How cybercriminals are taking advantage of COVID-19: Scams, fraud, and misinformation

digitalshadows.com/blog-and-research/how-cybercriminals-are-taking-advantage-of-covid-19-scams-fraud-misinformation/

March 12, 2020

In the wake of large-scale global events, cybercriminals are among the first to attempt to sow discord, spread disinformation, and seek financial gain. In February 2020, the World Health Organization (WHO) released an advisory warning of ongoing scams involving the ongoing outbreak of COVID-19, the disease caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) and informally referred to as “coronavirus”. These scams aim to exploit people’s fear and uncertainty concerning the disease’s spread.

These can be broadly split into the following three categories:

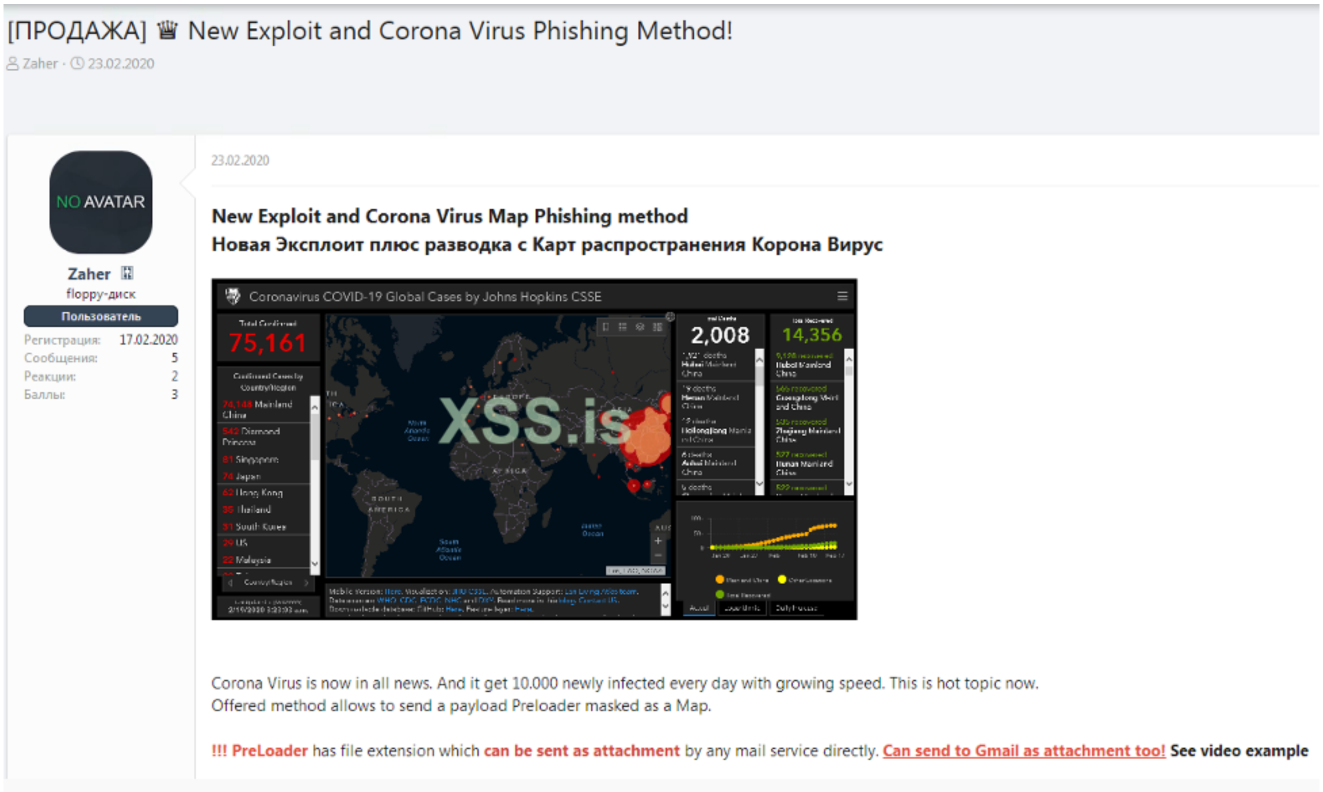
1. Phishing and social engineering scams
2. Sale of fraudulent or counterfeit goods
3. Misinformation

While COVID-19 itself presents a significant global security risk to individuals and organizations across the world, cybercriminal activity around this global pandemic can result in financial damage and promote dangerous guidance, ultimately putting additional strain on efforts to contain the virus.

COVID-19 phishing and social engineering scams

Phishing is one of, if not the single most common attack techniques. Reports of email phishing campaigns using COVID-19-related lures surfaced almost immediately after confirmed infections began increasing in January 2020. Health organizations such as the WHO and US Centers for Disease Control and Prevention (CDC) have been prime targets for impersonation due to their perceived authority: Attackers have been observed tempting victims with URLs or document downloads using promises of important safety documentation or infection maps.

COVID-19 has also been a popular topic of discussion on cybercriminal forums. For example, in February 2020, a user initiated a thread on the prestigious Russian-language cybercriminal forum XSS to advertise a new COVID-19-themed phishing scheme. The user advertised a method to deliver malware via an email attachment disguised as a distribution map of the virus’s outbreak, containing real-time data from the WHO. The map itself is an impersonation of a legitimate map created by the Johns Hopkins Center for Systems Science and Engineering (CSSE). The offering was priced at $200 for a “private build”, and if buyers also required a Java CodeSign certificate, the price would be $700.



[ПРОДАЖА] ♛ New Exploit and Corona Virus Phishing Method!

Zaher · 23.02.2020

NO AVATAR
Zaher
floppy-диск
Пользователь

Регистрация:	17.02.2020
Сообщения:	5
Реакции:	2
Баллы:	3

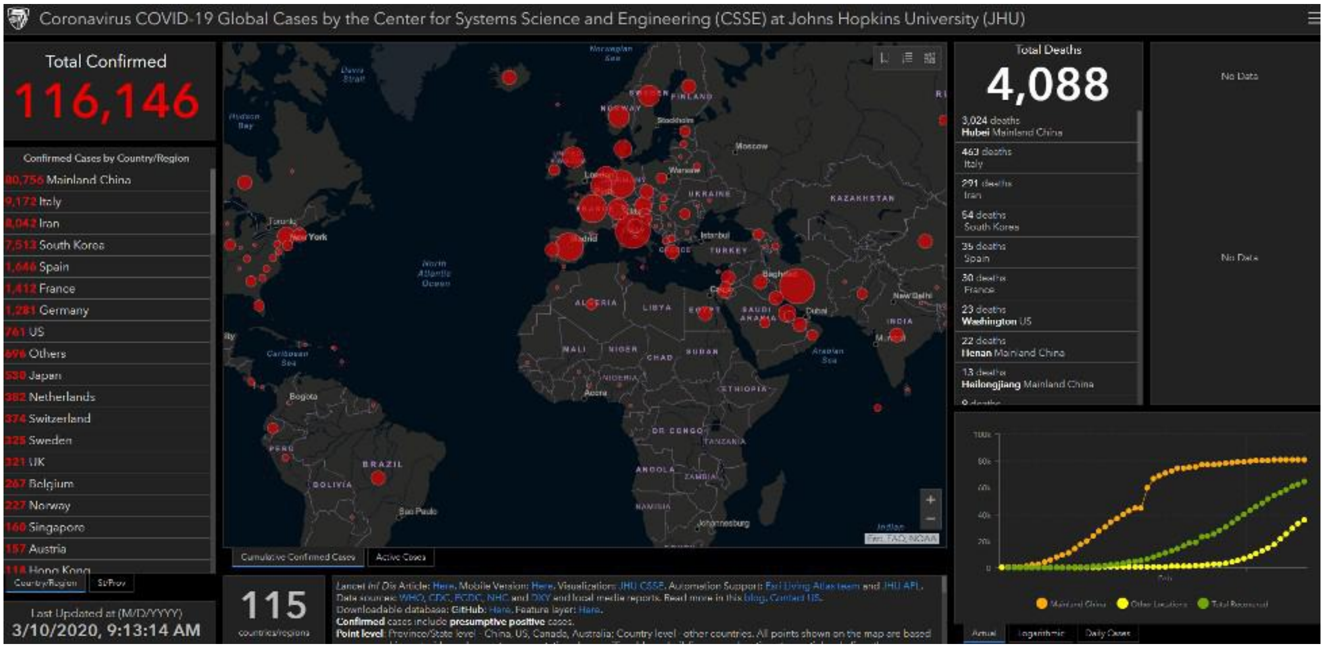
23.02.2020

New Exploit and Corona Virus Map Phishing method
Новая Эксплоит плюс разводка с Карт распространения Корона Вирус

Corona Virus is now in all news. And it get 10.000 newly infected every day with growing speed. This is hot topic now.
Offered method allows to send a payload Preloader masked as a Map.

