



RiskIQ i3:

COVID-19 Daily Update

04/01/2020

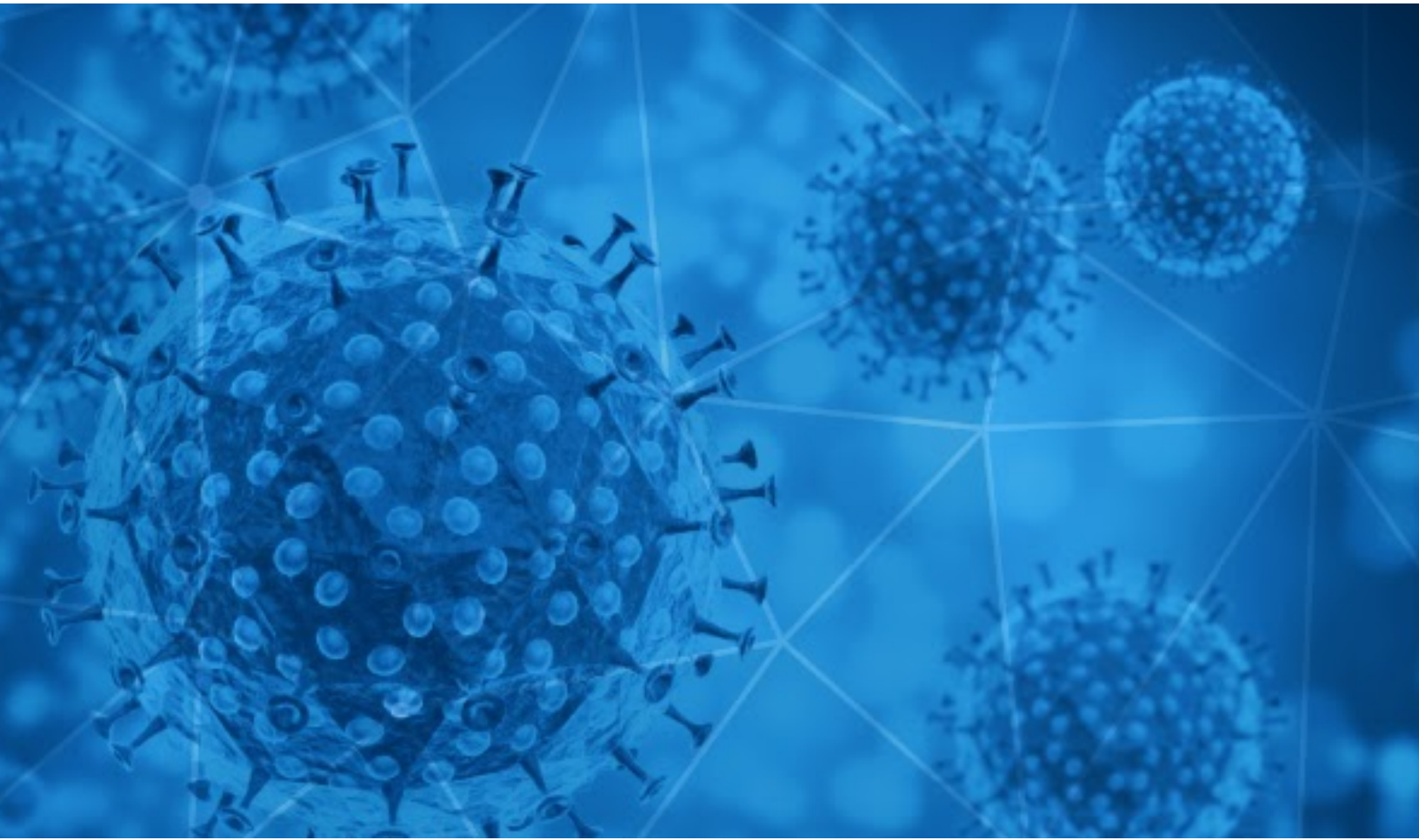


Table of Contents

Methodology	3
Disclaimer	3
Notable Events: Previous 24 Hours	4
Digital Exploitation	6
New Blacklist Data	6
COVID-19 Email Spam Statistics	7
COVID-19 Host, Domain, and Mobile App Tracking	10
Facts and Figures at a Glance	11
Global	11
U.S.	11
Highest COVID-19 Case Count - U.S.	11
Stay-At-Home/Shelter-In-Place Orders	12
Governmental Guidance	13
State & Local Governments	13

Methodology

The information provided in this report is limited to open source and publicly available data discovered through standard, commonly known browsing techniques and keyword searches. To provide efficient results, RiskIQ may use websites that require payment in exchange for aggregation of data that is otherwise publicly available without payment and could be obtained by anyone accessing the correct sites or engaging the correct third parties to obtain the information. Information presented in this report is cross-checked against multiple sources for full verification; however, some assessments and conclusions are based on incomplete information and represent the RiskIQ analyst's judgment based on patterns and data available.

