Hindawi
Journal of Advanced Transportation
Volume 2021, Article ID 6627264, 19 pages
https://doi.org/10.1155/2021/6627264

Review Article

Cybersecurity and Countermeasures at the Time of Pandemic

Rabie A. Ramadan,[1,2] **Bassam W. Aboshosha**,[3] **Jalawi Sulaiman Alshudukhi**,[1] **Abdullah J. Alzahrani**,[1] **Ayman El-Sayed**,[4] **and Mohamed M. Dessouky**[4,5]

[1]*College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia*
[2]*Department of Computer Engineering, Cairo Universality, Cairo University, Giza, Egypt*
[3]*Department of Computer Engineering, Higher Institute of Engineering, El-Shorouk, Cairo, Egypt*
[4]*Department of Computer Science & Engineering, Faculty of Electronic Engineering, Menoufia University, Shebeen El-Kom, Egypt*
[5]*Department of Computer Science & Artificial Intelligence, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia*

Correspondence should be addressed to Rabie A. Ramadan; rabie@rabieramadan.org

Received 27 November 2020; Revised 7 December 2020; Accepted 23 January 2021; Published 16 February 2021

Academic Editor: Muhammad Arif

With the emergence of one of this century's deadliest pandemics, coronavirus disease (COVID-19) has an enormous effect globally with a quick spread worldwide. This made the World Health Organization announce it as a pandemic. COVID-19 has pushed countries to follow new behaviors such as social distancing, hand washing, and remote work and to shut down organizations, businesses, and airports. At the same time, white hats are doing their best to accommodate the pandemic. However, while white hats are protecting people, black hats are taking advantage of the situation, which creates a cybersecurity pandemic on the other hand. This paper discusses the cybersecurity issues at this period due to finding information or finding another related research that had not been discussed before. This paper presents the cybersecurity attacks during the COVID-19 epidemic time. A lot of information has been collected from the World Health Organization (WHO), trusted organizations, news sources, official governmental reports, and available research articles. This paper then classifies the cybersecurity attacks and threats at the period of COVID-19 and provides recommendations and countermeasures for each type. This paper surveys the cybersecurity attacks and their countermeasures and reports the ongoing cybersecurity attacks and threats at this period of time. Moreover, it is also a step towards analyzing the efficiency of the country's infrastructure as well as hackers and criminals' social behavior at the time of the pandemic.

1. Introduction

Humanity has been suffering from several diseases and epidemics since the early days. However, the volume and prevalence of these diseases have not increased dramatically over the past decades, as happening recently. This noticeable shift in recent times is the result of multiple factors where geography and widespread trade could be one of the reasons in pandemic spread. In these early years, malaria, tuberculosis, leprosy, flu, smallpox, and more appeared first [1].

In the last decades, several epidemics had been spread. The most prominent of which are new types of influenza, swine flu (H1N1), bird flu, and several types of coronaviruses, including severe acute respiratory syndrome (SARS), Middle East respiratory syndrome (MERS), and 2019 novel coronavirus. 2019 coronavirus is known as 2019-nCoV or coronavirus disease 2019 (COVID-19). Other epidemics have also spread in the last decade, perhaps the most dangerous was the Ebola virus spread to several African countries and the Zika virus which had been spread in South America. Before 2009, avian influenza (2003) emerged and caused about 400 deaths and SARS virus (2002) had killed 800 people worldwide. Figure 1 shows the epidemic's history starting from 430 BC to date. The figure shows the epidemic

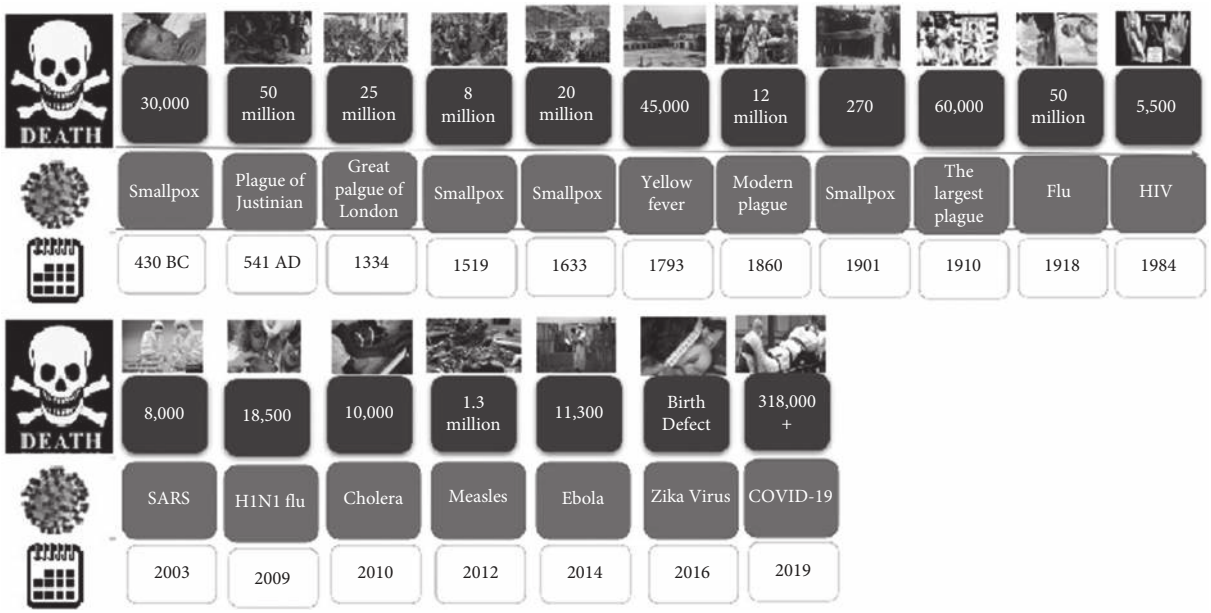

Figure 1: The history of epidemics [2, 3].

time, the epidemic name, and the number of death cases [2, 3].

Researchers use a simple tracking of a disease known as the reproductive number, named R0 or "R naught." Such a number indicates how many other people, in turn, will be affected on average by each infected person. Such a measure can be seen in Figure 2, which shows how many people were infected from a single person. As shown, measles is at the top of the list where R0 is within 12–18, which makes it the most contagious. This suggests that a person infects on average 12 to 18 other persons from his circle. While measles is considered the most virulent, immunization efforts reduced its propagation.

However, even though the scientists are very close to a vaccine, it is very complex to predict the true impact of COVID-19 [4]. In addition, no vaccine has been discovered yet. Such epidemics cause panic and anxiety in the world due to death acceleration among those who are infected and the number of people infected every day [5, 6]. Such pandemics cause the stock markets to collapse as well as other world's finance, business, and investment, which may bring down the economies of those infected countries. Also, its continued spread among countries shakes global stability and incurs huge human losses. This puts heavy burden on the global economy that may require years to compensate for it. However, while the world focuses on the health and economic threats that COVID-19 poses, cyberthreats increase during these times, as the environment is well suited for cybercriminals to strike. Cybercriminals around the world undoubtedly take advantage of this crisis [7].

The motivation of this work is to record the malware activities at the time of the pandemic, especially COVID-19. In addition, at the time the world is busy with treating the people and their health, this paper reports people's behavior in terms of security, either computer security and physical security. This paper also introduces different countermeasures that are used by the IT administrations to avoid security violations at the time of the pandemic.

The contributions of this paper are as follows:

(i) This paper investigates the recent malicious cyberattacks during the COVID-19 pandemic and how COVID-19 impacted the cybersecurity threat landscape so far.

(ii) It reports the history of the pandemics and their effect.

(iii) This paper draws some conclusions about physical security and the people's behavior during the time of the pandemic.

(iv) This paper draws some recommendations to organizations and individuals that can be applied to reduce the risk of being impacted.

(v) This research is considered, up to our knowledge, the first research to report and survey the cyberattacks at this short period of time, where collecting the cybersecurity information was a very hard job. Therefore, the main sources of information reported in this paper depend on trusted organizations, accurate news, and available research articles.

(vi) This paper surveys the different countermeasures for the different cybersecurity attacks reported in the paper.

This paper is structured as follows. Section 2 describes the regular cybersecurity attacks and their classifications in regular times. Section 3 is the core section of this research where it describes in detail the cybersecurity classifications and examples at the time of COVID-19. We call the

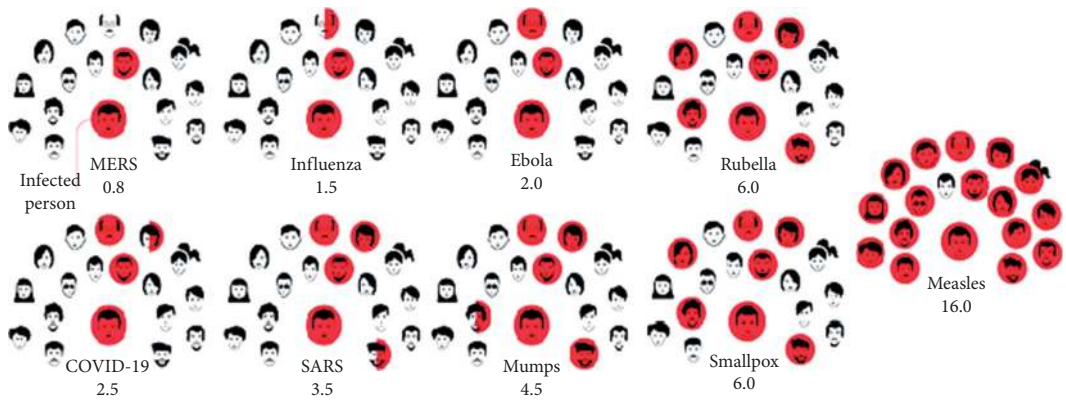

Figure 2: The average number of susceptible infected people.

cybersecurity at the time of COVID-19 as "Cybersecurity Pandemic."The cybersecurity countermeasures and some of our recommendations are discussed in Section 4. The paper is concluded with the "Conclusion" section.