!!! PreLoader has file extension which **can be sent as attachment** by any mail service directly. **Can send to Gmail as attachment too!** **See video example**

XSS post on COVID-19-related phishing scam



Coronavirus COVID-19 Global Cases by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)

Total Confirmed
116,146

Confirmed Cases by Country/Region

80,756	Mainland China
9,172	Italy
8,042	Iran
7,513	South Korea
1,646	Spain
1,412	France
1,281	Germany
761	US
696	Others
530	Japan
382	Netherlands
374	Switzerland
325	Sweden
321	UK
267	Belgium
227	Norway
160	Singapore
157	Austria
118	Hong Kong

Last Updated at (M/D/YYYY)
3/10/2020, 9:13:14 AM

115
countries/regions

Total Deaths
4,088

3,024 deaths
Hubei Mainland China
463 deaths
Italy
291 deaths
Iran
54 deaths
South Korea
35 deaths
Spain
30 deaths
France
23 deaths
Washington US
22 deaths
Henan Mainland China
13 deaths
Heilongjiang Mainland China

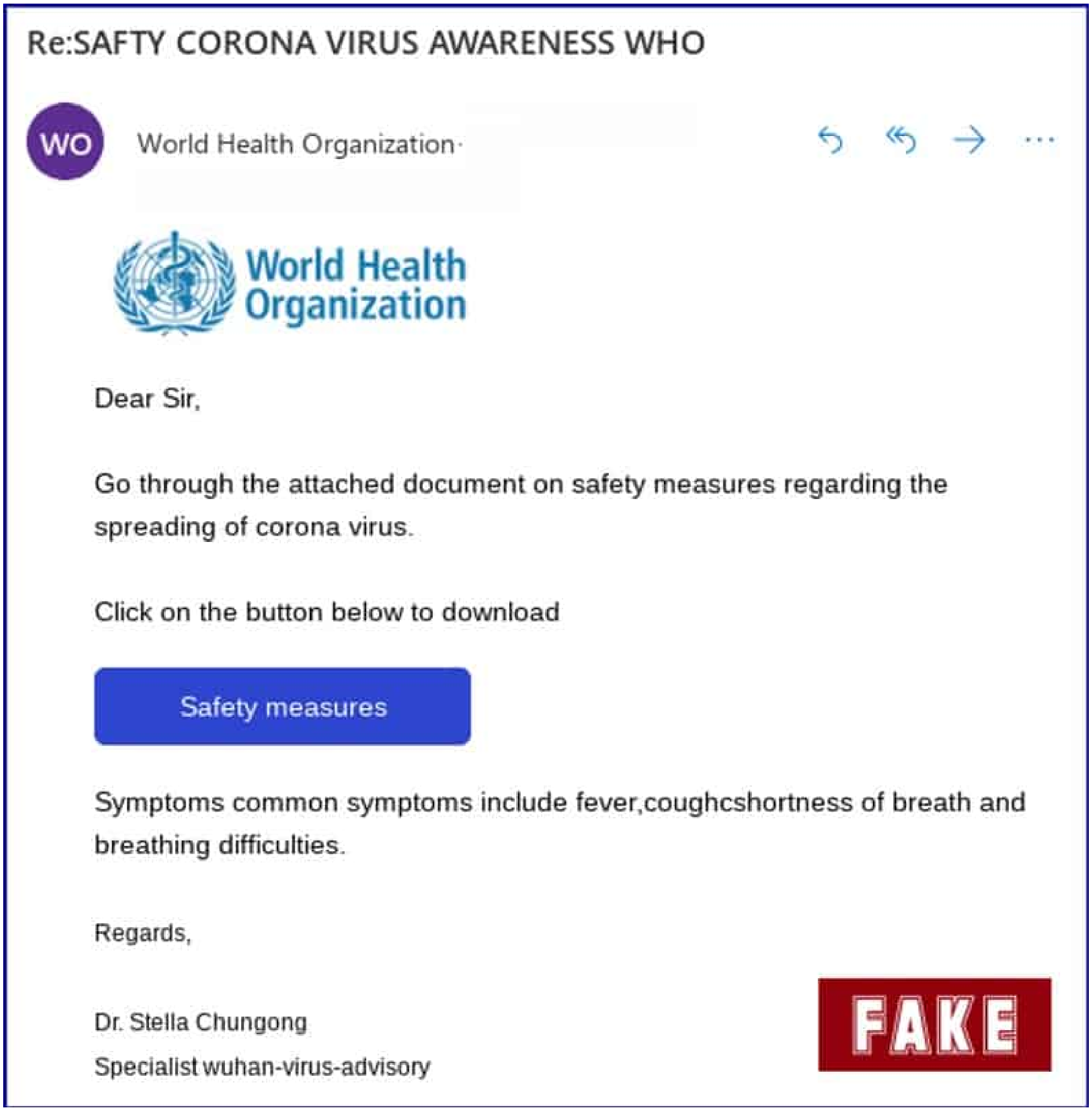
No Data

No Data

Lancet Inf Dis Article: Here. Mobile Version: Here. Visualization: JHU CSSE. Automation Support: Esri Living Atlas team and JHU APL.
Data sources: WHO, CDC, ECDC, NHC and DXY and local media reports. Read more in this blog. Contact US.
Downloadable database: GitHub: Here. Feature layer: Here.
Confirmed cases include **presumptive positive** cases.
Point level: Province/State level - China, US, Canada, Australia; Country level - other countries. All points shown on the map are based

Legitimate Johns Hopkins COVID-19 distribution map

Another phishing scam, as detailed by Sophos, impersonated an official email correspondence from the WHO. The email contained a link to purported document on preventing the spread of the virus, but redirected victims to a malicious domain which attempted to harvest credentials. The email contained several grammatical and format errors, which can be used by attackers to narrow down their victims and bypass spam filters. We discussed this technique in our blog on The Ecosystem of Phishing.



Re:SAFTY CORONA VIRUS AWARENESS WHO

WO World Health Organization·

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

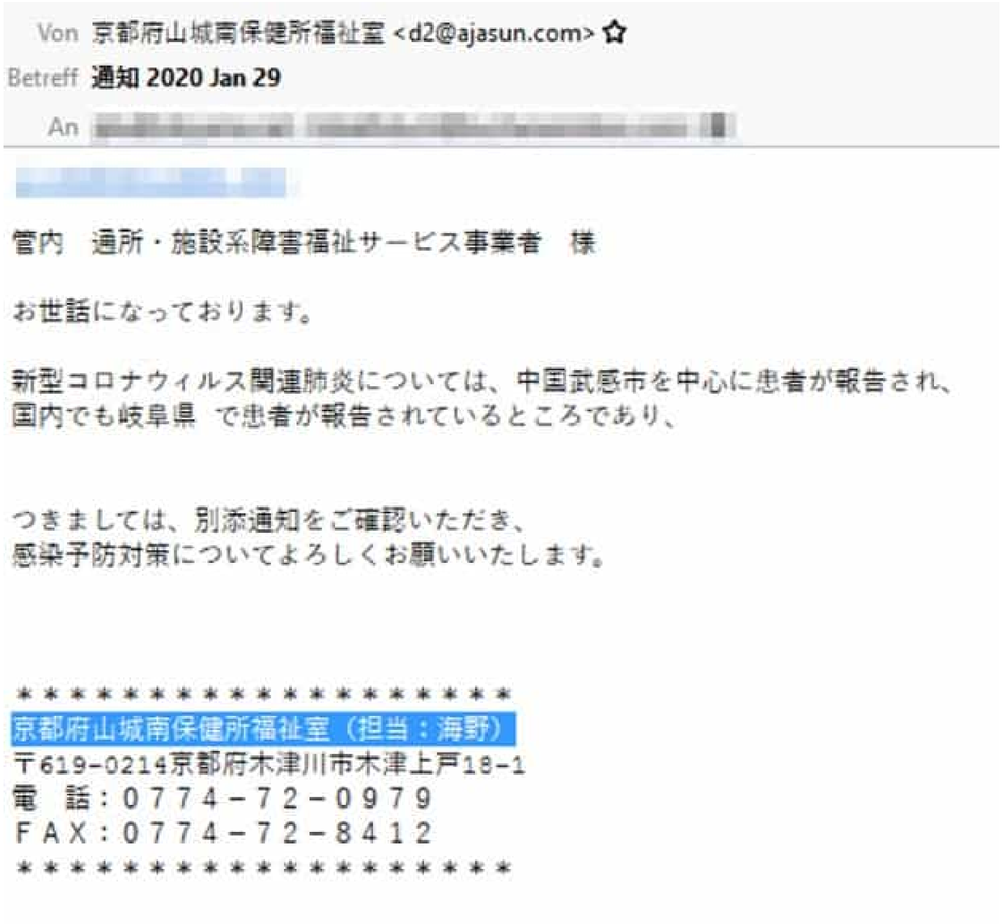
Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

Phishing scam impersonating the WHO (Source: Sophos)

These campaigns are often targeted towards geographies which have significant numbers of COVID-19 infections. In late January 2020, a phishing campaign targeted individuals in Japan with emails claiming to be from disability welfare service providers and public health centers. The emails used lures of documents containing information on alerts of new COVID-19 infections as well as preventative measures against the virus. However, when accessed, the documents attempted to download and install Emotet, an information stealing malware.

Similarly, individuals in Italy, which has the highest number of confirmed infections of COVID-19 outside of China, were targeted by a phishing campaign in March 2020 which impersonated WHO officials and attempted to distribute the Trickbot trojan.



