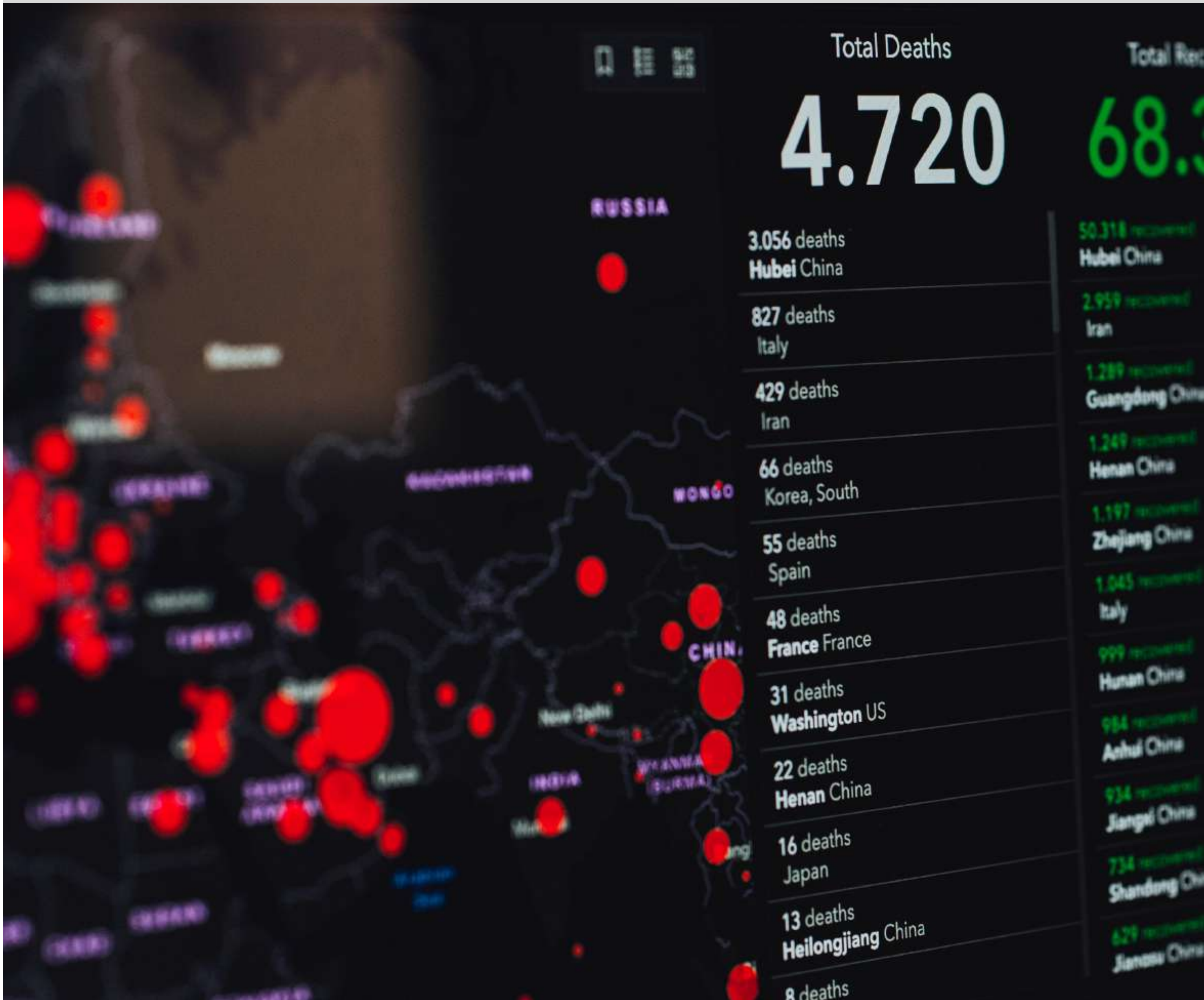
COVID-19 and CyberCrime

How rogue nations and cyber criminals are exploiting a global crisis

This report provides some tools and solutions at our Govt's disposal to stay ahead - NOW



