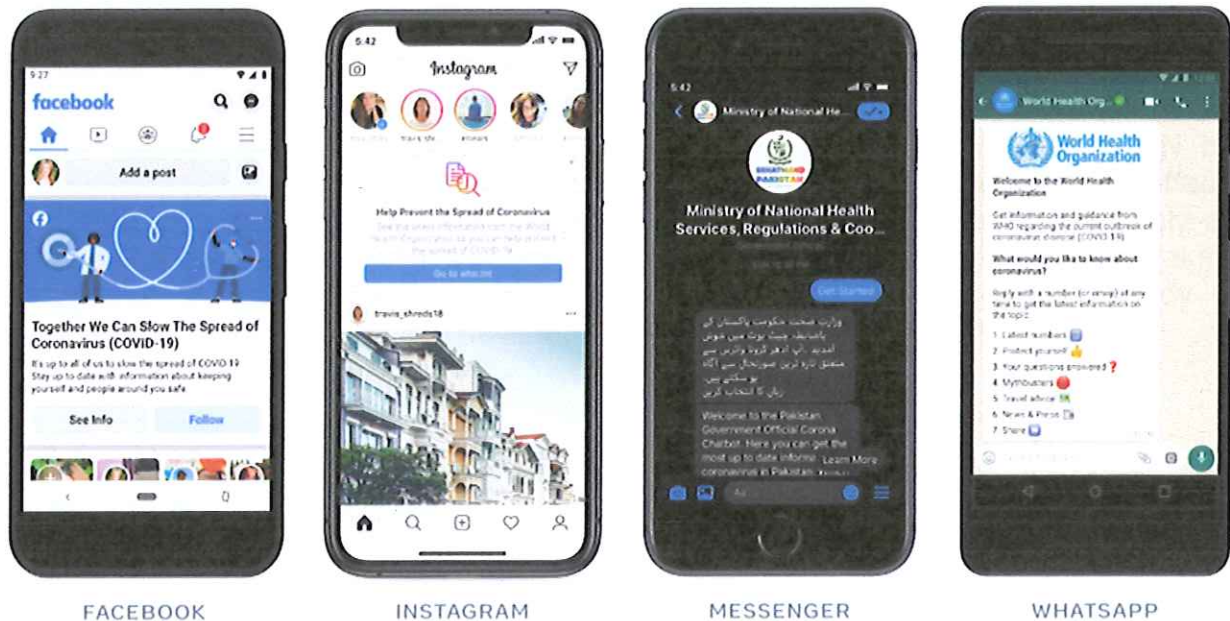
By Nick Clegg, VP of Global Affairs and Communications

THIS IS THE EXHIBIT MARKED "HNm-02"
REFERRED TO IN THE ANNEXED AFFIDAVIT
/DECLARATION OF HILARY NZIGI MUTAMBAI
SWORN/DECLARED BEFORE ME ON THIS
20th DAY OF MAY 2020 AT
NAIROBI IN THE REPUBLIC OF KENYA

COMMISSIONER FOR OATHS



Ever since the World Health Organization (WHO) declared COVID-19 a global public health emergency, we've been working to connect people to accurate information and taking aggressive steps to stop misinformation and harmful content from spreading. Today we're sharing an update on these efforts across our apps.

Connecting People to Reliable Information



On Facebook and Instagram: In January, we started showing educational pop-ups connecting people to information from the WHO, the CDC and regional health authorities toward the top of News Feed in countries with reported person-to-person transmissions and in all countries when people search for COVID-19 related information. We show similar pop-ups at the top of Instagram Feed in the hardest hit countries and when anyone taps on a COVID-19 related hashtag.

Last week, we launched the COVID-19 Information Center, which is now featured at the top of News Feed on Facebook in several countries and includes real-time updates from national health authorities and global organizations, such as the WHO. The COVID-19 Information Center will be available globally soon.

Through these efforts across Facebook and Instagram, we've directed more than 1 billion people to resources from health authorities including the WHO – more than 100 million of whom clicked through to learn more.

We're also giving the WHO as many free ads as they need and millions in ad credits to other health authorities so they can reach people with timely messages.