Von 京都府山城南保健所福祉室 <d2@ajasun.com> ✩
Betreff **通知 2020 Jan 29**
An [redacted]

[redacted]

管内　通所・施設系障害福祉サービス事業者　様

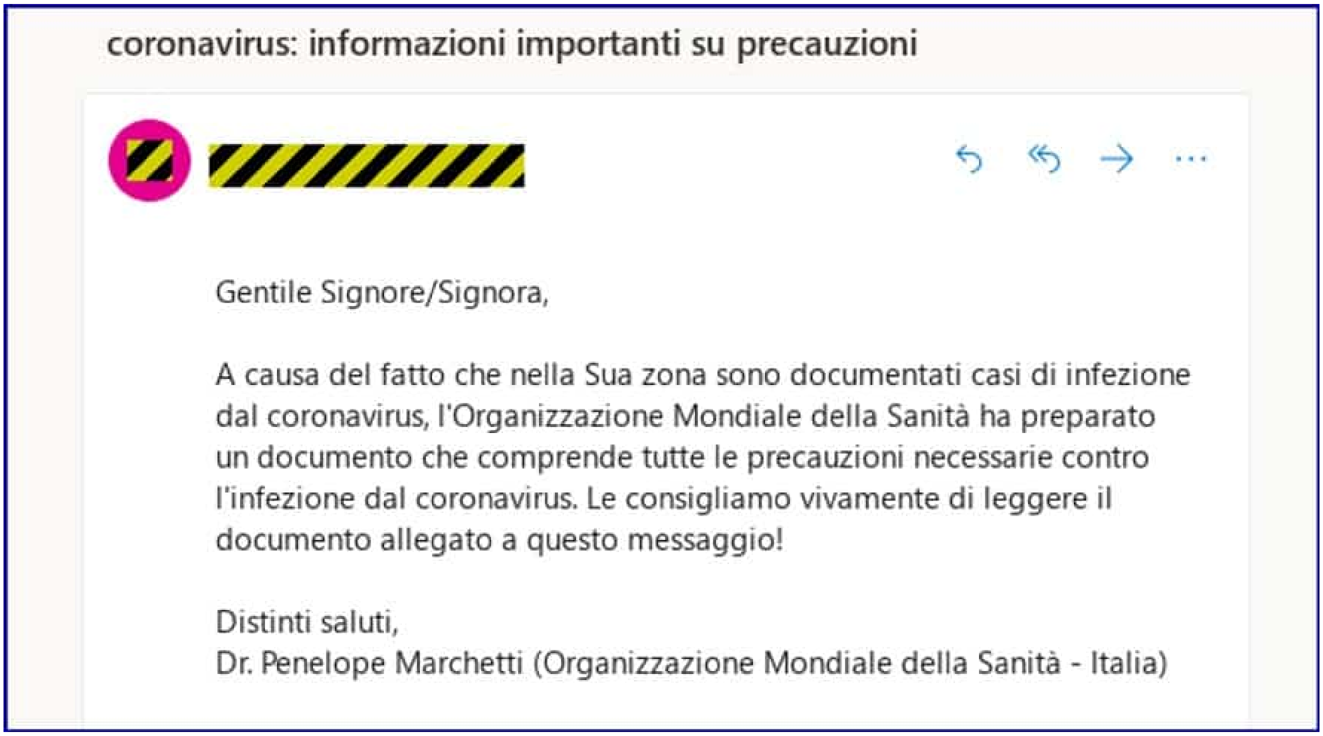
お世話になっております。

新型コロナウィルス関連肺炎については、中国武感市を中心に患者が報告され、
国内でも岐阜県　で患者が報告されているところであり、

つきましては、別添通知をご確認いただき、
感染予防対策についてよろしくお願いいたします。

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
京都府山城南保健所福祉室（担当：海野）
〒619-0214京都府木津川市木津上戸18-1
電　話：０７７４－７２－０９７９
ＦＡＸ：０７７４－７２－８４１２
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

Japanese-language phishing email (Source: IBM)



coronavirus: informazioni importanti su precauzioni

[redacted] [redacted]

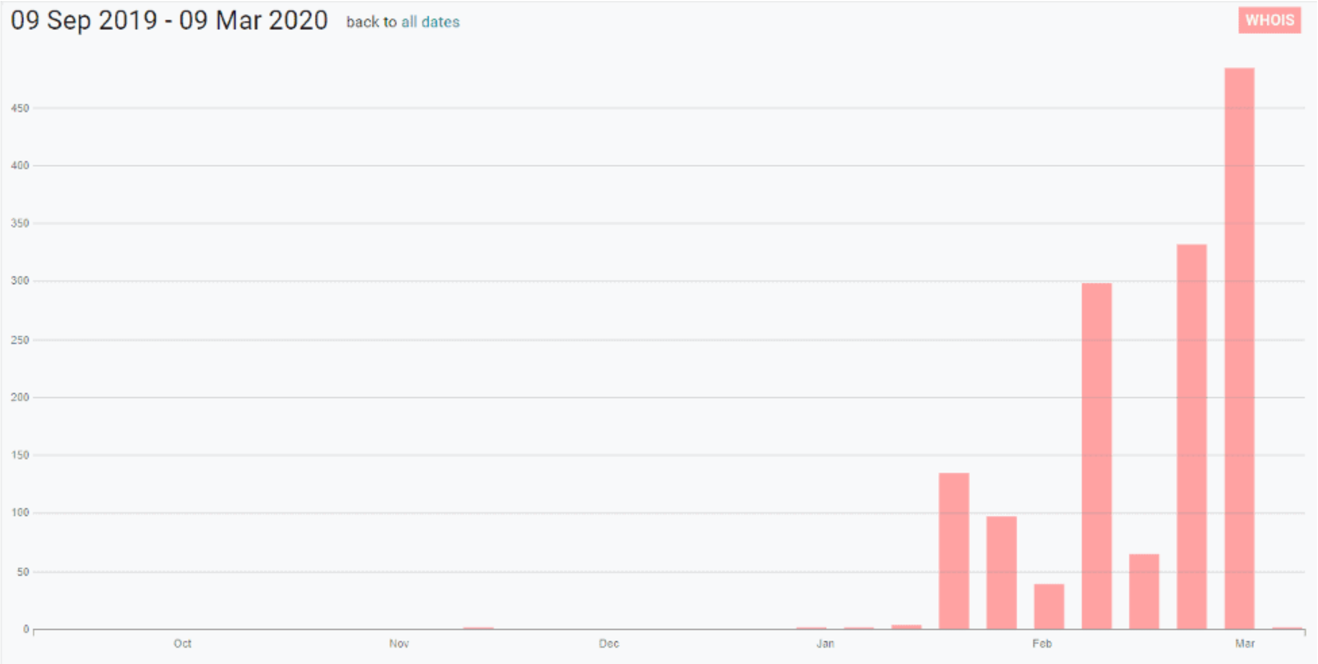
Gentile Signore/Signora,

A causa del fatto che nella Sua zona sono documentati casi di infezione dal coronavirus, l'Organizzazione Mondiale della Sanità ha preparato un documento che comprende tutte le precauzioni necessarie contro l'infezione dal coronavirus. Le consigliamo vivamente di leggere il documento allegato a questo messaggio!

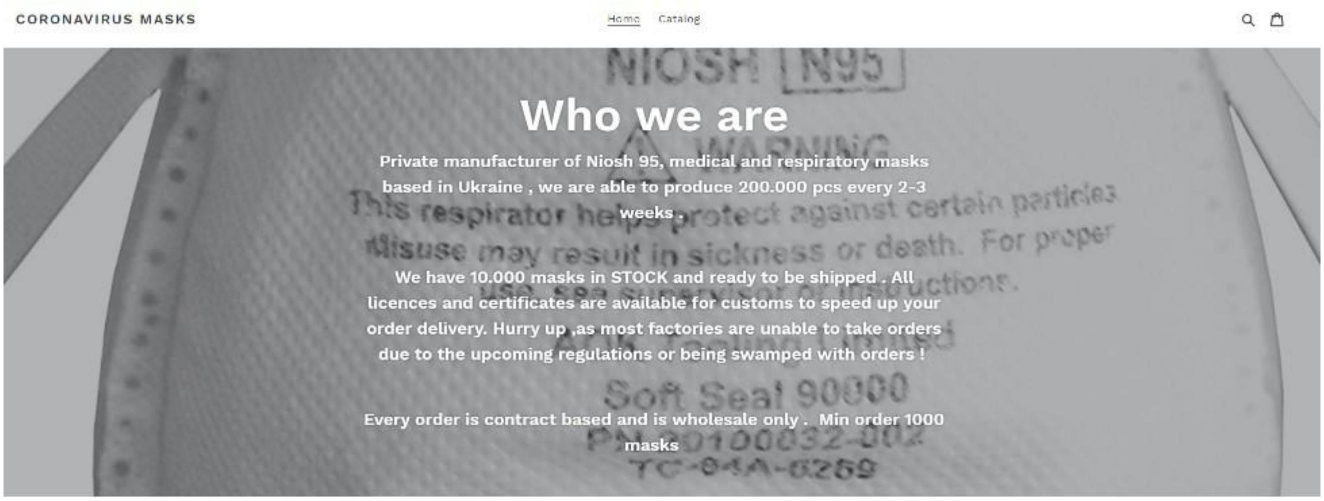
Distinti saluti,
Dr. Penelope Marchetti (Organizzazione Mondiale della Sanità - Italia)

Italian-language phishing email (Source: Sophos)

Organizations like the WHO or CDC are also not the only ones at risk of being impersonated. Since January 2020, the number of COVID-19-related domains registered has increased significantly: Digital Shadows has identified over 1,400 domains registered over the past three months. While many of these are likely legitimate and dedicated to providing information on the virus and its spread, it is almost certain that a portion have been created with malicious intent. Malicious domains can be used to spread misinformation, host phishing pages, impersonate legitimate brands, and sell fraudulent or counterfeit items. In March 2020, the UK's National Fraud Intelligence Bureau (NFIB) reported over 21 cases of COVID-19-related fraud schemes, resulting in losses of over £800,000 in the UK alone. The NFIB cited specific examples which included the fraudulent sale of face masks and sites which promised victims a map of COVID-19 infections near them in return for a bitcoin payment.



