electronics

MDPI

Article

Protective Factors for Developing Cognitive Skills against Cyberattacks

María Cazares [1], Walter Fuertes [2], Roberto Andrade [3], Iván Ortiz-Garcés [4,*] and Manuel Sánchez Rubio [5]

[1] IDEIAGEOCA Research Group, Universidad Politécnica Salesiana, Quito 010105, Ecuador; mcazares@ups.edu.ec
[2] Computer Science Departament, Universidad de las Fuerzas Armadas ESPE, Sangolquí 171103, Ecuador; wmfuertes@espe.edu.ec
[3] Facultad de Ingeniería en Sistemas, Escuela Politécnica Nacional, Quito 170525, Ecuador; roberto.andrade@epn.edu.ec
[4] Facultad de Ingeniería y Ciencias Aplicadas, Escuela de Ingeniería en Tecnologías de la Información, Universidad de las Américas, Quito 170513, Ecuador
[5] Faculty of Engineering, Universidad Internacional de la Rioja, 26006 Logroño, Spain; manuel.sanchezrubio@unir.net
* Correspondence: ivan.ortiz@udla.edu.ec

Abstract: Cyberattacks capitalize on human behaviors. The prevalence of cyberattacks surged during the COVID-19 pandemic, fueled by the increased interconnectivity of individuals on online platforms and shifts in their psychological dynamics due to the pandemic's context. The enhancement of human factors becomes imperative in formulating a robust cybersecurity strategy against social engineering in the post-COVID-19 era and in anticipation of analogous pandemics. This study aims to propose a model for delineating strategies across various phases of cyberattacks, grounded in the cyber kill chain model, while also encompassing cognitive mechanisms for adaptive responses. This approach aims to cultivate defensive cognitive factors like resilience and self-efficacy. To achieve this objective, we conducted an exploratory study adhering to Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. Subsequently, we pursued a descriptive and correlational study based on prevalent attacks during the pandemic. The intention was to pinpoint proactive factors conducive to the development of cognitive capabilities to counter cyberattacks. These insights could pave the way for the creation of training programs and technological solutions aimed at mitigating the impact of such cyberattacks.

Keywords: cybersecurity model; cyberattacks; social engineering; cognitive mechanisms

Citation: Cazares, M.; Fuertes, W.; Andrade, R.; Ortiz-Garcés, I.; Rubio, M.S. Protective Factors for Developing Cognitive Skills against Cyberattacks. *Electronics* **2023**, *12*, 4007. https://doi.org/10.3390/electronics12194007

Academic Editor: Krzysztof Szczypiorski

Received: 22 May 2023
Revised: 8 August 2023
Accepted: 5 September 2023
Published: 23 September 2023

1. Introduction

The COVID-19 pandemic has forced significant social, technological, cultural, and environmental changes [1]. In education, COVID-19 has forced students worldwide to study at home [2]. In work and employment, an increase in working from home was announced in the USA in 2020, and 34% of companies worldwide consider working remotely permanently [3]. The COVID-19 pandemic has generated significant challenges to cybersecurity due to the imposed accelerated migration to teleworking, tele-education, and the execution of a wide range of daily activities from home, where network infrastructures and setups were not sufficiently advanced and have not previously considered security aspects at such a high level. Having people connecting remotely and the changes in their roles and dynamics (e.g., changes in the way they shop, work, learn, and do their daily activities) increased cybersecurity-related demands. In the context of uncertainty and the moments of anxiety, depression, and/or stress generated by the pandemic, these lifestyle changes have made people more vulnerable. These aspects cause emotional and cognitive stress, which undoubtedly generates new cybersecurity challenges [4].

According to Interpol [5], phishing attacks have increased by 59%, and fake news campaigns have hindered the authorities' efforts to control the pandemic worldwide. Specialized security firms have worked to improve their algorithms and solutions to detect cyberattacks, while [5,6] have deployed programs to raise awareness about cybersecurity among the population. According to the security reports published by McAfee [7–11], there has been a considerable increase in security attacks, as shown in Table 1. This information is like other security reports submitted by similar cybersecurity companies such as ESET, Checkpoint, Kaspersky, TrendMicro, and Cisco.

Table 1. Growing cyberattacks during pre- and post-COVID-19.

Cyberattacks	2018 [8]	2019 [9]	2020 [10]
Malware	700,000,000	900,000,000	1,200,000,000
Ransomware	16,000,000	1,000,000	1,250,000

Although there is a certain pattern of the continuous growth of cyberattacks, in the case of phishing attacks the number of attacks increased twice during the COVID-19 pandemic, as shown in Table 2, based on the analysis of reports from McAfee [12]. Phishing attacks were modified during COVID-19 to use information related to COVID-19 to take advantage of people's interests. This context is corroborated by the reports presented by the Anti-Phishing Working Group (APWG) [13] and Interpol [5]. The increase in phishing attacks may be related to the conclusions of the study by Albladi et al. [14]: with more time spent using the Internet and more people interacting in cyberspace, the risk of falling victim to deception becomes greater.

Table 2. Growing phishing attacks during pre- and post-COVID-19.

Year	2019 [9]	2020 [10]	2021 [11]	2022 [12]
Spam traffic	56.36%	52.48%	56.33%	45.56%
An anti-phishing system was triggered	246,231,645 times	482,465,211 times	434,898,635 times	253,365,212 times

In this study, we present exploratory research on the landscape of cybercrime and common cyberattacks during the time of the pandemic, which was an era of crisis that created changes in behavior patterns in human activities through digital environments, which increased the probability of being a victim of cyberattacks. To better understand the meaning of cybercrime, we can consider the following definitions. The Commission of the European Communities defines cybercrime as "criminal acts committed using electronic communications networks and information systems or against such networks and systems" [3]. In addition, the Council of Europe Convention on Cybercrime defines cybercrime as "a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability" [3]. Among the most critical examples of cybercrime are social engineering attacks, typically conducted through identity theft. One of the most sensitive is phishing attacks, which steal credentials to scam users through commercial transactions. This study proposes the modeling of phishing attacks based on the cyber kill chain model, including human behavior in cyberspace during the pandemic caused by COVID-19, taking into consideration the growth of human interactions with cyberspace during this time. The proposed model could be applied to a post-pandemic context or could be applied in the case of another possible similar pandemic.

The questions that guided this research are the following:

(i) Is there a variation in cyberattacks during the period of the COVID-19 pandemic?
(ii) Has the context of the COVID-19 pandemic increased the susceptibility of being a victim of cyberattacks?

(iii) How can we model user behavior during the COVID-19 pandemic in the face of a cyberattack employing the steps of the cyber kill chain?

Then, we review the systematic literature based on the preferred reinforcement elements for systematic reviews and meta-analysis guidelines [15], identify the variants and characteristics of cyberattacks, and learn how adversaries have taken advantage of people's psychological factors in the face of COVID-19. Moreover, we determine the psychological impact of a non-experimental correlational study based on Pearson's coefficient to determine the increase in cyberattacks in the face of the new demands for Internet use during the pandemic.

The main contributions of our work can be summarized as follows: (i) It offers an exploratory study on common cyberattacks during COVID-19; (ii) a descriptive study about the characteristics and variants of cyberattacks, as well as the psychological impact and behavior of victims during COVID-19; (iii) a correlational study on the increase in cyberattacks as a consequence of the elevated demand for Internet use during the pandemic; (iv) and a modeling of phishing attacks based on the cyber kill chain model that considers the perceived human behavior in the examined period. The literature review aims to determine cyberattack variables and their characteristics during the COVID-19 pandemic, as well as to assess the psychological impact on victims and human behavior during COVID-19. Finally, we focus on presenting a correlational study that explores the reasons for the increase in cyberattacks during COVID-19.

The remainder of this article is structured as follows. Section 2 comprises an exploratory analysis of social engineering attacks during the COVID-19 pandemic. Section 3 presents the methods and techniques used in this research. Section 4 details a proposal for modeling a phishing attack based on a cyber kill chain that considers people's psychological factors. Section 6 discusses and interprets findings and the lessons learned. Finally, Section 7 concludes this work and presents future work directions.

2. Exploratory Analysis of Social Engineering Attacks during the COVID-19 Pandemic

In an analysis conducted by Imperva professionals, they observed an increase in attacks on the following four types of web applications in the COVID-19 platform: Protocol manipulation attacks increased by 76%; remote code execution (RCE) increased by 68%; SQL injection (SQLi) increased by 44%; and cross-site scripting (XSS) increased by 43%. For instance, healthcare organizations were victims of multiple attacks during COVID-19, compromising their operations through IoT systems and legacy software vulnerabilities via the execution of cross-site scripting and ransomware attacks. Although these attacks existed before the COVID-19 pandemic, unfortunately their criticality increased due to the importance of health systems in the context of controlling the COVID-19 virus. Another critical aspect to consider is that ransomware attacks generally employ a social engineering attack at an initial stage, commonly phishing. Some specialized security companies mention this, such as the FBI, INTERPOL, and EUROPOL. According to [7–12], during the COVID-19 pandemic, the number of attacks increased by 35%.

2.1. Social Engineering Attacks

During the COVID-19 pandemic, people sought helpful information to prevent the spread of the coronavirus disease. At the same time, adversaries tried to trick people into clicking links that would drive them to fake sites to steal valuable data, such as usernames and passwords, credit card information, and other personal information.

