

# AUTHORITIES STEP UP CYBER AWARENESS EFFORTS FOR COVID-19

17 July 2020

The explosion of cyber attacks and online fraud enabled by COVID-19 and the rapid (and, in some cases, haphazard) deployment of a global remote work force<sup>[1]</sup> have pushed agencies responsible for consumer and citizen protection into higher gear. Their approaches have ranged from passive postings to aggressive countermeasures, according to their differing resources and mandates.

## Canada

The Canadian Centre for Cyber Security (“**CCCS**”) recently published a new Bulletin detailing how the ongoing COVID-19 pandemic has affected cyber threat activity.<sup>[2]</sup>

The CCCS found that, as of late-April 2020, over 120,000 new domains had been registered with some type of COVID-19 theme, a large proportion of which the CCCS considered to be malicious or related to fraudulent activity. There are also SMS phishing campaigns operating, claiming to be notices from governmental authorities of emergency relief. These are operations specifically geared to leverage the anxiety and uncertainty the pandemic has generated.

In total, the CCCS makes seven key conclusions:

1. **Malicious cyber actors** were using the pandemic as a hook or pretense in communications designed to execute cybercrime or cyberespionage;
2. **The health sector had increased exposure** and sensitivity to ransomware attacks as the health-related services remained under extreme pressure while dealing with the pandemic;

3. Cyberespionage efforts would likely focus more on **stealing intellectual property** relating to COVID-19, as well as intelligence about the government responses to the pandemic;
4. **State-sponsored cyber threats** might suffer a short-term reduction in staffing as governments refocused priorities, but this could give way to a long-term increase in focus on digital espionage as travel restrictions and social distancing protocols hinder more traditional methods;
5. **Misinformation and influencer campaigns** designed to erode trust in official statements continue, increasing the risk of hampering public health responses, as well as increasing the milieu of public anxiety that can make executing cyber threats more effective;
6. The increase in remote working will create **more targets for malicious cyber actors to exploit**, taking advantage of the likelihood that local networks will not be hardened to attacks to the same degree that a workplace can be; and
7. **Authoritarian regimes will likely take advantage** of the pandemic to justify and deploy surveillance technologies on its populace, which could affect expatriates and Canadians working and living abroad.

The CCCS is supplementing its reports with more actionable materials and, in some cases, action by the CCCS itself:

- CCCS publishes alerts and advisories—often several times a day—on “potential, imminent or actual cyber threats, vulnerabilities or incidents affecting Canada's critical infrastructure.”<sup>[3]</sup>
- It regularly posts short, consumer and small business-friendly pieces such as “Have You Been Hacked?,”<sup>[4]</sup> “Secure Your Accounts and Devices With Multi-Factor Authentication”<sup>[5]</sup> and “Security Considerations for Mobile Device Deployments.”<sup>[6]</sup>
- Anecdotally, we can also report that CCCS is reaching out to directly (and confidentially) to Canadian businesses it learns have been compromised, to offer assistance and resources.

The Financial Transactions and Reports Analysis Centre (**FINTRAC**) recently issued a Special Bulletin reporting COVID-19-related trends in money laundering and fraud.<sup>[7]</sup> The bulletin identifies and measures various types of fraud, including phishing scams in which criminals “pretending to be linked to Employment Insurance benefits, Canada Emergency Response Benefit (CERB), the Public Health Agency of Canada or other businesses” lure victims with texts and emails soliciting financial information or containing malware.

# United States

In the U.S., the Federal Bureau of Investigation has warned of fake emails from the Centers for Disease Control and Prevention (**CDC**) purporting to provide information on COVID-19. It has also warned of a rise in phishing emails, counterfeit treatments or equipment for pandemic preparedness.<sup>[8]</sup> Meanwhile, the Federal Trade Commission (**FTC**) has released a general overview of the steps that it is taking to combat scams related to COVID-19 and provided a specific list of seven types of COVID-19 scams that are targeting businesses<sup>[9]</sup>:

1. **“Public health” scams:** The online attackers send messages that claim to be from the CDC, World Health Organization (**WHO**), or other public health offices. They may ask for Social Security numbers, tax IDs, etc. or a link or download a document.
2. **Government check scams:** Cybercriminals are calling and emailing out of the blue claiming there’s money available from a government agency if you just make an up-front payment or provide some personal information.
3. **Business email compromise (BEC) attacks:** Where your employee gets a message that appears to come from a higher-up in the company directing the employee to wire money, transfer funds, send gift card codes, etc. This problem is compounded by teleworking employees as they are unable to walk down the hall to verify a questionable directive.
4. **IT scams:** The attacker calls or messages the employee claiming to come from the technology staff at the company asking for a password or directing the recipient to download certain software.
5. **Supply scams:** Scammers design websites that mimic the look of well-known online retailers and claim to have the essentials.
6. **Robocall scams:** There is a new cop of illegal calls where employees are pitched bogus test kits and sanitation supplies. This recording particular targets “small business who may be affected by the Coronavirus,” warning them to “ensure your Google listing is correctly displaying otherwise customers may not find you online during this time.”<sup>[10]</sup>
7. **Data scams:** Malicious cyber actors are taking advantage of the mass move to telework by exploiting a variety of publicly known vulnerabilities in VPNs and other remote working tools and software. Potential vulnerabilities due to remote working and usage of personal networks and devices have allowed hackers to infiltrate data-rich networks.

In addition to its in-depth, pieces, the FTC issues email alerts, often several per week,

alerting consumers and businesses about emerging threats and scams, as well as the results of FTC investigations.

## Britain and the World

A number of international bodies have made similar efforts, highlighting many of the same risks, and taking arguably more aggressive stances against the wave of illicit activity:

- The World Health Organisation has released guidelines, instructing people to be aware that cybercriminals are attempting to impersonate trusted health authorities across the globe. It has warned the public that cybercriminals send fraudulent emails as well as messages on forums like WhatsApp in relation to COVID-19.<sup>[11]</sup>
- The EU Commissioner for Justice and Consumers, following the common position endorsed by the CPC network,<sup>[12]</sup> made a call to action by reaching out to various social media and technology companies requiring their cooperation in removing scams from their platforms. The companies responded to the Commissioner with a positive affirmation of call to action by extending their support in the prevention of cybercrime.<sup>[13]</sup>
- In Europe, the EU Agency for Cybersecurity (ENISA) has also warned of a widespread increase in so-called 'phishing attacks'. In the UK alone, fraudsters exploiting COVID-19 fears have scammed £2m.<sup>[14]</sup>
- To deal with the ubiquitous issue of online frauds related to the COVID-19 pandemic, the European Commission and Member State consumer protection authorities have launched a number of joint measures. On March 20, 2020, the Consumer Protection Cooperation Network authorities of the Member States,<sup>[15]</sup> with the support of the Commission issued a common position on the most reported scams and unfair practices. The goal of this initiative is to raise awareness and assist online platforms in identifying illegal practices, take them down and prevent their resurgence.
- The Computer Emergency Response Team for the EU institutions, bodies and agencies (**CERT-EU**) has undertaken the necessary measures to assess the cyber aspects of the COVID-19 pandemic. A plan has been devised by CERT-EU, in the form of various Security Guidelines, to address any potential threat to EU Institutions, bodies and agencies in the realm of cybersecurity. The CERT-EU Security Guidelines aim to highlight the various elements of the plan and also provide a series of recommendations.<sup>[16]</sup>
- Great Britain's National Cyber Security Centre (**NCSC**) and the United States Cybersecurity and Infrastructure Security Agency (**CISA**, part of the Department of Homeland Security) and issued a joint alert. The joint alert highlights ongoing activity by

advanced persistent threat (**APT**) groups against organizations involved in both national and international COVID-19 responses. The primary targets are healthcare bodies, pharmaceutical companies, academia, medical research organizations, and local governments.

## Is it working?

It's difficult to assess the extent to which these actions are affecting the overall picture. Some studies suggest that cyber attacks peaked in March and began trailing off<sup>[17]</sup>—long before many of the advisories and actions we describe above. Microsoft attributes the decline, at least in part, to a successful game of catch-up by IT professionals to harden companies' defences. Nonetheless, 12 million attacks are still occurring daily, an increase of 20% over February 2020.<sup>[18]</sup> So the threat remains constant. One assumes that all this activity by various global agencies is at least raising the median level of threat awareness and consumer and business sophistication. This is surely a positive development, which future studies will presumably quantify.