COVID-19-related domains registered over the past six months (Source: Digital Shadows' Shadow Search)



Who we are

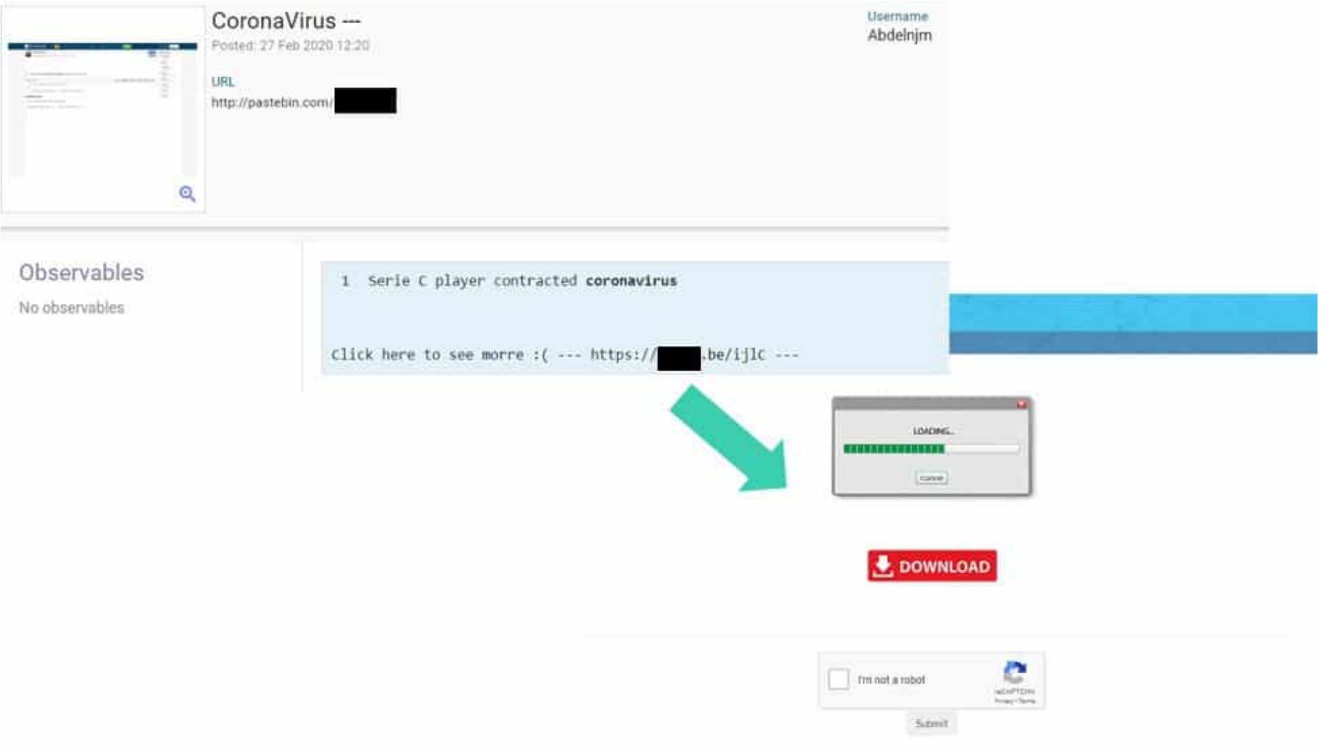
Private manufacturer of Niosh 95, medical and respiratory masks based in Ukraine , we are able to produce 200.000 pcs every 2-3 weeks .

We have 10.000 masks in STOCK and ready to be shipped . All licences and certificates are available for customs to speed up your order delivery. Hurry up ,as most factories are unable to take orders due to the upcoming regulations or being swamped with orders !

Every order is contract based and is wholesale only . Min order 1000 masks

Potentially fraudulent site offering discounted face masks

Even domains which contain no overt references to the virus have been identified. Below is an example on Pastebin that uses the lure of a purportedly infected Italian footballer to direct individuals to a malicious site.



CoronaVirus ---

Posted: 27 Feb 2020 12:20

URL

http://pastebin.com/[redacted]

Username

Abdelnjm

Observables

No observables

```
Serie C player contracted coronavirus


Click here to see morre :( --- https://[redacted].be/ijlC ---
```

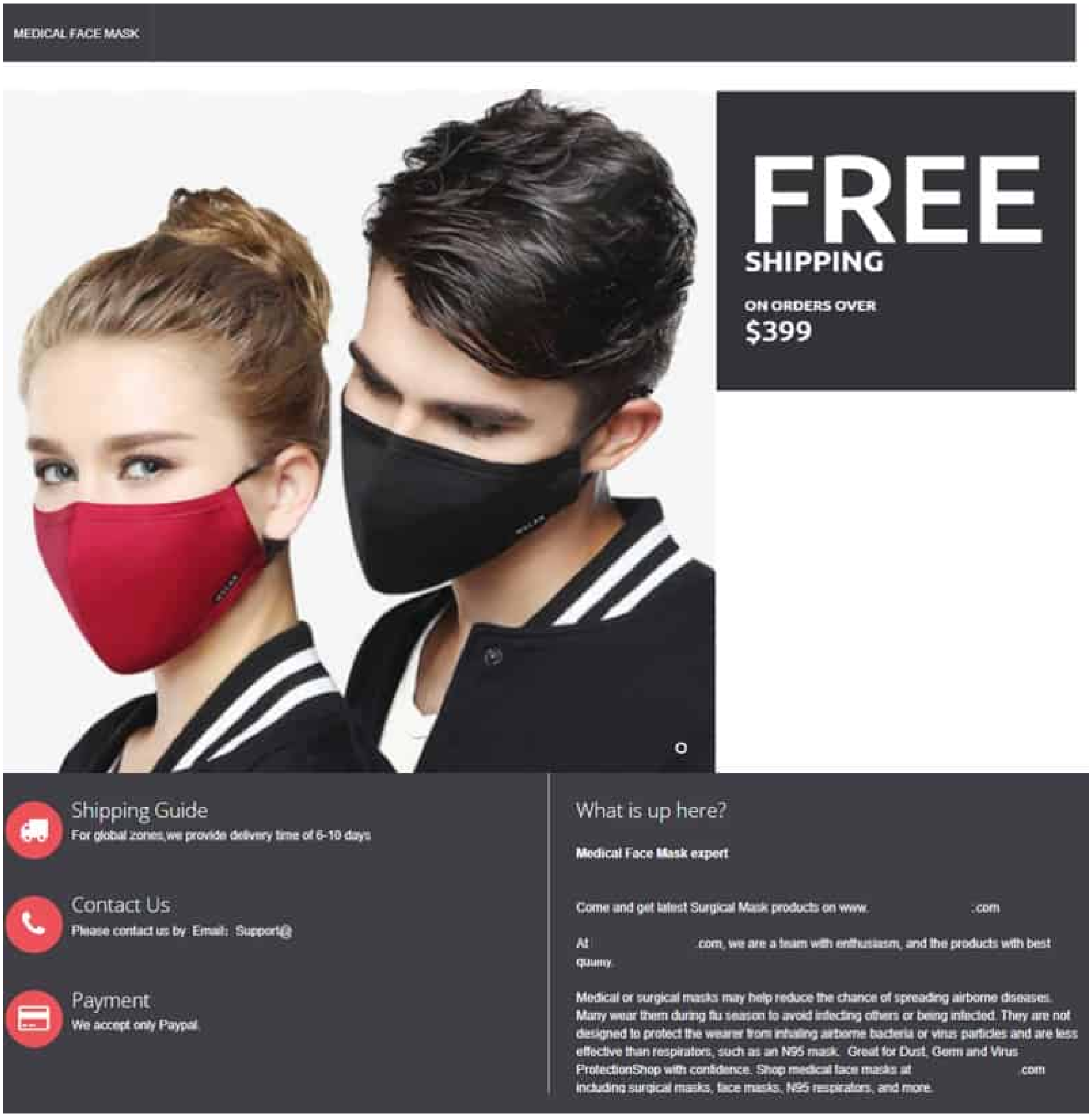
Pastebin post with a malicious COVID-19-related link (Source: Digital Shadows' Shadow Search)

COVID-19 fraudulent and counterfeit goods

The COVID-19 outbreak has contributed to a global shortage of healthcare equipment. Supplies like face masks and hand sanitizer have been out of stock at many major retailers, and prices on ecommerce websites have in some cases tripled over the past few weeks. This shortage is likely in part driven by the spread of misinformation. Face masks are essential for the safety of medical staff but have little effect on preventing healthy individuals from infection: The WHO recommends face masks should not be used unless caring for an individual with a suspected COVID-19 infection.

China is the world's largest global supplier of medical face masks, manufacturing approximately 80% of face masks worldwide. Due to the COVID-19 outbreak, production and exports from China have been severely limited over the past few months. This has put a strain on manufacturers outside of China, creating a market for counterfeit products and fraudulent listings.

As mentioned earlier, hundreds of potentially shady websites have popped up that claim to offer heavily discounted face masks. Even if the products are legitimate, there is no guarantee that the products even exist to begin with.



MEDICAL FACE MASK

FREE
SHIPPING
ON ORDERS OVER
$399

Shipping Guide
For global zones,we provide delivery time of 6-10 days

Contact Us
Please contact us by: Email: Support@

Payment
We accept only Paypal.

What is up here?