In the context of the COVID-19 pandemic, adversaries sent messages impersonating a trustworthy authority such as the World Health Organization (WHO). In [16], the author mentions that emails sent during the COVID-19 pandemic used subject lines such as "2020 Coronavirus updates" or "2019-nCov". Table 3 indicates the types of existing social engineering attacks.

Table 3. Types of social engineering attacks.

Type	Description
Baiting	It is a social engineering technique where the attacker arouses the victim's interest or curiosity in a trap to steal information or access their system through malware.
Invoice Fraud	This technique is used to gain access to a victim's email address. In an example of this technique, the recipient is tricked into believing that they must make an immediate payment.
Phishing	It is one of the most-used social engineering techniques, where attackers trick users to obtain information or breach their devices. Attackers impersonate a legitimate organization or entity to send emails to deceive recipients.
Vishing	Also known as voice phishing. It is a social engineering attack focused on phone lines. The attacker performs the scam by calling a legitimate entity to obtain confidential information, such as credit card details.
Pretexting	Pretexting is another type of social engineering. The attacker creates a good pretext, scenario, and coherent story to steal information from the victims.
Spear Phishing	It is a phishing attack where the objective is to obtain information from a specific user or organization. A previous study is made to choose the victim.
Scareware	It is a type of malware used with social engineering techniques. It seeks to scare, cause fear, and shock the user to install and buy software that is not needed.

2.2. Attacks on Teleconference Systems

Novel cyberattacks and unknown vectors of attack increased during the COVID-19 pandemic. For instance, we can mention Zoom bombing and unknown malware variants such as Azolurt or Maze. During a Zoom bombing, an adversary injects objectionable content such as pornographic material and violent images into online meetings. During the first months of the year 2020, accounts of teleconference systems were sold on hacker forums [17]. During the COVID-19 pandemic, the FBI revealed that it received many reports regarding hijacked videoconferences; e.g., two Massachusetts schools reported the intruders' presence in their online classrooms [18].

2.3. Fake News

Fake news refers to fabricated information published to cause panic or influence the decision process to achieve financial or political goals. Some factors increase the problem of fake news. The first is the technological dimension; with information technologies' growth, news, whether real or fake, has more impact and a larger audience. The second is the social dimension. News is affected by the way social media presents it on popular online platforms [19]. During the COVID-19 pandemic, the World Health Organization declared a global info-demic issue, and it asked tech companies to act against misinformation. Facebook is banning coronavirus-related posts that may be harmful, while Google's Trust and Safety team has been tasked with removing conspiracy theories and misinformation. Misinformation-driven panic has pushed people to seek measures against COVID-19 on malicious sites. For instance, [20] mentions that they found 788 fake sites directly related to COVID-19 products.

The security firm CheckPoint claims that, since the beginning of January 2020, more than 16,000 new domains related to the coronavirus have been registered, and about 20% of them were classified as potentially dangerous [21].

2.4. Malware

Adversaries try to install malicious code on people's computers. According to [10], adversaries used online interactive COVID-19 maps, fake news, websites, and phishing emails to take advantage of people's fears and need for information to introduce the Azolurt

malware and steal credentials and accounts. More than 600 malicious applications were detected during COVID-19 [22]. API endpoints seem to be targeted by malicious actors following imprisonment measures across the planet, with one attack seeing fifteen million events aimed toward one single API endpoint for the Android app [23]. Anyone with a link could access confidential documents related to the UK's NHS coronavirus trailing app hosted in Google Drive. The documents contain privacy protection information and further plans the app could take [24]. Over 6400 Edison Mail users were hit by a security bug that allows others to access an account in an update rolled out on its iOS app [25]. The following are the most impactful attacks carried out on mobile devices during the COVID-19 pandemic (see Figure 1).

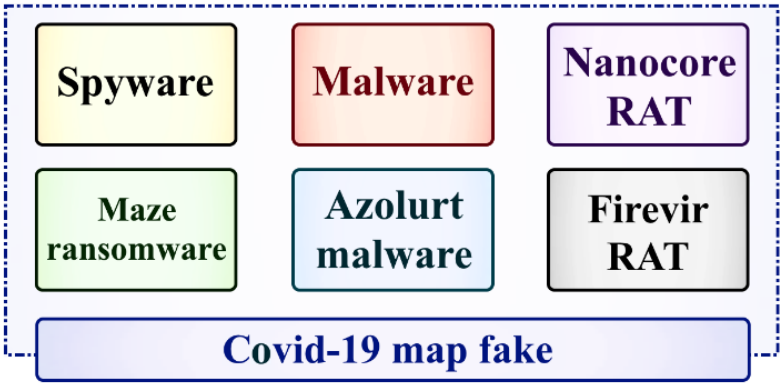

Figure 1. Mobile malware during COVID-19.

2.5. Phishing

Phishing is a form of social engineering characterized by a computer attack aimed at deceiving individuals to obtain their personal and confidential information. Some common forms of phishing include email phishing, malware-based phishing, content poisoning of host files, injection through man-in-the-middle attacks and using search engines [26]. In this article, we specifically study email phishing, considering that over 238.4 billion emails are sent worldwide every day. In 2020, there were 241,342 phishing/vishing/smishing/pharming victims, representing a 52.47% increase compared to 2019, with a loss of 54,241,075 dollars [27]. Although no anti-spam filtering system can guarantee 100% effectiveness against spam, phishing, or other malicious emails, automated and regular scans can significantly reduce the risk of data loss. Currently, the approaches used to detect phishing remain dependent on users and self-mimicking. User-dependent detection involves communication methods to identify phishing, such as phishing tests to assess user awareness. On the other hand, the automated approach includes software-based distributions, block lists, heuristic analyses based on multiple criteria, threat intelligence for security incidents and event management systems, and the use of Machine Learning (ML) and Artificial Intelligence (AI) technologies [28]. Among the proposed systems, random forest-based classifiers are found to be the most effective for evaluating whether a given URL refers to a phishing site [26].

As a result, the most vulnerable group of users are those who lack a support system. It is crucial to understand that the ability of human users to accurately detect phishing emails directly impacts the level of risk faced by organizations or individuals. Unfortunately, previous research has shown that individuals often fall victim to phishing attacks, both in controlled laboratory settings and in real-world environments, despite receiving phishing awareness training [29]. People may be aware of cybersecurity risks when engaging online, but they can still make wrong decisions and accept malicious emails or infected pages. This susceptibility is associated with how humans process information systematically and heuristically [30]. Emotional exploitation techniques are employed to influence heuristic decision-making, using a sense of authority or urgency to persuade recipients. Attackers may also present themselves as authoritative figures, such as a CEO or an official entity [31].

Individuals might judge emails differently based on factors like time pressure, their level of trust, and the level of detail in the email content, all of which can influence their decision [32]. For instance, participants in a phishing study were better able to identify phishing content when it included co-branded companies [33]. Conversely, attackers have perfected persuasion techniques to exploit emotional factors that can affect judgment in decision-making processes. Some attackers create a sense of limited opportunity, such as offering exclusive travel deals [34]. Furthermore, impulsivity and a tendency for sensation-seeking have been linked to making mistakes in detecting phishing emails, as individuals using heuristic thinking tend to overlook details [28]. In [35], it was proposed that people who are overconfident in their ability to identify phishing may make errors due to omitting important details.

3. Methods and Techniques

This section presents the methods, techniques, and stages used during this research. The first process consists of a literature review to determine cyberattack variables and characteristics during the COVID-19 pandemic. The second is a literature review to determine the victims' psychological impact and human behavior during COVID-19. The third procedure focuses on presenting a correlational study exploring the increase in cyberattacks as Internet use rises due to COVID-19. Based on these preliminary results, we present a proposal for modeling phishing attacks using the cyber kill chain model, considering human behavior due to the COVID-19 pandemic. We performed an exploratory, descriptive, and correlational study. It is exploratory as it attempts to study a problem whose impact is not clearly defined, and it is conducted to understand it better. It is descriptive because it describes the nature of a social problem, focusing on why a specific phenomenon occurs. Finally, it is correlational as it attempts to determine the relationship between two or more study variables, manipulating them to obtain conclusions about the existing relationships. To provide the orientation and delimitation of the study, we try to resolve the following research questions:

RQ1: Is there a variation in cyberattacks during the period of the COVID-19 pandemic?

RQ2: Has the context of the COVID-19 pandemic increased the susceptibility of being a victim of cyberattacks?

RQ3: How can we model user behavior during the COVID-19 pandemic in the face of a cyberattack employing the steps of the cyber kill chain?

The literature reviews were based on the PRISMA guidelines [15], which promote a modular approach of four stages: identification, screening, eligibility analysis, and inclusion. The identification stage included different steps such as study selection, inclusion and exclusion criteria, manual search, and removal of duplicates. The screening stage consisted of the review of titles and abstracts. The eligibility analysis stage was executed by reading the full texts of the selected articles. Finally, the inclusion stage consisted of data extraction. These phases are briefly described below. Identification of Study Selection consisted of constructing the following search strings that employ Boolean operators to connect the following keyboard strings:

"(COVID-19)" AND "(CYBERATTACKS OR CYBERSECURITY)";

"(COVID-19)" AND "(HUMAN FACTORS)";

"(COVID-19)" AND "(HUMAN BEHAVIOUR)";

"(COVID-19)" AND "(VECTOR ATTACKS)".