Disclaimer

The information provided in this report is "as-is" and Customer acknowledges and agrees that RiskIQ makes no representation or warranty, express or implied, as to the accuracy or completeness of the information. Customer agrees that RiskIQ shall not have any liability resulting from Customer's use of this information.

Notable Events: Previous 24 Hours

The Pentagon committed to sending [2,000 ventilators](#) from its military stocks to the Federal Emergency Management Agency (FEMA) and the Department of Health and Human Services (HHS). To date, the Pentagon has not shipped any of these ventilators due to a lack of guidance from FEMA and HHS. Pentagon officials reported 1,000 ventilators are ready to ship immediately once given direction and the remaining 1,000 can be shipped within days of receiving an order.

Michigan now ranks [third in the nation](#) for COVID-19-related deaths with 259 total fatalities, behind only New York and New Jersey. The majority of the state's cases are located in the Detroit metropolitan area, with 80% of cases reported in Oakland, Macomb, and Wayne counties.

Texas Governor Greg Abbott on Tuesday told Texans to [stay at home](#) for the next month unless they are taking part in essential services and activities, announcing a heightened statewide standard to stem the spread of the new coronavirus. He also announced that schools would remain closed until at least May 4.

Florida Governor Ron DeSantis has issued a [mandatory safer-at-home order](#) for the entire state of Florida, starting Thursday at midnight. The order mandates that Floridians stay home and requires "all persons in Florida to limit their movements and personal interactions outside of their home" to essential services or activities for the next 30 days.

Carnival Cruise Line said it will raise approximately [\\$6 billion](#) in debt and equity while also suspending dividends. The company said these moves, based on assumptions about COVID-19, will provide it with enough liquidity to remain in compliance with its debt covenants for twelve months. Carnival is incorporated offshore, which prevents the company from qualifying for relief under the \$2.2 trillion CARES Act.

Iceland is conducting [large-scale COVID-19 testing](#), having already tested roughly 5% of its population as of 03/31/2020. Biopharma company DeCode Genetics tested 9,000 self-selected individuals and found 1% of tested individuals were positive for the virus. Though only 1% tested positive, 50% of confirmed cases in the study were reportedly asymptomatic. The Directorate of Health cautioned that there may be biases in the data since screening is voluntary.

The U.S. intelligence community concluded China has [under-reported](#) both the total number of COVID-19 cases and the number of related fatalities, according to three U.S. officials. The

classified report allegedly concludes China's numbers are fake. Coronavirus task force member Dr. Deborah Birx stated China's data has influenced the world's assumptions about the virus.

The National Institute of Allergy and Infectious Diseases greenlit a [drug trial](#) evaluating the effects of Remdesivir on COVID-19 patients. The drug has been previously used to treat Ebola and has known adverse effects that resolved over time, including decreased liver function and gastrointestinal issues.

All England Lawn Tennis Club officials [cancelled Wimbledon](#) this year due to the pandemic, marking the first time the event has been cancelled since World War Two. There will be no professional tennis anywhere in the world until at least 07/13/2020.

Digital Exploitation

The Zeus Sphinx banking Trojan recently resurfaced after a three years hiatus as part of a coronavirus-themed [phishing](#) campaign, according to BleepingComputer. The malware has been used in the past to harvest financial data via web injections that make use of social engineering in order to convince infected users to hand out authorization codes and credentials.

The Cofense Phishing Defense Center (PDC) has witnessed a surge in COVID-19 phishing campaigns found in environments protected by [Proofpoint and Microsoft Office 365 ATP](#). While these Secure Email Gateways are designed to safeguard end users from clicking on malicious links and attachments, both failed in a new phishing attack, PDC recently observed.