SafeSwiss® March, 2020

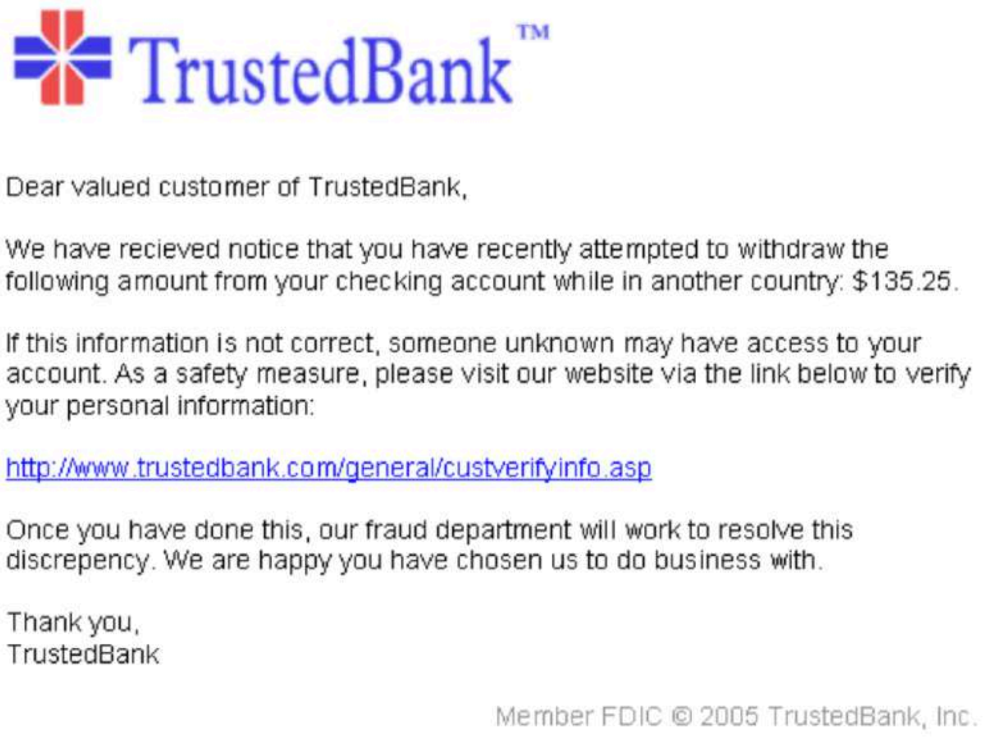
Abstract

For the truly nefarious, even a crisis is an opportunity. Canadian, American and European authorities have noticed an uptick in cybercrime incidents as more people work from home. The threat expands further as government employees and legislatures attempt to move to remote workspaces this week. Together, corporate and government employees could be facing billions of dollars in additional costs from ransomware, phishing or malware attacks. The flow of information has never been so weaponized as it has in recent years. The biggest and most brazen attacks seem to have been launched by the Russian, Iranian and North Korean state authorities. To protect citizens and states, tools such as end-to-end encryption and zero-trust architecture need to be deployed in mainstream applications.

Introduction

For the truly nefarious, even a crisis is an opportunity. Paddon (2020) reports Canadian and American authorities have noticed an uptick in cybercrime incidents as more people work from home. Sharton (2020) believes cybercriminals are leveraging the fact that authorities and resources are being focused on fighting the COVID-19 pandemic to target vulnerable internet users who may be working from home for the first time. “Companies may eventually face the prospect of functioning with little to no personnel on-site or skeleton crews in IT and other important support functions,” says Sharton.

85% of companies executives surveyed by the CNBC Technology Executive Council said at least half of their employees are now working remotely, while 36% of them said they have noticed a consequent rise in the number of cybersecurity threats (Rosenbaum, 2020). One executive even said the number of phishing and cyber scams his team had noticed were up by 40% since the pandemic erupted. On the other side of the Atlantic, British companies have reported a 400% spike in similar cybersecurity threats over the past six weeks (Corfield, 2020).



