

IDENTITY & SECURITY

Protecting businesses against cyber threats during COVID-19 and beyond



Neil Kumaran

[Latest stories](#)

[Products](#)

[Topics](#)

[About](#)

[RSS Feed](#)



maintain a high rate of detection even though 63% of the malicious docs blocked by Gmail are different from day to day.

To further help you defend against these attacks, today we're highlighting some examples of COVID-19-related phishing and malware threats we're blocking in Gmail, sharing steps for admins to effectively deal with them, and detailing best practices for users to avoid threats.

The attacks we're seeing (and blocking)

Every day, Gmail blocks [more than 100 million](#) phishing emails. During the last week, we saw 18 million daily malware and phishing emails related to COVID-19. This is in addition to more than 240 million COVID-related daily spam messages. Our ML models have evolved to understand and filter these threats, and we continue to block more than 99.9% of spam, phishing, and malware from reaching our users.

The phishing attacks and scams we're seeing use both fear and financial incentives to create urgency to try to prompt users to respond. Here are some examples:

- Impersonating authoritative government organizations like the World Health Organization (WHO) to solicit fraudulent donations or distribute malware. This includes mechanisms to distribute downloadable files that can install backdoors. In addition to blocking these emails, we worked with the WHO to clarify the importance

[Latest stories](#)[Products](#)[Topics](#)[About](#)[RSS Feed](#)

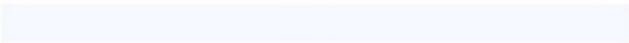
Solidarity Response Fund. Help WHO fight COVID-19 > Spam x



2:16 PM (2 hours ago) ☆ ↶ ⋮

This message seems dangerous
Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Looks safe



The world has never faced a crisis like COVID-19. The pandemic is impacting communities everywhere. **It's never been more urgent to support the global response.** The humanity, solidarity and generosity of people and organizations everywhere is also unprecedented. But we can't stop now.

The World Health Organization (WHO) is leading and coordinating the global effort with a range of partners, supporting countries to prevent, detect, and respond to the pandemic. **Donations support WHO's work, including with partners, to track and understand the spread of the virus; to ensure patients get the care they need and frontline workers get essential supplies and information; and to accelerate research and development of a vaccine and treatments for all who need them.**

See below for more ways to give, Via BTC (Bitcoin). Every donation helps support life-saving work for the world.

BTC Address: *****

- This example shows increased phishing attempts of employees operating in a work-from-home setting.

[Latest stories](#)

[Products](#)

[Topics](#)

[About](#)

[RSS Feed](#)

COVID-19 PAYMENT Spam



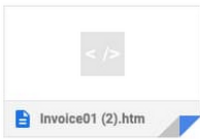
Miller, Jane
to me

12:28 PM (3 hours ago)

This message seems dangerous
It contains a suspicious link that was used to steal people's personal information. Avoid clicking links or replying with personal information.

Good morning,
You are advised to download the attached invoice for your review. Please get back to us as soon as possible for payment to be processed.
Thanks,
Jane

Downloading this attachment is disabled. This email has been identified as phishing. If you want to download it and you trust this message, click "Not spam" in the banner above.



- This attempt targets organizations impacted by stay-at-home orders.

Kindly make a list and send it to us. Spam



Neil
to me

1:53 PM (2 hours ago)

This message seems dangerous
Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Find an article...

[Latest stories](#)

[Products](#)

[Topics](#)

[About](#)

[RSS Feed](#)

heightened attention on COVID-19.



Blog

Menu ▾

In G Suite, advanced phishing and malware controls are turned on by default, ensuring that all G Suite users automatically have these proactive protections in place.



These controls can:

- Route emails that match phishing and malware controls to a new or existing quarantine
- Identify emails with unusual attachment types and choose to automatically display a

[Latest stories](#)[Products](#)[Topics](#)[About](#)[RSS Feed](#)

Best practices for organizations and users

Admins can look at Google-recommended defenses [on our advanced phishing and malware protection](#) page, and may choose to enable the [security sandbox](#).

Users should:

- Complete a [Security Checkup](#) to improve your account security
- Avoid downloading files that you don't recognize; instead, use Gmail's built-in document preview
- Check the integrity of URLs before providing login credentials or clicking a link—fake URLs generally imitate real URLs and include additional words or domains
- [Avoid and report](#) phishing emails
- Consider enrolling in Google's [Advanced Protection Program](#) (APP)—we've [yet to see](#) anyone that participates in the program be successfully phished, even if they're repeatedly targeted

RELATED ARTICLE



[Latest stories](#)

[Products](#)

[Topics](#)

[About](#)

[RSS Feed](#)



Blog

Menu 

Follow Us




Google

[Privacy](#)

[Terms](#)

[About Google](#)

[Google Cloud Products](#)

Language 

 [Help](#)