2. Cybersecurity Attacks

This section provides a brief description of the regular attacks that will be discussed in this paper. Figure 3 shows the classification of cybersecurity attacks which are composed of four categories of attacks.

2.1. Flow Control Attack. Flow control attack means changing the predefined control flow of an application to achieve the attacker's goal. One of the earliest flow control attacks is the code injection attack, where a machine code is written in the program memory, creating a bug that directs the main program to the new exploited code. This attack could be mitigated by using the so-called W⊕X protection technique, which ensures that memory is writable or executable (but not both).

The other type of flow control attack is a code reuse attack in which a software flaw had been used to weave control flow to a malicious end via an existing codebase. For instance, the return-in-libc technique (RILC) is a relatively simple code-reuse attack that compromises the stack and transfers control to an existing libc function. It is often used to call a system to launch a process or to create a writable, executable memory area to bypass W⊕X [8].

2.2. Injection Attack. In the injection attack, an attacker provides a program with untrusted input. This input is processed as part of a command or query by an interpreter. In turn, this alters the execution of that program. Injection attacks are not new attacks, but they are categorized among the oldest but most dangerous web-based attacks. They can result in data theft, data loss, data integrity loss, denial of service, and complete system compromising. The injection attacks could be further classified into malware, false data, and sabotage:

(i) *Malware* is any malicious program or code that is harmful to systems or "malicious software." Hostile, disruptive, and deliberately irritating malware seeks to penetrate, destroy, or disable a device's operations, sometimes by taking part in the control of servers, operating systems, networks, tablets, and mobile devices. It interferes with normal functioning, as does human flu [9].

(ii) *False data* is the attack that targets measurements as well as data in various systems; one clear example is the power system where the false data attack tries to disrupt the system's normal operation [10].

(iii) *Sabotage* is a deliberate attempt to undermine a policy, initiative, or organization by subversion, obstruction, disturbance, or destruction. This could be through memory corruption, through crashing a machine or software, or even through the electromagnetic pulse.

2.3. Information Leakage Attack. Information leakage means disclosing information unintentionally to end users to breach the application security. Information leakage attack is divided into side-channel attacks and encryption key bypass:

(i) *Side-channel attacks (SCAs)* aim to extract secrets from a chip or system by measuring and analyzing their physical parameters. These attacks are a major threat to cryptographic system modules because many SCA techniques have successfully breached a cryptographing operation (for instance, encryption) that is algorithmically robust and obtains the secret key. SCAs could be unintentional or intentional or data-driven [11].

(ii) *Encryption key bypass* is the second type of information leakage attack, and it happens through phishing or insider attacks [12].

2.4. Denial of Service (DoS) Attack. Denial of service (DoS) attack means that the attacker tries to make the system/application resources unavailable to its intended users by temporarily or permanently disrupting its services. It has

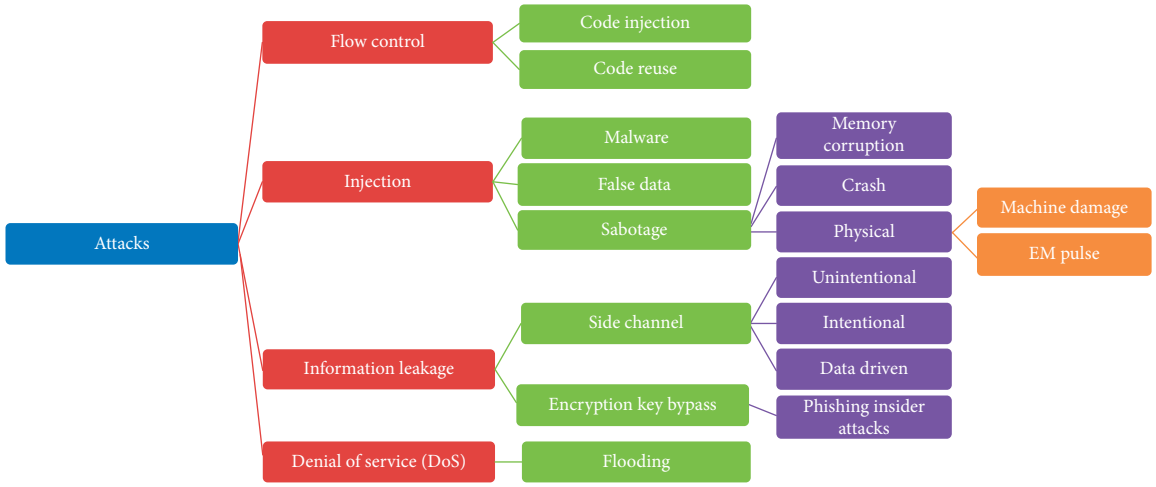

Figure 3: Cybersecurity attacks classification.

different shapes, but the most important method is flooding [13, 14].

3. Cybersecurity Pandemic

Cybersecurity at the time of COVID-19 is also considered another pandemic where many attacks are launched in a very short time. Although this pandemic and the whole world are busy searching for a cure, cybersecurity crimes had been increased these days. Figure 4 illustrates the infographic of the worldwide cybersecurity crimes during the COVID-19 pandemic.

Nowadays, there is an increasing interest in cybersecurity since COVID-19 pandemic started. This section classifies the cybersecurity threats and attacks based on the documented reported cases at the time of the COVID-19. Figure 5 shows the classifications of the different recent cyberattacks during the COVID-19 pandemic, and the details are described in the following sections. Also, Table 1 shows the cybersecurity attack types and related references.

3.1. Working from Home Malicious Cyberthreats. The COVID-19 pandemic caused many citizens to work for the first time from home. Working from home has other cybersecurity threats, such as intentional cybercrime. When any personal computer or mobile phone is compromised, unauthorized access to the stored information can have a devastating effect on personal, emotional, financial, and working life [15].

Figure 6 classifies the different types of working from home threats. In the following sections, major working from home threats are discussed.

3.1.1. Unsecured Home Networks. As part of controlling of the coronavirus (COVID-19) spread, several organizations have encouraged or forced their staff to work from home. This presents new cybersecurity challenges that must be managed. During the pandemic, almost all employees are connected through their home network, which is not secure enough as their work network; therefore, they are exposed to risks. All home networks, as well as machines, often lack security measures used to be in the company network, such as the following:

(i) *Antivirus Programs*. Antivirus solutions will allow the detection of malicious code. A successful antivirus system will always determine whether a file contains suspicious activities, avoiding destruction or stealing of information [17].

(ii) *Firewalls*. A firewall is a network traffic control protection tool. Firewalls generally process network traffic from the Internet to a specific system and may function in two separate ways: to permit all network packets and block only suspicious ones, or deny all packets and to accept only those which are considered appropriate [18].

(iii) *Intrusion Detection Systems (IDSs)*. IDS means monitoring the network traffic patterns and analyzing such traffic to detect any intrusion to the system. The IDS works by comparing the network activity to a defined database of vulnerabilities and their range of activities, such as violations of protection policies, ransomware, and port scanning [19].

(iv) *Intrusion Prevention System (IPS)*. It represents a shield between the outer environment and the internal network. It is a proactive system that rejects network traffic according to the vulnerability profile [19].

3.1.2. Different Technologies. When working from home, different technologies may be available at home than those available at work. Several concerns must be considered, such as the following:

(i) *Poor Experience*. When working from home, employees may need to use other software or unfamiliar applications differently, compared to what they used when they were at their offices. Here, a

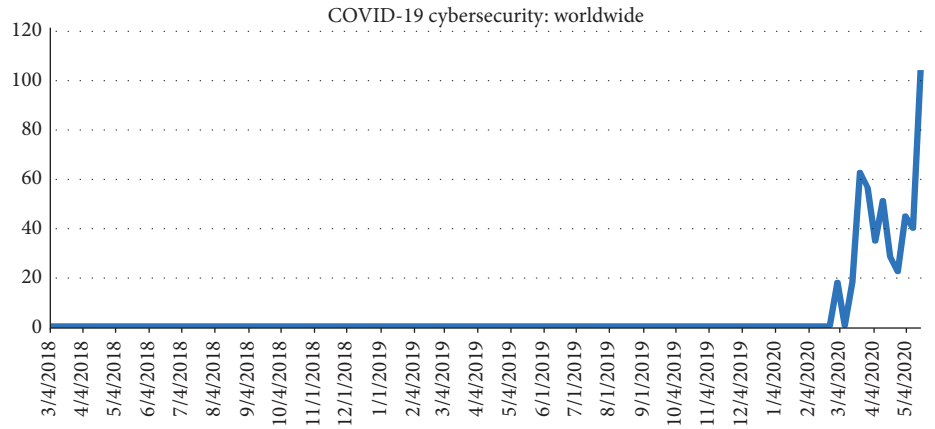

Figure 4: COVID-19 cybersecurity-based Google trends.

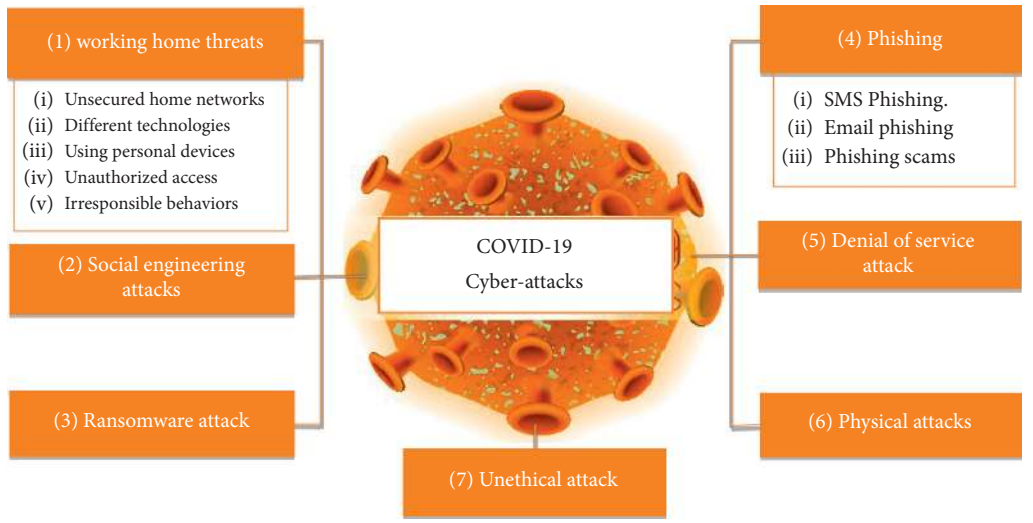

Figure 5: COVID-19 malicious cyberattacks.