On WhatsApp: People can sign up to receive the [WHO Health Alert](#) on WhatsApp, a daily report with the latest numbers of COVID-19 cases. It also includes tips on how to prevent the spread of the disease as well as answers to commonly asked questions that people can easily send to their friends and family. We're also working directly with health ministries in the UK, India, Indonesia, Singapore, Israel, South Africa and other countries

On WhatsApp and Messenger: We've built clear labels that show people when they have received a forwarded message, or chain message, so they know when they are receiving something that was not written by their immediate contacts. We've also set a limit on the number of times messages can be forwarded on WhatsApp to reduce the spread of viral messages, and we use advanced machine learning to identify and ban accounts engaged in mass messaging. Similarly, we'll soon begin testing stricter limits on Messenger to control the number of chats someone can forward a message to at one time.

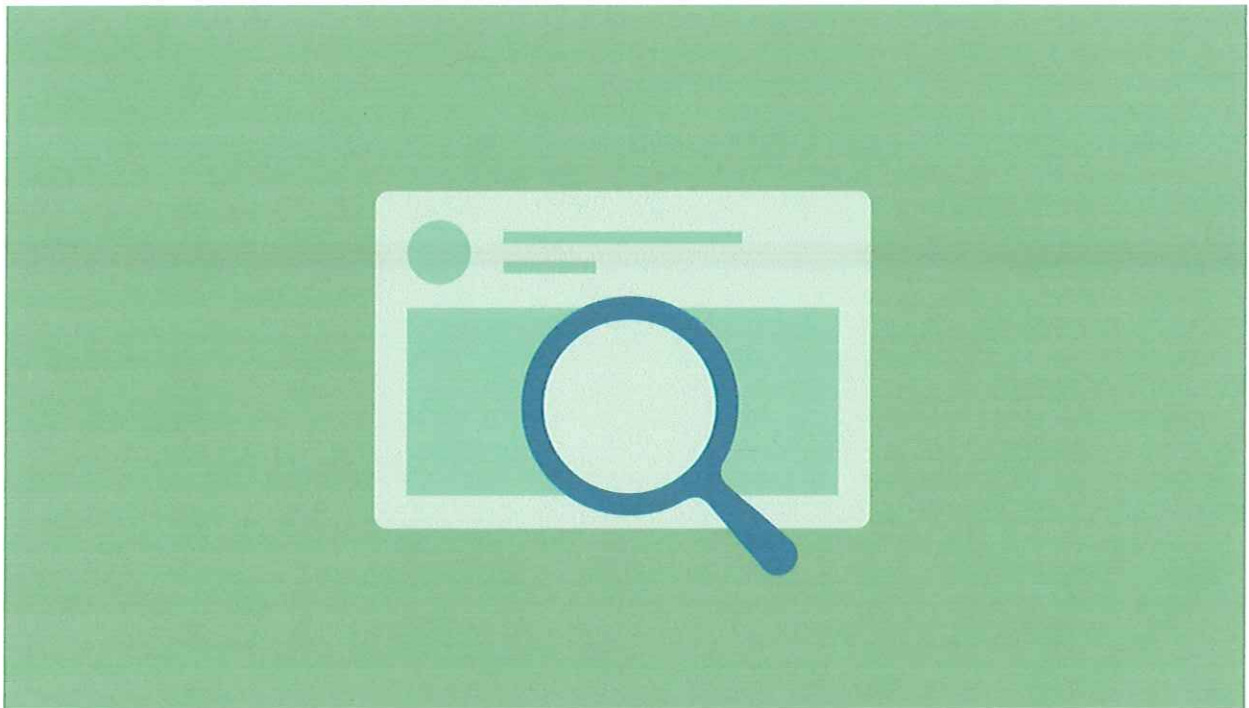
This is an evolving crisis, so as world health officials issue new guidance and warnings about COVID-19, we'll continue working with them to ensure people have access to accurate and authoritative information across all of our apps.

Facebook

An Update on Our Work to Keep People Informed and Limit Misinformation About COVID-19

April 16, 2020

By Guy Rosen, VP Integrity



Update on May 12, 2020 at 9:30AM PT: During the month of April, we put warning labels on about 50 million pieces of content related to COVID-19 on Facebook, based on around 7,500 articles by our independent fact-checking partners.

Ever since COVID-19 was declared a global public health emergency in January, we've been working to connect people to accurate information from health experts and keep harmful misinformation about COVID-19 from spreading on our apps.