Based on these strings, we conducted a manual search in the following databases: Springer, Scopus, IEEE, the Association for Computing Machinery (ACM), the Web of Science, and Science Direct. These databases were chosen since they are the most relevant sources of information corresponding to cyberattacks during the COVID-19 pandemic.

The inclusion criteria were: (i) papers, conferences, and book chapters published between 2020 and 2021; and (ii) design research, experimental and not experimental, related to human factors in phishing attacks. The exclusion criteria were papers published in scientific databases and international organizations that include aspects of COVID-19 but do not consider security attacks during the pandemic or human factors affected during the pandemic. Through this process, we identified 175 articles; 119 were presented at conferences, 52 were journal articles, and 4 were book chapters. Thirty-eight articles have been removed as duplicates.

For screening, we carried out a screening process for the 137 remaining papers to select the main contributions. This process was based on papers' titles and abstracts using a free web application created for the systemic review process called Rayvan [15]. This web application allows each reviewer to see the collected papers' titles and abstracts, maintaining a blinded review process. Initially, 73 articles were identified for full-text reading that focuses on analyzing safety aspects during the COVID-19 pandemic, and then a total of 50 studies were considered to analyze the correlation between human factors and cyberattacks during the period of the COVID-19 pandemic (see Tables 4 and 5), based on the PRISMA methodology shown in Figure 2.

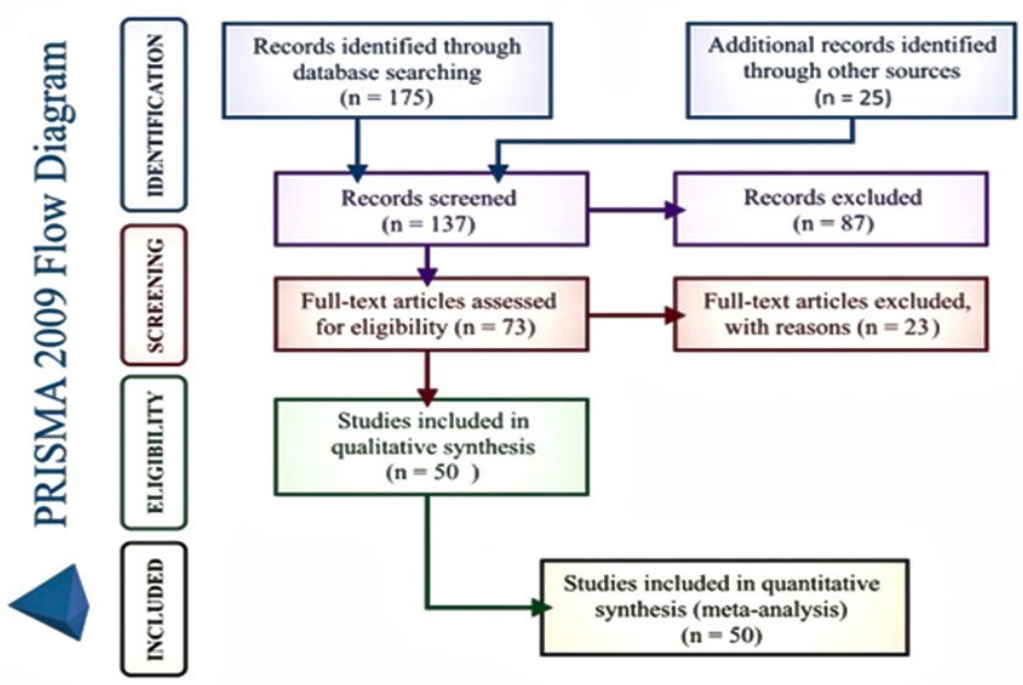

Figure 2. PRISMA is stated as the Preferred Reporting Item for Systematic Reviews and Meta-Analyzes. The figure shows the technical process followed to report the systematic literature reviews and meta-analyses that evolved in this study.

Regarding the inclusion stage or data extraction and cyberattacks, Weil et al. [36] mention that the COVID-19 epidemic has generated a global transformation in education, healthcare, business, industry, government, entertainment, social life, spirituality, and religious practices. For instance, the restriction of access to educational institutions leads to the creation of virtual learning environments using online video conferencing systems. Gupta et al. [37] declare that various sectors implemented robotics applications to avoid social contact. Robots were used for sanitization and cleaning, medicine and food delivery, food packing, self-driving vehicles, and food inspection. Additionally, Gupta mentions the use of AI-enabled body temperature monitoring in some airports, schools, and subways. A wide range of technologies has gained more relevance during the COVID-19 pandemic. Some representative examples include online video conferencing systems, virtual labs, chatbots, drone delivery, remote access, robots, 3-D printing, web online payment, contactless

payment, virtual reality apps, and video streaming. On the other hand, Tawalbeh et al. [38] report that because of the COVID-19 pandemic, there was an increase in cyberattacks. Healthcare organizations were victims of multiple attacks aiming to compromise their operations through IoT systems and legacy software vulnerabilities.

Table 4. Primary and secondary sources for literature review for cyberattacks during COVID-19.

Security Attacks	Number of Sources	Main Sources
Fake news and missing information	9	[39–47]
IoT	1	[48]
Phishing	6	[49–55]
Wi-Fi attacks	1	[56]
Malware	1	[57]
DDoS	2	[58,59]
Ransomware	1	[60]
Info stealer	2	[61,62]

Table 5. Primary and secondary sources for literature review for human behaviors during COVID-19.

Human Factors	Number of Sources	Reference
Behavior	3	[63–65]
Health	2	[66,67]
Education	2	[68,69]
Financial, teleworking	2	[70,71]
Teleworking	2	[72,73]
Economy	2	[74,75]
General	1	[76]

4. Exploratory Study of Human Factors in Cyberattacks during the COVID-19 Pandemic

4.1. Psychological Impact and Behaviors during the Pandemic

Another critical aspect of the impact of the COVID-19 pandemic on people is the incurred lifestyle change. This behavior change is one of the main consequences of social isolation, along with restrictive measures that cause people to lose freedom and create a lower perception of social support, leading to feelings of loneliness and boredom [4]. Based on the literature review carried out on public open data from organizations such as the Organization for Economic Co-operation and Development (OECD), the Office for National Statics by United Kingdom, and the United States Census Bureau (USCB), a great number of changes have occurred in people's lifestyles, which are presented in Table 6. During the COVID-19 pandemic, people changed or empathized with specific products. Certain items gained attention during the COVID-19 pandemic, like cosmetic and personal care products, digital entertainment, food and beverage, pharmaceutical/health, education and online courses, tools, gardening, do-it-yourself, and household products [77].

Table 6. People's lifestyles changes during the COVID-19 pandemic.

Mobility	Health	Shopping	Human Contact
Stayed at home more	Washed hands more	Went to shops less	Applied social distancing
Traveled less	Cleaned the house more	Shopped online more	Wore protective face masks outside
Avoided public transport	Did more exercise	Used less cash	Avoided public places like bars and restaurants
Worked from home	Visited more mental health services	Avoided certain shopping times	Canceled plans with family or friends

The relevance of the Internet in the world has never been greater than in the year 2020, since the quarantine caused by COVID-19 changed people's lifestyles. Confinement measures, the universal use of masks, migration to teleworking and tele-education, and new habits concerning consumption, work, studies, and interpersonal relationships have enabled a shift regarding using the network of networks. According to Organization for Economic Co-operation and Development (OECD) estimates, electronic commerce grew by around 108% globally. At the same time, the use of digital tools doubled in just the first two months of the COVID-19 pandemic [78]. Online stores have increased by 60%. However, the growth of these numbers has also caused an alarming increase in cyber threats. For the last quarter of 2020, there was a 75% increase in the probability of being a victim of cybercrime compared to 2019. Cyberattacks are intensifying due to the growth of adversaries' ability to access personal and business data and due to the fact that they face lower protection barriers due to the massive use of teleworking and greater socialization in social networks [5]. We analyzed data from the Office for National Statistics [1], and UNICEF [2], UK Data Service [63], Staszkiewicz [64] the World Bank [69], Burton [65], Chandola [78]. The data have the following formats: CSV, JSON, and XML.

Adversaries are aware that people have changed their behavior. Social media was one of the primary sources of fake news during the COVID-19 pandemic. Consequently, it had a relevant impact and disastrous effects on the pandemic's control [79]; e.g., certain information had the objective of inducing mental fatigue, leading to anxiety, phobia, panic spells, depression, obsession, irritability, and delusions related to COVID-19. Attackers can focus on carrying out their attack knowing that home security infrastructure is less efficient than that of enterprises and that people are interested in learning about COVID-19 effects. Information about COVID-19 does not just focus on the growth of the number of COVID-19 cases or information on vaccination processes; people also search for topics such as tax or economic incentives, miracle cures against COVID-19, entertainment, online shopping, and e-commerce. Based on a web scraping analysis of security reports issued by international organizations such as the FBI, INTERPOL, and specialized security sites such as Kaspersky, TrendMicro, Checkpoint, and ESET, we collected a compilation of impersonating attacks using known brands during COVID-19 based on the persons' needs, as shown in Table 7 [80].