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Example of Phishing attempt. Source: Andrew Levine / Public domain

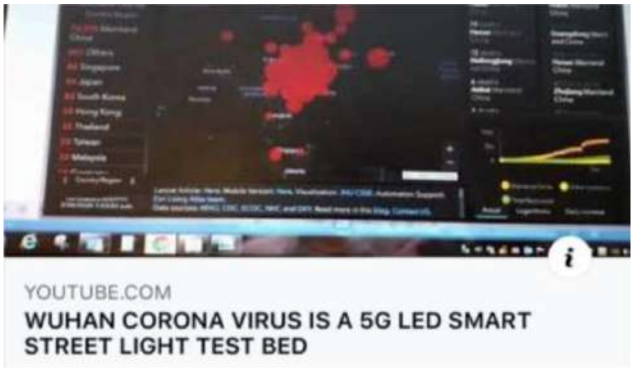
The most common threats emerging during this tumultuous time are phishing, malware and ransomware attacks, according to cybersecurity experts (Adriano, 2020). For many employees, connecting to the corporate server through a virtual private network (VPN) isn't something they're familiar with. Considering how rapidly the COVID-19 pandemic spread, it seems likely that corporations may have rushed their instructions and guides for employees to connect. This leaves severe vulnerabilities for the cybercriminals to exploit. Even in cases where the VPN connection is secured, attackers have found vulnerabilities in home network infrastructure and private internet connections to launch their attacks (Doffman, 2019).

The threat expands further as government employees and legislatures attempt to move to remote workspaces this week. Nicole Coughlin Raimundo, chief information officer for the Town of Cary, North Carolina, U.S., has noticed a spike in the number of phishing campaigns her team faces since moving to work-from-home (WFH). Cary's IT team has deployed security measures like antivirus, endpoint and remote support solutions, but employees' home networks may not be as secure as the town's office network (Rosenbaum, 2020).

Together, corporate and government employees could be facing billions of dollars in additional costs from ransomware, phishing or malware attacks. Aggregate cybersecurity costs for the entire economy could boom this year, just as the recession hits, applying the costs everyday users and taxpayers face. However, there seems to be much more at stake than just money. State-sponsored cyber attacks add yet another regretful and petrifying dimension to this crisis.

State-Sponsored Panic

The flow of information has never been so weaponized as it has in recent years. Bradshaw & Howard (2019) found that the number of countries using misinformation for political purposes online had jumped from 28 in 2017 to 70 in 2019. The most prominent countries in their findings are now also involved in a misinformation campaign against their own citizens as well as against rival states.