Medical Face Mask expert

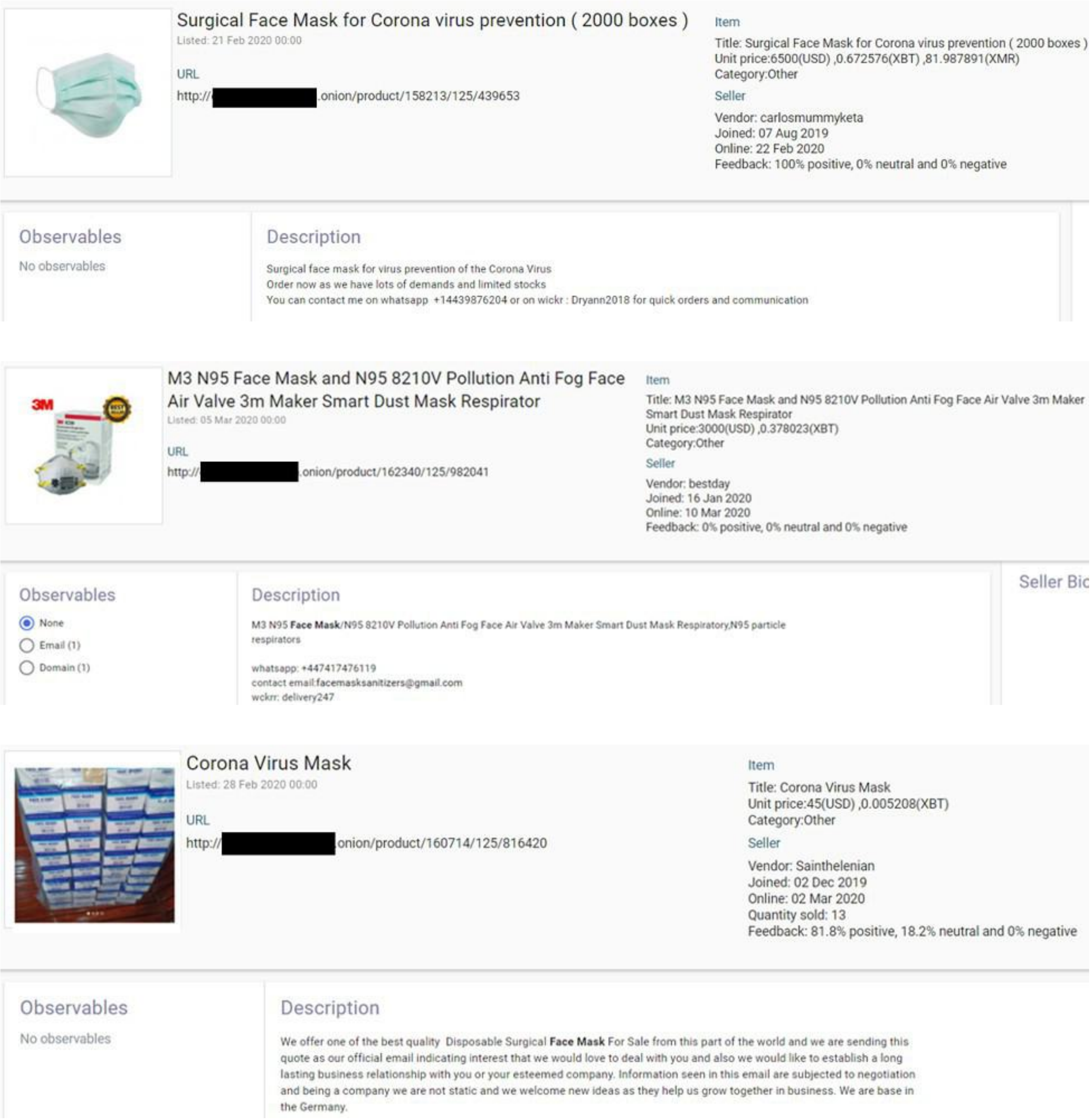
Come and get latest Surgical Mask products on www.[redacted].com

At [redacted].com, we are a team with enthusiasm, and the products with best quaity.

Medical or surgical masks may help reduce the chance of spreading airborne diseases. Many wear them during flu season to avoid infecting others or being infected. They are not designed to protect the wearer from inhaling airborne bacteria or virus particles and are less effective than respirators, such as an N95 mask. Great for Dust, Germ and Virus ProtectionShop with confidence. Shop medical face masks at [redacted].com including surgical masks, face masks, N95 respirators, and more.

Website selling discounted face masks

Medical equipment has even been observed for sale on cybercriminal marketplaces. Listings on Empire, an English-language dark web marketplaces, specifically mention COVID-19 to help push their goods. One listing offers 2,000 boxes of surgical face masks for $6,500. Vendors like these typically engage in the sale of illicit drugs, but have clearly seen a market opportunity to branch out into medical equipment.



Surgical Face Mask for Corona virus prevention (2000 boxes)

Listed: 21 Feb 2020 00:00

URL

http://[redacted].onion/product/158213/125/439653

Item

Title: Surgical Face Mask for Corona virus prevention (2000 boxes)
Unit price:6500(USD) ,0.672576(XBT) ,81.987891(XMR)
Category:Other

Seller

Vendor: carlosmummyketa
Joined: 07 Aug 2019
Online: 22 Feb 2020
Feedback: 100% positive, 0% neutral and 0% negative

Observables

No observables

Description

Surgical face mask for virus prevention of the Corona Virus
Order now as we have lots of demands and limited stocks
You can contact me on whatsapp +14439876204 or on wickr : Dryann2018 for quick orders and communication

M3 N95 Face Mask and N95 8210V Pollution Anti Fog Face Air Valve 3m Maker Smart Dust Mask Respirator

Listed: 05 Mar 2020 00:00

URL

http://[redacted].onion/product/162340/125/982041

Item

Title: M3 N95 Face Mask and N95 8210V Pollution Anti Fog Face Air Valve 3m Maker Smart Dust Mask Respirator
Unit price:3000(USD) ,0.378023(XBT)
Category:Other

Seller

Vendor: bestday
Joined: 16 Jan 2020
Online: 10 Mar 2020
Feedback: 0% positive, 0% neutral and 0% negative

Observables

● None
○ Email (1)
○ Domain (1)

Description

M3 N95 **Face Mask**/N95 8210V Pollution Anti Fog Face Air Valve 3m Maker Smart Dust Mask Respiratory,N95 particle respirators

whatsapp: +447417476119
contact email:facemasksanitizers@gmail.com
wckrr: delivery247

Seller Bic

Corona Virus Mask

Listed: 28 Feb 2020 00:00

URL

http://[redacted].onion/product/160714/125/816420

Item

Title: Corona Virus Mask
Unit price:45(USD) ,0.005208(XBT)
Category:Other

Seller

Vendor: Sainthelenian
Joined: 02 Dec 2019
Online: 02 Mar 2020
Quantity sold: 13
Feedback: 81.8% positive, 18.2% neutral and 0% negative

Observables

No observables

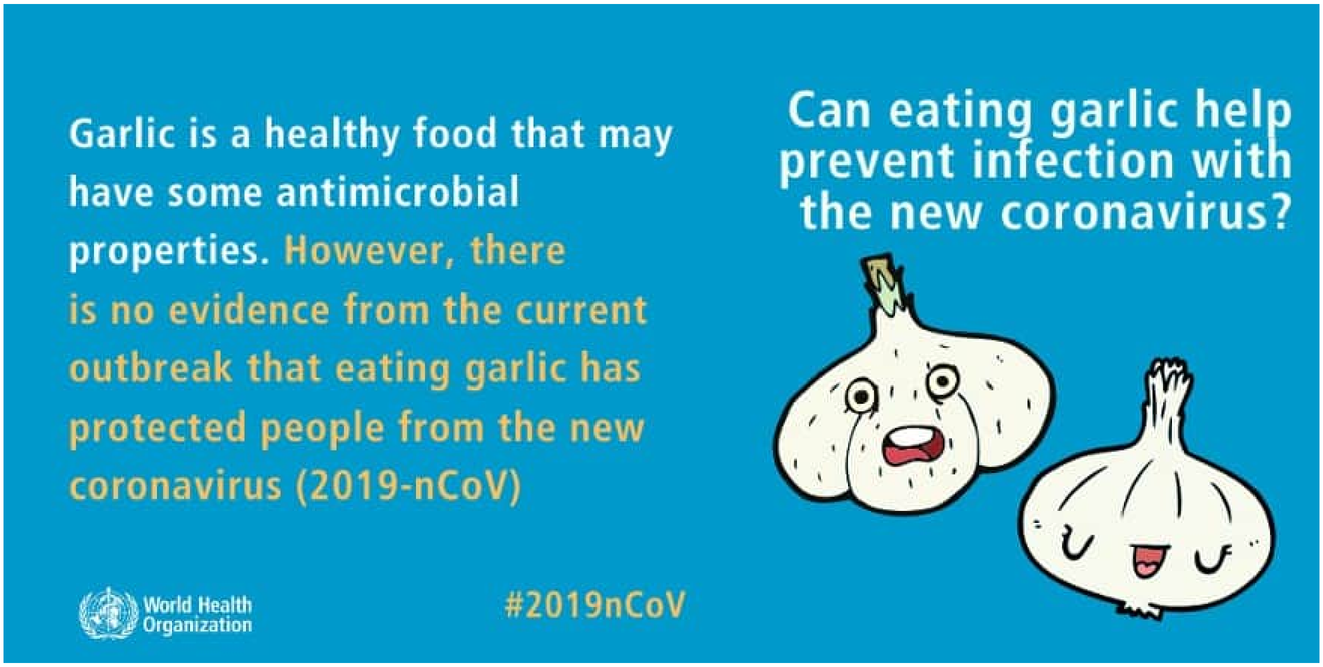
Description

We offer one of the best quality Disposable Surgical **Face Mask** For Sale from this part of the world and we are sending this quote as our official email indicating interest that we would love to deal with you and also we would like to establish a long lasting business relationship with you or your esteemed company. Information seen in this email are subjected to negotiation and being a company we are not static and we welcome new ideas as they help us grow together in business. We are base in the Germany.

Listings for face masks on Empire market (Source: Digital Shadows' Shadow Search)

COVID-19 misinformation / infodemic

COVID-19-related misinformation has primarily been spread via social media and private messaging platforms. Misinformation does not always have the same tangible financial impact as other types of cybercriminal activity, but it can still be used to cause panic, incite racism and xenophobia, promote harmful at-home cures, and result in shortages of supplies and critical medical equipment. The WHO has labelled this proliferation of information – both legitimate and not – as an "infodemic", and have assembled a dedicated team to manage the spread of potentially harmful misinformation.