Table 1: Pandemic cybersecurity classifications.

Attack type	References
Remote access infrastructure attacks	[9, 11–13]
Social engineering attacks	[14–16]
Phishing attack	[17–21]
Distributed denial of service (DDoS) attack	[22–27]
Ransomware attack	[24, 28–31]
Physical attacks	[32–41]
Unethical attacks and behaviors	[24, 27, 31]

new challenge is defined, which is the employee's ability to learn new technologies. In addition, they might not be able to ask an office workmate for help, as they normally do. So, it should be checked how staff are coping, not just how to use new technologies but also how they are adapting to having to work in a very different environment [20].

(ii) *Less Functionality*. The software and application programs used at home may have fewer features and capabilities than the office software.

(iii) *Productivity*. The previous two factors may directly affect the throughput, and in the worst case, some tasks may be unachieved or canceled or may not be accomplished within the deadline limits.

3.1.3. Personal Devices. When working from home, employees usually use their personal devices; most probably, they feel more comfortable using them. However, personal computers or laptops are very likely to exist. Therefore, the following risks might be in place [20]:

(i) *Lack of Performance*. Organizations often used high-performance workstations with higher processing elements and memory storage capacity than personal computers or laptops or mobiles.

(ii) *Usage of Untrusted Programs*. They expose data to different threats that might lead to data loss or to improper operations and processes which increases the risk of potential malware.

(iii) *Lack of Backup Mechanisms*. These may have some loss of data or at least losing the recent updates.

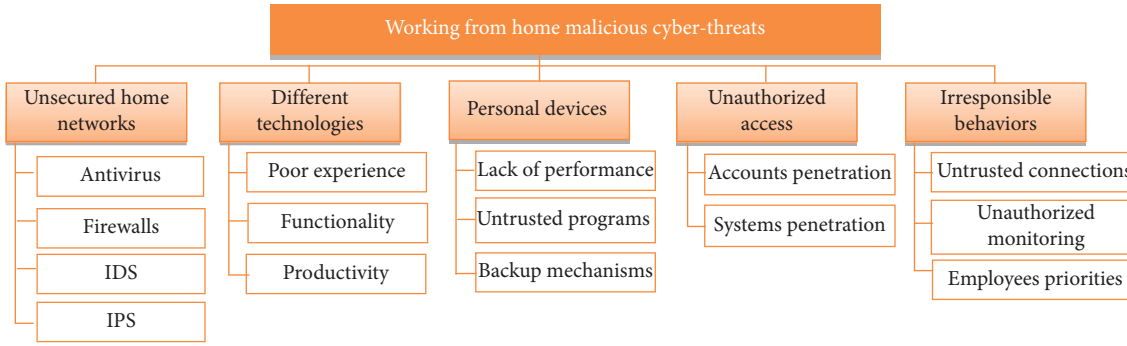

Figure 6: Threats of working from home.

3.1.4. Unauthorized Access. It is an important problem that happened due to working at home. The attackers continue to attempt to access the system without any authorization. The following threats may apply:

(i) *Penetration of Employee Accounts*. Many organizations had rapidly deployed new infrastructures not used before and created new employee accounts to get access. Most employees choose simple passwords, which might lead to privacy breach or system vulnerability. The most common passwords revealed how repetitive and ignorant of potential security threats are. The UK's National Cyber Security Center (NCSC) breach analysis showed that, worldwide, 123456 is used as a password by 23.2 million victims' accounts.

(ii) *Penetration of Corporate Systems*. Due to the pandemic, many of the organizations deployed new network infrastructure rapidly to cope with work from home environment. Malicious cyber actors are leveraging a number of established vulnerabilities on VPNs and other remote work devices and applications to take advantage of this transfer to work from home. Due to the rising number of organizations and people using online communication tools, such as Zoom and Microsoft Teams, malicious cyber actors hijack online meetings, teleconferences, and online courses, which have been established without security controls (e.g., password).

3.1.5. Irresponsible Behaviors. Here, the recommended security policy could be violated when employees work from home and follow irresponsible behaviors such as [22] the following:

(i) *Untrusted Connections*. Some of the employees work from outside of their home using public Wi-Fi networks, which are considered as a perfect entry point for system attack and data theft.

(ii) *Unauthorized Monitoring*. Employees who are working at home may be susceptible to unauthorized monitoring from untrusted personnel such as a spiteful neighbor and spy.

(iii) *Employee Priorities*. When working from home, employees have different priorities where exceptional family care needs impact personnel availability.

3.2. Social Engineering Attack. The social interfingering attack is another type of cybersecurity threat where malicious cyber actors use foundational social engineering techniques to enable a person to perform specific acts. Those actors leverage human characteristics such as interest and anxiety regarding the coronavirus pandemic to persuade possible victims to [23] the following:

(i) *Click a Link or Download an App*. Clicking a link may lead to a phishing website or downloading malware. For example, during the pandemic, an Android application has been developed for the actual coronavirus outbreak tracker. Attacks aim to trick the user into giving their administrative access to the "CovidLock" where ransomware is installed on their systems.

(ii) *Open a Malware-Containing File*. This comes from opening an email attachment with phrases related to COVID-19 updates or new medication. Malicious cyber actors spoof the sender as the email comes from an authentic person or entity, such as the WHO, or a person at the WHO, with "Dr." Actor sends phishing emails with links with a fake login page in many cases. Another example would be an email originated from the human resources (HR) department of a company with an attachment for the recipients to open. These emails include Coronavirus file attachments or related COVID-19 issues such as "President discusses the budget savings due to coronavirus." These may be called malicious file attachments with malware payloads [28].

The uptick in socially engineered cyberattacks is mainly targeted financial and personally identifiable information (PII) data [23].

3.3. Ransomware Attack. Ransomware is a type of malicious money-extorting attack. In general, the malware operates by disabling the whole operating network or by encrypting a

user's data, which allows the user to compensate for it. Attacks by ransomware are primarily aimed at large organizations because they have a large volume and are ready to pay for them.

Bitcoin had become one of the most popular currencies that is demanded by attackers as payment because of their anonymity and transaction speed. Ransomware is considered a serious challenge to every type of business, not only by locking the data from access but also by selling the information if the user did not pay the ransom. Well, loss of life is not expected in these situations [29, 42].

However, if an intruder reaches the health care system in a health disaster all around the planet, therefore, severe human casualties may be incurred. COVID-19 and ransomware give hackers a unique, versatile platform for attacks. Medical services are more critical than ever and are often easy malware targets. The criminals are certain that the health organizations are going to pay the ransom when clinics, emergency facilities, and public institutions are attacked since they are overloaded by health problems and cannot continue to shut down their networks. It may be an entire tragedy during a pandemic.

Interpol also alerted hospitals and medical institutions that during heightened fear and communication in the medical environment, they are at risk of being attacked by ransomware attackers. Combined with the famous fact that IT systems are outdated so much, it is possible that today's medical facilities run software with a known exploit. Attackers take advantage of this situation by

(i) Running ransomware attacks faster

(ii) Recruiting others to maximize their impact

(iii) Ransomware-as-a-service is utilized effectively on the dark web

Since the rate of ransomware attacks is increasing, especially during the COVID-19 time, the following sections introduce several accidents of ransomware attacks.

3.3.1. A Food Delivery Service in Germany Faced a Bitcoin Ransom Attack. COVID-19 pandemic forced Germany to take severe actions, implementing severe restrictions on the restaurant industry. As a result, German citizens have become more dependent on still operating delivery services. One is Liefrando, which supplies food from over 15,000 restaurants. Cyberattackers have launched a ransomware attack on the German food delivery company "Takeaway.com" (Liefrando.de). Food orders were received but could not be processed; consumer refunds were to be issued by Liefrando. This can cause certain companies to compensate for cybercriminals or invest in security systems for sophisticated threats [33].

Liefrando tweets that orders paid online and were not delivered due to the system attack will be refunded as soon as possible, and the situations are repairing as shown in Figures 7(a) and 7(b).

3.3.2. Coronavirus Vaccine Test Lab Attacked by Maze Ransomware. In London, cyberattackers using Maze Ransomware attacked the business Hammersmith Medicines Study (HMR), which leaked thousands of patients' personal details. The company involved is reported to have carried out testing to develop the Ebola vaccine as well as medication that could cure the disease of Alzheimer's and had been on hold until they were targeted with Maze malware to carry out research on possible coronavirus vaccines. The HMR reported that their IT department discovered the attack on 14th March 2020, but they were able to restore both services effectively by the day's end [43].

On 21st March 2020, the attackers reported tens of thousands of patients' information between the ages of 8 and 20. Medical records, copies of passports, driving licenses, insurance details, and more were compromised. HMR Managing Director and clinical manager and the doctor confirmed that they do not wish to compensate for the ransom: "I would rather quit company instead of charging a ransom to these men." Criminal users also use the RaaS model (Ransomware-as-a-service), which provides certain crooks named affiliates with malicious technology. The members are liable for distributing the initial ransomware and eventually charging the malware developers. The attack is most commonly committed by spam mail campaigns and RDP (Remote Desktop Protocol) attacks. Therefore, hospitals may be attacked by mistake merely because malicious actors target their victims through network vulnerability rather than names of the organization [43].