YOUTUBE.COM

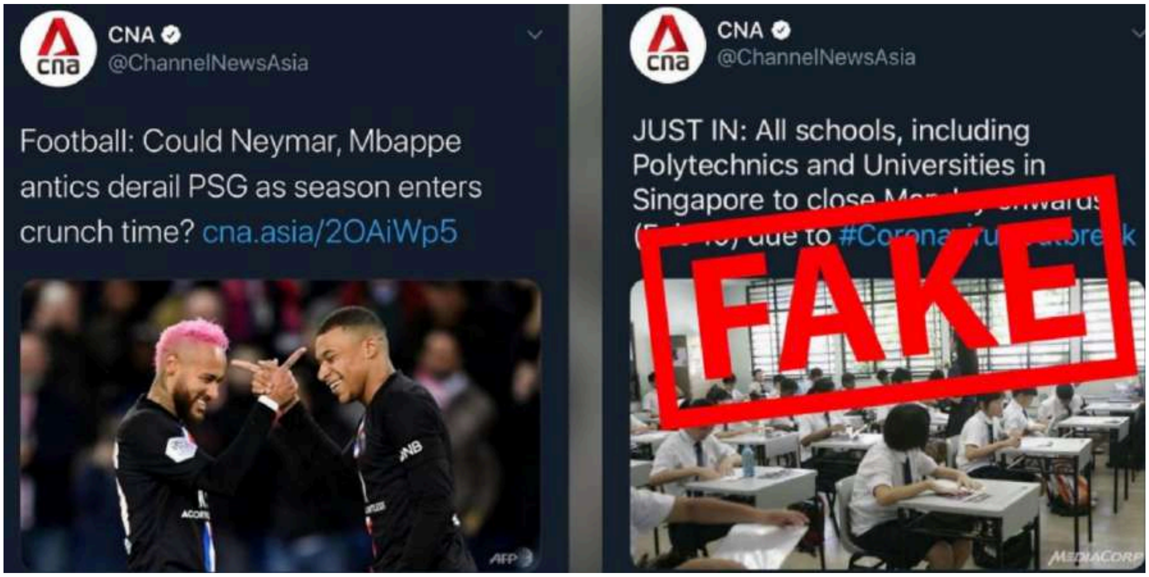
WUHAN CORONA VIRUS IS A 5G LED SMART STREET LIGHT TEST BED

Example of misinformation, Source: Cellan-Jones, 2020

Social media platforms in Iran, China, Venezuela and Egypt have all been flooded with false and misleading claims and conspiracy theories that have caused widespread distress and panic during this health crisis (Beavers, 2020).

Nearly all these conspiracy theories are focused on the origins of the COVID-19 virus and the intentions of its creators.

However, the biggest and most brazen attacks seem to have been launched by the Russian state authorities. An internal European Union briefing states that Russia's state- aligned media has launched a significant disinformation campaign against the West to worsen the impact of the coronavirus, generate panic and sow distrust (Emmott, 2020). "For the Kremlin, Covid-19 is an opportunity as well as a crisis," says Foxall (2020). "Russia has long sought to subvert the rules-based international order by creating fractures within Western societies, or taking advantage of pre-existing ones."



CNA @ChannelNewsAsia

Football: Could Neymar, Mbappe antics derail PSG as season enters crunch time? cna.asia/2OAiWp5

CNA @ChannelNewsAsia

JUST IN: All schools, including Polytechnics and Universities in Singapore to close [illegible] onwards [illegible] due to #Corona[illegible]

Example of Misinformation, Source: Lim, 2020

Designed as viral social media posts, the false claims include accusations that illegal migrants were importing the virus into countries, that the virus was a bioweapon developed by China, or that the U.S. had created the virus to weaken other nations (Jozwiak, 2020).

The Kremlin's disinformation campaign isn't just targeted abroad. According to health experts, Russian President Vladimir Putin's administration has also clamped down on the number of reported cases of coronavirus in Russia to prevent the public from fully acknowledging the crisis (Greenberg & Fomina, 2020). Despite its population of 140 million, Russia reported 147 cases of coronavirus disease, and zero fatalities, as of March 18.

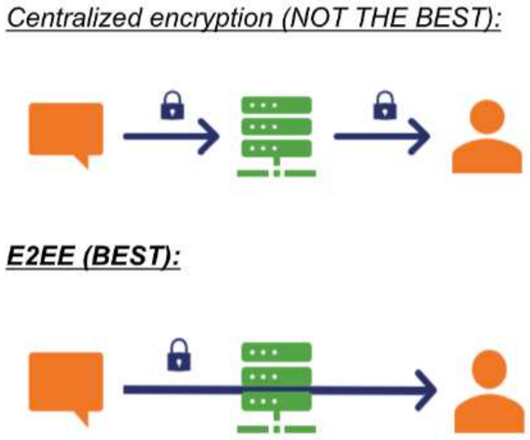
Solutions

Governments have clamped down on the disinformation. Canada's Communications Security Establishment stated they have already taken down fake websites posing as government agencies and misdirecting Canadians. The intelligence agency also warned that health organizations across the country now face an «elevated level of risk» of cyber security incidents (Tunney, 2020).

However, the government's arsenal for cybersecurity may be limited while fighting a war on several fronts. As government infrastructure and citizen data comes under attack from other states and nefarious criminals with sophisticated tools, nations need equally sophisticated forms of protection.