Table 7. Impersonating cyberattacks during COVID-19 pandemic.

Category	Brand	Description
Entertainment	Netflix	Free access Suspension notification Cancellation confirmation Update payment details Create new password Unusual activity
	Disney Plus	
Governance	OMS	Vaccine (process, post-effects) Cures and treatment for COVID-19 COVID-19 spreading COVID-19 symptoms
	WHO	
	Health organizations	
	FBI INTERPOL EUROPOL	
Commerce	Walmart Best Buy Woolworths Marks and Spencer Amazon	Schedule time Vaccine distribution Gift cards Open shops

4.2. Results of Extraction of Human Factor Used during Cyberattacks

Then we used basic statistical methods to define a Pearson coefficient to validate the correlation between cyberattacks, tele-education, telework, and psychological factors. The relationships obtained from this correlation can be seen in Table 8. The selected psychological factors directly influence and present a high positive correlation between Internet use and cyberattacks, having a value of (0.210). On the other hand, cyberattack and psychological factors and the system's vulnerability have a value of (0.430), giving us a significant correlation. As a result, we infer that there are greater possibilities that both factors move in the same direction (see Figure 3).

Table 8. Correlation among cyberattacks, psychological factors, and technology.

Correlations				
		Computer Attack	**Psychological Factor**	**System Vulnerability**
Computer Attack	Pearson's Correlation	1.000	0.210 **	0.430 **
	Sig. (Bilateral)		0.000	0.000
	N	51.931	51.931	51.931
Psychological Factor	Pearson's Correlation	0.210 **	1.000	−0.015 **
	Sig. (Bilateral)	0.000		0.001
	N	51.931	51.931	51.931
System Vulnerability	Pearson's Correlation	0.430 **	−0.015 **	1.000
	Sig. (Bilateral)	0.000	0.001	
	N	51.931	51.931	51.931

** The correlation is significant at the 0.01 level (bilateral).

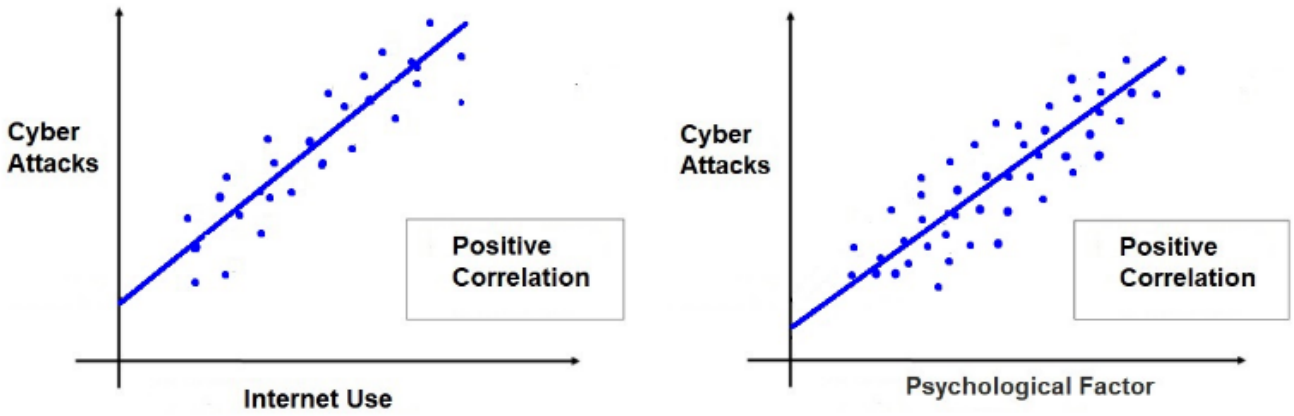

Figure 3. (**Left**) correlation between Internet demand and cyberattacks; (**right**) correlation between psychological factors and cyberattacks.

The results obtained reflect a probable fact known by security experts; the cybersecurity strategy also depends on a cognitive approach. So, one of the main issues today in the context of the COVID-19 pandemic is the environment of uncertainty where users and cybersecurity specialists need to improve their cognitive agility. To understand the process that an attacker could use, in this study we adopted the cyber kill chain model [77] that includes the following phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and exfiltration with psychological factors during the COVID-19 pandemic.

RQ1. Is there a variation in security attacks during the period of the COVID-19 pandemic?

Based on the literature review, in the works [47–51], we can observe no significant variation in the types of phishing attacks that existed before COVID-19. On the other hand, no new types of attacks have been detected. However, we observed that these attacks are adaptable to the current context of the COVID-19 pandemic. Furthermore, complementing the study by [17], who mentions that ransomware and XSS attacks have been the most relevant due to their volume during COVID-19, it should be noted that there is an increase in social engineering attacks. Attacks have improved their effectiveness due to people's increased connection and interconnection to digital media and services and the need to acquire information during the pandemic. The context of the COVID-19 pandemic has generated changes in social, technological, and cultural aspects worldwide. Teleworking and tele-education have become essential to give continuity to daily operations and activities in the world. This migration of activities to the home environment, where cybersecurity mechanisms (firewall, IDS, SIEM, among others) are less efficient and advanced than the organizations' physical facilities, has enabled cyber adversaries to increase the scope and impact of their attacks.

COVID-19 has generated an increase in the need for access to data, information, and social networks to be aware of the issues inherent to the pandemic, such as infection growth and medication. Moreover, knowing that daily activities related to entertainment, shopping, or social relations have shifted entirely to the digital realm, adversaries have intelligently made variations in the form of their attacks to exploit this new reality imposed by the pandemic. As a representative example, phishing attacks that used content related to COVID-19 (e.g., possible protection measures against the coronavirus) have become very common.

RQ2. Has the context of the COVID-19 pandemic increased the susceptibility of being a victim of cyberattacks?

The context of COVID-19 has generated a change in some people in human factors such as anxiety, depression, and uncertainty due to the social and economic crisis of the pandemic. In some cases, these changes have prompted people to seek refuge in social media to maintain human interaction in the face of a state of confinement and the need to obtain information related to the social and economic aspects of COVID-19. Based on the literature review, we can observe an increase in fake news and misinformation events. Although these events do not fall under the category of cybercrime, they can be used by attackers to increase uncertainty and a negative context that increases the susceptibility of people to being attacked. Moreover, knowing that social engineering attacks focus on cognitive manipulation, the more information sent to a person, the greater the probability of changing their cognitive bias. Adversaries are aware that when humans are in a stage where psychological factors such as anxiety, depression, frustration, or loneliness are high, they become more vulnerable, and they are the weakest link in the cybersecurity chain. Hence, they focus on these aspects in their social engineering attacks. It is safe to assume that adversaries carry out these types of behavioral and technical analyses. In that case, it is essential that cybersecurity specialists and people, in general, understand the process related to an attack and how cyberattacks are adaptable to each context, as is the case with the COVID-19 pandemic.

For this reason, we model cyberattacks in the context of the pandemic by considering psychological factors. Psychological factors can be leveraged for an attack where the victim in the same exploration phase is experiencing a restriction or loss of physical freedom and feels socially isolated. Due to the pandemic, the adversary knows that people resorted to being connected for more extended periods. However, psychological factors can also be used as defense strategies, thus improving people's resilience and self-efficacy. In this way, security mechanisms can be generated, especially in the delivery phase in which the role of people is more relevant than that of technological solutions. International organizations have highlighted this aspect and have promoted a hybrid set of strategies (i.e., social and technical) during the COVID-19 pandemic.

The conducted SLR identifies that common cyberattacks such as phishing, ransomware, mobile malware, or XSS not only remained during the pandemic but also increased their

volume. Through the use of the full-text review in the PRISMA methodology's inclusion process, it was possible to identify that the pandemic influenced the growth of human factors such as stress, anguish, and despair caused by the perception of danger, loneliness, and loss of physical freedom. Adversaries took advantage of these factors to improve their social engineering attacks by including content related to the coronavirus.

Adversaries also focused on the people's emotional vulnerability during this pandemic, knowing that messages referring to job stability, economic incentives, or vaccination plans would be of interest. Their critical judgment could be affected by this context. The SLR identifies that the COVID-19 pandemic prompted a mandatory use of the Internet for education, work, or service payment activities, which allowed the attackers to have a greater possibility of carrying out their attacks [55–67]. The correlational study carried out based on the data obtained in the SLR shows that a longer time spent on the Internet and the impact on psychological factors present a positive correlation coefficient that allows inducing a direct relationship between these two elements and the increase of cybersecurity attacks.

RQ3. How can we model the user behavior during the COVID-19 pandemic in the face of a cyberattack employing the steps of the cyber kill chain?

There is a generalization of people's behaviors in digital media in the recognition phase. Lifestyle changes are driven by the pandemic, such as telecommuting, accessing social media, and online shopping, which have allowed cyberattacks to become more widespread. In the weaponization phase, media such as email messages, web pages, and mobile applications are still used to prepare the cyberattack. In the delivery phase, there are two aspects in which technological solutions and the optimization of cognitive processes can be employed for the defense of security. Modeling cyberattacks with a cyber kill chain allows us to understand the attack process executed by adversaries. Although the model does not detail the techniques and tools used and does not identify the attacker's behavior, it provides a macro vision of the cyberattack process for establishing cybersecurity strategies. Understanding each attack stage and associating it with the human factor that the adversary will exploit could support establishing security strategies based on people's psychological and cognitive characteristics.