3.3.3. Ransomware Strikes a Biotech Firm Researching Possible COVID-19 Treatments. When the COVID-19 pandemic had spread through the US, hackers targeted a biotechnology firm headquartered in California that produces instruments that researchers use to learn about coronavirus. The organization is part of an International Alliance that is currently sequencing cells from COVID-19 patients to see whether the disease's cure is feasible. A financial divulgation form submitted in the United States by the 10x Genomics Inc. to the Securities and Exchange Commission confirmed it had experienced a suspected ransomware attack involving the hacking of client details. The organization restored "no direct day-to-day effect" regular activities and stated that it collaborated with law enforcement to examine the violation [44].

Biotech Firm 10x Genomics Inc. had also been targeted by a REvil team using ransomware from Sodinokibi as shown in Figure 8. The attack had been disclosed by the organization in its SEC report on 1st April. On "an.onion" website, a screenshot of the folder directory was reported on the attacker's domain (called REvil), which stated "We extract 1 TB of data from your secure disk "/netapp/scada." We will publish the first portion in three days if you do not e-mail us. It's CYA." [44].

(a) (b)

Figure 7: "Liefrando.de" food supplier tweets [33]. (a) "Liefrando" tweets for refunding orders. (b) "Liefrando" tweets for repairing the situation and accepting orders only.

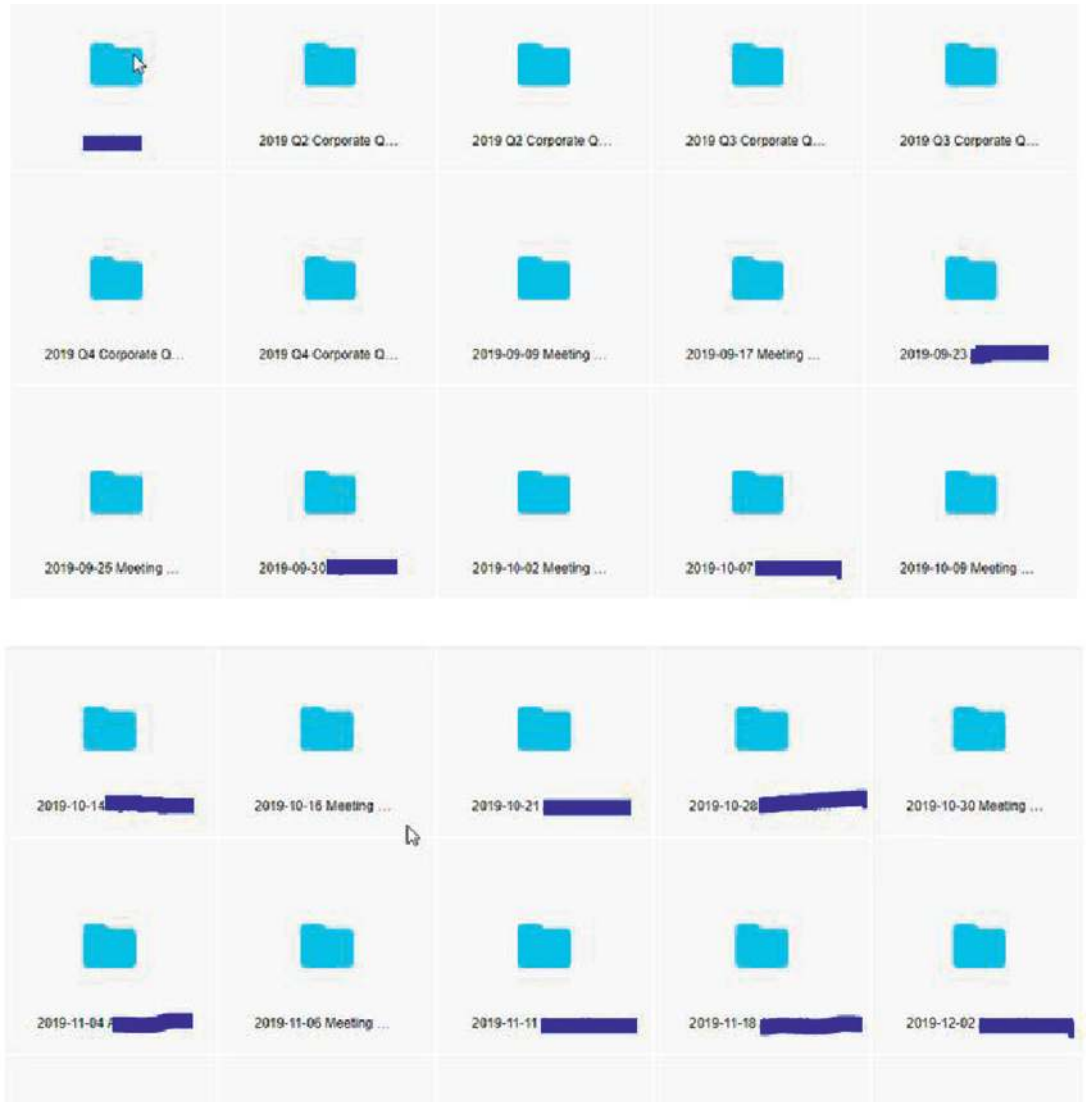

Figure 8: A screen shot folders of files from "10x Genomics" hacked by REvil attacker [44].

3.4. Phishing Attacks. During COVID-19 time, the attackers send different emails or SMS messages with false claims such as having a "cure" or encouraging donation. Like other phishing schemes, these emails and SMS use real-world problems to try to manipulate people into clicking. The scam messages (or phishes) can be very difficult to detect and are intended to get people to react without thinking [45].

Phishing attacks could be classified into three basic types: SMS phishing, email phishing, and phishing scams. These types will be discussed in detail in the next sections.

3.4.1. SMS Phishing. Most attempts at phishing occur via email, but the National Cyber Security Center (NCSC) has identified some attempts to do phishing with text messages. Historically, SMS phishing has used cash rewards as part of the appeal, including granting grants and rebates (such as a tax rebate). Coronavirus-related phishing continues to target the pandemic's financial theme, especially financial support services [46].

SMS messages, for example, use the UK government theme to gather username, address, name, and bank details from victims. The SMS messages from "COVID" and "UKGOV" directly link the phishing website. Figure 9 presents this example of malicious messages that can come in other ways than by email. Besides, SMS, WhatsApp, and other message services are also included as possible channels. In their phishing campaigns, malicious cyber actors are likely to continue to use financial issues. In particular, new government-assistance programs to respond to COVID-19 will probably be used as topics for phishing campaigns [34].

3.4.2. Phishing Emails. Because of the latest coronavirus condition (COVID-19), computer criminals send emails pretending to have a "cure" to the infection, offer financial rewards, or persuade the victim to donate. Like other phishing schemes, such messages play on real-world issues to try to get you to click the provided phishing link. Some of the examples of phishing emails include coronavirus updates, new confirmed cases, outbreaks, and emergency services. Such emails may contain an invitation to an individual to access an URL that is used by malicious cyber actors to steal sensitive details such as usernames and passwords, credit card information, and other personal data, as shown in Figure 10 [47].

The Australia Post reported, as shown in Figure 11, on the COVID-19, a phishing email that was being impersonated by them on Thursday, 19th March 2020. The purpose of this email was to mislead the recipient to access a website that collects Personal Identifying Information (PII) under the illusion of offering advice on travels to countries with COVID-19-verified cases. If the cybercriminals have acquired the PII, they frequently open bank accounts or credit cards on behalf of the victim, using illicit funds to purchase expensive goods or convert money through failed cryptocurrencies, including bitcoin [48].

Figure 12 shows one of the COVID-19-themed phishing emails where the sender presents to be one of the well-known health organizations inviting the recipients to access new information about the COVID-19 virus in their local areas through clicking on a given link [48].

The COVID-19 phishing emails containing fake word documents and other attachments that include hidden computer viruses have also been provided by the Advanced Cyber Security Center (ACSC). Throughout this case, the phishing email pretends to be from the WHO and calls on the receiver to open the attachment. The attached file, when opened, includes malicious software that immediately gets installed on the recipient's computer and allows a malicious agent permanent exposure to certain forms of malware, including spyware or customized contact details (in order to attack acquaintances, the family, and other scams), as shown in Figure 13 [48].

3.4.3. Phishing Scams. The scam messages, or "phishes" are intended to make the person respond without thought and can be quite difficult to spot. Cybercriminals often create a variety of schemes targeted at a growing number of marginalized people. The ACSC was made aware of an international scam that invites people as casual employees or volunteers to help the "Coronavirus Relief Fund." Applicants are advised to accept the provision of donations for social programs of COVID-19. In reality, people who have been innocently caught up in this scam turn into money-mules for cybercrime syndicates, transferring criminal gains into untraceable cryptocurrency. Australians were similarly attacked [49].

On 20th March 2020, Advanced Center for Computing and Communication (ACCC) alerted Australians of a phishing email that asks them to fill an attached form to get $2500 as COVID-19-assistance payments. The attachment contains an embedded macro, which installs malware to your computer. People are advised not to open the attachments and just uninstall the document if such phishing emails are obtained, as illustrated in Figure 14 [48].

3.5. Denial of Service (DoS) Attack. Denial-of-Service (DoS attack) is a computer attack in which the attacker attempts to momentarily or permanently make the services or Internet resources inaccessible to their intended users. Service denial is usually accomplished by flooding the target system or resource with superfluous requests for the intent of overloading and blocking the fulfillment of any or all valid requests [16].

The incoming traffic that reaches the target originates from several separate sites in a distributed denial-of-service attack (DDoS attack). Distributed attacks of denial of service aimed at websites and online services. The aim is to maximize traffic across them, rather than to enable the server or network to run. The goal is to make the website or service inoperative [16].