We've now directed over 2 billion people to resources from the WHO and other health authorities through our COVID-19 Information Center and pop-ups on Facebook and Instagram with over 350 million people clicking through to learn more.

But connecting people to credible information is only half the challenge. Stopping the spread of misinformation and harmful content about COVID-19 on our apps is also critically important. That's why we work with over 60 fact-checking organizations that review and rate content in more than 50 languages around the world. In the past month, we've continued to grow our program to add more partners and languages. Since the beginning of March, we've added eight new partners and expanded our coverage to more than a dozen new countries. For example, we added MyGoPen in Taiwan, the AFP and dpa in the Netherlands, Reuters in the UK, and others.

To further support the work of our fact-checking partners during this time, we recently announced [the first round of recipients](#) of our \$1 million grant program in partnership with the International Fact-Checking Network. We've given grants to 13 fact-checking organizations around the world to support projects in Italy, Spain, Colombia, India, the Republic of Congo, and other nations. We will announce additional recipients in the coming weeks.

Once a piece of content is rated false by fact-checkers, we reduce its distribution and show warning labels with more context. Based on one fact-check, we're able to kick off similarity detection methods that identify duplicates of debunked stories. For example, during the month of March, we displayed warnings on about 40 million posts related to COVID-19 on Facebook, based on around 4,000 articles by our independent fact-checking partners. When people saw those warning labels, 95% of the time they did not go on to view the original content. To date, we've also removed hundreds of thousands of pieces of misinformation that could lead to imminent physical harm. Examples of misinformation we've removed include harmful claims like drinking bleach cures the virus and theories like physical distancing is ineffective in preventing the disease from spreading.

Today we're sharing some additional steps we're taking to combat COVID-19 related misinformation and make sure people have the accurate information they need to stay safe.

Informing People Who Interacted With Harmful COVID-19 Claims

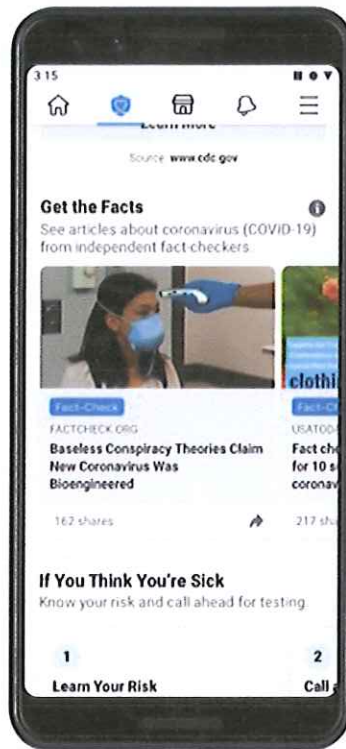
We're going to start showing messages in News Feed to people who have liked, reacted or commented on harmful misinformation about COVID-19 that we have since removed. These messages will connect people to COVID-19 myths [debunked by the WHO](#) including ones we've removed from our platform for leading to imminent physical harm. We want to connect people who may have interacted with harmful misinformation about the virus with the truth from authoritative sources in case they see or hear these

claims again off of Facebook. People will start seeing these messages in the coming weeks.



Making It Easier for People to Get the Facts

To make it easier for people to find accurate information about COVID-19, we recently added a new section to our COVID-19 Information Center called Get the Facts. It includes fact-checked articles from our partners that debunk misinformation about the coronavirus. The fact-check articles are selected by our News curation team and updated every week. This is now available in the US. We will soon add it to [Facebook News](#) in the US as well.



As this pandemic evolves, we'll continue focusing on the most effective ways to keep misinformation and dangerous hoaxes about COVID-19 off our apps and ensure people have credible information from health experts to stay safe and informed.



National Cyber
Security Centre
a part of GCHQ



CISA
CYBER+INFRASTRUCTURE

Advisory: COVID-19 exploited by malicious cyber actors

Version 1.0

8th April 2020

1 of 11
THIS IS THE EXHIBIT MARKED "HNM-03"
REFERRED TO IN THE ANNEXED AFFIDAVIT
/DECLARATION OF HILARY NZICKI MUTUAMBA
SWORN/DECLARED BEFORE ME ON THIS
29th DAY OF MAY 2020 AT
NAIROBI IN THE REPUBLIC OF KENYA
COMMISSIONER FOR OATHS

This is a joint advisory from the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Introduction

This advisory provides information on exploitation by cyber criminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice.