5. Modeling of Cyberattacks Based on the Cyber Kill Chain

5.1. Psychological Impact and Behaviors during the Pandemic

The results of this study corroborate the relation between human factors and cybersecurity attacks. Elements such as time of connectivity to the Internet, social and entertainment media, and the psychological behavior of the user could increase the susceptibility to attacks. Regarding this point, our interest is defining how the human factor in cyberattacks (psychological behavior) could be taken into consideration in the development of cyber-exercises.

Human factors: A negative psychological impact is another consequence of the COVID-19 outbreak. The literature review found that emerging mental health problems are related to stress, anxiety, depression, frustration, and uncertainty.

Protective factors: Psychological resilience is the ability to support or retrieve psychological well-being. In social threat situations such as a pandemic, strengthening individual strategies helps in the acceptance of anxiety and the management of negative emotions to achieve the successful re-adaptation process [77]. The establishment of social support is a strategy to reduce the likelihood of developing psychological distress and psychiatric conditions. The results of the research in [81] in 2020 suggest that the belief that we can face social threat situations (self-efficacy) helps to maintain mental health and reduce risky behaviors. From the psychology perspective, the user could use protective strategies such as cognitive agility, effective communication, and social support to deal with anxiety, depression, and distress and generate resilience against cyberattacks (see Figure 4).

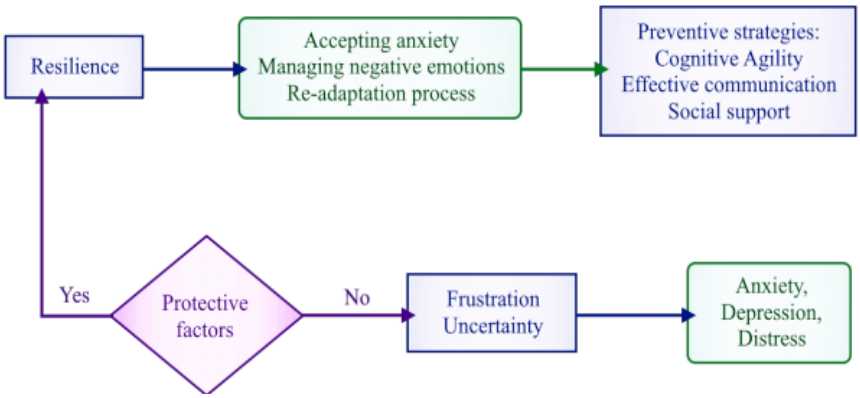

Figure 4. Protective factors to face cyberattacks.

Risk factors: Cognitive and affective factors can influence people's decision-making processes, especially when they are subjected to high levels of anxiety, depression, and distress, such as those generated within the COVID-19 pandemic. Ref. [82] mentions that feelings of frustration and uncertainty can occur in processes when there is an inadequate provision of essential services such as food or water. During the period of the COVID-19 quarantine, these feelings intensified. Additionally, inadequate information generates a stress factor. During the COVID-19 pandemic, the lack of information in the first month led to people's confusion [83].

5.2. Modeling Cyberattacks with Cyber Kill Chain

Cyberattacks leave behind behavioral patterns that can be analyzed to detect malicious activities. Studying the behavior of attackers in various cyberattack scenarios can help develop behavioral models that can be used to identify patterns and distinguish them from legitimate user actions. The systematic literature review allows an understanding of the different vectors that are related to the cybersecurity context, and based on these aspects it can be determined which cognitive elements could be included in each of the phases of the cyber kill chain model.

For the second step, we include the preventive strategies in the seven phases of the cyber kill chain (see Figure 5). The cyber kill chain is used in cybersecurity to describe the various stages that a cyber attacker typically goes through during a targeted attack. It was developed by Lockheed Martin [77]. By understanding the cyber kill chain, cybersecurity professionals can implement measures to detect and prevent attacks at various stages.

To clarify the cyber kill chain process under the COVID-19 scenario where people are connected online, they will use fake web pages with content, medicines, treatment, and vaccines; fake apps with COVID-19 growth maps; emails with false information; and fake messages on social networks. The use of emails to carry out phishing has been highly influential, showing its growth worldwide during 2020. The adversary sends an email impersonating a recognized body such as the World Health Organization (WHO) and generates a message with content that creates interest, such as actions to avoid contagion. The adversary uses official logos so that his mail has a formal presentation. A decomposition of the main elements of the false messages was performed. The elements that these messages have, in general, are a logo, title, name or description, text related to fake content, links to malicious sites, and the message's source [83]. Then, in the weaponization phase, the adversaries look for tools that allow them to carry out their attack. Next, in the delivery phase, the attacker tries to deliver the malicious code, for which he uses an embedded link or a document attached to the email. People are often not good at storing large amounts of new information and generating automatic processes that adapt to their environment. In the context of COVID-19, their systemic thought processes must face work activities, family, and feelings caused by the pandemic, such as anxiety or uncertainty. Not paying attention to the link or attachment description can be of high impact against a cyberattack.

At this point, if the adversary successfully delivers the malicious code, he will proceed with the subsequent exploitation, installation, command and control, and exfiltration phases, in which he can gain control of the machine and steal information or disrupt the service.

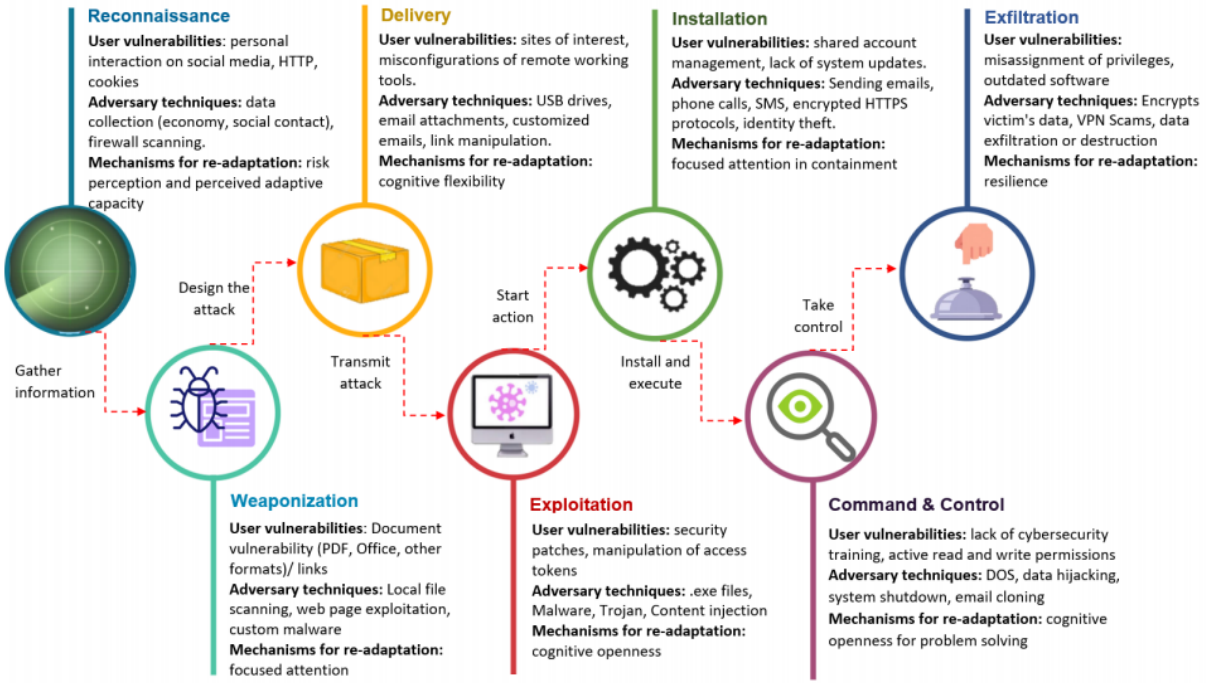

Figure 5. This figure represents the adaptation of the cyber kill chain model developed by Lockheed Martin. We propose to model a phishing attack, focusing on the cognitive human factor, in a sequence of seven steps.

In each phase, we identify both the vulnerabilities of the user and the techniques that attackers use to achieve their purpose. In addition, our model includes the elements of prevention of an attack from the cognitive aspects that would help people face each of the phases. For this reason, we include the mechanisms for re-adaptation by the user [81]. As illustrated in Figure 5, each of the phases comprises the process conducted by an attacker, ranging from identifying the target to taking control and stealing information or disrupting operations. Establishing an attack model would allow technicians to develop the appropriate defensive measures. However, we consider that the context of the COVID-19 pandemic has generated a greater relevance of the human factor over the technological tools in cybersecurity defense processes. Within this context, we can show that the "Reconnaissance" and "Weaponization" phases of the cyber kill chain relate to psychological factors such as social isolation and restrictive measures that cause lifestyle changes. Adversaries can use people's experiences of loss of freedom, loneliness, and boredom to build profiles of their needs and use them to develop weapons of cyberattacks that could be effective in their objective of stealing information or disrupting services. In the "Delivery" phase, we can show that defense strategies need to consider human factors. Strengthening protective factors such as resilience and self-efficacy will help to develop mechanisms for re-adaptation to this new reality.