The standard solution recommended by experts is end-to-end encryption (**E2EE**). End-to-end encryption facilitates the type of encrypted communication that only the sender and receiver can read/see. A signal of its effectiveness is the fact that the several governments, including Australia, the UK and US, attempted to block Facebook's implementation of **E2EE** on its WhatsApp platform (Thakkar, 2019). This indicates that **E2EE** may supersede national intelligence agency capabilities and could thus be an effective tool to safeguard private, sensitive or classified data.

The other cutting-edge solution is Z**ero-Trust** (or 0-trust) file sharing. Developed by John Kindervag, principal analyst at Forrester Research Inc. in 2010, **Zero Trust Network**, or **Zero Trust Architecture** is now moving into mainstream adoption (Pratt, 2018). This method goes further than simply encrypting the file, it stores it on a virtual server that is placed behind a firewall.



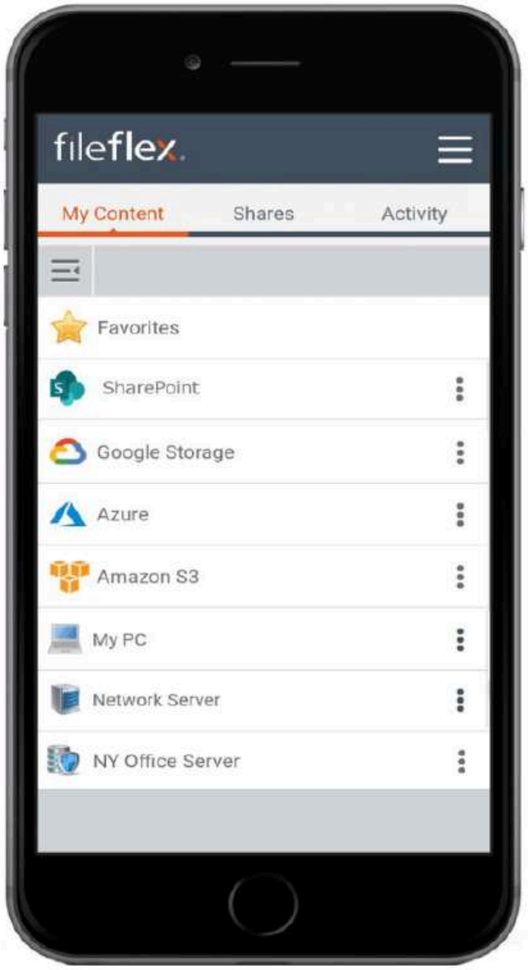
This system allows company users to access their files from anywhere, using any device, since they never need to store, download or share the files themselves.

Combining these two cutting-edge techniques could deliver precisely the platform government institutions and medical researchers need to safeguard their

sensitive research information/data, and provide a new tool in the fight against COVID-19 misinformation across the web. Which is why SafeSwiss has amalgamated **E2EE** along with the **zero-trust** architecture of **FileFlex** (developed by the Canadian company QNEXT) - a platform for remote data access and hybrid IT infrastructure.

The "never trust, always verify" model that underlies **FileFlex's** platform allows users to access their data from anywhere and any device without compromising on security. Every interaction, piece of information and communication is stored behind an industrial-grade firewall that counteracts third-parties regardless of their sophistication.

And so, on the one hand, while we expect, but cannot yet assume with undiluted certainty, that the upper levels of the Canadian government such as the Prime Minister's Office (PMO), the Canadian Security Intelligence Service (CSIS), and our Diplomatic Core (Global Affairs), already utilize **E2EE** and **zero-trust** architecture among other tools. But on the other hand, what we do know, is that the majority of medical researchers, healthcare workers and other government employees have never had access to such sophisticated tools as they rely on their local IT networks in their respective government agencies/ministries.



Demonstration of the FileFlex platform.

Source: SafeSwiss

Now that a substantial number of medical researchers and government employees are compelled to work from home, the Canadian government could adopt quick and convenient commercial solutions such as **E2EE** email/text/telephony, and **FileFlex** to rapidly safeguard their workforce and the nation's critical data. While some current remote workers feel somewhat safe in the knowledge that they are using a virtual private network (VPN), it is interesting to note, that "By 2023, 60% of enterprises

will phase out most of their remote access VPNs in favour of the safer Zero Trust Architecture" – Gartner.