COVID-19 exploitation

An increasing number of malicious cyber actors are exploiting the current COVID-19 pandemic for their own objectives. In the UK, the NCSC has detected more UK government branded scams relating to COVID-19 than any other subject. Although, from the data seen to date, the overall levels of cyber crime have not increased both the NCSC and CISA are seeing a growing use of COVID-19 related themes by malicious cyber actors. At the same time, the surge in home working has increased the use of potentially vulnerable services, such as Virtual Private Networks (VPNs), amplifying the threat to individuals and organisations.

APT groups and cyber criminals are targeting individuals, small and medium businesses and large organisations with COVID-19 related scams and phishing emails. This advisory provides you with an overview of COVID-19 related malicious cyber activity. It offers practical advice that individuals and organisations can follow to reduce the risk of being affected. The IOCs provided within the accompanying .csv and .stix files of this advisory are based on analysis from CISA, NCSC, and industry.

Note: this is a fast-moving situation and this advisory does not seek to catalogue all COVID-19 related malicious cyber activity. You should remain alert to increased activity relating to COVID-19 and take proactive steps to protect yourself and your organisation.

Summary of attacks

APT groups and cyber criminals are exploiting the COVID-19 pandemic as part of their cyber operations. These cyber threat actors will often masquerade as trusted entities. Their activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised. Their goals and targets are consistent with long-standing priorities such as espionage and information operations.

Cyber criminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware.

Both APT groups and cyber criminals are likely to continue to exploit the COVID-19 pandemic over the coming weeks and months. Threats observed include:

- Phishing, using the subject of coronavirus or COVID-19 as a lure
- Malware distribution using coronavirus or COVID-19 themed lures
- Registration of new domain names containing coronavirus or COVID-19 related wording
- Attacks against newly (and often rapidly) deployed remote access or remote working infrastructure.

Social engineering techniques

Malicious cyber actors rely on basic social engineering methods to entice a user to carry out a specific action. These actors are taking advantage of human traits such as curiosity and concern around the coronavirus pandemic in order to persuade potential victims to:

- Click on a link or download an app that may lead to a phishing website, or the downloading of malware, including ransomware.
 - For example, a malicious Android app purports to provide a real-time coronavirus outbreak tracker but instead attempts to trick the user into providing administrative access to install 'CovidLock' ransomware on their device.¹
- Open a file (such as an email attachment) which contains malware.
 - For example, email subject lines contain COVID-19 related phrases such as 'Coronavirus Update' or '2019-nCov: Coronavirus outbreak in your city (Emergency).'

To create the impression of authenticity, malicious cyber actors may spoof sender information in an email to make it appear to come from a trustworthy source, such as the World Health Organization (WHO) or an individual with 'Dr.' in their title. In several examples, actors send phishing emails that contain links to a fake email login page. Other examples purport to be from an organisation's human resources (HR) department and advise the employee to open the attachment.

Malicious file attachments containing malware payloads may be named with coronavirus or COVID-19 related themes, such as "President discusses budget savings due to coronavirus with Cabinet.rtf."

Note: A non-exhaustive list of IOCs related to this activity is provided within the accompanying .csv and .stix files linked to this advisory.

¹ <https://www.techrepublic.com/article/covidlock-ransomware-exploits-coronavirus-with-malicious-android-app/>

Phishing

The NCSC and CISA have both observed a large volume of phishing campaigns which use the social engineering techniques described above.

Examples of phishing email subject lines include:

- 2020 Coronavirus Updates
- Coronavirus Updates
- 2019-nCov: New confirmed cases in your City
- 2019-nCov: Coronavirus outbreak in your city (Emergency).

These emails will contain a call to action encouraging the victim to visit a URL that malicious cyber actors use for stealing valuable data, such as usernames and passwords, credit card information and other personal information.

SMS Phishing

Most phishing attempts come by email but the NCSC and CISA have observed some attempts to carry out phishing by other means, including text messages (SMS).

Historically, SMS phishing has often used financial incentives, including government payments and rebates (such as a tax rebate) as part of the lure. Coronavirus-related phishing continues this financial theme, particularly in light of the economic impact of the epidemic and governments' employment and financial support packages.