The model considers the cognitive processes of people as central elements and complements these with the development of solutions based on cognitive systems (machine learning, deep learning, and reinforcement learning) to development behavior analyses for estimating and alerting about possible risky actions by users. They understand the cognitive process of a person during a phishing attack, and this allows us to model and consider the application of deep learning, neural networks, or reinforcement learning as possible complements to reduce the probability of the success of a phishing attack by

developing solutions or tools that support the cognitive process of people in the face of possible cyberattack scenarios.

The main objectives are to understand that not all people have similar forms of cognitive processing or act in a similar way when faced with a cyberattack, to be able to develop solutions based on cognitive systems that adjust to the behavior of each person, which would allow estimating the risk in real time, and being able to establish a proactive cybersecurity strategy. We propose that the cyber kill chain model include stimulating cognitive strategies at the level of executive functions, attention, and perception. This can encourage the acquisition of protective behaviors, such as managing privacy on social networks, blocking unknown contacts, changing passwords, using antiviruses, and limiting one's opinion publications, not only from a technical perspective, but also from social and cognitive perspectives.

The model extracts relevant features such as language patterns, linguistic cues, visual elements, sender information, and domain analyses from vector attacks, which could support the capture of cognitive factors. Considering that the modeling of each episode of cyberattacks could contain a mixture of various vector attack scenarios when different cognitive factors from users could be under development, the use of episodic training as a strategy could leverage the idea of learning from different episodes or scenarios rather than just from individual data points [84]. For instance, in the context of detecting phishing attacks based on cognitive factors, episodic training can be applied to improve the performance of machine learning models by exposing them to various phishing scenarios, making them more robust and capable of generalizing across different attack patterns. Additionally, clearer images can potentially make phishing attempts more convincing and harder to detect by users, especially in periods of significant anxiety such as the COVID-19 pandemic, when some cognitive factors could be changed. So, the use of deep learning algorithms such as Unsupervised Unified Image Dehazing and Denoising Networks (UU-DeNets) could be used effectively. UU-DeNets are image processing techniques primarily used to improve the visual quality of hazy and noisy images [82]. While these techniques are not directly related to detecting phishing attacks, they can still be applied in certain scenarios to enhance the quality of images used in phishing emails or phishing websites which enhance cognitive processing.

6. Discussion

According to Tarnowski [77], we can establish a set of technological solutions such as SIEM, IPS, firewalls, and antiviruses to reduce the attacker's capacity in any of these phases. However, the delivery phase needs to consider the user as a part of countermeasures. Along these lines, the director of SANS mentions that a delivery phase that includes the human being is more decisive in stopping cyberattacks than technological solutions [83]. Even security solutions that include Artificial Intelligence can have false positives and negatives that require human actions to refine them (human in the loop).

We can examine the possibility of a mass attack by exploring the same characteristics observed in individuals worldwide who exhibit similar behaviors. For example, these behaviors may include spending more time online to search for information, experiencing more times when they may feel anxiety or frustration generated by the uncertainty of the pandemic, seeking social contact using technological means, and connecting to work, education, or home activities from a less secure form of environment. As mentioned above, expensive tools such as SIEM, IPS, and firewalls, among others, help reduce attacks. Their deployment is carried out jointly on the premises of the organization. By migrating people to a work-from-home mode, work environments are made less safe from a technological perspective because not all of these tools are available there.

In defense strategies, it is necessary to take into consideration the people. Social isolation and restrictive measures cause lifestyle changes, which attackers can use in the "Reconnaissance" and "Weaponization" phases of cyberattacks. The experiences of loss of freedom, loneliness, and boredom can build profiles of people's needs and, with these

elements, malicious actors can develop weapons of cyberattacks that could be effective in their objective of stealing information or disrupting services. Strengthening protective factors such as resilience and self-efficacy will help to develop mechanisms for re-adapting to this new life scenario and reduce the vulnerability of people to cyberattacks.

Based on the proposed model, it is possible to define security tools and detection algorithms designed to reduce a cyberattack's effectiveness in the first three phases before the adversary can have greater control of the technological system. This study highlights that although technological solutions are relevant for the continuity of operations, they are also a window of opportunity for the generation of cyberattacks that seek to disrupt services or steal information. Additionally, it shows that the human factor, which has always been considered a key element in cybersecurity strategies, has further increased its relevance during this pandemic. Since the beginning of the pandemic, specialized organizations have mentioned that the control of the coronavirus depends on the behavior and critical judgment of people; this criterion is transferred in the same way to the digital world where the success or failure of a cyberattack will depend on the role and action of people.

This study proposes integrating human factors into technological solutions against social engineering cyberattacks. This is a relatively new field that requires further research to generate scientific evidence that can reduce the vulnerability of digital systems in which humans spend more time and interact with a greater number of people, especially after the COVID-19 pandemic, which has modified behaviors in the workplace, commerce, and education sectors. Cyberpsychology is emerging as a promising research area with significant future potential.

7. Conclusions

The pandemic was a catalyst for social, cultural, and technological changes worldwide. Although from the perspective of technological growth the pandemic has pushed the growth of solutions focused on tele-education, teleworking, and online services, it is also true that it has indirectly led to an increase in cybersecurity attacks.

Cross-site scripting and ransomware attacks have been relevant during the pandemic due to their use and impact in the financial and health domains. These attacks have disrupted computer systems, caused the infection of millions of machines, and exposed people's sensitive information. Cyberattacks during the pandemic maintained their fundamental attack characteristics, such as the use of cookies, the injection of malware through email, and the use of fake news.

Adversaries have taken advantage of the pandemic context to modify their attacks using information related to COVID-19 to take advantage of people's need to learn information about the coronavirus and the development of daily activities. Some psychological factors such as stress, anxiety, and depression, which reflect a combination of the feelings of loss of freedom and social isolation generated by the pandemic, have been used by adversaries to be more effective in their social engineering attacks. This study made it possible to understand how adversaries took advantage of psychological factors in cyberattacks, an aspect that could allow the establishment of more effective security mechanisms. To understand the process that a phishing attacker could use for taking advantage of psychological factors during the COVID-19 pandemic, we adapted in this study the cyber kill chain model that included reconnaissance, armament, and delivery, exploitation, installation, command and control, and exfiltration phases. In certain stages of the cyberattack, such as delivery, the actions carried out by people are of greater relevance than those established by technological solutions. Therefore, it is convenient to focus on hybrid solutions that strengthen people's cognitive processes to detect cyberattacks. They can contribute to the effectiveness of minimizing the impact of cyberattacks.

Author Contributions: Conceptualization, W.F. and M.C.; methodology, R.A.; formal analysis, R.A.; investigation, R.A. and M.C.; writing—review and editing, R.A. and W.F.; project administration, W.F.; funding acquisition, I.O.-G. and M.S.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Office for National Statistics. Coronavirus and the Social Impacts on Great Britain. 2021. Available online: https://www.ons.gov.uk/peoplepopulationandcommunity/ (accessed on 31 October 2022).
2. UNICEF. COVID-19 Archives. UNICEF DATA. 2021. Available online: https://data.unicef.org/resources/resource-topic/covid-19/ (accessed on 31 October 2022).
3. Sodhi, A.; Social Media Law & Cybercrime. Social Science Research Network SSRN. 2020. Available online: https://ssrn.com/abstract=3541485 (accessed on 31 October 2022).
4. Serafini, G.; Parmigiani, B.; Amerio, A.; Aguglia, A.; Sher, L.; Amore, M. The psychological impact of COVID-19 on the mental health in the general population. *QJM Int. J. Med.* **2020**, *113*, 531–537. [CrossRef] [PubMed]
5. Interpol. INTERPOL Report Shows Alarming Rate of Cyberattacks During COVID-19. 2020. Available online: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-reportshows-alarming-rate-of-cyberattacks-during-COVID-19 (accessed on 31 October 2022).
6. Europol. Office of the European Union, Luxembourg. 2020. Available online: https://www.europol.europa.eu/sites/default/files/documents/european_union_terrorism_situation_and_trend_report_te-sat_2020_0.pdf (accessed on 31 October 2022).
7. McAfee. 2017. Available online: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2017.pdf (accessed on 3 November 2022).
8. McAfee. 2018. Available online: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2018.pdf (accessed on 3 November 2022).
9. McAfee. 2019. Available online: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2019.pdf (accessed on 3 November 2022).
10. McAfee. 2020. Available online: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2020.pdf (accessed on 3 November 2022).
11. McAfee. 2021. Available online: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2021.pdf (accessed on 3 November 2022).
12. McAfee. 2022. Available online: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2022.pdf (accessed on 3 November 2022).
13. Anti-Phishing Work Group—APWG. Interisle Study Shows 61% Increase in Phishing Attacks, More Brands Targeted, and 257% Increase in Cryptocurrency Phishing. 2022. Available online: https://apwg.org/interisle-study-shows-61-increase-in-phishing-attacks-more-brands-targeted-and-257-increase-in-cryptocurrency-phishing/ (accessed on 3 November 2022).
14. Albladi, S.M.; Weir, G.R.S. User characteristics that influence judgment of social engineering attacks in social networks. *Hum. Centric Comput. Inf. Sci.* **2018**, *8*, 5. [CrossRef]
15. Arya, S.; Kaji, A.H.; Boermeester, M.A. PRISMA Reporting Guidelines for Meta-analyses and Systematic Reviews. *JAMA Surg.* **2021**, *156*, 789–790. [CrossRef] [PubMed]
16. Venkatesha, S.; Reddy, K.R.; Chandavarkar, B.R. Social Engineering Attacks during the COVID-19 Pandemic. *SN Comput. Sci.* **2021**, *2*, 1–9. [CrossRef] [PubMed]
17. Susukailo, V.; Opirskyy, I.; Vaslyshyn, S. Analysis of the attack vectors used by threat actors during the pandemic. In Proceedings of the IEEE 15th International Conference on Computer Sciences and Information Technologies, Zbarazh, Ukraine, 23–26 September 2020; pp. 261–264. [CrossRef]
18. Setera, K.; FBI. FBI Warns of Teleconferencing and Online Classroom Hijacking during COVID-19 Pandemic: March. 2020. Available online: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic (accessed on 13 November 2022).
19. Anansaringkarn, P.; Neo, R. How can state regulations over the online sphere continue to respect the freedom of expression? A case study of contemporary 'fake news' regulations in Thailand. *Inf. Commun. Technol. Law* **2021**, *30*, 283–303. [CrossRef]
20. Bracci, A.; Nadini, M.; Aliapoulios, M.; McCoy, D.; Gray, I.; Teytelboym, A.; Gallo, A.; Baronchelli, A. Dark Web Marketplaces and COVID-19: Before the vaccine. *EPJ Data Sci.* **2021**, *10*, 6. [CrossRef] [PubMed]
21. Check Point Blog. Check Point. *Coronavirus-Themed Domains 50% More Likely to be Malicious than Other Domains*. 2020. Available online: https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-morelikely-to-be-malicious-than-other-domains/ (accessed on 15 November 2022).
22. Roberts, G.; Avast. The Year of Fake News, COVID-19 Scams and Ransomware. 2020. Available online: https://blog.avast.com/es/2020-year-in-review-avast (accessed on 15 November 2022).
23. Kent, J. Cequence security. Tales from the Front Lines: Attackers on Lockdown Focus on API. 2020. Available online: https://www.cequence.ai/blog/tales-from-the-frontlines-attackers-on-lockdown-focus-on-apis/ (accessed on 15 November 2022).
24. Burgess, M.; Wired. Secret NHS Files Reveal Plans for Coronavirus Contact Tracing App. 2020. Available online: https://www.wired.co.uk/article/nhs-covid-19-app-health-status-future (accessed on 18 November 2022).

