United States Senate

April 13, 2020

Amanpal S. Bhutani
Chief Executive Officer
GoDaddy Inc.
14455 North Hayden Road, Ste. 226
Scottsdale, Arizona 85260

Dear Mr. Bhutani:

We write regarding recent reports that cybercriminals are registering domain names that include references to the coronavirus or online communications platforms in widespread use at this time of social distancing—such as Zoom, Google Classroom, and Microsoft Teams—to conduct "phishing" schemes, install malware, spread misinformation about the virus, or otherwise take advantage of Internet users. As people the world over turn increasingly to the Internet for information about the coronavirus and use online applications to work, learn, and keep in contact with friends and family, it is imperative that domain name registrars not turn a blind eye to such illicit activity but, rather, act to protect the Internet-using public.

While the coronavirus was first detected in late-2019, it did not start to enter the public consciousness until January 2020 when the disease began to take hold in nations outside China. Prior to this time, registrations for domain names containing coronavirus-related terms were negligible to non-existent.[1]

As the disease—and awareness of it—spread, it is not surprising that governments, health authorities, and legitimate businesses would register domain names containing terms like "coronavirus" and "covid" in order to inform the public and provide essential goods and services. For example, the United States government registered and maintains a website at coronavirus.gov that provides Americans with the latest information on the coronavirus, including how to protect themselves and what to do if they get sick. The World Health Organization similarly registered coronavirus.com.

However, the exponential growth in registrations containing "coronavirus," "covid," and similar terms since late-January suggests that cybercriminals and other malevolent actors are attempting to take advantage of the pandemic. An analysis by intelligence firm Recorded Future found that coronavirus-related domain names drastically increased after January 19, 2020 with over 1,000 new such domain names registered daily by the end of February.[2] A separate analysis by threat

[1] https://www.recordedfuture.com/coronavirus-panic-exploit/
[2] https://subscriber.politicopro.com/article/2020/03/criminals-and-merchants-flock-to-coronavirus-website-names-3978631

intelligence firm RiskIQ found more than 10,000 new coronavirus-related domains daily by mid-March, including 35,000 such domains on March 16 alone.[3]

A review of the websites found at these domain names confirms what the sheer number of registrations made obvious: cybercriminals and malevolent actors are exploiting the coronavirus pandemic to take advantage of Internet users. Journalists for business technology website *ZDNet* reviewed a random sample of such websites and discovered that "in nine out of ten cases" the sites were "scam[s] . . . peddling fake cures" or "private sites, most likely used for malware distribution."[4] Security firm Check Point found that coronavirus-related domains were 50% more likely to be malicious than other domains registered between January and early-March 2020.[5] And, cyber risk scorecard provider NormShield identified at least 362 domains registered in 2020 with names that reference drugs touted as potential treatments for the coronavirus (e.g., remdesivir, chloroquine) that are likely phishing sites.[6]

This illicit activity has now spread as bad actors have begun to register domain names that reference online communications platforms in widespread use during this time of social distancing. A recent analysis by Check Point uncovered more than 1,700 domain names registered since the start of 2020 containing a reference to videoconferencing platform "Zoom"—25% of which were registered in just the last full week of March.[7] Of these domains, Check Point found that 4% contain suspicious characteristics.[8] The firm found additional phishing websites impersonating other online communication platforms, including Google Classroom and Microsoft Teams.[9]

As cybercriminals and other malevolent actors seek to take advantage of the coronavirus pandemic, it is critical that domain name registrars like yours (1) exercise diligence and ensure that only legitimate organizations can register coronavirus-related domain names and domain names referencing online communications platforms; (2) act quickly to suspend, cancel, or terminate registrations for domains that are involved in unlawful or harmful activity; and (3) cooperate with law enforcement to help bring to justice cybercriminals profiting from the coronavirus pandemic.