Guardicore Labs reported on 04/01/2020 that they uncovered a sustained malicious campaign dating back to May 2018 that targets Windows machines running MS-SQL servers to deploy backdoors and other kinds of [malware](#), including multi-functional remote access tools and cryptominers. According to Hacker News, the attack employs password brute-force to breach Microsoft SQL servers with weak credentials exposed to the Internet.

Computer [hackers](#) attacked Italy's social security website, forcing it to shut down on Wednesday, 04/01/2020. The attacks occurred as people began applying for COVID-19 benefits, according to Reuters.

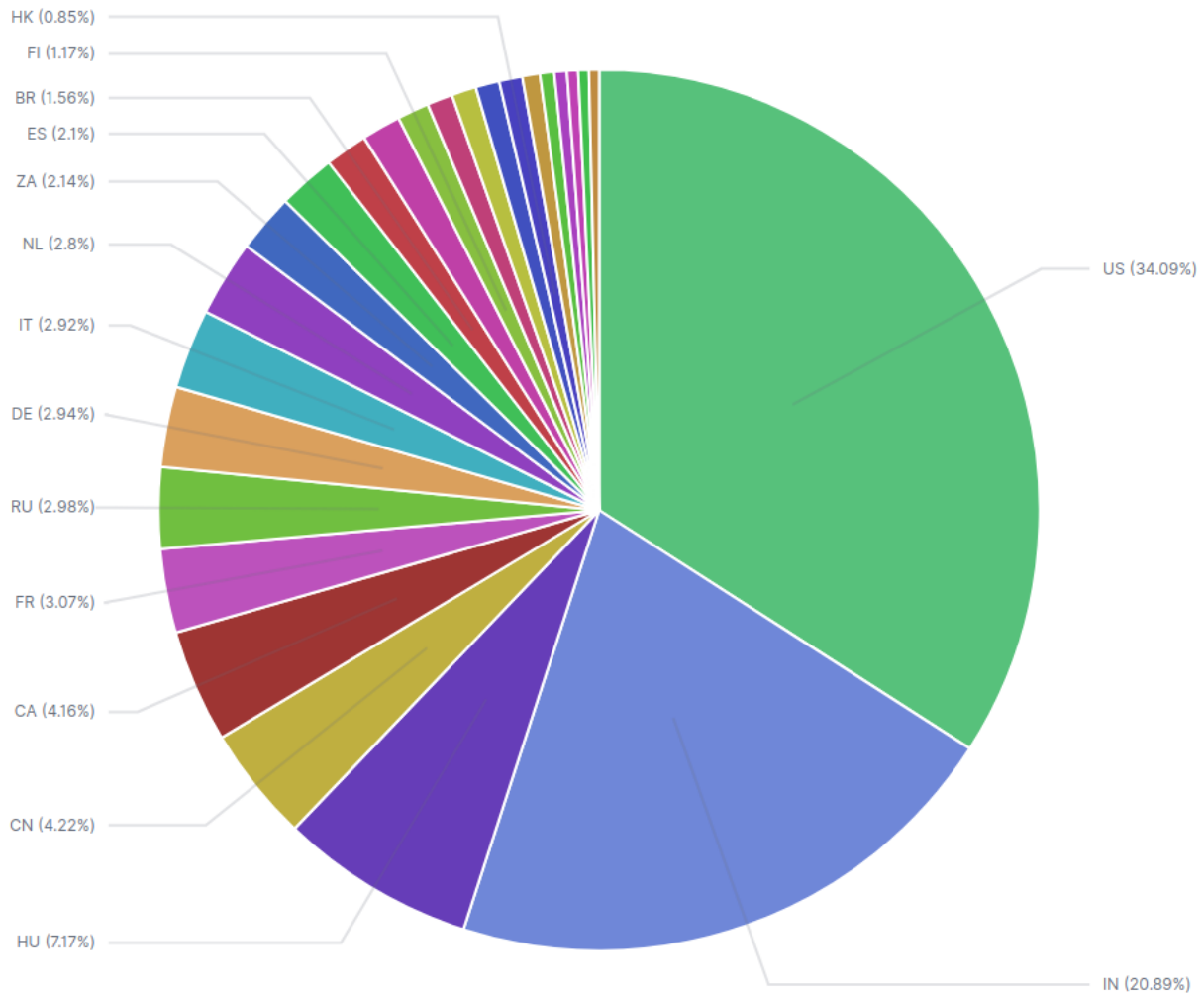
LookingGlass analyzed the security flaws previously reported about [Zoom](#) teleconferencing software. After looking at 1,689 fully qualified domain names using the Zoom name they found 534 network elements that exhibit behavior that was consistent with a vulnerable or suspicious domain. These domains are being used to steal credentials, install malware, and redirect users to potentially malicious destinations. Likewise, HackerNews reported that [Zoom windows users](#) are vulnerable to the 'UNC path injection' vulnerability that could let remote attackers steal login credentials. Related reporting by Business Insider found that trolls are [breaking into Alcoholics Anonymous meetings](#) held via Zoom and harassing participants with slurs and mentions of alcohol. Zoom said it was "deeply upset" to learn of the incident and encouraged users to turn on maximum security settings.