For example, a series of SMS messages uses a UK government themed lure to harvest email, address, name, and banking information. These SMS messages, purporting to be from 'COVID' and 'UKGOV,' (see figure 1) includes a link directly to the phishing site (see figure 2).

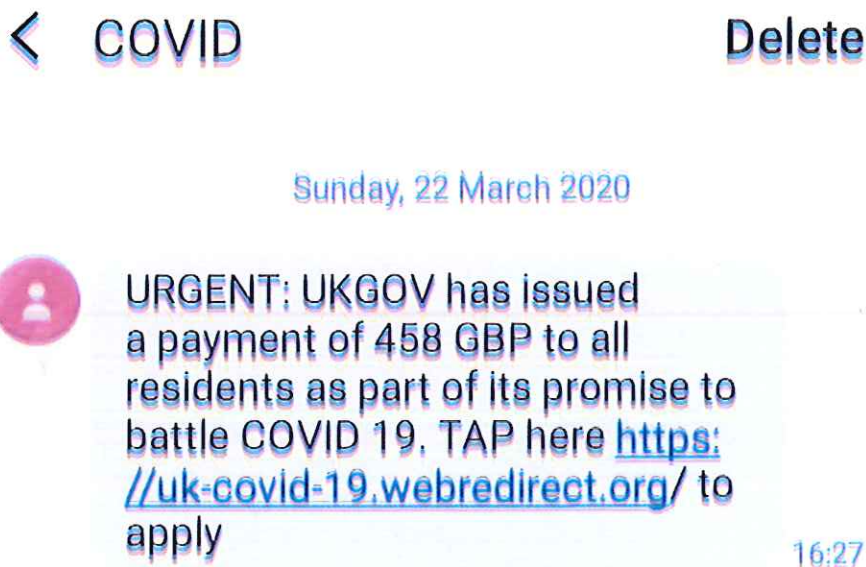


Figure 1 – UK Government themed SMS phishing

GOV.UK

Tell us what you think of GOV.UK
Take a short survey to give us your feedback

Home > Housing and local services > Council Tax

Enter Your Post Code To Apply for COVID-19 Relieve

NHS COVID-19 Relieve system.

Enter a postcode
For example SW1A 2AA

What you need to know

- Relieve coverage so far

Last updated: 20 March 2020

Is this page helpful? [Yes](#) [No](#) [Is there anything wrong with this page?](#)

Services and information	Departments and policy
Benefits Births, deaths, marriages and care Business and self-employed Childcare and nurseries	Education and learning Employing people Environment and countryside Housing and local services
	How government works Departments Worldwide Publications

Figure 2 - UK Government themed phishing page

As this example demonstrates, malicious messages can arrive by methods other than email. In addition to SMS, possible channels include WhatsApp and other messaging services. Malicious cyber actors are likely to continue using financial themes in their phishing campaigns. Specifically, it is likely that they will use new government compensation schemes responding to COVID-19 as themes in phishing campaigns.

Phishing for credential theft

A number of actors have used COVID-19 related phishing to steal user credentials. These emails will include previously mentioned COVID-19 social engineering techniques, sometimes complemented with urgent language to enhance the lure.

If the user clicks on the hyperlink, a spoofed login webpage appears which includes a password entry form. These spoofed login pages may relate to a wide array of online services including - but not limited to - email services provided by Google or Microsoft, or services accessed via government websites.

To further entice the recipient, the websites will often contain COVID-19 related wording within the URL (for example, 'corona-virus-business-update,' 'covid19-advisory' or 'cov19support'). These spoofed pages are designed to look legitimate or

accurately impersonate well-known websites. Often the only way to notice malicious intent is through observing the website URL. In some circumstances, malicious cyber actor specifically customise these spoofed login pages for the intended victim.

If the victim enters their password on the spoofed page, the attackers will be able to access the victim's online accounts such as their email inbox. This access can then be used to acquire personal or sensitive information, or to further disseminate phishing emails, using the victim's address book.

Phishing for malware deployment

A number of threat actors have used COVID-19 related lures to deploy malware. In most cases, actors craft an email that persuades the victim to open an attachment or download a malicious file from a linked web page. When they open the attachment the malware is executed, compromising the victim's device.