Institutions that provide public information on the COVID-19 pandemic are the primary aims of such attacks.

Figure 9: UK government-themed SMS phishing [34].

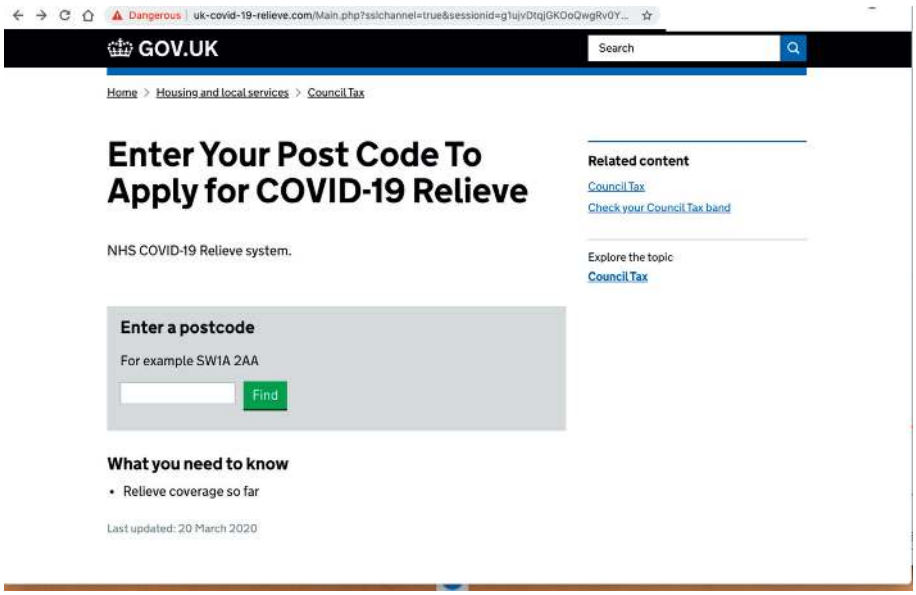

Figure 10: UK government-themed phishing page [47].

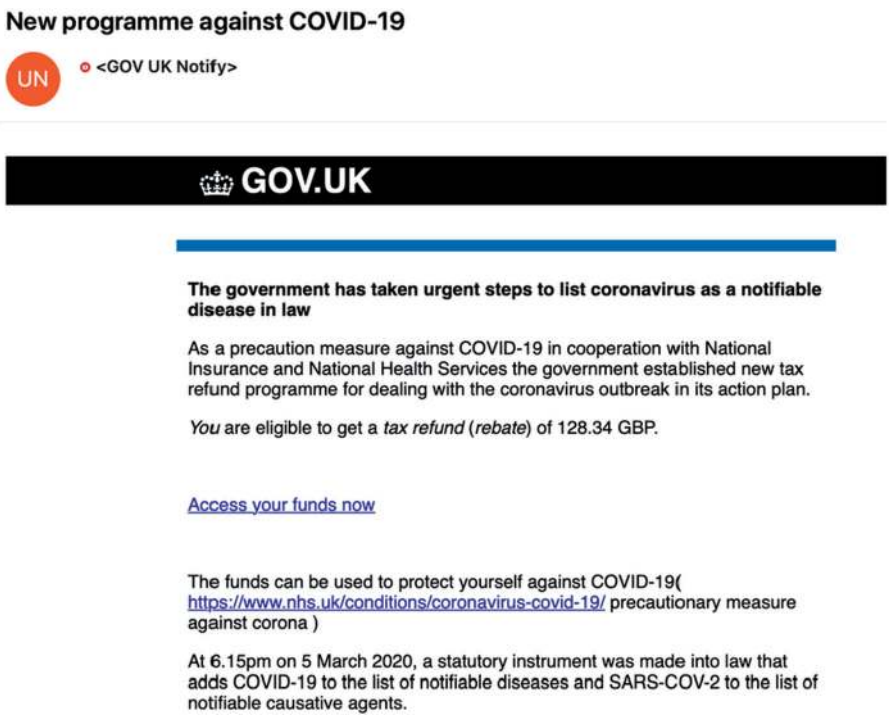

Figure 11: Email misled the recipient to access a website that collects his/her personal identifying information (PII) [48].

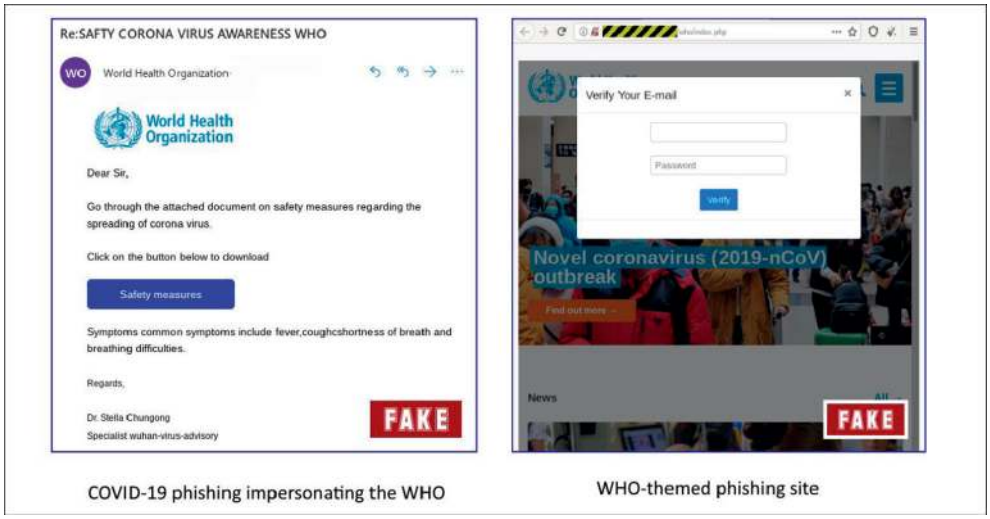

Figure 12: A well-known international health organization-themed phishing page [48].

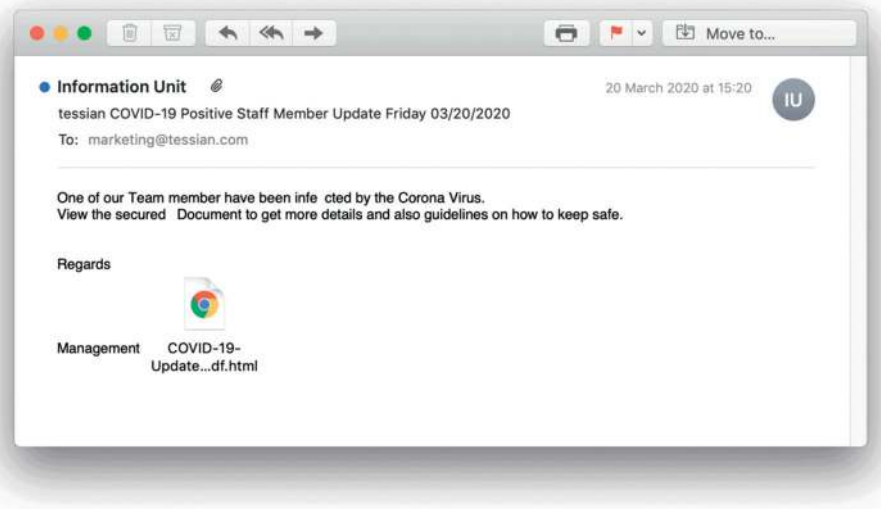

Figure 13: Phishing email containing fake Word documents and other attachments that include hidden computer viruses [48].

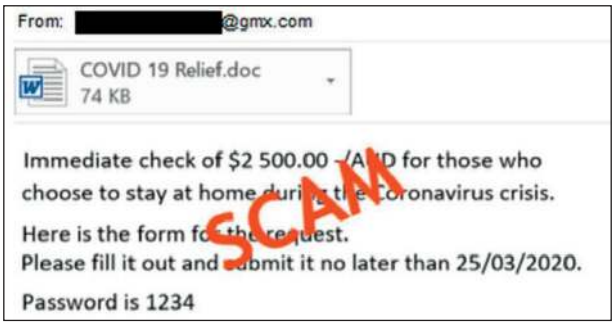

Figure 14: International scam invites people as casual employees or volunteers to help the "Coronavirus Relief Fund" [48].

These institutions include local, state, federal, tribal, media outlets, medical, and health industry agencies. It is anticipated that DDoS will target more of the entities listed above and that attacks against spread phishing would increase. There are several examples of the DDoS recent attacks:

(i) *The U.S. Department of Health and Human Services.* It has experienced a cyberattack on its computer network, where the incident aimed at disrupting the answer to the coronavirus pandemic. The attack was in the form of overloading the HHS servers with millions

of requests for several hours. Extra protection has been implemented by the HHS agency to prevent any future attack. Besides, a continuous monitoring strategy for the network is now in place. This makes HSS and federal networks work normally till the time of writing this article [21].

(ii) *Italy's Social Security Website (INPS)*. Here, attackers were able to force the website to shut down. Therefore, severe disruption to the INPS occurred, as shown in Figure 15. This cyberattack has disrupted COVID-19 payouts. The cyberattack posed questions regarding the health of the digital network in Italy as it deals with the coronavirus emergency. But the riskiest situation is that a sophisticated cybergroup would exploit any of the vulnerabilities and technological defects of a web application to raise the magnitude of the DDoS and finally be ransomed for stopping their activities. This puts Italy's officials in an uncompromising situation and to make a decision of two evils: accept the ransom and launch a wave of identical attacks on public infrastructure or refuse and leave poor citizens unable to seek financial aid because they desperately need it. As early as possible, DDoS protectors ought to offer their support to the concerned organizations, or the first big instance is that cybercriminals steal lives away [30].