New Blacklist Data

Note: No new updates. Please see the COVID-19 Daily Update (dated 03/31/2020) for the most recent data.

COVID-19 Email Spam Statistics

RiskIQ analyzed its spam box feed for the time period of 03/31/2020-04/01/2020. During this period, RiskIQ analyzed 173,164 spam emails containing either “*corona*” or “*covid*” in the subject line. There were 19,479 unique subject lines observed during the reporting period. The spam emails originated from 10,997 unique sending email domains and 15,489 unique SMTP IP Addresses. Analysts identified 518 emails which sent an executable file for Windows machines.



Spam emails by country of origin

Top 25 Subjects

1. 23,135 - Here is your chance to contribute in India's war against COVID-19!
2. 8,362 - The Mask that can prevent Coronavirus now
3. 6,681 - (Quick delivery) Protective mask and Diagnostic kit for COVID-19, goggles, infrared thermometer, protective clothing
4. 5,388 - How to protect your body from COVID-19
5. 4,272 - Coronavirus is spreading, this specialized mask can control it
6. 3,325 - The Corona Letter: What after nationwide lockdown ends?
7. 3,222 - URGENT NEED: U.S. Department of Health & Human Services/COVID-19 Face Mask/Forehead thermometers
8. 2,477 - H-1B visa: US govt to consider visa extension for Indians amid Coronavirus crisis | India lockdown: Follow Satya Nadella's tips to work from home
9. 2,378 - Re:[## 10641 ##] COVID-19/BALANCE PAYMENT
10. 2,005 - Your Automated Investment Future Corona Millionaire.
11. 1,664 - Keep your brain & studies alive during the COVID-19 quarantine & lockdown
12. 1,590 - COVID19 Offer -85%
13. 1,522 - How to ace a telephonic job interview | H-1B visa: US govt to consider visa extension for Indians amid Coronavirus crisis
14. 1,512 - Insurers prepare for Covid-19 claims
15. 1,484 - Coronavirus – Border Closures and Global Freight Movement
16. 1,323 - Droht CORONAVIRUS? Mit Atemmaske können Probleme vorgebeugt werden
17. 1,321 - Kann das CORONAVIRUS vorgebeugt werden? Atemmaske für wirksamen Schutz
18. 1,293 - COVID-19 THẬN TRỌNG Y TẾ, AN TOÀN VÀ CẬP NHẬT VACCINE MỚI (COVID-19 PRECAUTIONS HEALTH, SAFETY AND UPDATES new vaccine)
19. 1,292 - Coronavirus, Grippe? Hier ist die Atemmaske mit einem speziellen Filter
20. 1,286 - Würdest du das CORONAVIRUS stoppen? Die Atemmaske schützt auch vor neue Infektion
21. 1,284 - Hast du Angst vor dem Corona-Virus? Neue Atemmaske, schütze deine Lieben
22. 1,275 - Die Corona-Krise..., Vertriebstopps..., Stellenangebote, Newsletter-Bestätigung, Betriebsnachfolge, Tipps und Story
23. 1,256 - A Whole New Workplace – COVID-19
24. 1,212 - ATEMMASKE zur Bändigung des Coronavirus - Sicherheit auf FFP2-Ebene

25. 992 - When will coronavirus peak in YOUR state? +Dwyane Wade Recalls the time LeBron Saved Carmelos's life

Top Subjects Containing Attachments with Executable Files for Windows Machines (PE/EXEs)

1. 378 - Customer Advisory - COVID-19 UPDATE WORLDWILD
2. 76 - COVID-19 UPDATE !!!
3. 53 - TNT Express Notification/ Your shipment was returned to our office!!! BECAUSE OF COVID-19 OUTBREAK.
4. 5 - Purchase Order (PO For-COVID-19 Products)
5. 4 - Corona-Virus Disease Τελευταίες προφυλάξεις και συμβουλές
6. 2 - Your shipment was returned to our office!!! BECAUSE OF COVID-19 OUTBREAK.