For example, the NCSC has observed various email distributed malware which deploys the Agent Tesla keylogger malware. The email appears to be sent from Dr Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization (WHO). This email campaign began on Thursday, March 19, 2020. Another similar campaign offers thermometers and face masks to fight the epidemic. The email purports to attach images of these medical products but instead contains a loader for Agent Tesla.

In other campaigns, emails included an Excel attachment (e.g. '8651 8-14-18.xls') or contained URLs linking to a landing page that – if clicked - redirects to download an Excel document such as 'EMR Letter.xls.' In both cases, the Excel file contains macros that, if enabled, execute an embedded dynamic-link library (DLL) to install the Get2 loader malware. Get2 loader has been observed loading the GraceWire Trojan.

The TrickBot malware has been used in a variety of COVID-19 related campaigns. In one example, emails target Italian users with a document purporting to be information related to COVID-19 (see figure 3). The document contains a malicious Macro which downloads a batch file (BAT) which launches JavaScript, which - in turn - pulls down the TrickBot binary, executing it on the system.

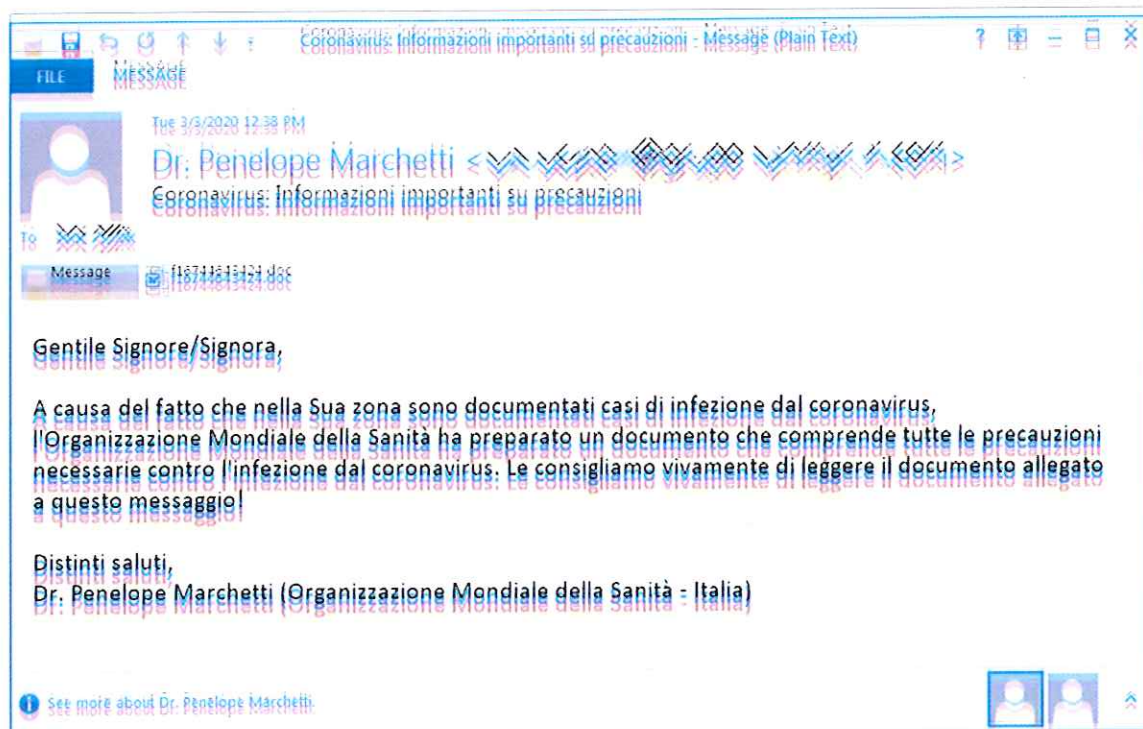


Figure 3 – Email containing malicious macro targeting Italian users²

In many cases, Trojans - such as Trickbot or GraceWire2 - will download further malicious files such as Remote Access Trojans (RATs), desktop-sharing clients and ransomware. In order to maximise the likelihood of payment, cyber criminals will often deploy ransomware at a time when organisations are under increased pressure. Hospitals and health organisations in the United States,³ Spain⁴ and across Europe⁵ have all been recently affected by ransomware incidents.