25. Kovacs, E.; Security Week. Over 6400 Edison Mail Users Hit by Security Bug in iOS App. 2020. Available online: https://www.securityweek.com/over-6400-edison-mail-users-hitsecurity-bug-ios-app (accessed on 25 November 2022).
26. Sushma, K.; Jayalakshmi, M.; Guha, T. Deep Learning for Phishing Website Detection. In Proceedings of the 2022 IEEE 2nd 183 Mysore Sub Section International Conference (MysuruCon), Mysuru, India, 16–17 October 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–6.
27. FBI's IC3. *2020 Internet Crime Report*; Federal Bureau of Investigation—Internet Crime Complaint Center: Washington, DC, USA, 2020; pp. 1–28.
28. Bikov, T.D.; Iliev, T.B.; Mihaylov, G.Y.; Stoyanov, I.S. Phishing in Depth—Modern Methods of Detection and Risk Mitigation. In Proceedings of the 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 20–24 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 447–450. [CrossRef]
29. AlGhanboosi, B.; Ali, S.; Tarhini, A. Examining the effect of regulatory factors on avoiding online blackmail threats on social media: A structural equation modeling approach. *Comput. Hum. Behav.* **2023**, *144*, 107702. [CrossRef]
30. Cole, S.; Kvavilashvili, L. Spontaneous and deliberate future thinking: A dual process account. *Psychol. Res.* **2021**, *85*, 464–479. [CrossRef]
31. Algarni, A.; Xu, Y.; Chan, T. Social Engineering in Social Networking Sites: The Art of Impersonation. In Proceedings of the 2014 IEEE International Conference on Services Computing, Anchorage, AK, USA, 27 June–2 July 2014; pp. 797–804. [CrossRef]
32. Jones, H.S.; Towse, J.N.; Race, N. Susceptibility to email fraud: A review of psychological perspectives, data-collection methods, and ethical considerations. *Int. J. Cyber Behav. Psychol. Learn.* **2015**, *5*, 13–29. [CrossRef]
33. Valaskivi, K. Hybrid CoE Strategic Analysis 5: Beyond Fake News: Content Confusion and Understanding the Dynamics of the Contemporary Media Environment. Version 4 June 2023 submitted to Journal Not Specified 7 of 7. 2018. Available online: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-5-beyond-fake-news-content-confusion-and-understanding-the-dynamics-of-the-contemporary-media-environment/ (accessed on 25 November 2022).
34. Verkijika, S.F. "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Comput. Hum. Behav.* **2019**, *101*, 286–296. [CrossRef]
35. Singh, K.; Aggarwal, P.; Rajivan, P.; Gonzalez, C. Training to Detect Phishing Emails: Effects of the Frequency of Experienced Phishing Emails. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Seattle, WA, USA, 28 October–1 November 2019; Volume 63, pp. 453–457. [CrossRef]
36. Weil, T.; Murugesan, S. IT Risk and Resilience—Cybersecurity Response to COVID-19. *IT Prof.* **2020**, *22*, 4–10. [CrossRef]
37. Gupta, A.; Singh, A.; Bharadwaj, D.; Mondal, A. Humans and Robots: A Mutually Inclusive Relationship in a Contagious World. *Int. J. Autom. Comput.* **2021**, *18*, 185–203. [CrossRef]
38. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M.; Saldamli, G. Predicting and preventing cyber attacks during covid-19 time using data analysis and proposed secure IoT layered model. In Proceedings of the Fourth International Conference on Multimedia Computing, Valencia, Spain, 19–22 October 2020; pp. 113–118. [CrossRef]
39. Schuetz, S.W.; Sykes, T.A.; Venkatesh, V. Combating COVID-19 fake news on social media through fact checking: Antecedents and consequences. *Eur. J. Inf. Syst.* **2021**, *30*, 376–388. [CrossRef]
40. Maakoul, O.; Boucht, S.; El Hachimi, K.; Azzouzi, S. Towards Evaluating the COVID'19 related Fake News Problem: Case of Morocco. In Proceedings of the 2020 IEEE 2nd International Conference on Electronics, Control, Optimization and Computer Science (ICECOCS), Kenitra, Morocco, 2–3 December 2020. [CrossRef]
41. Yoshikawa, K.; Awa, T.; Kusano, R.; Sato, H.; Ichino, M.; Yoshiura, H. A Fake News Dissemination Model Based on Updating Reliability and Doubt among Individuals. In Proceedings of the 2020 11th International Conference on Awareness Science and Technology (iCAST), Qingdao, China, 7–9 December 2020. [CrossRef]
42. Zaeem, R.N.; Li, C.; Barber, K.S. On Sentiment of Online Fake News. In Proceedings of the 2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), The Hague, The Netherlands, 7–10 December 2020. [CrossRef]
43. Abdelminaam, D.S.; Ismail, F.H.; Taha, M.; Taha, A.; Houssein, E.H.; Nabil, A. CoAID-DEEP: An Optimized Intelligent Framework for Automated Detecting COVID-19 Misleading Information on Twitter. *IEEE Access* **2021**, *9*, 27840–27867. [CrossRef] [PubMed]
44. De, S.; Agarwal, D. A novel model of supervised clustering using sentiment and contextual analysis for fake news detection. In Proceedings of the Third International Conference on Multimedia Processing, Communication Information Technology (MPCIT), Shivamogga, India, 11–12 December 2020; pp. 112–117.
45. Verma, S.; Paul, A.; Kariyannavar, S.S.; Katarya, R. Understanding the Applications of Natural Language Processing on COVID-19 Data. In Proceedings of the 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 5–7 November 2020. [CrossRef]
46. Hawa, S.; Lobo, L.; Dogra, U.; Kamble, V. Combating misinformation dissemination through verification and content driven recommendation. In Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 4–6 February 2021; pp. 917–924. [CrossRef]
47. Kapusta, J.; Benko, Ľ.; Munk, M. Fake News Identification Based on Sentiment and Frequency Analysis. In *Learning and Analytics in Intelligent Systems*; Springer: Cham, Switzerland, 2020; pp. 400–409. [CrossRef]
48. Hussain, F.; Abbas, S.G.; Shah, G.A.; Pires, I.M.; Fayyaz, U.U.; Shahzad, F.; Garcia, N.M.; Zdravevski, E. A Framework for Malicious Traffic Detection in IoT Healthcare Environment. *Sensors* **2021**, *21*, 3025. [CrossRef] [PubMed]