Top Countries Sending SPAM - Covid/Coronavirus Contained in Subjects (by Geolocation on SMTP IP Address)

- | | |
|--------------|--------------|
| 1. 54,246 US | 14. 2,280 GB |
| 2. 33,235 IN | 15. 1,855 FI |
| 3. 11,405 HU | 16. 1,488 VN |
| 4. 6,714 CN | 17. 1,444 AR |
| 5. 6,615 CA | 18. 1,386 BE |
| 6. 4,888 FR | 19. 1,355 HK |
| 7. 4,740 RU | 20. 1,027 TR |
| 8. 4,678 DE | 21. 826 KR |
| 9. 4,646 IT | 22. 735 TW |
| 10. 4,459 NL | 23. 647 UA |
| 11. 3,405 ZA | 24. 619 MX |
| 12. 3,346 ES | 25. 590 PY |
| 13. 2,477 BR | |

COVID-19 Host, Domain, and Mobile App Tracking

RiskIQ gathers data relating to newly-observed hosts and domains containing COVID-19, COVID19, or Coronavirus in the host or domain name and mobile apps containing COVID-19, COVID19, or Coronavirus in the title or description. A summary of data collected is contained in this section.

Domains and Hosts

Domains: 44,180

Hosts: 49,314

Hosts and Domains with Potential Mail Servers: 213

Email-Capable Domains and Hosts: 15,686

Live Hosts and Domains Not Parked: 19,713

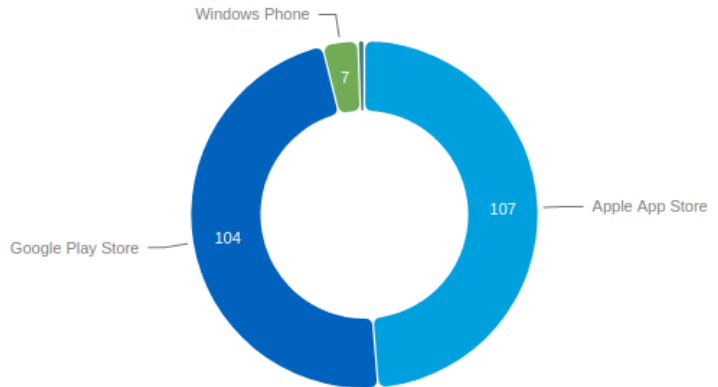
Mobile Apps

1. Apps in Official Stores: 219
 (See Graph)
 - a. Google Play Store: 104
 - b. Apple App Store: 107
 - c. Windows Phone: 7
 - d. Amazon: 1

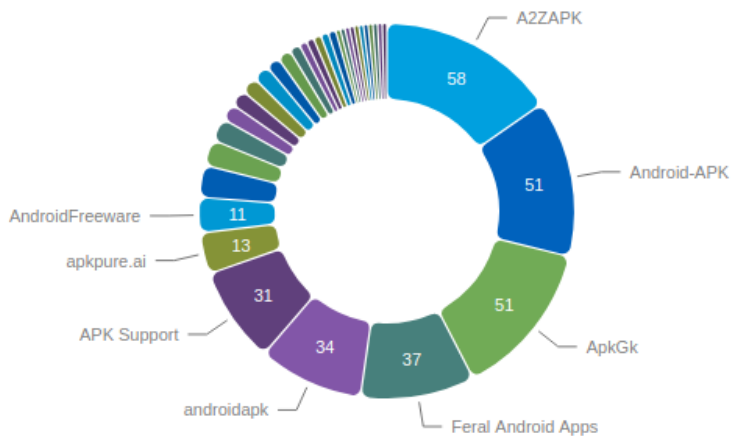
2. Apps in Secondary/Hybrid Stores: 363 (See Graph)

3. Blacklisted Mobile Apps by Store Type: 14
 - a. Secondary: 13
 - b. Hybrid: 1

Apps on Official Stores



Apps on Secondary and Hybrid Stores by store



Facts and Figures at a Glance

Data is from [Johns Hopkins Coronavirus Resource Center](#).