**Note:** Developments in the COVID-19-related malicious cyber activity are rapidly changing. We recommend all individuals and organizations to remain vigilant and take proactive steps to protect themselves. Our dedicated Cybersecurity and Privacy Team is available to assist your business and employees with COVID-19-related questions.

---

[1] See "COVID-19 raises cybersecurity risks," Gowling WLG Tech News, <https://gowlingwlg.com/en/insights-resources/articles/2020/covid-19-raises-cybersecurity-risks/> and "Cybersecurity and privacy risks in a remote work environment" (webinar), <https://gowlingwlg.com/en/insights-resources/on-demand-webinars/2020/cyber-security-privacy-risks-remote-environment/>.

[2] <https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threat-activity> a

[3] <https://cyber.gc.ca/en/alerts-advisories>.

[4] <https://cyber.gc.ca/en/guidance/have-you-been-hacked-itsap00015>

[5] <https://cyber.gc.ca/en/guidance/secure-your-accounts-and-devices-multi-factor-authentication-itsap30030>

[6] <https://cyber.gc.ca/en/guidance/security-considerations-mobile-device-deployments-itsap70002>

[7] FINTRAC, "Special Bulletin on COVID-19: Trends in Money Laundering and Fraud," July 2020, online: <https://www.fintrac-canafe.gc.ca/intel/operation/covid-eng>.

[8] <https://www.ic3.gov/media/2020/200320.aspx>

[9] <https://www.ftc.gov/news-events/blogs/business-blog/2020/03/seven-coronavirus-scams-targeting-your-business>

[10] <https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/smallbusinesslisting.mp3>

[11] <https://www.who.int/about/communications/cyber-security>

[12] [https://ec.europa.eu/info/sites/info/files/covid\\_19\\_scams\\_letter\\_to\\_platforms\\_march\\_2020.pdf](https://ec.europa.eu/info/sites/info/files/covid_19_scams_letter_to_platforms_march_2020.pdf)

[13] [https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/scams-related-covid-19\\_en#replies-from-online-platforms-including-measures-taken](https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/scams-related-covid-19_en#replies-from-online-platforms-including-measures-taken)

[14] <https://www.bbc.com/news/uk-england-52310804>

[15] The Consumer Protection Cooperation (CPC) network consists of authorities responsible for enforcing EU consumer protection laws to protect consumers' interests in EU and EEA countries.

[16] [https://cert.europa.eu/cert/newsletter/en/latest\\_MemosAndBriefs\\_.html](https://cert.europa.eu/cert/newsletter/en/latest_MemosAndBriefs_.html)

[17] Lee Mathews, "Microsoft: COVID-19 Cyber Attacks Peaked In March And Fell Off Quickly," Forbes (June 17, 2020), online: <https://www.forbes.com/sites/leemathews/2020/06/17/microsoft-covid-19-cyber-attacks-peaked-in-march-and-fell-off-quickly/#29f8c5efc9aa>

[18] Lee Mathews, "Microsoft: COVID-19 Cyber Attacks Peaked In March And Fell Off Quickly," Forbes (June 17, 2020), online: <https://www.forbes.com/sites/leemathews/2020/06/17/microsoft-covid-19-cyber-attacks-peaked-in-march-and-fell-off-quickly/#29f8c5efc9aa>

---

NOT LEGAL ADVICE. Information made available on this website in any form is for information purposes only. It is not, and should not be taken as, legal advice. You should not rely on, or take or fail to take any action based upon this information. Never disregard professional legal advice or delay in seeking legal advice because of something you have read on this website. Gowling WLG professionals will be pleased to discuss resolutions to specific legal concerns you may have.

---

**Related** Tech, Commercial Litigation, Class Actions

## Authors

### Brent J. Arnold

Partner - Toronto

 Email

[brent.arnold@gowlingwlg.com](mailto:brent.arnold@gowlingwlg.com)

 Phone


+1 416-369-4662

 vCard

Brent J. Arnold


### Umair Azam

Associate - Ottawa

 Email

umair.azam@gowlingwlg.com


 Phone  
+1 613-786-0094


 vCard  
Umair Azam

## **Kavi Sivasothy**

Associate - Toronto

 Email  
kavi.sivasothy@gowlingwlg.com

 Phone  
+1 416-369-7251

 vCard  
Kavi Sivasothy