(iii) *Brno University Hospital in Brno, Czech Republic*. Brno University Hospital is one of the Czech Republic's largest COVID-19-testing centers. There was a major disruption to the hospital services due to the cyberattack. The accident was nevertheless found to be too serious to about putting off immediate surgery and move to the neighboring St. Anne's University Hospital with new, emergency patients. At the incident, the hospital had to close down the entire IT network and two other divisions, Children's Hospital and the Motherhood Department, which were also impacted [24].

(iv) *Australia's Online Services Site (myGov)*. This site has had to confront a massive DDoS attack for many hours, stopping people from accessing it, as shown in Figure 16. The Minister of Health made the announcement after the lockout of thousands of Australians when seeking to access welfare programs. The federal government's online services site "myGov" has suspected the "serious Distributed Denial of Service (DDoS) attack." The online service witnessed ten times increase in visitors, from 6000 concurrent users to 55,001 users. Unfortunately, this means the 55,001 users could not access the service, which also highlights that other threats are still around [31].

3.6. Physical Attacks. Several reports and news reached out to say that the commercial crime has been increased; these reports abstracted that in the following statement: "It seems like there are some folks out there looking to be opportunistic." They depend on the fact that people are already in panic mode and need assistance [13, 35].

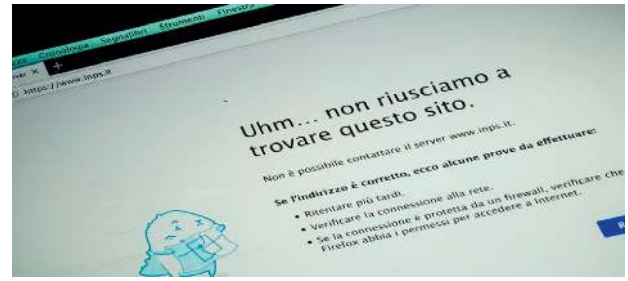

Figure 15: Italy's social security website has been forced to shut down [30].

Figure 16: "myGov" online services site is down by DDoS attack [31].

Several physical attacks that had been collected from different countries are presented as follows:

(i) *Vancouver*. The Vancouver Police Department (VPD) arrested 40 accused thieves in different stealing crimes during a week. These cases threaten the secrecy and privacy of corporate clients' and employees' data besides the corporates' infrastructures. Also, a new phenomenon appeared where three of the parked cars are hit the same way. The attackers smashed the window of the three cars. CTV News examined and compared it with the past four weeks four hours before active distancing steps came into practice. Such data indicate that industrial breakdowns increased by 46%, compared with 85 cases a week over the last four weeks, relative to an average of 58 accidents in the four weeks prior to the start of clear physical separation acts, and in downtown Vancouver, data show that the increase is more evident, which is more than doubled, from 15 accidents a week to almost 35 accidents a week [36].

(ii) *Burnaby*. A surveillance firm monitoring the Big Bend business via closed circuit TV (CCTV) showed the police that a man had broken in and attempted to steal cable. Officers soon had the area surrounded and caught him [37].

(iii) *United Kingdom (UK)*. The surveillance cameras of the UK National Health Service revealed the moment a man stole a bicycle belonging to an employee of the foundation to combat the coronavirus, as shown in Figure 17. The man appeared

Figure 17: The thief stole the bike [38].

on the video clip stealing a bike and then exited it from the portal of Leicester Donner Center, according to the metro website [38].

(iv) *South Africa*. It has been reported by one of the physical security agencies that individuals acting as good citizens distributed free face masks and hand sanitizers. By this way, they can gain access to people's homes and offices. In these cases, cybercriminals believe that people are scared and need to stay secure. The idea of being healthy at present is to use items for cleaning and to keep the house tidy [11, 32].

(v) *Hong Kong*. The police claimed two armed robbers were captured who robbed 600 stool rolls of toilet paper outside a grocery store—a warning that panic was seldom sponsored as a consequence of the outbreak of coronavirus. Local media reported that at about 5 a.m., a truck driver transported the toilet paper rolls to a store in the Mong Kok area. Around an hour later, three guys in their twenties, wearing caps and face masks, turned up. One of them threatened the driver with two guns, while the other two put 50 toilet paper packets or 600 rolls on a trailer. The toilet paper was eventually discovered in a local hotel, and two suspects were charged [39].

(vi) *Spain and Portugal*. The police claimed that the masks in Portugal, gloves, and other personal protection equipment (PPE) had been robbed from a medical supplies business located in Santiago, Galicia, which was in high demand because of the pandemic COVID-19. Throughout the closed factory at a northern city manufacturing park, hundreds of masks had been strongly stacked. But, the photographs released in the last days reveal piles of empty boxes in the building that appear to have been ransacked, as shown in Figure 18. Based on the incident, a joint investigation by both Portuguese and Spanish authorities was conducted. The man is believed to be a property company director [40].

(vii) *Thailand*. Thai police discovered a recycling factory used to repackage used face masks to be sold as new [50].

(viii) *Egypt*. The Egyptian security forces had launched several campaigns during the past period against the exploiters of the emerging outbreak of the coronavirus, including manufacturers and dealers of unknown medical supplies. There were numerous incidents of seizing the exploiters of the corona crisis, whether by raising prices without justification or the perpetrators of commercial fraud crimes, in light of the Egyptian Ministry of Interior's pursuit since the beginning of the crisis of the spread of the coronavirus [25].

(ix) *Giza*. Recently, a tailor had been arrested because he manufactured medical masks of poor quality and sold them to citizens for illegitimate profits, taking advantage of the crisis of the spread of the coronavirus. He had a thousand medical masks and 2,000 masks in the process of being prepared. In the same context, the investigation of the police department managed to arrest four people in possession of 12500 anonymous medical masks with the intention of selling them to citizens.

(x) *Cairo*. A merchant had been arrested, in possession of 24 medical gel packs for sterilization, 20 disinfectant packages, and 423 masks, of unknown origin, for the purpose of selling and making illegal profits. Similarly, the Security Directorate seized a factory producing unsterile medical masks made from unknown sources, and the owner of the factory was arrested. Inside the factory, they found 100 thousand masks ready for sale and three tons of fabrics for future fabrication. Moreover, a hospital worker was arrested in a car loaded with 13,000 medical masks and 25,000 gloves, which had been manufactured in the previous factory. Figures 19 and 20 show some of the medical supplies that do not conform to the specifications of quality.

3.7. Unethical Attacks and Behaviors. Fear of the spread of the novel coronavirus and the severe losses it causes, whether in terms of human casualties or the economic crisis resulting from it and the accompanying extremely serious effects on the global economy, have led to a new "global information war" between countries in order to secure the necessary equipment to combat the deadly virus. Figure 21 shows the rate of the abused keywords related to COVID-19.

As conditions, losses, and fears worsen, countries are scrambling to take measures to secure the necessary

Figure 18: A national police officer surveys a pile of empty boxes left in a huge mask theft in Santiago [40].

Figure 19: Medical supplies not conforming to the specifications of quality [25].

Figure 20: Medical stock [25].

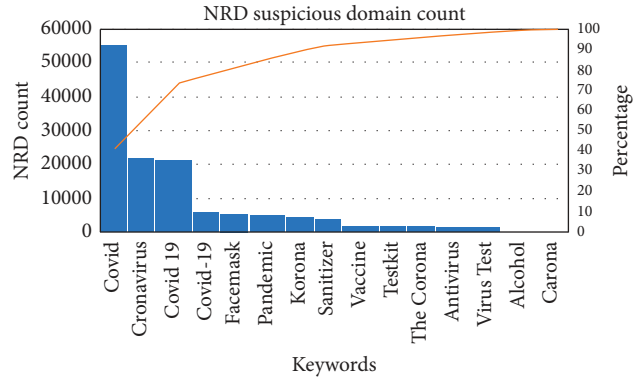

Figure 21: Daily report on newly suspicious domains.

equipment and supplies, such as masks and virus detection tests. Here are some of the unethical attacks:

(i) American buyers could have managed to control a shipment of face masks, which were transferred from China to France. American buyers offered three times what their French counterparts paid.

(ii) Turkey banned the export of personal protective equipment and had retracted foreign sales of muzzles.

(iii) The Czech authorities had confiscated one of Chinese shipments containing millions of gags donated from China to Italy when they passed via the Czech Republic.

(iv) A similar incident occurred in Kenya, where a shipment of 6 million masks destined for Germany disappeared mysteriously.

4. Countermeasures

This section presents some cyberattack countermeasures followed by some general recommendations for companies, organizations, and users. However, looking at the details of attacks, the types of attacks could be classified according to the defense strategies into software-based, hardware-based, and network-based. Table 2 presents some of the countermeasures for the previously mentioned attacks, which are categorized according to the defense strategies.

Furthermore, there are several technical recommended countermeasures related to COVID-19 cybersecurity attacks. These countermeasures are illustrated in Table 3.

5. Open Research Issues

This section shows some of the open challenges in terms of security, especially at the time of pandemic, as follows.

5.1. Attacks on Privacy. With the increase of connectivity to the Internet and people forced to work from home, some security measures were ignored. Remote access is implemented through different methodologies. Adversaries take the benefit of the situation, having easy access to the personal computers as well as to companies' servers. Eavesdropping, traffic analysis, and data mining are common attacks. This is still an open issue to be considered.

5.2. Authorization and Access Control. Authorization is typically implemented through access controls. Both have to be implemented by establishing a secure connection between the end user and the server. With work from home, IT administration is not that effective. Therefore, certain other methodologies need to be implemented for certain situations.

5.3. End-to-End Security. End-to-end security means applying security to the end nodes such as endpoints, personal and company devices. Cryptographic techniques are not sufficient for end-to-end security. Both ends' verification is a must for secure connections.

5.4. Physical Security. It became very clear that physical security at the time of pandemic became a challenge, and regular methods are insufficient to handle critical situations; even surveillance cameras were not enough [53].