To better understand if your company is meeting these expectations, we request answers to the following questions by April 20, 2020:

1. What steps do you take to ensure that entities seeking to register domain names are legitimate, and not cybercriminals or other malevolent actors? Which, if any, of these steps have been added since the onset of the coronavirus pandemic?

---

[3] https://www.zdnet.com/article/thousands-of-covid-19-scam-and-malware-sites-are-being-created-on-a-daily-basis/
[4] *Id.*
[5] https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/
[6] https://www.normshield.com/wp-content/uploads/2020/04/NormShield-Covid19-Drug-Research-final-5-compressed.pdf
[7] https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/
[8] *Id.*
[9] *Id.*

2. What additional steps, if any, do you take to ensure that entities seeking to register domain names that contain coronavirus-related terms, such as "coronavirus," "covid," "pandemic," "virus," or "vaccine," are legitimate, and not cybercriminals or other malevolent actors?

3. What additional steps, if any, do you take to ensure that entities seeking to register domain names that reference drugs touted as potential treatments for the coronavirus, such as "remdesivir," "chloroquine," "hyrdroxychloroquine," "Plaquenil," "azithromycin," "metformin," "favipiravir," "interferon," "lopinavir," "ritonavir," or "arbitol," are legitimate, and not cybercriminals or other malevolent actors?

4. What additional steps, if any, do you take to ensure that entities seeking to register domain names that reference Zoom, Google Classroom, Microsoft Teams, or other online communications platforms are legitimate, and not cybercriminals or other malevolent actors?

5. What steps do you take on an ongoing basis to ensure that registrants are not using their registered domains for unlawful or harmful activity?

6. What are the penalties for registrants found to be using their registered domains for unlawful or harmful activity?

7. What steps do you take to cooperate with law enforcement when registrants are suspected of using their registered domains for unlawful activity?

8. Since the start of 2020, how many applications have you received for domain names that contain coronavirus-related terms, such as "coronavirus," "covid," "pandemic," "virus," or "vaccine?" How many of these domain names have your registered? Please provide this information broken down on a monthly basis.

9. Since the start of 2020, how many registrations for domain names that contain coronavirus-related terms, such as "coronavirus," "covid," "pandemic," "virus," or "vaccine," have you suspended, cancelled, terminated, or referred to law enforcement? Please provide this information broken down on a monthly basis.

10. Since the start of 2020, how many applications have you received for domain names that reference drugs touted as potential treatments for the coronavirus, such as "remdesivir," "chloroquine," "hyrdroxychloroquine," "Plaquenil," "azithromycin," "metformin," "favipiravir," "interferon," "lopinavir," "ritonavir," or "arbitol?" How many of these domain names have your registered? Please provide this information broken down on a monthly basis.

11. Since the start of 2020, how many registrations for domain names that reference drugs touted as potential treatments for the coronavirus, such as "remdesivir," "chloroquine," "hyrdroxychloroquine," "Plaquenil," "azithromycin," "metformin," "favipiravir," "interferon," "lopinavir," "ritonavir," or "arbitol," have you suspended, cancelled,

terminated, or referred to law enforcement? Please provide this information broken down on a monthly basis.

12. Since the start of 2020, how many applications have you received for domain names that reference Zoom, Google Classroom, Microsoft Teams, or other online communications platforms? How many of these domain names have your registered? Please provide this information broken down on a monthly basis.

13. Since the start of 2020, how many registrations for domain names that reference Zoom, Google Classroom, Microsoft Teams, or other online communications platforms have you suspended, cancelled, terminated, or referred to law enforcement? Please provide this information broken down on a monthly basis.

Thank you in advance for your attention to this critical matter. Due to the closure of many Senate offices during the coronavirus outbreak, physical signatures are unavailable. The listed senators have asked to be signatories to this letter.

Should have any questions, please contact Jeff Hantson in Senator Hirono's office at Jeff_Hantson@hirono.senate.gov.

Sincerely,

Mazie K. Hirono
United States Senator

Margaret Wood Hassan
United States Senator

Cory A. Booker
United States Senator