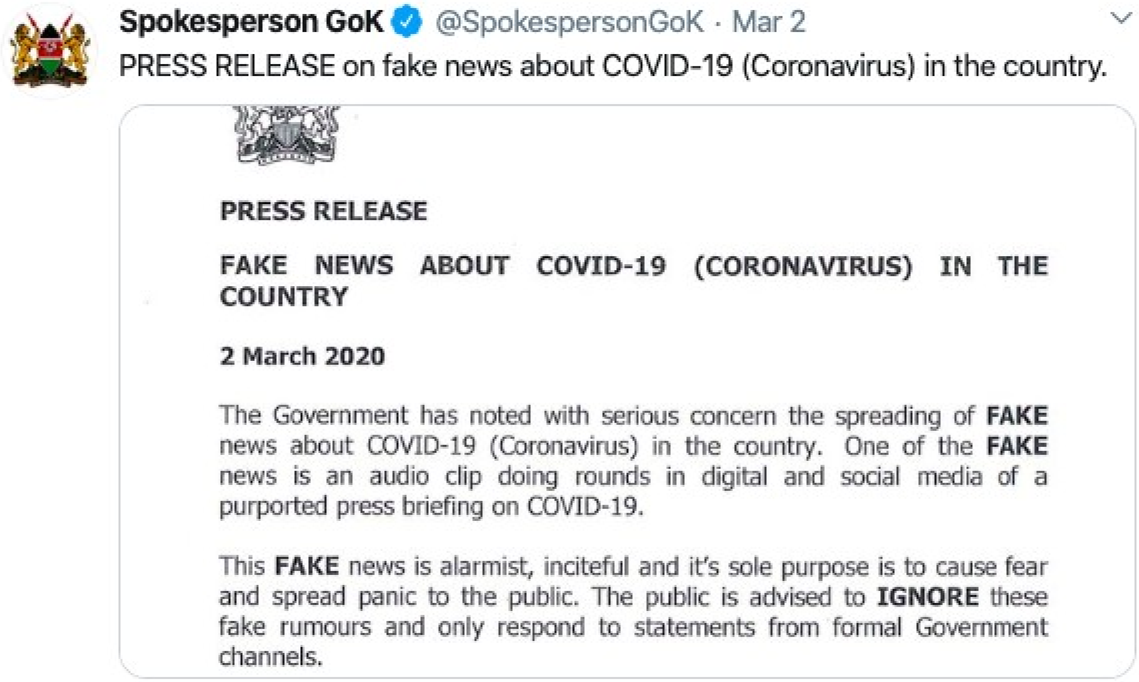


Garlic is a healthy food that may have some antimicrobial properties. However, there is no evidence from the current outbreak that eating garlic has protected people from the new coronavirus (2019-nCoV)

Can eating garlic help prevent infection with the new coronavirus?

WHO graphic debunking at-home cures (Source: WHO)

Official government entities have also taken steps to curb misinformation. Below is a tweet from the official account for the spokesperson of the Government of Kenya denouncing the spread of misinformation.



Spokesperson GoK @SpokespersonGoK · Mar 2

PRESS RELEASE on fake news about COVID-19 (Coronavirus) in the country.

PRESS RELEASE

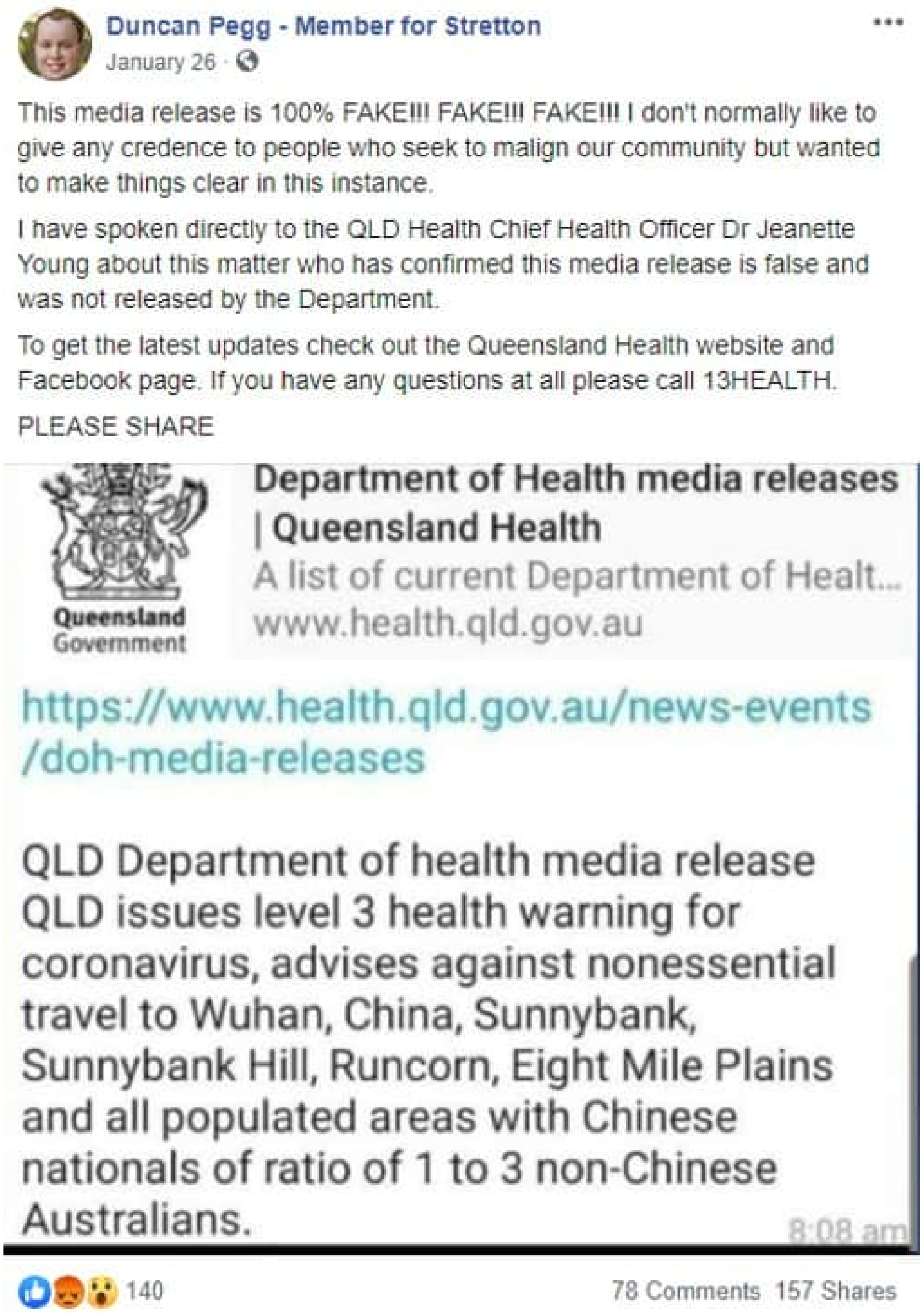
FAKE NEWS ABOUT COVID-19 (CORONAVIRUS) IN THE COUNTRY

2 March 2020

The Government has noted with serious concern the spreading of **FAKE** news about COVID-19 (Coronavirus) in the country. One of the **FAKE** news is an audio clip doing rounds in digital and social media of a purported press briefing on COVID-19.

This **FAKE** news is alarmist, inciteful and it's sole purpose is to cause fear and spread panic to the public. The public is advised to **IGNORE** these fake rumours and only respond to statements from formal Government channels.

Additionally, an Australian Member of Parliament also denounced a fraudulent social media post that was impersonating the Australian Department of Health, advising individuals to avoid areas populated with Chinese nationals.



Duncan Pegg - Member for Stretton

January 26 ·

This media release is 100% FAKE!!! FAKE!!! FAKE!!! I don't normally like to give any credence to people who seek to malign our community but wanted to make things clear in this instance.

I have spoken directly to the QLD Health Chief Health Officer Dr Jeanette Young about this matter who has confirmed this media release is false and was not released by the Department.

To get the latest updates check out the Queensland Health website and Facebook page. If you have any questions at all please call 13HEALTH.

PLEASE SHARE

Department of Health media releases | Queensland Health

A list of current Department of Healt...

www.health.qld.gov.au

https://www.health.qld.gov.au/news-events/doh-media-releases

QLD Department of health media release QLD issues level 3 health warning for coronavirus, advises against nonessential travel to Wuhan, China, Sunnybank, Sunnybank Hill, Runcorn, Eight Mile Plains and all populated areas with Chinese nationals of ratio of 1 to 3 non-Chinese Australians.