As always, you should be on the lookout for new and evolving lures. Both the NCSC⁶ and CISA^{7,8} provide guidance on mitigating malware and ransomware attacks.

Exploitation of new home working infrastructure

Many organisations have rapidly deployed new networks, including VPNs and related IT infrastructure, to cater for the large shift towards home working.

Malicious cyber actors are taking advantage of this on this mass move to home working by exploiting a variety of publicly known vulnerabilities in VPNs and other remote working tools and software. In several examples, the NCSC and CISA have

² <https://www.bleepingcomputer.com/news/security/trickbot-malware-targets-italy-in-fake-who-coronavirus-emails/>

³ <https://securityboulevard.com/2020/03/maze-ransomware-continues-to-hit-healthcare-units-amid-coronavirus-covid-19-outbreak/>

⁴ <https://www.computing.co.uk/news/4012969/hospitals-coronavirus-ransomware>

⁵ <https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/>

⁶ <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>

⁷ <https://www.us-cert.gov/ncas/tips/ST18-271>

⁸ <https://www.us-cert.gov/Ransomware>

observed actors scanning for publicly known vulnerabilities in Citrix. Citrix vulnerability (CVE-2019-19781) and its exploitation has been widely reported online, since early January 2020. Both the NCSC⁹ and CISA¹⁰ provide guidance on CVE-2019-19781 and continue to investigate multiple instances of this vulnerability's exploitation.

Similarly known vulnerabilities affecting VPN products from vendors Pulse Secure, Fortinet and Palo Alto continue to be exploited. CISA provides guidance on the Pulse Secure vulnerability¹¹ and the NCSC provides guidance on the vulnerabilities in Pulse Secure, Fortinet, and Palo Alto.¹²

Malicious cyber actors are also seeking to exploit the increased use of popular communications platforms (such as Zoom or Microsoft Teams) by sending phishing emails that include malicious files with names such as 'zoom-us-zoom_#####.exe' and 'microsoft-teams_V#mu#D_#####.exe' (# representing various digits that have been reported online).¹³ The NCSC and CISA have also observed phishing websites for a number of popular communication platforms. In addition, attackers have been able to hijack teleconference and online classrooms that have been set up without security controls (e.g. passwords) or with unpatched versions of the communications platform software.¹⁴

The surge in home working has also led to an increase in the use of Microsoft's Remote Desktop Protocol (RDP). Attacks on unsecured RDP endpoints (i.e. exposed to the internet) are widely reported online,¹⁵ and recent analysis¹⁶ has identified a 127% increase in exposed RDP endpoints. The increase in RDP use could potentially make IT systems, without the right security measures in place, more vulnerable to attack.¹⁷

Indicators of compromise

The NCSC and CISA are working with law enforcement and industry partners to disrupt or prevent these malicious COVID-19 themed cyber activities. We have published a non-exhaustive list of COVID-19 related IOCs via the following links:

- CSV file: https://www.us-cert.gov/sites/default/files/publications/AA20-099A_WHITE.csv
- Stix File: https://www.us-cert.gov/sites/default/files/publications/AA20-099A_WHITE.stix.xml

⁹ <https://www.ncsc.gov.uk/news/citrix-alert>

¹⁰ <https://www.us-cert.gov/ncas/alerts/aa20-031a>

¹¹ <https://www.us-cert.gov/ncas/alerts/aa20-010a>

¹² <https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities>

¹³ <https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/>

¹⁴ <https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic>

¹⁵ <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> and

¹⁶ <https://blog.reposify.com/127-increase-in-exposed-rdps-due-to-surge-in-remote-work>

¹⁷ <https://www.us-cert.gov/ncas/tips/ST18-001>

In addition, there are a number of useful resources online, which provide details of COVID-19 related malicious cyber activity:

- Recorded Futures' report, [Capitalizing on Corona Panic, Threat Actors Target](#)
- DomainTools' [Free COVID-19 Threat List – Domain Risk Assessments for Coronavirus Threats](#)
- GitHub list of [IOCs used in COVID-19 related cyberattack campaigns](#), gathered by GitHub user, Parth D. Maniar
- GitHub list of [Malware, spam, and phishing IOCs that involve the use of COVID-19 or coronavirus](#) gathered by SophosLabs
- Reddit master thread to collect [intelligence relevant to COVID-19 malicious cyber threat actor campaigns](#)
- Tweet regarding the MISP project's dedicated [#COVID2019 MISP instance](#) to share COVID-related cyber threat information