As the world fights a crisis of unprecedented proportions, amplified by the misinformation campaigns of rogue nations, Canadian authorities and industry leaders must work together to safeguard the nation's health, data and future. We believe a solution driven by science and technology is the need of the hour.

About David Bruno :

As founder and CEO of a global cyber security firm, David specialises in anti-fraud and anti-corporate espionage systems worldwide. Through his company, Secure Swiss Data (now SafeSwiss®), he provides financial sector solutions for the digital and interactive FINTECH sectors. For 20 years he has worked to provide security protections to the masses and has invested his own money in a free E2EE encrypted email server for the public. He is a contributor and member of Electronic Frontier Foundation EFF advocating for defending digital civil liberties. He also educates on the surveillance of email in general and the importance of encryption, especially for vulnerable populations like refugees.

References

Adriano, L. (n.d.). Expert: Phishing attacks against work-from-home employees are on the rise. Retrieved from https://www.insurancebusinessmag.com/ca/news/cyber/expert-phishing-attacks-against-workfromhome-employees-are-on-the-rise-217178.aspx

Beavers, O. (2020, March 20). Pompeo says China, Russia, Iran are spreading disinformation about coronavirus. Retrieved from https://thehill.com/policy/national-security/488659-pompeo-says-china-russia-iran-are-spreading-disinformation-about

Canada's health sector at risk of cyberattacks as COVID-19 fear spreads: CSE | CBC News. (2020, March 19). Retrieved from https://www.cbc.ca/news/politics/health-covid-cyberattack-pandemic-1.5502968

Cellan-Jones, R. (2020, February 26). Coronavirus: Fake news is spreading fast. Retrieved from https://www.bbc.com/news/technology-51646309

Corfield, G. (2020, March 20). Online face mask sales scams, 400% uptick of coronavirus phishing reports: Brit cops'; workload shifts online along with the nation's. Retrieved from https://www.theregister.co.uk/2020/03/20 coronavirus_scam_reports_police_up_400pc/

Doffman, Z. (2019, August 20). New Cyberattack Warning For Millions Of Home Internet Routers: Report. Retrieved from https://www.forbes.com/sites/zakdoffman/2019/08/20/new-study-warns-guest-networks-open-millions-of-home-internet-routers-to-cyberattack/#1dd9f08c664d

Emmott, R. (2020, March 18). Russia deploying coronavirus disinformation to sow panic in West, EU document says. Retrieved from https://ca.news.yahoo.com/russia-feeding-disinformation-coronavirus-sow-092759812.html

Erprose. (2020, March 20). Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems. Retrieved from https:/www.cnbc.com/2020/03/20/phishing-spam-spike-as-hackers-use-coronavirus-to-hit-remote-work.html

Foxall, A. (2020, March 19). Coronavirus conspiracies are a gift to Russia&#39;s disinformation machine. Retrieved from https://www.telegraph.co.uk/politics/2020/03/19/coronavirus-conspiracies-gift-russias-online-disinformation/

Jozwiak, R. (2020, March 19). EU Monitors Say Pro-Kremlin Media Spread Coronavirus Disinformation. Retrieved from https://www.rferl.org/a/eu-monitors-say-pro-kremlin-media-spread-coronavirus-disinformation/30495695.html

Paddon, D. (2020, March 18). Fraudulent COVID-19 emails specifically target Canadians, security firm says. Retrieved from https://www.thestar.com/business/2020/03/18/fraudulent-covid-19-emails-specifically-target-canadians-security-firm-says.html

Pratt, M. K. (2018, January 16). What is Zero Trust? A model for more effective security. Retrieved from https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

Russia says it has hardly any coronavirus cases. Doctors say otherwise. (2020, March 20). Retrieved from https://codastory.com/waronscience/russia-coronavirus-mistrust/

Sharton, B. R. (2020, March 20). Will Coronavirus Lead to More Cyber Attacks? Retrieved from https://hbr.org/2020/03/will-coronavirus-lead-to-more-cyber-attacks