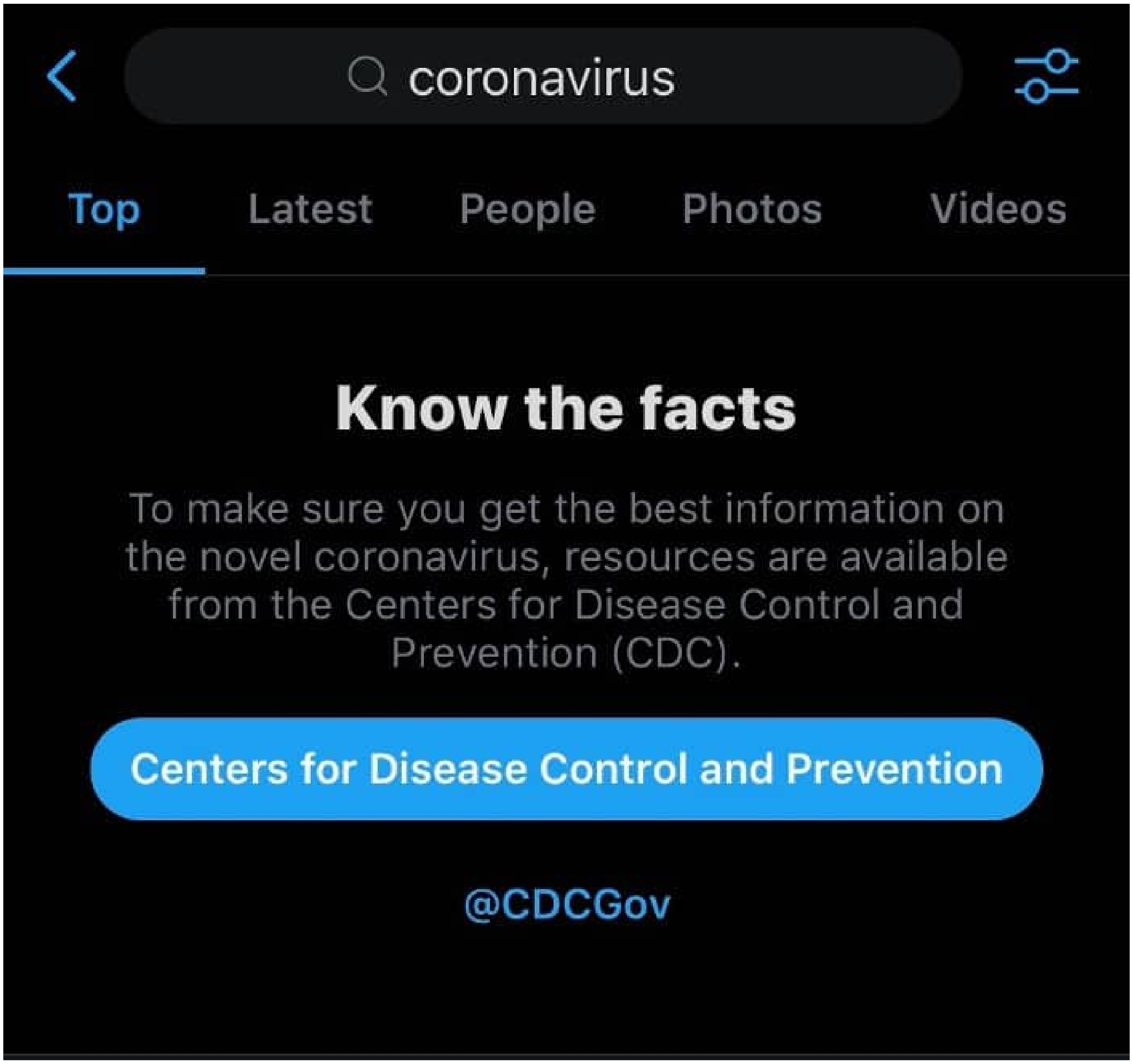
8:08 am

140

78 Comments 157 Shares

Australian MP denouncing the spread of misinformation

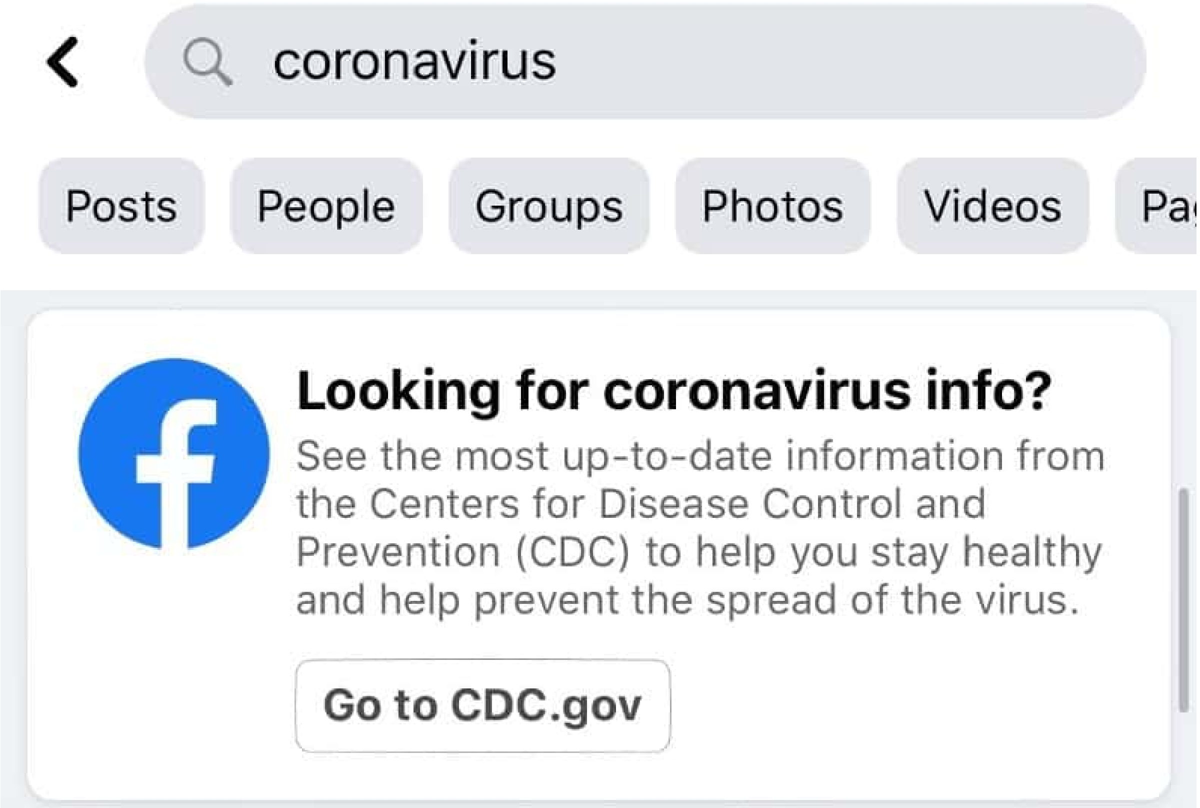
Social media platforms themselves have also taken a proactive approach to help prevent the spread of false information related to COVID-19 by flagging posts which may be illegitimate and hiring third-party organizations to fact-check posts. When searching COVID-19-related terms on platforms like Twitter, Facebook, and even Instagram, users are prompted to obtain information from official sources. This can even help streamline the dissemination of legitimate information by providing centralized results.



Know the facts

To make sure you get the best information on the novel coronavirus, resources are available from the Centers for Disease Control and Prevention (CDC).

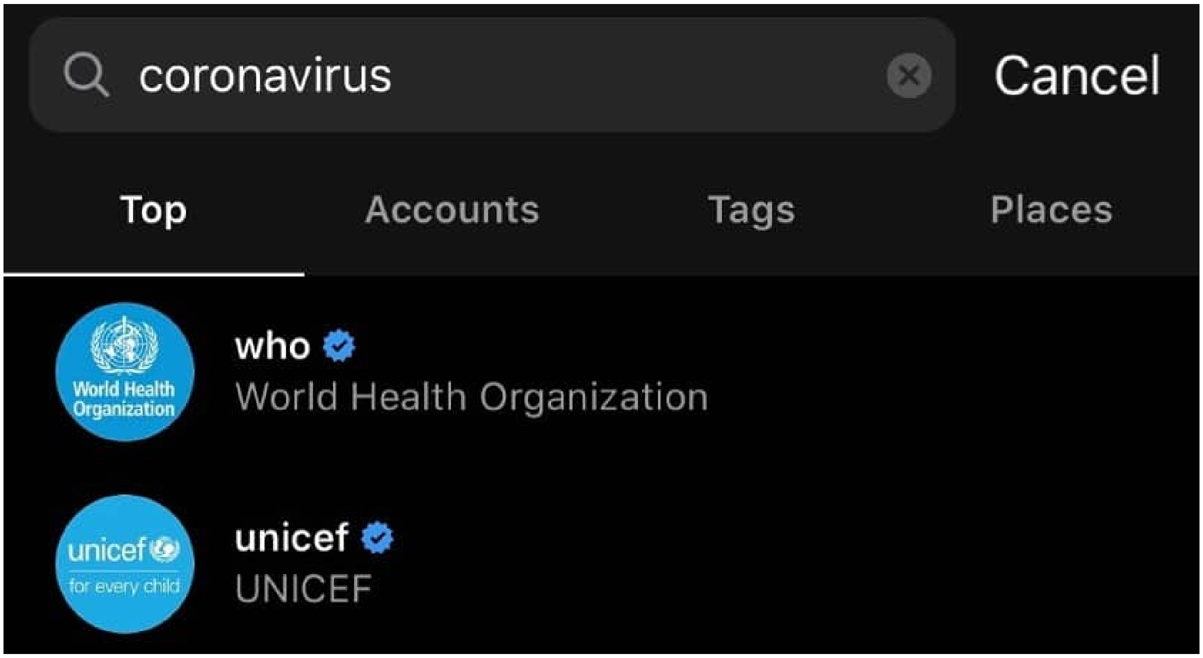
Twitter search directing users to the official CDC account



Looking for coronavirus info?