Conclusion

Malicious cyber actors are continually adjusting their tactics to take advantage of new situations, and the COVID-19 pandemic is no exception. Malicious cyber actors are using the high appetite for COVID-19 related information as an opportunity to deliver malware and ransomware and to steal user credentials. Individuals and organisations should remain vigilant. For genuine information about the virus, please use trusted resources such as the UK government website¹⁸, Public Health England¹⁹ or NHS websites²⁰.

Mitigating the risk

Following the NCSC and CISA advice set out below should help mitigate the risk to individuals and organisations from malicious cyber activity related to both COVID-19 and other themes:

- NCSC guidance for the public to help them spot, understand and deal with suspicious messages and emails: <https://www.ncsc.gov.uk/guidance/suspicious-email-actions>
- NCSC phishing guidance for organisations and cyber security professionals: <https://www.ncsc.gov.uk/guidance/phishing>
- NCSC guidance on mitigating malware and ransomware attacks: <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>
- NCSC guidance on home working: <https://www.ncsc.gov.uk/guidance/home-working>

¹⁸ <https://www.gov.uk/coronavirus>

¹⁹ <https://www.gov.uk/government/organisations/public-health-england>

²⁰ <https://www.nhs.uk/conditions/coronavirus-covid-19/>

- NCSC guidance on End User Device security: <https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/vpns>
- CISA guidance for defending against COVID-19 cyber scams: <https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams>
- CISA Insights: Risk Management for Novel Coronavirus (COVID-19), which provides guidance for executives regarding physical, supply chain, and cybersecurity issues related to COVID-19: https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf
- CISA Alert (AA20-073A) on enterprise VPN security: <https://www.us-cert.gov/ncas/alerts/aa20-073a>
- CISA website providing a repository of the agency's publicly available COVID-19 guidance: <https://www.cisa.gov/coronavirus>

Phishing guidance for individuals

The NCSC's [suspicious email guidance](#) explains what to do if you've already clicked on a potentially malicious email, attachment or link. It provides advice on who to contact if your account or device has been compromised and some of the mitigation steps you can take (such as changing your passwords). It also offers NCSC's top tips for spotting a phishing email:

- **Authority** - Is the sender claiming to be from someone official (like your bank, doctor, a solicitor, government department)? Criminals often pretend to be important people or organisations to trick you into doing what they want.
- **Urgency** - Are you told you have a limited time to respond (like in 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.
- **Emotion** - Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.
- **Scarcity** - Is the message offering something in short supply (like concert tickets, money or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.

Phishing guidance for organisations and cyber security professionals

Organisational defences against phishing often rely exclusively on users being able to spot phishing emails. However, you should widen your defences to include more technical measures. This will improve your resilience against phishing attacks.

In addition to educating users on defending against these attacks, you should consider [NCSC's guidance for organisations](#) that splits the mitigations into four layers, on which you can build your defences:

1. Make it difficult for attackers to reach your users

2. Help users identify and report suspected phishing emails (see CISA Tips, [Using Caution with Email Attachments](#) and [Avoiding Social Engineering and Phishing Scams](#))
3. Protect your organisation from the effects of undetected phishing emails
4. Respond quickly to incidents

NCSC and CISA also recommend organisations plan for a percentage of phishing attacks to be successful. Planning for these incidents will help minimise the damage caused.

Communications platforms guidance for individuals and organisations

Due to COVID-19, an increasing number of organisations and individuals are turning to communications platforms (such as Zoom and Microsoft Teams) for online meetings. In turn, malicious cyber actors are hijacking online meetings that are not secured with passwords or that use unpatched software.

Tips for defending against online meeting hijacking (Source: FBI March 30, 2020 press release, [FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic](#)):

- Do not make meetings public. Instead, require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to meeting on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options. Change screensharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications.
- Ensure telework policies address requirements for physical and information security.

Disclaimers

This report draws on information derived from NCSC, CISA and industry sources. Any findings and recommendations made have not been provided with the intention of avoiding all risks, and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favouring by CISA.