5.5. DoS Attacks. DoS became the most dominant attacks, especially on governmental websites that provide emergency services to people. More extreme types of DDoS attacks include a mechanism known as "memcaching," which utilizes vulnerable, open-source object-caching schemes to escalate access requests and inundate sites with more than one terabyte of traffic.

5.6. Malware. A large number of malwares have been created targeting many of the devices, especially devices with limited resources that are mostly used at the time of the pandemic. The currently available techniques are still not enough to detect the new malware.

Table 2: Attacks' defense strategies and the countermeasure techniques.

Defense strategy	Countermeasure techniques
Network-based	(i) Encrypting IP data, IPSec was developed. IPSec has been used for several years to create a private virtual network (VPN) between a remote device and a trustworthy network (i.e., an intranet company), which establishes protected connections through the Internet. (ii) TCP sat above the IP to efficiently send the packets (i.e., retransfer missing packets) and requested packets to be initially sent. (iii) SSL was designed to provide end-to-end protection between two computers that sit across the TCP (transmission control protocol) comparing to the layer-based protocol only. (iv) Securing web page access, SSL/TLS is widely used with https.
Software-based	(i) Quantum cryptography is an up-and-coming technology that simultaneously produces two parts of a common, secret cryptographic key by utilizing a quantum state of light [51]. (ii) Continuous risk assessment: no two businesses are identical. This is why each organization has its own risk profile based on its scale, regional structure, market operating environment, etc. Each organization will take a set of measures needed as prerequisites for enforcing security controls, including the detection of threats, weaknesses, and risks, and developing and implementing protection controls that mitigate such risks. (iii) Based on the company assessment of the risk, data could only be protected by a password. For remote access, other sophisticated methods might be required, such as biometric authentication and random PIN. (iv) To strengthen and protect information protection, it may be useful to record the processes and controls enforced in a formalized set of policies and procedures, maintain a consistent and accurate method of knowledge delivery, and increase employee understanding and engagement. (v) The best approach to protect data is to remove any records that are no longer required for everyday business purposes. Data backup and archiving must ensure that data are retained as long as it is necessary for a particular location (server, unique files, etc.) and excluded from the business network, thus limiting the risk of unauthorized access to confidential information.
Software-based with hardware-based	(i) Cryptography is an important method to secure the data exchanged between users through the encryption of the data such that it can be decrypted only by authorized users with the appropriate keys. The most used mechanism for data protection is cryptography. One of the latest cryptography techniques introduced by the US National Institute of Standards and Technology (NIST) is Advanced Hash Standard (ASH). It is used for applications involving high-speed encryptions a replacement to the RSA with 2048-bit key and for impracticable involvement of the certifying authorities [52] (ii) Companies will ensure that all their infrastructure (hardware and software), including security software (e.g., antivirus programs) is up-to-date and the new updates are enabled, so no exceptions might occur. It is, therefore, important that businesses ensure that a third-party software agreement is effective to support maintenance and upgrading services.
Network-based with software-based	(i) A recent study field where the network professionals and the visualization group need to integrate expertise to map network traffic utilizing improved visualization techniques. Network specialists with the extensive technical expertise in networking technologies can also examine the graphic display of the results [26]. (ii) Companies are supposed to ensure that access for leavers, contractors, or any outside parties who have already demanded access to the company's network is adequately restricted and promptly terminated. Manual controls or automated controls should disable domain accounts that have not connected to the network during a given period of time. A broad variety of controls mitigate such risks.

Table 3: Cybersecurity attacks and the countermeasure techniques.

Cybersecurity attack	Countermeasures techniques
(1) Remote access infrastructure attacks	(i) Strengthen your home network using firewall, IDS, and IPS.
(2) Different technologies	(i) Prepare new technologies, support team, and hotlines for employees to be able to ask for help. (ii) Test the new technologies and application programs features and ensure that they work as described.
(3) Using personal devices	(i) Only download mobile applications and software from trusted sources. (ii) Regular scans are required on personal devices and computers. (iii) Backup all your important information regularly.
(4) Unauthorized access	(i) Use strong passwords. (ii) Update passwords periodically. (iii) Make sure that any administration vulnerabilities are mitigated. (iv) Remove or disable any third party that is not needed anymore.

Table 3: Continued.

Cybersecurity attack	Countermeasures techniques
(5) Social engineering attacks	(i) If the used machine is working property, you must contact the IT administrator/department. (ii) If the bank details were provided, the bank authorities have to be notified. (iii) If you think your account has already been hacked (you may have received messages sent from your account that you do not recognize, or you may have been locked out of your account), refer to service provider guidance on recovering a hacked account. (iv) Full antivirus (AV) scan should be conducted to clean up any problems it finds. (v) If the password is provided, it has to be changed immediately.
(6) Phishing attacks	(i) Carefully handle SMS text messages related to COVID-19, either the word "COVID-19" is stated in the subject line, attachment, or hyperlink, and be cautioned about COVID-19-related calls. (ii) Before opening an email or SMS, consider who is sending it to you and what they are asking you to do. Organization call could be an appropriate way to verify the email or the SMS message. (iii) Avoid contacting the phone number or replying to the email address stated in the message or the message came from. It is most likely belonging to a scammer.
(7) Distributed denial of service (DDOS) attack	(i) Use systems for intrusion detection (IDS) and intrusion protection (IPS). (ii) Use good antivirus and antispyware protection on all Internet-connected devices. (iii) Apply file and folder hashes to identify system files and folders where they have been compromised. (iv) Reverse DNS lookup for source address verification. (v) Applying filters on unnecessary traffic minimizes the DoS attack. Also, you can contact your ISP to filter closer to the source and reduce the bandwidth used by the attack. (vi) Hardening practices on all computers, particularly servers and directory and resource servers exposed to the public.
(8) Ransomware attack	(i) Backup all of your important files and save them on an external drive (e.g., in the cloud) independently of your system. (ii) Deactivate obsolete or third-party components that may be used as points of entry. (iii) Download applications from only trusted platforms or any other software. (iv) Must not click on emails that you do not expect to receive or from an unacquainted sender. (v) As usual, notify the local police if you suspect that you are the victim of a crime. (vi) Remote users might need to use software different from what they do in their offices (or use familiar apps in a different way). For these features, you should produce written guides and test how the software operates as described.
(9) Physical attacks	(i) Ensure that staff know what to expect if their computer is lost or stolen, such as who to talk to. Encourage users to record losses as early as possible. (ii) Ensure data encryption at rest, securing computer data if damaged or compromised. Most modern computers are encrypted, but encryption will also need to be activated and installed. (iii) Reporting odd activities such as looking through windows of closed shops or attempting to unlock doors. (iv) Maintain windows clear of merchandise, clear all cash from the premises, protect all doors and windows with strong locks, and ensure the alarms, surveillance cameras, and exterior lighting are in proper working order. (v) Check companies frequently to ensure that no protective equipment is destroyed or removed.

6. Conclusion

This paper reviews the cybersecurity attacks at the time of COVID-19 pandemic. It reviews the history of pandemics faced the world at different time periods. The paper showed that every pandemic has its own spread percentage. It also explores the different types of cybersecurity that appeared before the pandemic. Attacks are classified into flow control, injection, information leakage, and denial of service (DoS). The flow control is extended further to code reuse. The injection type of attacks is extended to false data, malware, and sabotage, where sabotage is shown in various forms such as crash, memory corruption, and physical attacks. The information leakage includes further side-channel and encryption key bypass attacks, while DoS involves flooding attack. The paper goes beyond the regular cybersecurity attacks to to study other newly developed attacks such as working from home threats, social engineering attacks, ransom attacks, and phishing, DoS, unethical, and physical attacks. These attacks are studied in view of the pandemic. Attacks within each type are classified further and explained in detail. Furthermore, the paper introduced a set of countermeasures and recommendations classified according to the defense strategies.

Future work includes

(i) Artificial intelligence (AI) and their roles in containing the pandemic. Many of the AI techniques have been used recently to detect coronavirus using image processing, coughing, and/or temperature analysis. An investigation into these topics will be beneficial to the security community.

(ii) Studying the effectiveness of the current network infrastructure at the time of the pandemic. As

mentioned in this paper, the network infrastructure and lack of its security cause a large number of security breaches. Therefore, one of our future directions is to investigate the root causes of threats and attacks related to the network infrastructure.

(iii) Detailed analysis to all of the stated malwares including their signatures and their effect. The current attacks and malwares have different signatures, and studying such signatures help reducing or avoiding their risks.

(iv) Studying the effectiveness of the current countermeasures, especially at the time of pandemics. There are many reported cases and steps that were taken by the IT and security specialists; reporting such techniques to the security community will be beneficial.

(v) Deep investigation into people psychology in recent times as well as in previous pandemic periods. Apart from the security, the psychological behavior of people during the pandemic time will be a great help to psychologists.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This research was funded by the Scientific Research Deanship at the University of Ha'il, Saudi Arabia, through project number RG-20019.

References

[1] S. I. Hay, A. J. Tatem, A. J. Graham, S. J. Goetz, and D. J. Rogers, "Global environmental data for mapping infectious disease distribution," *Advances in Parasitology*, vol. 62, pp. 37–77, 2006.

[2] M. Carrion and L. C. Madoff, "ProMED-mail: 22 years of digital surveillance of emerging infectious diseases," *International Health*, vol. 9, no. 3, pp. 177–183, 2017.

[3] F. A. Culver, B. Paul, and D. Cavanagh, "RT-PCR detection of avian coronaviruses of galliform birds (chicken, turkey, pheasant) and in a parrot," in *SARS-and Other Coronaviruses*, pp. 35–42, Humana Press, Totowa, NJ, USA, 2008.

[4] H. Lu, C. W. Stratton, and Y. W. Tang, "Outbreak of pneumonia of unknown etiology in Wuhan, China: the mystery and the miracle," *Journal of Medical Virology*, vol. 92, no. 4, pp. 401-402, 2020.