49. Abroshan, H.; Devos, J.; Poels, G.; Laermans, E. A phishing Mitigation Solution using Human Behaviour and Emotions that Influence the Success of Phishing Attacks. In Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization, Utrecht, The Netherlands, 21–25 June 2021. [CrossRef]
50. Akdemir, N.; Yenal, S. How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails. *SAGE Open* **2021**, *11*, 215824402110318. [CrossRef]
51. Furini, M.; Mirri, S.; Montangero, M.; Prandi, C. Untangling between fake-news and truth in social media to understand the COVID-19 Coronavirus. In Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 7–10 July 2020. [CrossRef]
52. Al-Turkistani, H.F.; Ali, H. Enhancing Users' Wireless Network Cyber Security and Privacy Concerns during COVID-19. In Proceedings of the 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA), Riyadh, Saudi Arabia, 6–7 April 2021. [CrossRef]
53. Hijji, M.; Alam, G. A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. *IEEE Access* **2021**, *9*, 7152–7169. [CrossRef]
54. Baseskioglu, M.O.; Tepecik, A. Cybersecurity, Computer Networks Phishing, Malware, Ransomware, and Social Engineering Anti-Piracy Reviews. In Proceedings of the 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 11–13 June 2021. [CrossRef]
55. Chandra, N.A.; Putri Ratna, A.A.; Ramli, K. Development of a Cyber-Situational Awareness Model of Risk Maturity Using Fuzzy FMEA. In Proceedings of the 2020 International Workshop on Big Data and Information Security (IWBIS), Depok, Indonesia, 17–18 October 2020. [CrossRef]
56. Sharma, R.; Sharma, N.; Mangla, M. An Analysis and Investigation of InfoStealers Attacks during COVID'19: A Case Study. In Proceedings of the 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), Jalandhar, India, 21–23 May 2021. [CrossRef]
57. Muttoo, S.; Badhani, S. An Analysis of Malware Detection and Control through COVID-19 Pandemic. In Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 17–19 March 2021; pp. 637–641.
58. Cvitić, I.; Peraković, D.; Periša, M.; Jurcut, A.D. Methodology for Detecting Cyber Intrusions in e-Learning Systems during COVID-19 Pandemic. *Mob. Netw. Appl.* **2021**, *28*, 231. [CrossRef]
59. Said Elsayed, M.; Le-Khac, N.-A.; Jurcut, A.D. Dealing With COVID-19 Network Traffic Spikes [Cybercrime and Forensics]. *IEEE Secur. Priv.* **2021**, *19*, 90–94. [CrossRef]
60. Jarjoui, S.; Murimi, R.; Murimi, R. Hold My Beer: A Case Study of how Ransomware Affected an Australian Beverage Company. In Proceedings of the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 14–18 June 2021. [CrossRef]
61. Ahsan Pritom, M.M.; Schweitzer, K.M.; Bateman, R.M.; Xu, M.; Xu, S. Data-Driven Characterization and Detection of COVID-19 Themed Malicious Websites. In Proceedings of the 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), Arlington, VA, USA, 9–10 November 2020. [CrossRef]
62. Wang, L.; He, R.; Wang, H.; Xia, P.; Li, Y.; Wu, L.; Zhou, Y.; Luo, X.; Sui, Y.; Guo, Y.; et al. Beyond the virus: A first look at coronavirus-themed Android malware. *Empir. Softw. Eng.* **2021**, *26*, 82. [CrossRef]
63. UK Data Service. UK Data Service COVID-19 Data. 2020. Available online: https://www.ukdataservice.ac.uk/get-data/themes/covid-19/covid-19-data.aspx (accessed on 25 November 2022).
64. Staszkiewicz, P.; Chomiak-Orsa, I.; Staszkiewicz, I. Dynamics of the COVID-19 Contagion and Mortality: Country Factors, Social Media, and Market Response Evidence From a Global Panel Analysis. *IEEE Access* **2020**, *8*, 106009–106022. [CrossRef]
65. Burton, S.; Puddephatt, J.; Baines, L.; UNICEF Innocenti: Children and COVID-19 Research Library. UNICEF Office of Research—Innocenti. 2021. Available online: https://www.unicefirc.org/covid-children-library?tag=behaviour (accessed on 5 December 2022).
66. Balanzá-Martínez, V.; Kapczinski, F.; de Azevedo Cardoso, T.; Atienza-Carbonell, B.; Rosa, A.R.; Mota, J.C.; De Boni, R.B. The assessment of lifestyle changes during the COVID-19 pandemic using a multidimensional scale. *Rev. Psiquiatr. Salud Ment.* **2021**, *14*, 16–26. [CrossRef] [PubMed]
67. World Bank. Understanding the Coronavirus (COVID-19) Pandemic Through Data. *Universal Health Coverage Data.* 2021. Available online: https://datatopics.worldbank.org/universal-health-coverage/coronavirus/ (accessed on 25 November 2022).
68. University of Essex, Institute for Social and Economic Research. *Understanding Society: COVID-19 Study, 2020: Special Licence Access, School Codes*; UK Data Service; University of Essex, Institute for Social and Economic Research: Colchester, UK, 2021. [CrossRef]
69. World Bank. World Bank Education COVID-19 School Closures Map. 2020. Available online: https://www.worldbank.org/en/data/interactive/2020/03/24/world-bank-educationand-covid-19 (accessed on 25 November 2022).
70. Eurofond. Living, Working and COVID-19 Data. *Data.Europa.Eu.* 2020. Available online: https://data.europa.eu/data/datasets/living-working-and-covid-19-data?locale=en (accessed on 25 November 2022).
71. Crooks, C.L.; Hogg, J.L.; Martin, S.M.; Grant, J.; Lemoie, K.; Robbins, M. Understanding Generational Factors in the Workplace: Current Considerations for Telework Practices and the Digital Native. In Proceedings of the 2020 IEEE International Professional Communication Conference (ProComm), Kennesaw, GA, USA, 19–22 July 2020.

72. Government of Canada. Percentage of Workforce Teleworking or Working Remotely, and Percentage of Workforce Expected to Continue Teleworking or Working Remotely after the Pandemic, by Business Characteristics. 2020. Available online: https://open.canada.ca/data/en/dataset/9909c57f-b84e-4cc9-9255-3d526f60ef4d (accessed on 28 November 2022).
73. Larrea-Araujo, C.; Ayala-Granja, J.; Vinueza-Cabezas, A.; Acosta-Vargas, P. Ergonomic Risk Factors of Teleworking in Ecuador during the COVID-19 Pandemic: A Cross-Sectional Study. *Int. J. Environ. Res. Public Health* **2021**, *18*, 5063. [CrossRef] [PubMed]
74. Kalinowski, A.; Research Sources and Guides: COVID-19's Impact on Business: Data. Stanford Graduate School of Business Library. 2020. Available online: https://libguides.stanford.edu/covid19 (accessed on 29 November 2022).
75. Georgetown University. Tracking COVID-19 Unemployment and Job Losses. 2021. Available online: https://cew.georgetown.edu/cew-reports/jobtracker/#tool-3-tracking (accessed on 30 November 2022).
76. Kolokotroni, O.; Mosquera, M.C.; Quattrocchi, A.; Heraclides, A.; Demetriou, C.; Philippou, E. Lifestyle habits of adults during the COVID-19 pandemic lockdown in Cyprus: Evidence from a cross-sectional study. *BMC Public Health* **2021**, *21*, 786. [CrossRef] [PubMed]
77. Tarnowski, I. How to use cyber kill chain model to build cybersecurity? *Eur. J. High. Educ. IT* **2017**. Available online: https://tnc17.geant.org/getfile/tnc17_paper_TNC17-IreneuszTarnowski-HowToUseCyberKillChainModelToBuildCybersecurity_-En.pdf (accessed on 5 December 2022).
78. Chandola, T.; Kumari, M.; Booker, C.L.; Benzeval, M. The mental health impact of COVID-19 and lockdown-related stressors among adults in the UK. *Psychol. Med.* **2020**, *52*, 2997–3006. [CrossRef] [PubMed]
79. Sokolov, M.; The Drum. The Pandemic Infodemic: How Social Media Helps (and Hurts) during the Coronavirus Outbreak. 2020. Available online: https://www.thedrum.com/opinion/2020/03/03/the-pandemic-infodemic-how-socialmedia-helps-and-hurts-during-the-coronavirus (accessed on 5 December 2022).
80. Kaspersky. Google Blocking 18 m Coronavirus Scam e-mails Every Day. 2020. Available online: https://www.kaspersky.com/resource-center/definitions/cookies (accessed on 5 December 2022).
81. Chin, S.W.; Zheng, J.Y. Seeing is believing examining self-efficacy and trait hope as moderators of youths' positive risk-taking intention. *J. Risk Res.* **2020**, *24*, 819–832. [CrossRef]
82. Ding, B.; Zhang, R.; Xu, L.; Liu, G.; Yang, S.; Liu, Y.; Zhang, Q. U2D2Net: Unsupervised Unified Image Dehazing and Denoising Network for Single Hazy Image Enhancement. *IEEE Trans. Multimed.* **2023**, 1–16. [CrossRef]
83. Mohamed, G.; Visumathi, J.; Mahdal, M.; Anand, J.; Elangovan, M. An Effective and Secure Mechanism for Phishing Attacks Using a Machine Learning Approach. *Processes* **2022**, *10*, 1356. [CrossRef]
84. Zhang, R.; Yang, S.; Zhang, Q.; Xu, L.; He, Y.; Zhang, F. Graph-based few-shot learning with transformed feature propagation and optimal class allocation. *Neurocomputing* **2022**, *470*, 247–256. [CrossRef]