Global

Total Cases: 883,225
Total Fatalities: 44,156
Countries w/ Confirmed Cases: 180

U.S.

Total Cases: 189,753
Total Fatalities: 4,090
Jurisdictions Reporting Cases: 54 (50 states, District of Columbia, Puerto Rico, Guam, and U.S. Virgin Islands)

Highest COVID-19 Case Count: U.S.

States

1. New York: 76,049
2. New Jersey: 18,997
3. California: 8,584

Counties

1. New York City (NY): 43,119
2. Westchester County (NY): 9,967
3. Nassau County (NY): 8,544
4. Suffolk County (NY): 6,713
5. Cook County (IL): 4,496
6. Wayne County (MI): 3,735
7. Bergen County (NJ): 3,202
8. Los Angeles County (CA): 3,037
9. Rockland County (NY): 2,863
10. King County (WA): 2,330

Stay-At-Home/Shelter-In-Place Orders

State	Start Date	End Date
California	03/19	TBD
Illinois	03/21	04/30
New Jersey	03/21	TBD
New York	03/22	TBD
Connecticut	03/23	04/22
Kentucky	03/23	TBD
Louisiana	03/23	04/13
Ohio	03/23	04/06
Oregon	03/23	TBD
Washington	03/23	04/06
Delaware	03/24	05/15
Indiana	03/24	04/06
Michigan	03/24	04/13
New Mexico	03/24	04/10
Massachusetts	03/24	05/04
West Virginia	03/24	TBD
Hawaii	03/25	04/30
Wisconsin	03/25	04/24
Vermont	03/25	04/15
Idaho	03/25	04/15
Colorado	03/26	04/11
Minnesota	03/27	04/10
New Hampshire	03/27	05/04
Montana	03/28	04/10
Rhode Island	03/28	04/13
Alaska	03/28	04/11
Kansas	03/30	04/19
North Carolina	03/30	04/29
Maryland	03/30	TBD
Virginia	03/30	06/10
Arizona	03/31	04/30
Tennessee	03/31	04/14
Washington, DC	04/01	04/24
Texas	04/02	04/30
Florida	04/03	04/30

Governmental Guidance

State & Local Governments

California

As of 04/01/2020, California has 8,584 confirmed COVID-19 cases and 183 deaths. California Governor Gavin Newsom launched a [“Stay Home. Save Lives. Check In”](#) campaign to check on the well-being of California’s older residents. Gov. Newsom also announced a new statewide hotline. The hotline will be available to answer questions regarding the crisis in addition to asking for assistance. [San Francisco International Airport](#) announced all international flights will be consolidated on one concourse from 04/01/2020 until the end of May.

Illinois

As of 04/01/2020, Illinois has 5,998 confirmed cases of COVID-19 and 100 deaths. Illinois Governor JB Pritzker [extended Illinois’ stay-at-home order](#) to 04/30/2020. The extension announcement included continued suspension of on-site learning. Remote learning is expected to count towards school days.

Massachusetts

As of 04/01/2020, Massachusetts has 6,620 confirmed cases of COVID-19 and 89 deaths. Massachusetts Governor Charlie Baker [announced](#) Massachusetts’ stay-at-home order will extend through 05/04/2020. Worcester officials have begun converting [DCU Arena](#) in Worcester into a field hospital. FEMA is expected to deliver medical supplies on 04/01/2020.

New York

As of 04/01/2020, New York has 76,049 confirmed COVID-19 cases and 1,714 deaths. New York City started building a 350-bed hospital at the [Billie Jean King National Tennis Center](#) in Flushing Meadows-Corona Park.

Washington, DC

As of 04/01/2020, the Washington, D.C. region has a total of 4,061 confirmed COVID-19 cases with 1,249 in Virginia, 1,986 in Maryland, and 507 in the District. D.C. officials [announced](#) they would start sending personal protective equipment to healthcare facilities. The Baltimore-based



RiskIQ
22 Battery, 10th Floor
San Francisco, CA 94111
United States

company Under Armour said it would produce masks, face shields, and fanny packs for The University of Maryland Medical System. George Washington University Hospital reported it would offer drive-through COVID-19 testing for any D.C. resident with a provider referral.

End Report