[5] Y. Bai, L. Yao, T. Wei et al., "Presumed asymptomatic carrier transmission of COVID-19," *JAMA*, vol. 323, no. 14, pp. 1406-1407, 2020.

[6] X. Yang, Y. Yuan, J. Xu et al., "Clinical course and outcomes of critically ill patients with SARS-CoV-2 pneumonia in Wuhan, China: a single-centered, retrospective, observational study," *The Lancet Respiratory Medicine*, vol. 395, no. 10223, pp. 497–506, 2020.

[7] C. Hadnagy, *Social Engineering: The Art of Human Hacking*, John Wiley & Sons, Hoboken, NJ, USA, 2010.

[8] "Getting around non-executable stack (and fix). Bugtraq," 2020, http://ouah.bsdjeunz.org/solarretlibc.html.

[9] R. K. C. Chang, "Defending against flooding-based distributed denial-of-service attacks: a tutorial," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 42–51, 2002.

[10] X. Liu and Z. Li, "False data attack models, impact analyses and defense strategies in the electricity grid," *The Electricity Journal*, vol. 30, no. 4, pp. 35–42, 2017.

[11] M. M. H. Onik, N. Al-Zaben, H. P. Hoo, and C.-S. Kim, "A novel approach for network attack classification based on sequential questions," *Annals of Emerging Technologies in Computing*, vol. 2, no. 2, pp. 1–14, 2018.

[12] C. Kaur, A. B. Jasmeen, and S. Behal, "Distributed denial of service attacks: a threat or challenge," *New Review of Information Networking*, vol. 24, pp. 31–103, 2019.

[13] NIST, *FIPS140-2: Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2002, https://csrc.nist.gov/publications/detail/fips/140/2/final.

[14] S. Kotey, E. Tchao, and J. Gadze, "On distributed denial of service current defense schemes," *Technologies*, vol. 7, no. 1, pp. 19–1, 2019.

[15] K. Scarfone, P. Hoffman, and M. Souppaya, "Guide to enterprise telework and remote access security," *NIST Special Publication*, vol. 800, p. 46, 2009.

[16] L. Hu and X. Bi, "Research of DDoS attack mechanism and its defense frame," in *Proceedings of the 2011 3rd International Conference on Computer Research and Development*, Shanghai, China, 2011.

[17] J. R. Davidson and J. L. Wright, *Recommended Practice for Securing Control System Modems. No. INL/EXT-07-12635*, Idaho National Laboratory (INL), Idaho Falls, ID, USA, 2008.

[18] J. W. Scheeres, *Establishing the Human Firewall: Reducing an Individual's Vulnerability to Social Engineering Attacks. No. AFIT/GIR/ENG/08-04*, Air Force Institute of Tech Wright-Patterson Afb Oh Graduate School of Engineering And Management, 2008.

[19] K. D. Mitnick and W. L. Simon, *The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders and Deceivers*, John Wiley & Sons, Hoboken, NJ, USA, 2009.

[20] F. Mouton, M. M. Malan, and S. V. Hein, "Development of cognitive functioning psychological measures for the SEADM," in *Proceedings of the 2012 Human Aspects of Information Security & Assurance*, Heraklion, Greece, 2012.

[21] S. Shira and J. Jennifer, "Cyber-attack hits U.S. Health Agency amid COVID-19 outbreak," 2020, https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.

[22] J. Debrosse and D. Harley, "Malice through the looking glass: behaviour analysis for the next decade," in *Proceedings of the 19th Virus Bulletin International Conference*, Geneva, Switzerland, 2009.

[23] F. Mouton, L. Leenen, M. M. Malan, and H. S. Venter, "Towards an ontological model defining the social engineering domain," in *Proceedings of the 2014 IFIP International Conference on Human Choice and Computers*, Turku, Finland, 2014.

[24] C. Cimpanu, "Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak," 2020, https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/.

[25] A. Amany, "Selling used masks," 2020, http://shorturl.at/ctCNQ.

[26] F. Fischer, F. Mansmann, D. A. Keim, S. Pietzko, and M. Waldvogel, "Large-scale network monitoring for visual analysis of attacks," in *Proceedings of the 2008 International Workshop on Visualization for Computer Security*, Cambridge, MA, USA, 2008.

[27] Reuters, "Italy's social security website hit by hacker attack," 2020, https://www.reuters.com/article/us-health-coronavirus-italy-cybercrime/italys-social-security-website-hit-by-hacker-attack-idUSKBN21J5U1.

[28] L. Kim, "Google saw more than 18 million daily malware and phishing emails related to COVID-19 last week. The Verge," 2020, https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams.

[29] Cyber Threat Alliance, "Lucrative ransomware attacks: analysis of the cryptowall version 3 threat," 2016, https://www.cyberthreatalliance.org/resources/lucrative-ransomware-attacks-analysis-cryptowall-version-3-threat/.

[30] REUTERS, *Italy's Social Security Website Hit by Hacker Attack*, REUTERS, London, UK, 2020, https://www.reuters.com/article/us-health-coronavirus-italy-cybercrime/italys-social-security-website-hit-by-hacker-attack-idUSKBN21J5U1.

[31] J. Gourley, "MyGov website crashes as thousands seek Centrelink help amid coronavirus pandemic, Government backflips on claims cyber attack to blame," 2020, https://www.abc.net.au/news/2020-03-23/mygov-website-down-centrelink-massive-queues-coronavirus/12080558.

[32] P. Zhou, X.-L. Yang, X.-G. Wang et al., "A pneumonia outbreak associated with a new coronavirus of probable bat origin," *Nature*, vol. 579, no. 7798, pp. 270–273, 2020.

[33] Bisson and David, "Food delivery website in Germany targeted by DDoS attackers, Tripwire," 2020, https://www.tripwire.com/state-of-security/security-data-protection/food-delivery-website-in-germany-targeted-by-ddos-attackers/.

[34] C. Askew, "Stay safe and secure online during COVID-19," 2020, https://www.citywidefinancial.co.uk/stay-safe-and-secure-online-during-covid-19/.

[35] ISO 13491-1, *Banking—Secure Cryptographic Devices (Retail), Part 1: Concepts, Requirements and Evaluation Methods*, ISO, Geneva, Switzerland, 2007, https://www.iso.org/standard/41214.html.

[36] A. Kotyk and B. Miljure, "40 suspects arrested in connection to recent break and enter crimes: VPD," 2020, https://bc.ctvnews.ca/40-suspects-arrested-in-connection-to-recent-break-and-enter-crimes-vpd-1.4895846.

[37] Burnaby Now, "Alleged cable thief surrounded, arrested at closed Burnaby business," 2020, https://www.burnabynow.com/news/alleged-cable-thief-surrounded-arrested-at-closed-burnaby-business-1.24114417.

[38] L. Middleton, "Thief steals NHS worker's bike as she works overtime during coronavirus crisis," 2020, https://metro.co.uk/2020/03/29/thief-steals-nhs-workers-bike-works-overtime-coronavirus-crisis-12472878/.

[39] BBC, "Coronavirus: armed robbers steal hundreds of toilet rolls in Hong Kong," 2020, https://www.bbc.com/news/world-asia-china-51527043.

[40] C. Smith, "COVID-19: business man arrested for stealing two million face masks' from warehouse of bankrupt firm in Spain," 2020, https://www.theolivepress.es/spain-news/2020/04/07/covid-19-businessman-arrested-for-stealing-two-million-face-masks-from-warehouse-of-bankrupt-firm-in-spain/.

[41] G. Pulighe and F. Lupia, "Food first: COVID-19 outbreak and cities lockdown a booster for a wider vision on urban agriculture," *Sustainability*, vol. 12, no. 12, p. 5012, 2020.

[42] Kaspersky, "KSN report: PC ransomware in 2014–2016," 2020, https://securelist.com/pc-ransomware-in-2014-2016/75145/.

[43] L. Freedman, "COVID-19 vaccine test lab hit by maze ransomware, Jdsupra," 2020, https://www.jdsupra.com/legalnews/covid-19-vaccine-test-lab-hit-by-maze-88329/.

[44] J. Stone, "Ransomware strikes biotech firm researching possible COVID-19 treatments," 2020, https://www.cyberscoop.com/covid-19-ransomware-10x-genomics-data-breach/.

[45] Dark Reading Staff, "DDOS attack targets German food delivery service," 2020, https://www.darkreading.com/attacks-breaches/ddos-attack-targets-german-food-delivery-service/d/d-id/1337359.

[46] A. U. Surwade, "Phishing e-mail is an increasing menace," *International Journal of Information Technology*, vol. 12, pp. 611–617, 2019.

[47] J. Leyden, "Brazilian cops net "phishing Kingpin"," 2020, https://www.theregister.com/2005/03/21/brazil_phishing_arrest/.

[48] Australians Government, "Widespread reports of COVID-19 malicious scams being sent to Australians," 2020, https://www.staysmartonline.gov.au/alert-service/widespread-reports-covid-19-malicious-scams-being-sent-australians.

[49] P. Roberts, "More scam artists go phishing," 2004, https://www.pcworld.com/article/116330/article.html.

[50] N. Smith, "Coronavirus: police in Thailand discover used face masks "being re-packaged as new"," 2020, https://www.telegraph.co.uk/global-health/science-and-disease/coronavirus-police-thailand-discover-used-face-masks-re-packaged/.

[51] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973–993, 2014.

[52] Karlsruhe Institute of Technology, "Roadmap for cyber security research," 2019, https://phys.org/news/2019-03-roadmap-cyber.html.

[53] B. Aboushosha, R. A. Ramadan, A. D. Dwivedi, A. El-Sayed, and M. M. Dessouky, "SLIM: a lightweight block cipher for internet of health things," *IEEE Access*, vol. 8, pp. 203747–203757, 2020.