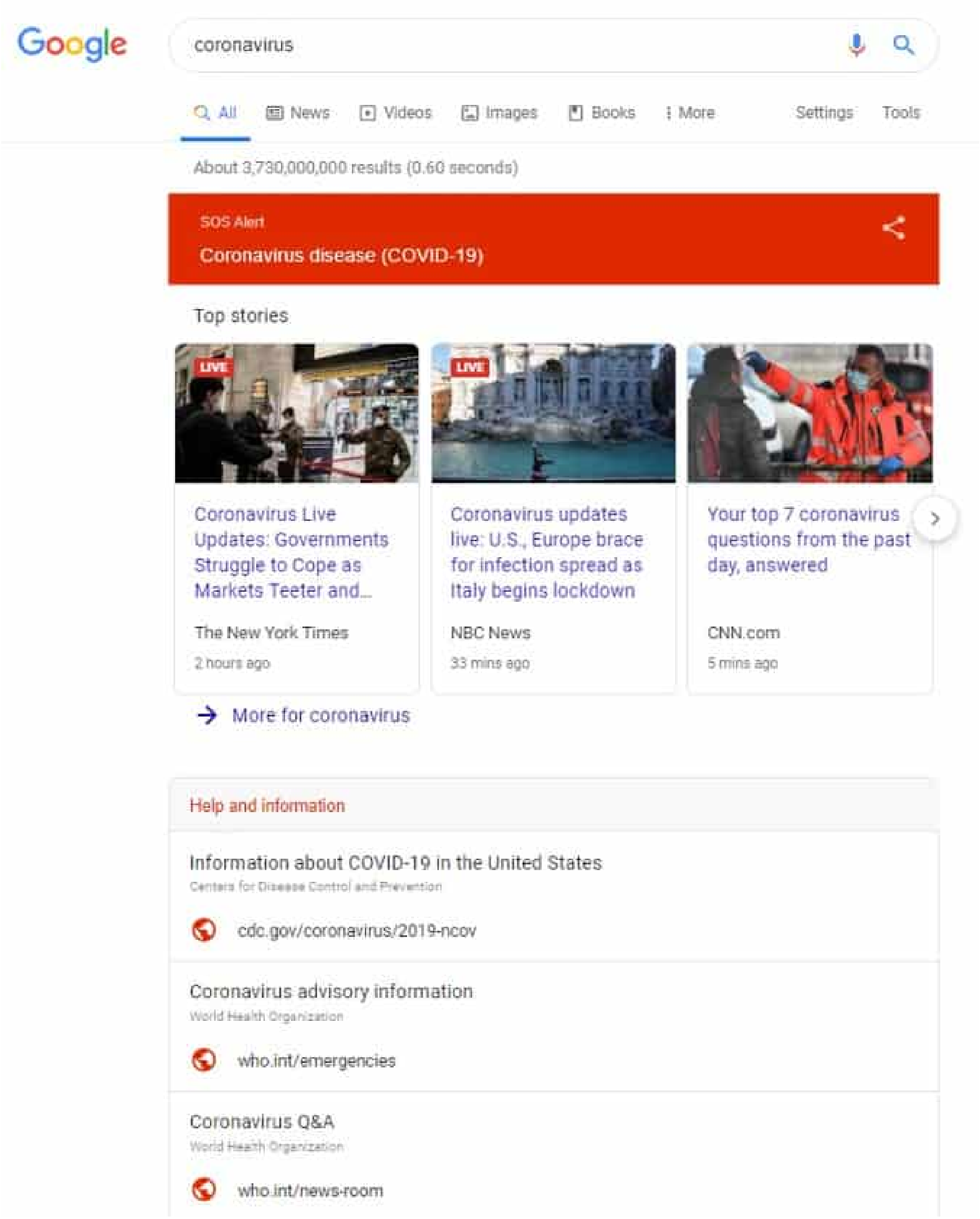
See the most up-to-date information from the Centers for Disease Control and Prevention (CDC) to help you stay healthy and help prevent the spread of the virus.

Facebook search directing users to the official CDC website



Instagram search directing users to the official WHO and UNICEF accounts

Search engines like Google have also manually intervened to help fight the spread of misinformation: When searching for COVID-19-related terms, users are provided an “SOS Alert”, which includes news articles from legitimate, vetted outlets and links to official resources from the CDC and WHO.



About 3,730,000,000 results (0.60 seconds)

SOS Alert

Coronavirus disease (COVID-19)

Top stories

Coronavirus Live Updates: Governments Struggle to Cope as Markets Teeter and...
The New York Times
2 hours ago

Coronavirus updates live: U.S., Europe brace for infection spread as Italy begins lockdown
NBC News
33 mins ago

Your top 7 coronavirus questions from the past day, answered
CNN.com
5 mins ago

More for coronavirus

Help and information

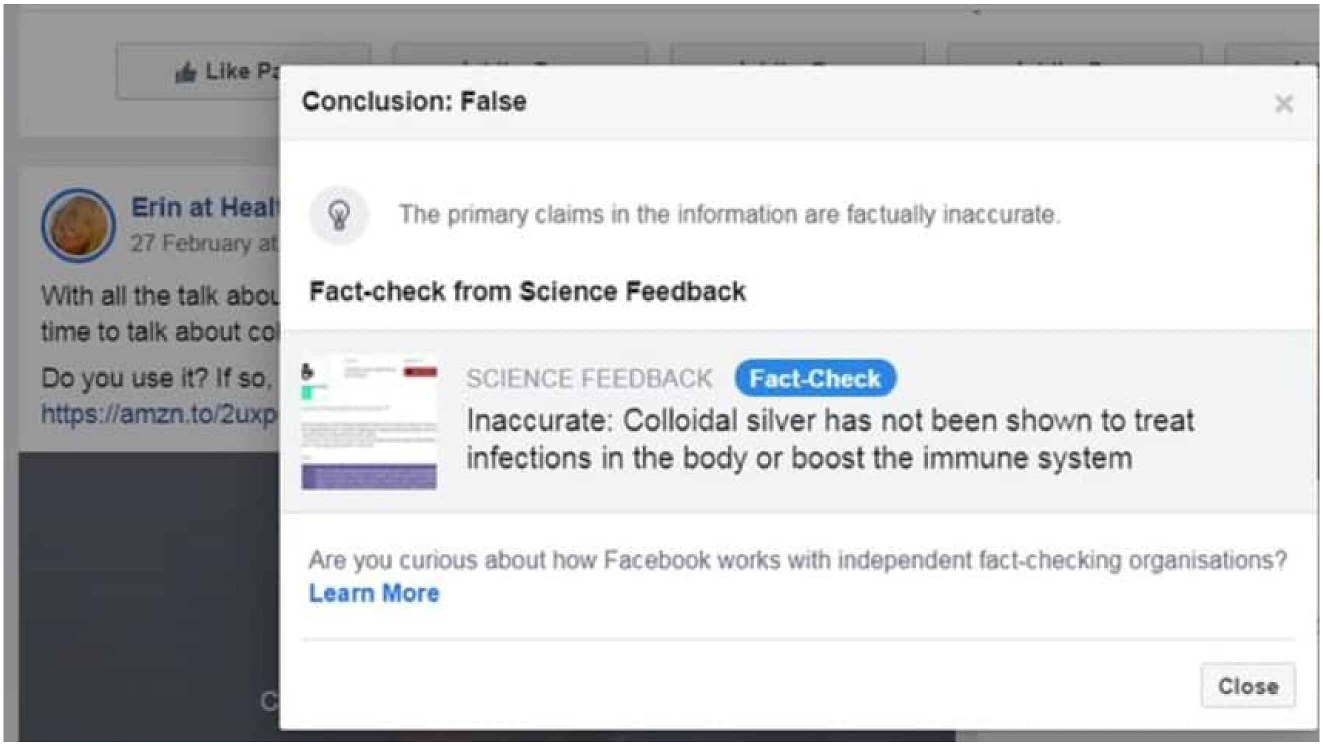
Information about COVID-19 in the United States
Centers for Disease Control and Prevention
cdc.gov/coronavirus/2019-ncov

Coronavirus advisory information
World Health Organization
who.int/emergencies

Coronavirus Q&A
World Health Organization
who.int/news-room

COVID-19 "SOS Alert" on Google

These measures are a great step in the right direction, and have likely already stopped the distribution of a significant amount of harmful material. Organizations have become more aware of the risks of the spread of misinformation over the past year, but there is still onus on users to ensure that the information they digest and share is legitimate. This is particularly important during global health crises, where the ramifications of misinformation can be deadly. For example, some recipes for making homemade hand sanitizers are not suitable for use on skin and can be ineffective in halting the transmission of COVID-19.



Conclusion: False

The primary claims in the information are factually inaccurate.

Fact-check from Science Feedback

SCIENCE FEEDBACK Fact-Check

Inaccurate: Colloidal silver has not been shown to treat infections in the body or boost the immune system

Are you curious about how Facebook works with independent fact-checking organisations?

Example of potentially dangerous at-home cures (Source: BBC)

COVID-19: Staying safe on and offline

- To help prevent the spread of misinformation, individuals should ensure that they only follow guidance from official national health institutions like the CDC and NHS, as well as international organizations like the WHO.
- The WHO recommends the following basic protective measures to prevent the spread and contraction of COVID-19:
  - Clean your hands frequently with an alcohol-based hand rub or wash them with soap and water.
  - Maintain at least 1 meter (3 feet) distance between yourself and anyone who is coughing or sneezing.
  - Avoid touching your eyes, nose, and mouth.
  - Practice respiratory hygiene: Cover your mouth and nose with your bent elbow or tissue when you cough or sneeze and dispose of used tissues immediately.
  - Stay home if you feel unwell. If you have a fever, cough, and difficulty breathing, seek medical attention and call in advance. Follow the directions of local health authorities.
- Use fact-checking tools to challenge potentially dubious claims on social media.

- Be wary of unsolicited correspondances that contain alarmist messaging and/or impersonate official health and safety institutions. Grammatical and formatting errors can help you identify malicious phishing emails.
- Be wary of emails soliciting charitable donations.
- Do not download files or visit unknown websites linked in unsolicited emails.
- Do not purchase medical equipment from unofficial third-party vendors (particularly on the dark web!). If a deal seems too good to be true, then it probably is.

Additional official resources: