Received: 9 December 2021 | Revised: 1 June 2022 | Accepted: 6 June 2022

IET Information Security

DOI: 10.1049/ise2.12073

The Institution of Engineering and Technology WILEY

REVIEW

The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19

Ali F. Al-Qahtani[1] | **Stefano Cresci**[2]

[1]College of Science and Engineering, Hamad Bin Khalifa University (HBKU), Doha, Qatar

[2]Institute of Informatics and Telematics (IIT), National Research Council (CNR), Pisa, Italy

Correspondence

Stefano Cresci, Institute of Informatics and Telematics (IIT), National Research Council (CNR), via G. Moruzzi 1, Pisa 56124, Italy.
Email: stefano.cresci@iit.cnr.it

Funding information

Qatar National Library, Grant/Award Number: QRLP10-G-1803022; Qatar National Research Fund

Abstract

The COVID-19 pandemic coincided with an equally-threatening scamdemic: a global epidemic of scams and frauds. The unprecedented cybersecurity concerns emerged during the pandemic sparked a torrent of research to investigate cyber-attacks and to propose solutions and countermeasures. Within the scamdemic, phishing was by far the most frequent type of attack. This survey paper reviews, summarises, compares and critically discusses 54 scientific studies and many reports by governmental bodies, security firms and the grey literature that investigated phishing attacks during COVID-19, or that proposed countermeasures against them. Our analysis identifies the main characteristics of the attacks and the main scientific trends for defending against them, thus highlighting current scientific challenges and promising avenues for future research and experimentation.

1 | INTRODUCTION

The COVID-19 pandemic had a dramatic worldwide impact on all sides of our lives, including the way business and social interactions are conducted, and the overall organisation of our work. Regarding the latter, lockdowns and the enforcement of social distancing measures resulted in an unprecedented number of people experiencing changes in their working habits. Many employees had to adapt – oftentimes even abruptly – to using digital platforms, messaging apps and novel communication channels for their everyday activities [1]. In a line, we witnessed a huge worldwide shift from office work to remote (home) work.

This high-level change implied several lower-level fundamental shifts in how work was conducted, especially from a security perspective. In fact, while office work was characterised by a mixture of physical and digital interactions —the latter occurring in relatively secure and monitored environments, remote working necessarily involved the use of digital systems operated in largely insecure and unmanaged environments. Moreover, a large number of people were not used to remote working and did not receive any specific training on how to work remotely in a secure way. The inevitable consequence was the increase of cyber-risks, which eventually resulted in a massive escalation of cyber-attacks [2, 3]. An early report from the International Association of IT Asset Managers (IAITAM) warned that working from home during the COVID-19 pandemic could allow for plentiful data breaches.[1] The warnings from the IAITAM report were later confirmed when a large-scale survey involving more than 3000 employees across 12 countries found that 94% of them experienced data breaches via cyber-attacks during the course of the pandemic, resulting in an average number of more than 2 breaches suffered per employee [1].

In addition to the regular and well-known security risks of remote working, other peculiar risks arose as a consequence of the chaos induced by the pandemic. As a paramount example, the widespread fear and uncertainty that followed the diffusion of COVID-19 resulted in a huge demand for information (e.g., how to protect from, or cure, the infection), which set the stage for the emergence of a COVID-19 infodemic [4, 5]. As part of such uncontrolled flow of information, a surge in the registration of covid-related domains was observed. Several investigations demonstrated that a large share of such new domains were

[1] https://www.techrepublic.com/article/covid-19-lockdowns-are-causing-a-huge-spike-in-data-breaches

outright malicious or, at the very least, suspicious to serve as threat vectors for the exploitation of cyber-attacks [6]. The most common type of attack related to the newly-created COVID-19 websites was phishing.[2]

Many cyber-attacks involve social engineering techniques to boost their chances of success. To this regard, the increased anxiety caused by the pandemic resulted in a higher success rate for cyber-attacks occurred during COVID-19 [7]. Coupled with the overall increase in cyber-attacks, this figure depicts a worrying scenario. Moreover, for workers employed in critical business sectors – such as healthcare professionals – the pandemic also meant exceptional workloads, with a consequent increase in stress which also affects the success rate of cyber-attacks. Indeed, a statistically significant positive correlation was measured in [8] between workload and the probability of a healthcare staff opening a phishing email. Finally, the steep increase in demand for certain goods such as personal protective equipment (e.g., masks and gloves) exposed health services and even governments to a plethora of digital scams, especially in the form of phishing attacks [9, 10]. Given this picture, it comes with little surprise that critical national infrastructures such as healthcare services and hospitals were among the most frequent targets of cyber-attacks during COVID-19 [1, 7].

1.1 | Scope and contributions

The COVID-19 pandemic was accompanied by an equally-dangerous epidemic of frauds and manipulations, as noted by the United Nations and the World Health Organization (WHO) [11]. When referring to the manipulation of online information, this digital epidemic was dubbed *infodemic*. In addition to this, the pandemic also created the conditions for the rise of a multitude of cyber-attacks and cybersecurity issues: the COVID-19 *scamdemic*. Within the scamdemic, phishing was by far the most frequent type of attack [7]. Phishing attacks that occurred during the pandemic also featured unique characteristics aimed at exploiting the peculiarities of COVID-19 in order to increase their chances of success. The combination of the large number of phishing attacks, together with their new characteristics, attracted scholarly attention and many dedicated studies. This survey reviews, summarises, compares and critically discusses 54 scientific studies and many reports by governmental bodies and security firms that investigated phishing attacks during COVID-19, or that proposed solutions and countermeasures against them. Our analysis identifies the main characteristics of the attacks and the main scientific trends for defending against them, thus highlighting current scientific challenges and promising avenues for future research and experimentation.

1.2 | Significance

The rise of cyber-attacks – and particularly of phishing attacks – occurred during COVID-19, combined with the increased vulnerabilities of critical systems and persons that underwent extreme levels of stress, holds the potential to cause serious real-world consequences and motivates research on this important topic.

1.3 | Organization

The remainder of our survey is organised as follows. In Section 2 we briefly discuss the recent meta-analyses, surveys and review articles that are mostly related to our present work. In doing that, we position our survey with respect to the existing ones. Then, we introduce the problem of phishing attacks during COVID-19. The results of our literature review are presented in Sections 3 and 4, which respectively focus on phishing attacks and countermeasures. Both sections are structured according to a top-down approach, where we first present the overall synthesis and the main themes that emerged from the surveyed studies, followed by the detailed discussion of each analysed study. Next, in Section 5 we critically discuss the main findings of our survey, also highlighting challenges and promising directions of future research and experimentation. Finally, in Section 6 we conclude our work by summarising the results of our literature review.

2 | BACKGROUND AND PRELIMINARIES

This section begins with a brief critical review of the existing surveys that are mostly related to our present work. Our analysis allows positioning this survey with respect to existing ones, highlighting the novelty and contributions of focussing on phishing attacks occurred during the pandemic. Subsequently, we introduce the problem of phishing and we highlight its importance within the broader landscape of COVID-19 cyber-attacks.

2.1 | Differences with existing surveys

The unprecedented consequences brought about by COVID-19 resulted in a remarkable wave of research produced to contrast the many covid-induced issues. Among this new wave of research are a number of studies that focussed on cyber-crime, cyber-attacks and cybersecurity issues occurred during the pandemic. Original research in this direction was complemented by a few survey papers. Here, we briefly review the existing surveys that investigated the relationship between cyber-attacks and COVID-19, highlighting their differences with respect to our present survey. Table 1 provides an overview of the existing surveys that are mostly related to our work. In the following we briefly describe each of these works.

[2] https://www.zdnet.com/article/thousands-of-covid-19-scam-and-malware-sites-are-being-created-on-a-daily-basis/

TABLE 1 Overview of recent related surveys and differences with this survey. Related surveys are listed in reverse chronological order

		Relatedness		
Survey	**Year**	**Phishing**	**COVID-19**	**Analysis**
Hijji & Alam [1]	2021	◐	●	High-level/descriptive
Lallie et al. [7]	2021	◐	●	High-level/descriptive
He et al. [10]	2021	◐	●	High-level/descriptive
Valiyaveedu et al. [3]	2021	●	○	In-depth/technical
Basit et al. [12]	2021	●	○	In-depth/technical
Salloum et al. [13]	2021	●	○	In-depth/technical
Alkhalil et al. [14]	2021	●	○	High-level/descriptive
Hakak et al. [15]	2020	◐	●	High-level/descriptive
Korkmaz et al. [16]	2020	●	○	In-depth/technical
This survey	–	●	●	In-depth/technical

Note: ○: unrelated; ◐: partially related; ●: related.

The analysis presented in [7] describes COVID-19 from a cyber-crime perspective and highlights the range of cyber-attacks experienced globally during the pandemic. Cyber-attacks were analysed and considered within the context of key global events to reveal the modus-operandi of cyber-attack campaigns. Results of the systematic and longitudinal analysis revealed that cyber-criminals leveraged salient events and governmental announcements to carefully craft and execute more effective cyber-crime campaigns. This work represents a nice introductory study on cyber-attacks and COVID-19, without however going into the details of neither attacks nor countermeasures. The survey in [1] presents the results of a systematic multivocal (i.e., grey and scientific) literature review of social engineering-based cyber-attacks during the COVID-19 pandemic. The survey covers 52 studies that investigated attacks such as phishing, scamming, spamming, smishing, and vishing, perpetrated via fake emails, websites, mobile apps, trojans, bots, and ransomware. This survey only discusses the high-level characteristics of the cyber-attacks, without providing a technical analysis of the techniques proposed for defending against them. The survey is also heavily focussed on grey literature and only to a lower extent on scientific literature. The study presented in [15] briefly reviews some of the malicious cyber activities associated with COVID-19 and the potential mitigation solutions. Being published in 2020, the analysis only covers attacks occurred within the first months of the pandemic. Among the surveyed types of cyber-attacks are denial of service, ransomware, spyware, phising and vishing, and other digital frauds. There is no specific focus on phishing nor a detailed analysis of the detection techniques. The meta-analysis presented in [10] identifies the key cybersecurity challenges, the solutions, and the areas of improvement in the health sector, with respect to the cyber-attacks occurred during the COVID-19 pandemic. The review highlighted a recent increase in cyberattacks (e.g., phishing campaigns and ransomware attacks) that exploit new vulnerabilities in technology and people. In turn, such vulnerabilities are due to changes in habits, behaviours, and working conditions caused by the COVID-19 pandemic. This meta-analysis is non-technical and not specific to phishing, but provides interesting insights into the challenges faced in the healthcare sector.

In addition to the above studies that heavily focussed on COVID-19, there also exists a few recent surveys, mostly technical ones, that investigated certain attacks and countermeasures without however considering the context of the pandemic. The recent study discussed in [3] critically reviews AI-based approaches for defending against phishing attacks. This survey exclusively focuses on Web phishing attacks and categorises defensive techniques as either: (i) URL-based, (ii) HTML-based, or (iii) visual similarity-based. Similarly to [3], the survey in [16] analyzes machine learning-based phishing detection systems that classify Web pages. In particular, it specifically focuses on the analysis of the main machine learning features used in such systems and on their impact on classifier's accuracy. The survey presented in [13] reviews works based on natural language processing techniques for detecting phishing emails, while the survey in [12] focuses on applications of artificial intelligence to detect phishing attacks.

The previous overview of the existing surveys, literature reviews and meta-analyses reveals that the majority of studies that considered the context of the pandemic, focussed on high-level, preliminary investigations rather than in-depth, technical analyses. In other words, such surveys mainly provided scoping reviews instead of systematic, detailed reviews. On the contrary, several technical surveys focussed on phishing attacks, but without specific reference to the pandemic. In the present survey we contribute to filling this gap by providing a detailed analysis of phishing attacks occurred during COVID-19, and their countermeasures.

2.2 | Phishing attacks during COVID-19

As sketched in Figure 1, phishing is a typology of cyber-attacks, heavily grounded in social engineering, where an attacker sends a maliciously-designed message with the goal of tricking the

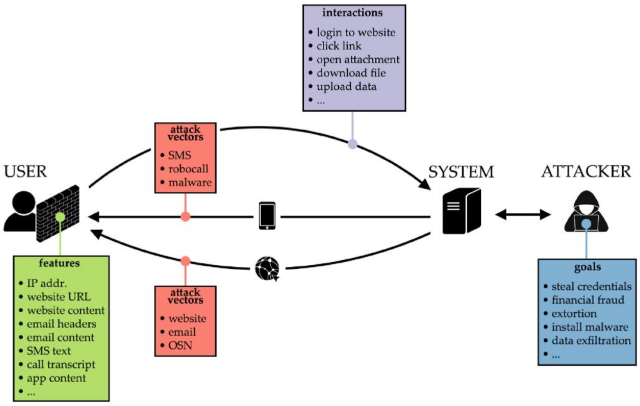

FIGURE 1 Complexity and dimensions of phishing attacks. Attacks can exploit several vectors, including websites, emails and Online Social Networks (OSNs), as well as SMSs, robocalls and malwares. As such, defensive techniques leverage a large set of different features to detect possible attacks. Phishing attacks can be perpetrated for a wide array of malicious goals, such as for stealing sensitive information and for financial fraud. This diversity of goals and techniques poses challenges to the detection of phishing attacks

victim into performing a specific action. Oftentimes, the malicious message points the victim to a system that is controlled by the attacker, from where the victim unwittingly downloads malicious software or simply discloses sensitive information with the attacker. Both the initial message and the system used to collect the victim's information are carefully crafted so as to resemble those of legitimate, authoritative and trustworthy entities (e.g., the WHO or National Health Service (NHS)). Successful phishing attacks can be perpetrated by exploiting a number of media, channels and technologies, including emails, websites and mobile devices. Moreover, both the messages and the systems used to mount phishing attacks can be personalised so as to allow gathering potentially any kind of personal and sensitive information. Because of these reasons, phishing attacks are extremely common and widespread, and often represent the first mandatory step in order to achieve complex frauds and network infiltrations, including Advanced Persistent Threats (APT) [17, 18]. Indeed, the first mandatory step in an APT kill chain involves gaining access to the target network, which can be achieved via phishing. After a successful phishing attack, the next step typically involves deploying a payload, such as a carefully crafted malware designed to be stealthy, which persists in the network for long periods of time, exfiltrating data or anyway helping fulfiling the APT objective for as long as it remains undetected. As practical examples occurred during the COVID-19 pandemic, phishing emails and text messages (e.g., SMSs or WhatsApp messages) were used to lure victims to fraudulent websites. The websites gathered personal data which was used to commit financial fraud or, in other cases, to instal malware (e.g., ransomware) which was then used to commit extortion [7]. To this regard, phishing attacks represent common entry points for a broad array of cyber-attack sequences [7, 12]. Phishing attacks can manifest in several different ways, which led scholars to identify a few noteworthy subcategories of attacks. Among these, smishing refers to phishing attacks that exploit mobile phone text messages (i.e., SMSs) to lure victims. Instead, vishing (i.e., voice phishing) refers to the use of telephony, robocalls and voice over IP to mount attacks. Finally, the term pharming is used when attackers rely on compromising systems (e.g., user devices or DNS servers) to redirect victims to malicious websites.

Based on the above, on the one hand promptly detecting phishing attacks and reducing their efficacy represents a critical step for defending against many cyber-attacks. On the other hand however, the multitude of subtypes, media and technologies exploited in phishing attacks poses challenges to their detection, since detection techniques must adapt and be effective across a broad spectrum of possible scenarios. As shown in Figure 1, current phishing attacks mainly leverage two media: the Internet (and especially the Web), and telephony. Within these media, a large number of different vectors can be used to perpetrate the attack (e.g., to deliver the malicious message). Among the attack vectors that are mostly used are emails, instant messages and messaging apps, online social networks (OSNs), websites, SMSs, robocalls and malware apps for mobile devices.[3] Also the goals of the attackers can be diverse and multifold, with attacks aimed at stealing personal credentials (e.g., usernames and passwords) for certain services, data exfiltration, financial fraud, extortion, or at installing malicious software such as ransomwares, trojans and key loggers. The multitude of ways in which phishing attacks can be mounted, demands the research and development of different techniques. As such, existing phishing detection systems are designed to leverage the combination of several different information for uncovering attacks, including IP addresses; email and SMS texts; websites text, URL, HTML code, images and metadata; voice transcripts; mobile app permissions; and more. The detailed literature analysis presented in the two following sections highlights attacks, and recent progress for defending against them, along these lines.

3 | ATTACKS

This section investigates phishing attacks occurred during the COVID-19 pandemic. We begin by discussing the main peculiar characteristics of covid-related phishing attacks in the broader context of COVID-19, and we conclude by presenting a detailed literature review of the many studies that investigated such attacks.

3.1 | Overview and synthesis

3.1.1 | The rise of phishing attacks

As anticipated, phishing represented by far the most frequent type of cyber-attack that occurred during the pandemic. Evidence for this figure emerges from basically all studies and

[3] https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

reports that investigated covid-related cyber-attacks. Examples of this kind include measurements related to March 2020 indicating an increase in phishing attacks in the region of 600% with respect to the previous month.[4] To quantify the number and scale of such attacks, Google reportedly blocked 18 million phishing emails related to the virus, in April 2020 [19].

Results reported in scientific literature corroborate the above findings. The analysis presented in [7] shows that phishing – including its subcategories, such as smishing and vishing – was involved in 86% of the attacks identified. Moreover, in the context of UK specific cyber-attacks, [7] analysed 17 different attacks, all of which involved phishing at some stage of the attack sequence. Similarly, [1] found that the most frequent social engineering–based attacks were phishing, scamming, spamming, smishing, and vishing. Pharming attacks were much less common but did occur in 13% of cases [7]. Figure 2 shows the relative frequency of all types of cyber-attacks during the COVID-19 pandemic, highlighting the massive frequency of phishing attacks, while Figure 3 drills down into the most frequent subcategories of phishing attacks. Scholars motivate the widespread occurrence of phishing attacks with their high cost-efficiency: attacks are relatively low-cost and with reasonable success rate. To this end, analyses also show that the relatively large likelihood of success for phishing attacks during COVID-19 depended on the strategy of exploiting salient events, media and governmental announcements to the advantage of the attackers [7]. Regarding the platforms mostly used to perpetrate these attacks, emails accounted for 25% of the attacks, followed by websites (20%) and mobile apps (13%) [1].

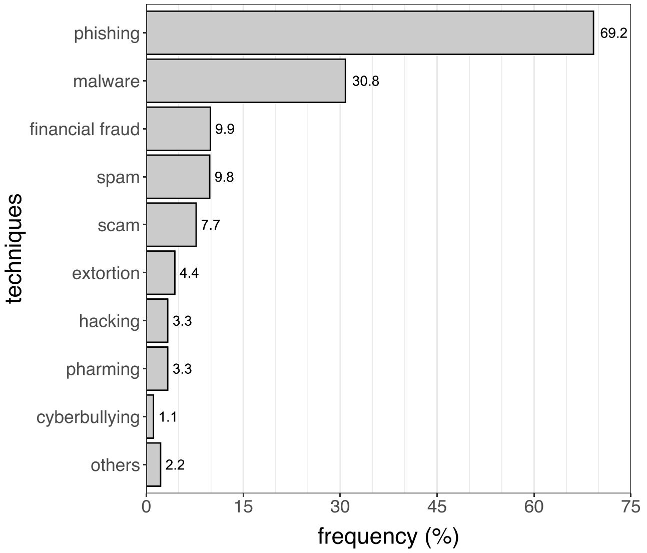

FIGURE 2 Frequency of the different techniques used for cyber-attacks occurred during COVID-19, over the total number of attacks. The sum of the frequencies exceeds 100% since some attacks used multiple techniques. Phishing includes all its subcategories: smishing, vishing and spear-phishing

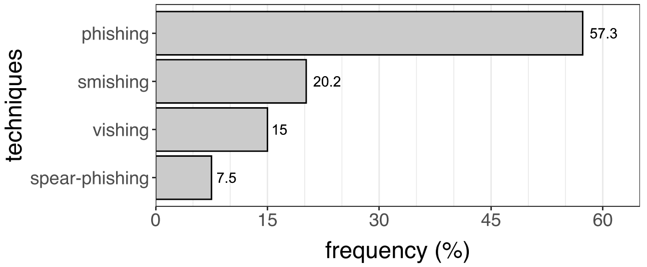

FIGURE 3 Relative frequency of the prevalent subcategories of phishing attacks occurred during COVID-19

3.1.2 | Vulnerability to phishing

The main vulnerabilities to covid-related phishing attacks derive from the changes induced by the COVID-19 pandemic. The scoping review presented in [10] identifies 5 main changes that are responsible for increased vulnerability to phishing and other cyber-attacks, during COVID-19. The first of such changes is represented by the decreased mobility and by the national border closures, which demanded increased reliance on remote work [9, 15, 20]. The shift to remote work often occurred abruptly, with little planning, and involved employees with limited previous experience or training [8, 21–23]. These conditions represented the second cause of increased vulnerability to phishing attacks. A third change is related to the necessary use of digital communication systems for personal interactions. This exposed both workers and users of given services to a variety of attacks [24].

The three previous causes of increased vulnerability affect nearly every sector of our society. However, some sectors – such as healthcare and governmental services – were affected even more because of their peculiar conditions and critical role in the pandemic. In these sectors, additional vulnerabilities arose. In particular, the healthcare sector significantly lags behind other industrial sectors in terms of cybersecurity and digital literacy [25, 26]. This made attacks against these targets more valuable and, consequently, more frequent. Finally, the increased demand for certain goods – above all, personal protective equipment – made healthcare and governmental services increasingly exposed to scams [9]. Typical phishing attacks of this kind involved luring emails purportedly selling goods in high demand, with the goal of tricking victims into disclosing sensitive information.

Other causes for the increased vulnerability to phishing attacks during COVID-19 are related to the extreme levels of stress, anxiety and uncertainty experienced during the peaks of the pandemic [7, 8]. While these conditions were experienced by everyone in covid-stricken countries, workers in the healthcare and governmental sectors suffered them even more. Finally, several studies highlighted that fraudsters systematically created ad-hoc phishing messages that echoed official announcements by governmental organisations, in order to boost

[4] https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

their credibility and their chances of success [7, 27]. In many cases, the delay between an official announcement and the attack exploiting such announcement was remarkably short – for example, in the region of a couple of days – which contributed to lure more victims and to reduce their capacity to detect the scam.

3.1.3 | Notable phishing attacks

The majority of notable phishing attacks occurred during COVID-19 revolved around impersonating government organisations, the WHO, the US Centre for disease Control and Prevention (CDC), the UK NHS, airlines, supermarkets and communication platforms [7]. Table 2 reports a list of some of the noteworthy attacks detected and documented in both scientific and grey literature, also describing their main characteristics, including the target, vector (e.g., website, email, SMS), goal and date of each phishing attack.

Among the attacks that have been thoroughly studied, is one where attackers impersonated the WHO. The attack vector was a WHO-branded email containing useful and legitimate guidance on how to protect from, and curb the spread of, the COVID-19 infection. Notably, the text of the email contained some grammatical errors and misspellings, and also made use of propaganda techniques [28] appealing to the reader's emotions

TABLE 2 Noteworthy phishing attacks detected and described in literature in the first months of the pandemic. Attacks are listed in reverse chronological order, whenever the date of the attack is available

Reference	Country	Target	Goal	Vector	Date
Xia et al. [34]	USA, Netherlands	Citizens	Credential theft	Website	17/04/2020
Xia et al. [34]	Malaysia	ATB, bell, Canadian Government	Malware, espionage	Website	14/04/2020
O'Donell [35]	World	Citizens	Credential theft	Email	31/03/2020
Rodger [36]	UK	Citizens	Credential theft	SMS	24/03/2020
Lallie et al. [7]	USA	Citizens	Malware	SMS	24/03/2020
Lallie et al. [7]	World	Citizens	Extortion	Email	20/03/2020
Pilkey [37]	Spain	Citizens	Malware	Email	10/03/2020
Pilkey [37]	USA	Citizens	Malware	Email	08/03/2020
Pilkey [37]	Italy	Citizens	Malware	Email	02/03/2020
Lallie et al. [7]	China	Citizens	Ransomware	Email	09/02/2020
Patranobis [38]	India	Chinese medical institutes	Credential theft	Email	06/02/2020
Pilkey [37]	Vietnam	Citizens	Malware	Email	03/02/2020
Lallie et al. [7]	China	Citizens	Credential theft	Email	02/02/2020
Vergelis [39]	USA	Citizens	Credential theft	Email	31/01/2020
Lallie et al. [7]	China	Citizens	Malware	Email	29/01/2020
Walter [40]	Japan	Citizens	Malware	Email	28/01/2020
Pilkey [37]	Phillipines	Citizens	Malware	Email	23/01/2020
Doffman [41]	China	Mongolian Ministry of foreign Affairs	Malware	Email	20/01/2020
Henderson et al. [42]	Vietnam	Chinese Government	Espionage	Email	06/01/2020
Del Rosso [43]	Libya	Citizens	Malware, data theft	Email	–
Greig [44]	World	Global shipping firms	Malware, espionage	Email	–
Lallie et al. [7]	World	Canadian businesses, citizens	Malware	Email	–
Lallie et al. [7]	Spain	Spanish medical institutes	Ransomware	Email	–
Lallie et al. [7]	UK	Citizens	Malware	SMS	–
Lallie et al. [7]	Spain	Citizens	Credential theft	SMS	–
Smithers [45]	UK	Citizens	Credential theft	Email, website	–
Vergelis [39]	Singapore	Citizens	Credential theft	Email	–
Xia et al. [34]	USA, Japan, Singapore	BOA, paypal, Apple, Chase	–	Website	–
Xia et al. [34]	Russia	Banco de Chile	–	Website	–

by emphasising the value of human lives [29]. In addition to the useful recommendations, the email also carried an attached ZIP file, purportedly containing an e-book about 'the complete research/origin of the coronavirus and the recommended guide to follow to protect yourselves and others'. Upon execution of the file contained in the archive, the GuLoader malware downloaded FormBook, a popular trojan used to collect data from the Windows clipboard, to keylog, and to steal Web browser data. Stolen data was sent back to a C&C server operated by the attackers [30]. Notably, the tactic of alternating legitimate and malicious information during an attack, in order to increase its credibility, is well-known and also used in other online scams, such as in the activity of social bots spreading untrustworthy information (e.g., fake news) [31]. Similar techniques were used in other attacks aimed at downloading malware on the victim's system. These attacks were based on a fake NHS website [32] and on a malicious website imitating the Johns Hopkins University COVID-19 dashboard [33], a Web resource that was widely used during the course of the pandemic. The WHO was also targeted by another attack. This time, it was reported that a group of hackers created a malicious website posing as an email login portal for WHO employees, in an attempt to steal their passwords. The attempt was declared to be largely unsuccessful by the WHO itself [10]. Nonetheless, the increased phishing attacks targeting the WHO and its partners led the WHO to issue a warning to the general public to raise awareness on these threats.[5] The warning page featured a dedicated section for phishing attacks.

In the US, another attack was based on emails impersonating the CDC and asking for donations to develop a COVID-19 vaccine. Donations were expected to be made in Bitcoins. In addition to the typical techniques used to convince victims, the attackers also asked recipients to share the message as much as possible, thus aiming to exploit the increased perceived trustworthiness of messages vetted by close ones [7, 46]. Finally, also communication platforms such as Zoom, Microsoft Teams and Google Meet, were impersonated in emails and through fake websites. The latter led to a surge of Web domain registrations, a significant share of which was later labelled as outright malicious or suspicious [47].

3.1.4 | The surge of covid-related domain registrations

The registration of covid-related domains was a prominent phenomenon that held the stage during the first months of the pandemic. This phenomenon is not new nor peculiar to COVID-19. In fact, it is widely recognized that malicious campaigns, including phishing, benefit from the prompt exploitation of salient events [48]. In the case of COVID-19 the surge in domain registrations was so significant and abrupt to motivate targeted scientific studies and even investigations by law enforcement agencies [49, 50]. Among these, a statistical report from Palo Alto researchers published at the end of March 2020 showed that a total of 116,357 new domain titles and registrations related to COVID-19 were made since the start of the year. Their results showed that 2% of such domains were clearly malicious and 34% were considered to be high-risk [6]. A subsequent analysis by the security firm Check Point reached similar results in May 2020, with 17% of the analysed domains deemed malicious or suspicious [47]. An investigation by the INTERPOL puts the rise of malicious domain registrations into context. The INTERPOL measured, from February to March 2020, a 569% growth in malicious registrations, including malware and phishing, and a 788% growth in high-risk registrations.[6] The rationale for exploiting covid-related domains in phishing attacks is straightforward. In fact, as identified in [7, 10], domains using keywords such as 'covid', 'coronavirus' and 'corona' are likely to appear as believable, and thus massively accessed. To boost accesses, fraudsters also included other reputable words such as WHO and CDC, or used appealing keywords such as 'corona-virusapps.com', 'anticovid19-pharmacy.com', and more.

The remaining share of domains that was not involved in phishing attacks or in other scams was related to non-malicious yet nonetheless shady and lucrative practices. The study discussed in [49] investigated the rationales for such covid-related domain registrations. Authors concluded that such domains were registered mainly for two reasons: (i) for attracting and then redirecting traffic to other, often totally unrelated, commercial services; or (ii) for domain parking – that is, the practice of registering a high-demand domain in advance, thus netting profits when reselling the domain later on, once the demand curve is at its peak.

3.1.5 | Consequences and economic impact

The majority of assessments about the consequences of phishing attacks derive from governmental bodies and security firms, with only a small minority of scientific studies covering this area. Independently of the source, all reports testify a sharp increase in costs and losses due to cyber-crime since the start of the COVID-19 pandemic. Overall, companies spent $110B worldwide for protecting against cyber-attacks in 2020, according to Accenture's annual security report [1]. A survey by BAE Systems highlighted the main factors that contributed to cyber-crime losses registered during the pandemic [51]. The main losses derived from: (i) IT overtime for incident response, remediation and clean-up; (ii) payments for ransomware attacks; (iii) operational outages; (iv) legal costs following a major attack (e.g., in cases of class action lawsuits); and (v) customer churn, with its associated financial costs.

Investigations from the US Federal Bureau of Investigation (FBI) contribute to quantify the overall losses and to estimate the trend with respect to pre-pandemic conditions. For instance,

[5] https://www.who.int/about/cyber-security

[6] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

the FBI estimated that spear phishing cost US businesses more than 1.8$B in 2020, up from 1.7$B in 2019. In a notorious case, a US business specialising in hand sanitizers wired nearly 1$M to hackers pretending to sell ventilators. Conversely, losses associated to generic phishing attacks decreased slightly, with 54$M in losses in 2020, down from 57$M in 2019.[7] This trend testifies the increased personalisation and sophistication of recent attacks, which in turn, mandates more advanced detection techniques to keep up with the rapid pace of the attackers.

According to the FBI, ransomware attacks were also a major source of losses, as already highlighted in the BAE Systems survey [51]. The average ransomware payment reported in Q4 2020 was in the region of 154,000$. Oftentimes however, more severe losses derived from downtime and customer churn rather than from the direct ransomware payment. In a notable case involving a large US healthcare provider, losses due to losing customers to rival providers during a ransomware attack summed up to 67$M. Moreover, while extortion and high ransomware demands were previously reserved for big-budget enterprises, such attacks also hit the small and medium business sector during the pandemic. The average ransomware payment demand for SMBs in 2020 was 5600$, while the costs of the incurred downtime reached 247,000$, which represents a 94% increase with respect to 2019. Then according to IC3, the overall cost of ransomware in the US tripled in 2020, with 29.1$M in losses compared to just 8.9$M in 2019. Notably, the FBI found that phishing emails were the primary cause of ransomware attacks, underlining the importance of defending against phishing for reducing the efficacy of many of cyber-attacks.

Among the few scientific studies that reported results on the economic consequences of phishing attacks, is the work in [7]. The analysis focussed on UK firms and revealed that by early May 2020, more than 160,000 suspect emails had been reported to the UK National Cyber Security Centre (NCSC). By the end of May, 4.6£M had been lost to COVID-19 related scams with around 11,206 victims of phishing campaigns. In response, the NCSC took down 471 fake online shops and Her Majesty's Revenue and Customs (HMRC) took down 292 fake websites [7].

3.2 | Detailed literature review

While the previous section highlighted the rise and the main characteristics of covid-related phishing attacks, this section summarises and presents the results of each study that investigated such attacks.

3.2.1 | Early and introductory works

Out of all the research published on cyber-attacks and COVID-19 – and specifically phishing attacks – the vast majority of existing studies focussed on providing descriptions and characterisations of the types of attacks. This large stream of research is characterised by relatively general, descriptive and high-level analyses, rather than by technical and detailed discussions. These contributions were among the first to be made in the aftermath of the pandemic, and served as initial assessments of such an unprecedented situation. Their utility was in raising awareness on the increased cybersecurity issues and in guiding subsequent, more technical and specific, research. An example of this kind is the work presented in [52], where the authors made a first step towards fully characterising the landscape of COVID-19 themed attacks. In detail, they considered five classes of attacks – namely, malicious websites, malicious emails, malicious mobile apps, malicious messaging, and misinformation. Then, they proposed mapping them to the Lockheed Martin's Cyber Kill Chain (LMCKC) [53], which is a model consisting of 7 stages: (i) reconnaissance, which corresponds to pre-attack planning; (ii) weaponization, which corresponds to setting up attack propagation mediums; (iii) delivery, which corresponds to the attackers penetration into a victim's system; (iv) exploitation, which corresponds to the wage of actual attacks; (v) installation, which corresponds to installation of malicious payloads; (vi) command-and-control, which corresponds to attacker's use of remote access to victims' systems; and (vii) objectives, which corresponds to the accomplishment of the attacker's pre-determined goal. Finally, they discussed the defence space, with recommendations on how to defend from malicious websites, malicious emails, malicious mobile apps, malicious messaging, and malicious misinformation. Similarly, the work presented in [54] provided a detailed review about the COVID-19 cybersecurity attacks with a critical analysis. The paper also showed the latest research contributions of cybersecurity during COVID-19, in the form of a literature review corroborated by examples of how Google and Microsoft managed their privacy and cybersecurity, as well as the deriving limitations. Then, the authors discussed the reasons why people are vulnerable to cyber-attacks, especially with the increase in online activities brought upon by the pandemic, and proposed unique solutions to those problems. The goal of the study reported in [55] was to examine the shift from physical- to cyber-crime at the onset of the COVID-19 pandemic. Thus, this work aimed to shed more light on how crime initially moved to cyberspace and what were the implications for organisations and individuals. The author's hypothesis is that there was a shift from physical to cyber-crime as a result of the mass quarantine around the world at the beginning of the pandemic. The author used data from news articles, government reports, private sector publications, FBI data, and press releases. The results showed that the United States Secret Service Cyber-Fraud Task Force actually registered an increase in frauds, and that according to the FBI, cyber-crime increased by 300% since the start of the pandemic. The analysis reported in [56] identified the top-ten cybersecurity threats that took place during the pandemic. Phishing emerged as one of the top threats, linked to many frequent attack vectors such as malicious domain attacks, malicious websites, malicious emails, malicious social media

[7] https://www.vadesecure.com/en/blog/cybercrime-statistics-top-threats-and-costliest-scams-of-2020

messaging, business email compromise and malicious mobile apps.

Instead, in [57] the authors discussed the types of phishing attacks and their impact during the COVID-19 lockdown. Specifically, they discussed different types and sub-types of attacks, such as deceptive phishing, whaling, spear-phishing, and pharming, also proposing some general recommendations for thwarting them. Similarly, the analysis presented in [58] discussed the security risks associated with working from home due to the COVID-19 pandemic and the imposed lockdown. It discussed the increase in cyber-attacks due to the pandemic and provided a number of general recommendations, including those directed to businesses for backing-up their data in case of a ransomware attack, recommendations for secure remote networks for employees working from home, encouraging employees to communicate with the IT department regarding any concerns, periodic penetration testing, and educating employees. The paper also discussed the challenges related to dealing with an attack. The author of [9] discussed how the pandemic-driven disappearance of home-work boundaries expanded the cyber-attack surface area. The study also gave recommendations for employers to encourage employees in using strong encryption on their home routers, strong passwords on personal accounts, and in being extremely vigilant with respect to their personal information. In addition to [9, 58], some other works also focussed on the security challenges introduced by the shift to remote working. Among these, [59] discussed how the sudden change to remote work impacted the security of many organisations. The author described how the pandemic left many organisations with no time nor resources to instal extra security measures on work-issued devices. The study recommended organisations to utilise multi-factor authentication instead of just passwords, and to rely on end-to-end encryption and virtual private networks (VPNs) for handling company data. Also the discussion in [60] outlined the many challenges and security concerns caused by the pandemic, and specifically, by the shift to remote working. The author discussed the increase in phishing scams that are preying on COVID-19 fears and panics, and how cyber-crime cost the world 6$ trillion annually by 2021. Similarly to the many other papers surveyed in this section, also this article ends with some general recommendations, including the use of multi-factor authentication, the use of a VPN with an encrypted network connection, updating the cybersecurity policies, and communication between employees and their IT department. The work in [61] discussed the cybersecurity issues that have occurred during the COVID-19 pandemic. The authors emphasised that there was a correlation between the pandemic and the increase in cyber-attacks. Furthermore, they also highlighted that healthcare organisations were one of the main victims of cyber-attacks during the pandemic. The pandemic has also raised the issue of cybersecurity in relation to: (i) the ‘new normal’ of expecting staff to work from home, (ii) the possibility of state-sponsored attacks, and (iii) increases in phishing and ransomware. According to the authors, mitigation techniques for these issues include raising user awareness, utilising VPNs and multi-factor authentication, ensuring firmware and antiviruses are updated, and a strong cybersecurity policy. Authors of [62] presented a discussion on the vulnerabilities caused by the pandemic and on the many types of cyber-attacks experienced worldwide. The ultimate goal of their analysis was to raise awareness on these issues, and on cybersecurity in general, as a mandatory defensive step in order to reduce the number and impact of the cyber-attacks that occurred as a consequence of the COVID-19 pandemic. The purpose of [63] was to raise awareness on the exploitation of the pandemic as a cyber-attack tool and to discuss possible remediation strategies. The research was conducted through a review of existing literature from websites and reputable databases, including Google Scholar and IEEE Xplore. The themes from the literature sources included the prevalence of phishing, scamming, spamming, and malware as the common attack vectors. Business enterprises, including operators in healthcare, finance, and Internet service provision, were advised to actively implement risk management plans to monitor attack vectors and to secure their systems, clients, and users from the COVID-19 attack tools.

Still within the large body of initial research on phishing attacks and COVID-19, other papers investigated a number of more specific issues. For example, the work in [20] focussed on challenges of the heathcare sector, by outlining why cyber-attacks have been particularly problematic during COVID-19 and by defining the ways in which healthcare industries could better protect patients' data. The paper discussed how the number of cyber-attacks increased five-fold after COVID-19, and that 90% of healthcare providers had already encountered data breaches. Among the proposed mitigation recommendations were penetration testing, well-defined software upgrade procedures, and the utilization of secure networks like virtual local area networks. Other scholars focussed instead on analysing and describing national experiences. Among them, [64] examined the extent to which organisations in the UK and their staff were likely to have been prepared for the unplanned outbreak of home working, along with the increased cyber-threats that they had to face. The preparedness of businesses was evaluated along the following directions: secure configuration, malware protection, network security, managing user privileges, incident management, monitoring, information risk management regime, user education and awareness, home and mobile working, and removable media controls. The results showed that the businesses that were undertaking actions in each of these steps were as follows: 90% for secure configuration, 88% for malware protection, 83% for network security, 80% for managing user privileges, 68% for incident management, 57% for monitoring, 35% for information risk management regime, 30% for user education and awareness, 25% for home and mobile working, and 23% for removable media controls. Results of this analysis were useful for promptly identifying those security directions requiring additional efforts. Instead, the author of [65] discussed how Croatia dealt with the pandemic-related cybersecurity concerns. The analysis revealed that Croatia has stayed completely silent with regards to cybersecurity hazards, and it has left companies to figure out their own ways of reacting to the increased cyber-threats, without even warning individuals. The analysis then moved on to discuss the cybersecurity threats associated with remote working, the Croatian cybersecurity legal regulation, Croatia's (lack of) response to the increased cybersecurity threats, and liability for personal data breaches arising from cybersecurity attacks. The author concluded by making some recommendations such as cybersecurity auditing, use of multi-factor authentication, and use of VPN solutions for connecting to the workplace. In [66], the authors conducted a study by identifying cyber-incidents in Indonesia that exploited COVID-19. The analysis made use of a timeline that mapped key events and cyber-attacks to analyse targeted sectors and their cybersecurity issues. The study illustrated how cyber-criminals artfully exploited pandemic issues and situations as baits for social engineering techniques. In the analysed cyber-incidents, criminals using social engineering techniques took advantage of the issue of COVID-19 by not having a specific target so that anyone could become a victim of their attacks. Finally, differently from all works described above, the analysis presented in [67] focussed on the skills needed by the cyber-security workforce in relation to the novel situation caused by the pandemic. Specifically, the authors argued that the cyber-security workforce, which was already suffering a digital skills crisis, also lacked the adequate soft skills required to effectively tackle the insider threat that was exacerbated by the pandemic. The work first examined the insider threat, and why it became so much more insidious because of COVID-19. Then, it looked into the essential soft skills required to tackle this threat, before examining how organisations could effectively implement an apprenticeship strategy capable of generating professionals with both hard and soft skills. The authors concluded that many of the covid-related issues could have been avoided if the industry had not relied so heavily on recruiting graduates rather than apprentices – that is, people trained directly in cybersecurity by the company itself.

3.2.2 | Systematic analyses

Following the first wave of introductory research, some scholars carried out systematic and large-scale analyses of some of the attacks that occurred during the first months of the pandemic. For instance, in [68] the authors carried out a comprehensive measurement study of online social engineering attacks, with specific references to phishing. By collecting, synthesising, and analysing DNS records, Transport Layer Security (TLS) certificates, phishing URLs, phishing website source code, phishing emails, web traffic to phishing websites, news articles, and government announcements, they tracked trends of phishing activity between January and May 2020 and sought to understand the key implications of the underlying trends. They found that phishing attack traffic in March and April 2020 skyrocketed up to 220% of its pre-COVID-19 rate, far exceeding typical seasonal spikes. The results also showed that there was a record high of phishing victims during this period, and that attackers remained several steps ahead of typical modern anti-phishing defenses. Findings from this analyses could be used to develop more effective phishing detection techniques. Then, the study in [27] developed a multi-level influence model to explore how cyber-criminals exploited the COVID-19 pandemic by assessing situational factors, identifying victims, impersonating trusted sources, electing attack methods, and employing social engineering techniques. Content and thematic analysis was conducted on 185 distinct COVID-19 cyber-crime scam incident documents, including text, images and photos provided by FraudWatch, a global online fraud and cybersecurity company tracking worldwide COVID-19 related cyber-crime. The analysis revealed interesting patterns about the sheer breadth and diversity of COVID-19 related cyber-crime incidents and how these crimes were continually evolving in response to changing situational factors related to the pandemic. Similarly, the aim of [69] was that of contributing to users' protection by exploring online perpetrators' modus operandi applied to exploit Internet users' coronavirus fears through phishing emails. To that end, the content of 208 coronavirus-themed phishing emails was examined. The data was collected by searching for variations of the terms ‘COVID-19 phishing emails’ from search engines, and then using the images from official websites such as the Action Fraud, FBI, or web pages of universities or companies' IT departments. 2372 images were collected in this way. The results showed that phishers mostly employed social engineering methods to coerce individuals into providing sensitive information. The authors also identified 9 main variations of phishing emails. While the previous work focussed on phishing emails, the authors of [70] presented a systematic study of coronavirus-themed Android malware. First, they made a daily growing COVID-19 themed mobile app dataset, which contains 4322 COVID-19 themed apk samples (2500 unique apps) and 611 potential malware samples (370 unique malicious apps) by the time of mid-November, 2020. The authors then presented an analysis of them from multiple perspectives including trends and statistics, installation methods, malicious behaviours and malicious actors behind them. The authors observed that the COVID-19 themed apps as well as malicious ones began to flourish almost as soon as the pandemic broke out worldwide. Most malicious apps were camouflaged as benign apps using the same app identifiers (e.g., app name, package name and app icon). Their main purposes were either stealing users' private information or making profit by using tricks like phishing and extortion. Notably, several of the characteristics identified in this study are currently exploited as part of many detection techniques for protecting against phishing attacks mounted by means of malicious apps [52]. Moving on with relevant systematic analyses, in [71] the authors presented the first measurement study of COVID-19 themed cryptocurrency scams. They first created a comprehensive taxonomy of COVID-19 scams by manually analysing the existing scams reported by users from online resources. Then, they proposed a hybrid approach to perform the investigation by (i) collecting reported scams in the wild, and by (ii) detecting undisclosed ones based on information collected from suspicious entities (e.g., domains, tweets, etc.). 195 confirmed COVID-19 cryptocurrency scams in total were collected, including many well-known cryptocurrency scams [72], such as: 91 token scams, 19 giveaway scams, 9 blackmail scams, 14 crypto malware scams, 9 Ponzi scheme scams, and 53 donation scams. Over 200 blockchain addresses associated with these scams were then identified, which led to at least 330 $K in losses from 6329 victims. For each type of scams, the tricks and social engineering techniques they used were further investigated. To facilitate future research, the authors released all the well-labelled scams to the research community.[8] The data for COVID-19 scams were obtained from BitcoinAbuse, CryptoScamDB, Threat Intelligence Platforms (e.g. AlienVault, McAfee), and StopScamFraud. The authors also obtained data about COVID-19 themed cryptocurrency scams using a semi-automated analysis on Etherscan to search for scam tokens, URLScan, RiskIQ, VirusTotal to search for scam domains, Koodous, VirusTotal, AVClass to find Android apps and label the app malware families, and Twitter and Telegram to identify more scams. Given the surge of covid-related malicious domain registrations, the authors of [34] focussed on identifying and characterising COVID-themed malicious domain campaigns, including the evolution of such campaigns, their underlying infrastructures and the different strategies taken by attackers behind these campaigns. Their exploration uncovered some common features of malicious domains, which can help to identify new malicious domains and to raise alarms at the early stage of their deployment. The results also showed peaks in malicious domain registrations in March 2020, indicating bulk registrations that accounted for 73.2% of all malicious domains. The first registered domain was ‘clientdoc.us’, which hosted multiple COVID-19 related phishing subdomains like ‘banking.covid19.hsbc.clientdocs.us’ and ‘covid19update.hsbc.clientdocs.us’. The authors also identified 15 verified attack campaigns that were used for phishing, malware, and domain squatting. Finally, similarly to the previous study, also [49] performed an analysis at Internet-scale of COVID-19 domain name registrations during the early stages of the virus' spread. The authors leveraged the DomainTools COVID-19 Threat List and additional measurements to analyse over 150,000 domains registered between 1 January 2020 and 1 May 2020. They identified two key rationales for covid-related domain registrations: (i) online marketing, by either redirecting traffic or hosting a commercial service on the domain; and (ii) domain parking, by registering domains containing popular COVID-19 keywords, presumably anticipating a profit when reselling the domain later on.

3.2.3 | Studies based on questionnaires, surveys and interviews

Another remarkable body of work about phishing and other cyber-attacks in relation to COVID-19 relied on the use of questionnaires, surveys and interviews as tools for assessing the perception, readiness and effect of such attacks on those that experienced them. As part of this literature, the idea of the study presented in [73] was to examine how teleworking affected employee perceptions of organizational efficiency and cybersecurity, before and during the COVID-19 pandemic. The research was based on an analytical and empirical approach. The quantitative approach involved the design of a structural equation model, one of the most widely-used approaches to causal inference [74], on a sample of 1101 respondents from the category of employees in Montenegro. Within the model, the authors examined simultaneously the impact of the employees' perceptions on the risks of teleworking, changes in cyber-attacks during teleworking, organisations' capacity to respond to cyber-attacks, key challenges in achieving an adequate response, as well as the perceptions of key challenges related to cybersecurity. Perhaps surprisingly, the main findings of the research were that teleworking had no impact on digital information security, and that teleworking had a positive and significant impact on organizational efficiency perceptions. Similar conclusions were reached in [24], where authors discussed how the pandemic impacted the IT industry in terms of the IT security implications, the impact on global IT, and the increase in COVID-19 phishing attacks and malware. The authors used a survey to demonstrate how the industry was able, for the most part, to cope with and address the challenges brought by the COVID-19 crisis. With similar techniques, the analysis carried out in [75] evaluated the cybersecurity culture readiness of organisations from different countries and business domains, when teleworking became a necessity due to the COVID-19 crisis. The authors designed a targeted questionnaire and conducted a web-based survey addressing employees while working from home during the COVID-19 spread over the globe. The questionnaire contained 23 questions and was available for almost a month, between April and May 2020. During that period, 264 participants from 13 European countries spent approximately 8 min to answer it. Gathered data were analysed from different perspectives, allowing to find answers regarding the information security readiness and the resilience of both individuals and organisations. Some of the results of the research showed that 53% of employees reported to not having received any cybersecurity guidance with regards to working from home, 44.44% had no possibility of working from home, and about 15% reported having faced some kind of cyber-threat. Still related to perceptions, the research in [76] examined the relationship between teleworking cybersecurity protocols during the COVID-19 era and employee perception of their efficiency and performance predictability. The premise of this research project was that teleworking could transform employees into unintentional insider threats. Interviews were conducted through video conferencing with nine employees in Virginia, USA to examine the problem and collect data. The data from the interviews was then analysed using narrative analysis to unpack some of the common themes from the interviews [77]. The major findings demonstrated that employees were trusting the cybersecurity protocols that their organisations implemented, but that they also believed

[8] https://covid19scam.github.io/

they were vulnerable, and that the protocols were not as reliable as in-person working arrangements. While the respondents perceived that the cybersecurity protocols lend to performance predictability, they also appeared to think it disrupted their efficiency.

Other studies focussed instead on the effects of cyberattacks and of the specific techniques used to carry them out. The experiment described in [78] examined the effects of persuasive appeals in phishing messages on judgements of credibility. Participants were tasked with reading a combination of legitimate and phishing e-mails to determine whether each message was legitimate or a scam. When phishing messages included more appeals to authority and likability, phishing susceptibility increased. However, as the number of fear and urgency appeals in the message increased, phishing susceptibility decreased, as it was easier for participants to detect the phishing attempt. Interestingly, results showed that appeals to authority and likability increased credibility, while appeals to fear, urgency, and social proof decreased judgements of credibility. Moving on, in [79], the authors investigated how the pandemic affected rates of cyber-victimization. The study considered the pandemic as a natural experiment, thus allowing the comparison between pre-pandemic rates of victimization and post-pandemic ones, leveraging datasets originally designed to track cyber-crime. In particular, the authors built two samples that they used to conduct a survey: (i) one related to the pre-COVID-19 situation consisting of 1109 participants, and (ii) another one for the post-COVID-19 situation counting 1021 participants. After considering how the pandemic may have altered routines and affected cyber-victimization, the study found that the pandemic did not radically alter cyber-routines nor changed cyber-victimization rates.

The last study that we reviewed in relation to attacks made use of a simulation to evaluate the vulnerability of different groups of employees to phishing during COVID-19 [80]. In particular, the authors performed a comparative study of cybersecurity awareness of employees working in different departments within the same organisation in Bangkok, Thailand. In their experiment, they exposed different employees to simulated phishing attacks and evaluated their actions. After data collection and analysis, the authors found significant differences in the cybersecurity awareness levels between Thai employees from technology-based departments (e.g., IT department) and social-based departments (e.g., HR department) within the same organisation, with the latter group that showed to be more vulnerable to phishing attacks than the former one. Simulations such as the one described in [80] have recently been regarded as a promising tool for training staff in preparation for future cyber-attacks. For instance, in the context of healthcare professionals, [81] proposed to carry out cybersecurity campaigns in which members of the IT departments send out fake phishing emails to the rest of the staff and provide further training to those who fail to identify the phishing emails. However, in spite of the widespread awareness of cybersecurity limitations of the healthcare sector [25, 26] and of the advices, such as those of [81], given several months before the outbreak of COVID-19, few enterprises enacted significant changes, which worsened the impact of the massive wave of phishing attacks occurred in the aftermath of the pandemic.

4 | COUNTERMEASURES

While the previous section focussed on the drivers and the characteristics of phishing attacks occurred during the COVID-19 pandemic, this section discusses the proposed defenses and countermeasures to such attacks.

4.1 | Overview and synthesis

The multitude of ways in which phishing attacks were mounted demanded the development of a broad array of different solutions. Each solution surveyed and described here exploits some characteristics of COVID-19 phishing attacks, such as those that we discussed in Section 3. First, we summarise the main approaches adopted for detecting phishing attacks during COVID-19. Then, we focus on the key factors that influence the effectiveness of machine learning solutions, that is: data, methods (i.e., algorithms) and features. Hence, we highlight the available datasets for this task, as well as the methods and the features used for developing detectors. Table 3 supports and complements this discussion by presenting a detailed classification and comparison of the techniques that were recently proposed for detecting COVID-19 phishing attacks.

4.1.1 | Approaches

Among all solutions that were recently proposed to defend from phishing attacks, the vast majority was aimed at detecting phishing *websites*, as also shown in Table 3. This finding is perhaps unsurprising, considering that emails and websites were the most frequent attack vectors exploited during the COVID-19 pandemic [1]. The most straightforward way to tackle the task of detecting COVID-19 phishing websites is by analysing website contents. Approaches of this kind typically revolve around assessing the presence or absence of covid-specific keywords in website names and contents (e.g., coronavirus, COVID-19, masks, n95, and more) [52]. Another frequent approach to the detection of phishing websites is based on the analysis of the website's URL. To this end, it was observed that attackers frequently used cybersquatting and typosquatting techniques, or techniques to obtain homograph domain names, to make COVID-19 themed malicious websites mimic legitimate ones [94], which highlights the importance and usefulness of detecting such modified URLs. Other approaches focus instead on the website's age, since malicious websites tend to be more recent than authoritative ones [91]. The works in Table 3 that target phishing websites represent notable examples of the combination of the aforementioned approaches.

TABLE 3 Detailed classification and comparison of some recently proposed techniques for detecting COVID-19 phishing, smishing and vishing attacks

Reference	Year	Focus	Dataset	Target	Method[a]	Features	Evaluation[b]
Mishra & Soni [82]	2021	Smishing	[83] + pinterest[c]	SMSs	Deep learning, RF, NB, DT	SMS text	Test accuracy = 0.98
Biswal [84]	2021	Vishing	[85]	Calls	SVM, LR, MP	Call transcript text	Test accuracy = 0.65
Wu & Guo [86]	2021	Phishing	Own (unreleased)	Emails	Document embeddings, anomaly detection	SMTP headers	Case-study and comparison against commercial solutions
Sarma *et al.* [87]	2021	Phishing	Mendeley[d]	Websites	kNN, RF, SVM, LR	URL, website content, website metadata	Test $F1$ = 0.98
Mukhopadhyay & prajwal [88]	2021	Phishing	Own (unreleased)	Emails, websites, malware	Blacklists, heuristics	IP, URL, email attachments	Case-study and comparison against commercial solutions
Ispahany & Islam [89]	2021	Phishing	DomainTools[e]	URLs	SVM, kNN, NB	URL	Test accuracy = 0.99
Xia *et al.* [34]	2021	Phishing	Own (unreleased)	Websites, URLs	Knowledge graphs, graph representation learning, graph clustering	IP, URL	Qualitative and case-study
Tawalbeh *et al.* [90]	2020	Phishing	Own (unreleased)	Malware	Deep learning	Email attachments	Training accuracy = 0.85
Saha *et al.* [91]	2020	Phishing	Kaggle[f]	Websites	MP	IP, URL, website metadata	Test accuracy = 0.93
Basit *et al.* [92]	2020	Phishing	UCI machine learning repository[g]	Websites	Ensemble of classifiers (RF, kNN, DT)	URL	Test accuracy = 0.97
Pritom *et al.* [93]	2020	Phishing	CheckPhish[b,h] DomainTools[e]	Websites	RF, kNN, DT, LR, SVM	URL, website metadata	Test accuracy = 0.98

[a] DT, decision tree; kNN, K-nearest neighbours; LR, logistic regression; MP, multilayer perceptron; NB, naïve Bayes; RF, random forest; SVM support vector machine.

[b] In case the reference paper reported multiple evaluation results, here we list only the best one.

[c] https://in.pinterest.com/seceduau/smishing-dataset.

[d] https://doi.org/10.1016/j.procs.2020.03.294.

[e] https://www.domaintools.com/resources/blog/free-covid-19-threat-list-domain-risk-assessments-for-coronavirus-threats.

[f] https://www.kaggle.com/akashkr/phishing-website-dataset.

[g] https://archive.ics.uci.edu/ml/datasets/phishing+websites.

[h] https://checkphish.ai/coronavirus-scams-tracker.

The second most-common approach for detecting phishing attacks grounds on the analysis of *emails*, another frequently used attack vector. Similarly to systems for detecting phishing websites, also many systems for phishing email detection are based on the analysis of email contents. For instance, covid-related keywords – such as those related to cures, guidelines, or offers – can be searched in subject lines and in the textual contents [52]. Instead, other techniques based on email content analysis focus on the links contained in the email, or on its attachments. The former systems typically analyse the URL of the links by means of the same techniques already described for the analysis of website's URLs. The latter are instead aimed at assessing the harmfulness of any file attached to the email, for instance by means of static and dynamic analyses of the file's content. Finally, another common approach to the detection of COVID-19 phishing emails is based on spotting email spoofing or masquerading attacks. Here, the analysis is aimed at verifying the identity of the sender, for example, by analysing the headers of the email [86].

COVID-19 themed *malicious apps* are another common vector for phishing attacks. A set of approaches for defending against this threat is based on computer vision techniques that assess the visual similarity of new app logos with those of legitimate existing apps [52]. Other techniques are instead based on static and/or dynamic analyses of the apps, in order to detect malicious ones (e.g., repackaged apps). A minority of approaches also aims at detecting spoofed app names, for example, by computing string edit distances between the names of new apps with respect to existing and popular ones.

Smishing and *vishing* attacks represent a minority of all phishing attacks occurred during the pandemic. As such, only few works specifically targeted these attacks, as also shown in Table 3. Textual analyses of the content of the messages—in the case of smishing, or of the call transcripts—in the case of vishing, is by far the most common approach for detecting these types of attacks. Such analyses can be carried out by the adoption of natural language processing techniques, for instance with the goal of spotting suspicious content, such as the presence of spoofed URLs, special characters, and COVID-19 themed keywords [52]. Other sophisticated approaches are also based on natural language processing, but this time the aim is that of detecting persuasive messages that make use of propaganda techniques [28] or other social engineering techniques [95]. These latter works lay at the intersection of cyberpsychology and natural language processing [96].

4.1.2 | Datasets

High quality and reference datasets represent an important resource to foster research and experimentation on novel scientific issues [97]. However, building such resources is notoriously challenging and time-demanding [98]. In the case of COVID-19 phishing attacks, publicly available reference datasets are few and far between. In addition to the aforementioned generic challenges, scholars interested in building a scientific dataset for covid-themed phishing attacks also had to account for the recency and unpredictability of the pandemic (and its associated scamdemic), and for its rapidly evolving nature. As a result, at the time of writing no reference dataset for COVID-19 phishing attacks exists and scholars tackling phishing detection either had to build their own dataset or to rely on existing, yet older, ones.

The only partial exceptions to the above consideration are the datasets released by DomainTools[9] and CheckPhish.[10] Both companies were extremely rapid to intervene against the deluge of malicious domains that plagued the Web during the first months of the pandemic. They curated and periodically updated lists of scam covid-themed websites and made such lists publicly available. As also shown in Table 3, datasets from DomainTools and CheckPhish were used by a subset of the papers that proposed website and URL COVID-19 phishing detection systems, such as [89, 93]. Unfortunately, as of now both the DomainTools and the CheckPhish datasets appear to be no longer publicly available. To partially ameliorate this issue, DomainTools suggested another publicly available dataset,[11] curated by the COVID-19 Cyber Threat Coalition. To the best of our knowledge, no scientific study has been conducted on such dataset.

The novelty of the issue and the lack of reference datasets forced many scholars interested in experimenting with COVID-19 phishing detection to build their own dataset. For instance, this route has been chosen for the development of the HOLMES [86] and EDITH [88] systems, and for the systems presented in [34, 90]. This approach has however several drawbacks. First, none of the datasets built in this way were made publicly available by the respective authors, thus hindering replicability and future research along this direction. Second, the datasets are related to very specific issues and have been collected with ad-hoc methodologies. As a practical example, the dataset used in [86] was obtained from the SMTP server of an unspecified firm. As a consequence of these limitations, datasets built ad-hoc for a specific study are often small, which raises concerns about the validity and generality of the results obtained from their analysis.

An orthogonal approach to building an ad-hoc dataset involves the use of well-known existing datasets. For instance, the datasets originally used in [83, 85] were also used to train and evaluate the systems recently proposed in [82, 84]. Similarly, other scholars used data published in well-known scientific repositories such as Mendeley, Kaggle and the UCI collection of machine learning datasets. However, also this solution presents an important drawback. In this case, some systems were designed with COVID-19 phishing attacks in mind, but the lack of specific reference datasets forced authors to evaluate their proposed system against other attacks. In many cases, the attacks contained in the used datasets occurred way before the start of the COVID-19 pandemic. Again, the concern is about the reliability of the results of such systems – some of which are remarkably good, as visible in Table 3 – that were designed and proposed for the COVID-19 scenario, but were evaluated otherwise.

4.1.3 | Methods and features

The previous section highlighted the limitations of current research with respect to the choice of datasets for training and evaluating detectors. Similar considerations also apply to the choice of machine learning algorithms and features. Indeed, the choice of a machine learning algorithm strongly depends on the characteristics of the available data [99]. To this regard, the most powerful and advanced analytical methods currently available are based on deep learning. Deep learning algorithms, however, require massive datasets for training, which are not yet available for the task of COVID-19 phishing detection. As such, and also due to the relatively limited time passed since the start of the pandemic, the vast majority of existing detectors are based on simpler, general-purpose and off-the-shelf classification algorithms. Table 3 shows that nearly all traditional classification algorithms were tested for the detection of COVID-19 phishing attacks. These include algorithms such as decision trees and random forests, logistic regression, k-nearest neighbours and support vector machines. Clearly, these represent the quickest and most straightforward way of tackling a classification task, such as that of phishing detection. Simplicity, scalability and mild data requirements however come at the cost of predictive power and generalisability. The adoption of more complex methods, such as those based on deep learning that were used in [82, 90], is still largely overlooked. A minority of systems are also based on ensembles of supervised classifiers—such as [92], or on unsupervised machine learning—such as [86].

The machine learning features used by the existing detectors are mainly based on the textual content of the item under investigation (e.g., a website, email, SMS, etc.). In fact,

[9] https://www.domaintools.com/resources/blog/free-covid-19-threat-list-domain-risk-assessments-for-coronavirus-threats

[10] https://checkphish.ai/coronavirus-scams-tracker

[11] https://www.cyberthreatcoalition.org/blocklist

the text has long been the most widely used data modality in many detection tasks [100]. In the context of phishing attacks, textual content can be found in emails, websites, OSNs, text messages (e.g., SMSs or any other message in instant messaging apps), call transcripts and app information. In addition, the analysis of URLs can also be considered as a form of text analysis. Because of the ubiquity of text, almost all COVID-19 phishing detection systems leverage textual features. The current state-of-the-art for extracting textual features is based on deep learning, and particularly, on artificial intelligence methods for natural language understanding [101]. However, the solutions exploited in the surveyed phishing detection systems are again largely based on more traditional and less powerful approaches. For example, bag-of-words features or simple sequences of characters and words (i.e., character and word *n*-grams) were used as text features in [84]. As such, the application of more recent and powerful text feature extraction techniques is still unexplored, with the exception of the HOLMES system that uses unsupervised word embeddings as text features [86]. The issue related to the use of simple and 'shallow' features also emerges when surveying systems that also leverage other data modalities. For example, many different features can be used for the detection of phishing websites, thus going beyond the mere analysis of the textual content of the website. Among such features are images, links, the HTML code and CSS documents of the website, JavaScript features, ActiveX Objects and forms [16]. However, the website classification systems reported in Table 3 almost exclusively rely on the analysis of the website's URL and on the assessment of the presence of certain covid-related keywords. Similarly, assessing the validity of URLs could involve querying DNS services and retrieving WHOIS and web traffic data [16], which is seldom done in the case of the analysed COVID-19 phishing detectors.

4.2 | Detailed literature review

The literature discussing countermeasures to phishing attacks is mainly organised in two large bodies of work. The first body of work proposes general and long-known recommendations, and discusses their application to the specific and novel situation caused by the COVID-19 pandemic. Part of the literature in this body of work overlaps, or is anyway similar, to the introductory works already discussed in Section 3.2.1. Instead, the second category of papers take an orthogonal approach to the problem of phishing attacks during COVID-19 and proposes ad-hoc technical solutions, the majority of which is based on machine learning, for automatically and promptly detecting such attacks.

4.2.1 | Works proposing general recommendations

Our analysis of the papers that provided actual recommendations to defend against phishing attacks reveals that the majority of works suggested a combination of the following three general strategies: (i) increasing user awareness of phishing attacks, which was suggested in [57, 61–63, 102]; (ii) resorting to multi-factor authentication, proposed in [57, 59–61, 65, 102]; and (iii) resorting to the use of VPNs, which was proposed in [59–61, 65, 102]. Among these works, the authors of [61, 102] provided all three aforementioned recommendations. In particular, [102] first conducted a survey to investigate the types of cyber-attacks that users suffered during COVID-19, as well as the level of knowledge and the technical challenges faced by users who switched to remote services during the pandemic. The survey highlighted phishing emails as the most common type of attack, corroborating previous findings [1, 7]. Part of the survey was also targeted at understanding victim behaviours when they were attacked. Surprisingly, as much as 62.5% of respondents admitted that they did not take any specific countermeasure because of a lack of awareness and understanding of the type of attack. Results such as those presented in this study motivate this body of research – namely, studies that analysed the initial situation of the pandemic and that rapidly intervened to provide simple, yet relatively effective, recommendations such as those listed above.

In addition to the previous 'horizontal' works that provided general recommendations, some scholars also carried out 'vertical' analyses by focussing on specific issues and relevant case-studies. As a notable example of this kind, [103] investigated the task of measuring cyber-resilience, a preliminary – yet mandatory – step towards the development of better countermeasures to cyber-attacks. The paper highlighted common misunderstandings in the definition and notion of cyber-resilience, which impair our capacity to measure it. They stressed the importance of considering systems' abilities to recover and to adapt, and not just to resist to cyber-attacks. The paper also proposed different methods for measuring cyber-resilience, taking into account cyber-security implementations as well as adversarial models. Still related to the analysis of cyber-resilience, [104] analysed how a global financial institution (GFI) dealt with the cybersecurity challenges posed by COVID-19. Authors conducted semi-structured in-depth interviews with 11 key actors from the GFI and leveraged Hollnagel's four abilities for resilient performance as a theoretical lens for their evaluation [105]. Among the main findings of the research was that the organisation performed well in terms of cyber-resilience, in the sense that the number and impact of cyber-incidents did not significantly increase after the COVID outbreak. The interviews also revealed that all four abilities of resilience were formally developed prior to the COVID-19 outbreak. The analysis however also showed that the favourable performance was obtained through many actions undertaken reactively rather than proactively, as it is instead advisable for a number of cybersecurity issues [106]. As such, [104] leaves open the question as to whether the four potentials should be developed beforehand, in order to perform resiliently during crises.

4.2.2 | Works proposing technical solutions

The general advices discussed in the previous section can be beneficial in reducing the frequency of successful phishing attacks [58]. This is the reason why so many researchers and practitioners rushed to make these recommendations in the first months of the COVID-19 pandemic. However, at the same time, none of these countermeasures is capable of completely solving the problem. For instance, studies that analysed advanced phishing attacks made via sophisticated phishing toolkits or via phishing-as-a-service, showed that such attacks are capable of evading two-factor authentication schemes [107]. The same result can also be achieved simply by mounting more elaborate social engineering attacks.[12] As such, the need for technical and intelligent systems for detecting such phishing attacks remains. In the remainder of this section we discuss relevant works that provided this kind of contribution.

As anticipated, the majority of technical countermeasures to phishing attacks is based on machine learning. As such, the main goal of the work discussed in [108] was to identify and propose ways in which machine learning techniques could be deployed for the detection of diverse types of cyber-crimes, such as phishing, identify theft, hacking, distributed denial of service, email bombing, and digital stalking. Authors discussed different types of machine learning-based implementations in cyber-crime mitigation, including the discussion of ways in which machine learning could contribute to phishing detection, with particular reference to the detection of phishing emails via analysis of the headers and body of the emails. The techniques proposed in [108] are effectively used in the following systems. In [86], the authors introduced a novel AI-based anomalous email detector – HOLMES – that can effectively tackle the challenge of anomalous email detection. HOLMES uses the email headers as input for the machine learning algorithm. Furthermore, it combines word embeddings with novelty detection to discover anomalous behaviours from a high volume of mirrored SMTP traffic in a large-scale enterprise environment. Its performance was measured in a limited number of case-studies, and its detection capability was compared with several well-known commercial detectors. The evaluation showed that HOLMES significantly outperformed those commercial products in all considered attack scenarios. During the development of the system, emphasis was also put with respect to its efficiency and capacity to run in environments characterised by a limited availability of computational resources. Also the EDITH system, proposed in [88], was designed to detect phishing emails. Specifically, EDITH (the Email Disintegration Intrusion-Detection of Trojan Hacktool) aims at identifying the embedded malware files and fake websites that are often present in phishing emails. EDITH takes emails exported from Thunderbird or Gmail and scans for URLs or attachments. It compares them to the VirusTotal database and applies a blacklist approach and heuristics to detect possible phishing and malicious emails. The peculiarity of this system is its capacity to simultaneously scan for phishing links and malware attachments. However, from the analytical perspective the system relies on rather simple methods (i.e., blacklists and heuristics). For the future it could thus be advisable to adopt a similar approach for the detection of phishing links and malware, but to consider the adoption of more powerful methods based on machine learning and AI. Similarly to [88], also the system proposed in [90] is designed to detect malicious emails. This time however, only the content of email attachments are analysed and, as such, the system is specifically focussed on detecting malware. Authors of [90] proposed to rely on deep learning for performing the detection. However, some important details of their methodology are undisclosed, including the type of deep learning architecture and the types of features used by their system.

Several systems were also developed to detect phishing websites. To this end, the analysis presented in [87] experimented with various machine learning classifiers, including k-nearest neighbors (kNN), random forest, support vector machines, and logistic regression. Authors relied on a public dataset available on Mendeley, comprising 5000 phishing websites and 5000 real websites, described by 48 machine learning features mostly based on website content and metadata. Results of the evaluation campaign in [87] showed that the random forest classifier achieved the best performance, with F1-score = 0.98. Comparable approaches were discussed in [92, 93]. In particular, [92] proposed an ensemble method to effectively detect website phishing attacks. The authors selected three well-known machine learning classifiers such as artificial neural network (ANN), kNN, and DT, to use in an ensemble method together with a random forest classifier (RF). The authors used a dataset from the UCI machine learning repository with 11,055 instances and 30 features. Similarly to [87], also in this case the dataset is almost balanced, with 4898 legitimate instances and 6157 phishing instances. The results show that the ensemble with kNN + RF achieved the best results, with accuracy = 0.97 and TP rate = 0.983, followed by the ANN + RF with TP rate = 0.981 and by the DT + RF with TP rate = 0.977. In [91] the authors proposed an ANN model that categorizes websites into either 1 of 3 categories: (i) phishing websites, (ii) suspicious websites, and (iii) legitimate websites. To perform the detection, the system leverages a publicly available Kaggle dataset comprising more than 10,000 instances of legitimate and phishing websites, described by features extracted from the IP address, the website's URL and its metadata. The ANN model used is the multilayer perceptron, a very simple kind of ANN architecture. As such, better results are foreseeable by the adoption of more sophisticated classification algorithms or ANN architectures. A somewhat simpler approach to the detection of phishing websites is the detection of phishing URLs. For this latter task, only the URL string of a website is considered, which inevitably leads to a much narrower array of possible features to leverage for the detection. Among the systems that tackled this task, is [89]. The authors proposed a classification approach that exploits

[12] https://www.agari.com/email-security-blog/phishing-attacks-two-factor-authentication/

only 5 features extracted from URLs. In addition to traditional and largely used features such as the length of the URL and features counting the number hyphens, [89] also used a feature computed as the Shannon entropy of the URL. Experimental results involved the use of support vector machines, kNN and naïve Bayes classifiers. The best classification results were achieved by kNN with accuracy = 0.99 on the test-set. Surprisingly, the authors measured no gain in detection performance when adding the entropy feature to the set of more traditional features – a finding that contrasted with earlier results [109, 110]. The reason for this result could however be due to the simplicity of the task tackled in [89], which could already be addressed with remarkable accuracy by only leveraging traditional URL features.

The work presented in [34] dealt with the proliferation of malicious domains campaigns. Differently from previous works that tackled the classification of *individual websites*, the goal of this work was the detection of *malicious campaigns*. Authors defined malicious domains campaigns as groups of related malicious websites. At first, they demonstrated the widespread presence of such campaigns, especially in the first months of the pandemic which were characterized by the surge of covid-related domain registrations. Then, they also proposed a detection strategy. The proposed solution is based on 3 steps: (i) the construction of a knowledge graph of domains, where related domains are linked together; (ii) the graph representation learning step, where an informative representation is computed for each node in the graph (i.e., each domain), in the form of a feature vector; and (iii) the graph clustering step, where similar domains are clustered together, based on their representation. In [34], the clustering step was used to group together the domains belonging to the same malicious campaign, thus effectively leading to discover and characterize malicious campaigns. Based on its characteristics, [34] represents one of the most advanced solutions to the detection of phishing (websites) in the context of COVID-19. First of all, it employs state-of-the-art methods, such as knowledge graphs, graph representation learning and graph clustering, instead of traditional classification algorithms. Then, it proposes a solution based on unsupervised machine learning, which was recently proven to be more resilient to the inevitable evolution of cyber-attacks [31, 111]. Finally, it focuses on the detection of groups of malicious websites, rather than individual websites, thus leveraging the inherent relationships between phishing websites and the additional information available in this way. Again, focusing on group analyses instead of the classification of individual entities is a promising direction of research in several areas of cybersecurity [31]. Among the other advantages of this work is the construction of large and detailed dataset, which however has not been publicly released to the scientific community.

To conclude our detailed analysis of proposed phishing countermeasures, we discuss systems for defending against smishing [82] and vishing [84] attacks. In detail, [82] proposed the DSmishSMS system, targeted at the detection of smishing SMSs. The system aimed to address some of the typical challenges related to the task of smishing detection, including the brevity of text messages which limits the number of available features, and the scarcity of labeled datasets to use for training a detector. To overcome these limitations, DSmishSMS only leveraged 5 features extracted from the text of the SMSs, including features aimed at encoding the authenticity of the URLs contained in the analyzed SMSs. The classification was obtained by leveraging an ANN trained with the back-propagation algorithm, which achieved accuracy = 0.98. Classifications from the ANN were also compared to those obtained with traditional algorithms, such as random forest, naïve Bayes and DT. The comparison showed that the ANN beat competitors by a tiny margin, at the expense of a slightly longer execution time. The RIVPAM system is instead aimed at the detection of vishing attacks [84]. Specifically, RIVPAM (Real-Time Vishing Prediction and Awareness Model) was designed to alert potential unwary vishing targets in real-time, during vishing attacks. The system uses a combination of natural language processing and machine learning to analyze conversations in real-time and is capable of issuing warning messages in case it detects a possible ongoing attack. The classification is performed by leveraging algorithms such as support vector machine, logistic regression and multilayer perceptron, which analyze some simple linguistic features (e.g., *n*-grams) extracted form the conversations. Vishing detection results achieved by RIVPAM are rather low, with the best reported accuracy = 0.65 on the test-set. Similarly to other surveyed systems that adopted shallow features and traditional classification algorithms, better results are foreseeable by the adoption of more advanced techniques for both the feature extraction and the classification steps.

5 | DISCUSSION: CHALLENGES AND FUTURE DIRECTIONS

Thoroughly investigating a problem represents the first step for reaching a satisfactory solution. This simple consideration and the relatively limited time passed since the start of the pandemic motivate and explain the first finding of our literature review. That is, the landscape of research on COVID-19 phishing attacks and their countermeasures is made of a majority of studies aimed at investigating attacks, with only a relative minority of works that proposed specific solutions to them. The analysis of the literature that investigated attacks revealed that scholars already explored different directions of research and evaluated different aspects of the attacks. For instance, while some papers provided a general (i.e., horizontal) overview of the cyber-attacks that occurred during COVID-19, out of which phishing represents the utmost example, others carried out more constrained yet detailed (i.e., vertical) analyses of specific issues. Among them are papers that investigated (i) the causes of vulnerability to phishing attacks during COVID-19 [7, 10], (ii) the rise of malicious domain registrations [34, 49], (iii) the economic impact of phishing attacks [7], (iv) the responses enacted by some countries to fight the rampaging COVID-19 scamdemic [64–66], (v) the peculiar cybersecurity challenges faced by the healthcare sector [10, 20, 22, 25], and more. As such, the body of research on covid-related phishing attacks appears to be diversified, dense and overall already mature. On the contrary, our detailed analysis of the proposed countermeasures to such attacks revealed a number of challenges and drawbacks.

5.1 | Current challenges

In Section 4 we identified a lack of reference datasets and we highlighted that the majority of proposed COVID-19 phishing detectors are based on simple and traditional classification algorithms and on small sets of shallow features. The first issue – that is, the limited availability of reference datasets – can be traced back to a combination of long-known and covid-related challenges. Firstly, building high-quality scientific datasets have always represented a very demanding task [98]. In addition, the impact and the recency of the pandemic left even less time and resources for scholars to tackle this task. As such, a general lack of extensive, high-quality data on the novel problem of covid-related phishing attacks is somehow expected at this stage. Nonetheless, this is causing several problems to the scholars working in this field. One general problem is that this lack of resources inevitably hinders the research on covid-related cyber-attacks. Moreover, another problem is related to the capability of training and evaluating automatic systems for phishing detection. In particular, the current situation where each detector was evaluated on a different dataset, many of which are small and not publicly available, inevitably raises concerns about the validity and generality of the evaluations reported in the existing papers.

The second issue unveiled by our analysis is related to the use of traditional (i.e., not state-of-the-art) machine learning algorithms and of shallow features. As shown, the majority of proposed phishing detectors was based on classification algorithms such as decision trees, random forests and support vector machines, instead of more recent and better performing solutions, such as those based on deep learning [112]. The same considerations can be made for the choice of machine learning features, which is not on par with current state-of-the-art solutions [113]. Notably, the issue with the choice of algorithms and features strictly depends on the lack of reference datasets. This is particularly true for the possible application of deep learning to the task of phishing detection, for which large datasets are needed in order to train and optimize deep neural networks that easily involve millions of parameters [114].

5.2 | Future directions of research

As anticipated, the body of research on covid-related phishing attacks is overall mature. However, some specific areas could nonetheless benefit from additional research. One of such areas is that related to the quantification of the effects (or impact) of the attacks. This task has been mostly left to cybersecurity firms and governmental agencies, but it could instead see a deeper academic involvement. Notably, measuring the effects of cyber-attacks currently represents an open and promising research direction that goes beyond phishing and COVID-19. In fact, quantifying effects is meaningful and needed in all those areas of cybersecurity that deal with relatively new types of attacks (e.g., fake news and all forms of online information manipulation [31]) and countermeasures [115]. Here, a better assessment and quantification of the consequences of phishing attacks during a major crisis could inform decisions for a broad array of stakeholders, including policymakers, law enforcement personnel, as well as all those scholars and practitioners actively involved in developing effective countermeasures.

Since each challenge comes with opportunities, the area related to the development of countermeasures to COVID-19 phishing attacks is the one that currently presents the majority of opportunities for future research. For example, the aforementioned lack of reference datasets for training and validating detectors, mandates additional work in this important direction. In fact, works aimed at collecting, developing and sharing scientific resources – including datasets, but also tools and software as well as benchmark platforms/frameworks – are much needed and are likely to have a strong impact in the scientific community. As such, this scientific endeavour represents a low-hanging fruit. Then, with more and better data it is foreseeable that more sophisticated and powerful detectors will be developed. In other words, we envision that the greater availability of resources will bootstrap the next wave of research on covid-related cyber-attacks, including the experimentation with those algorithms and techniques whose application was daunting or infeasible until now. Notably, not only does this direction of research involve new experimentation with deep learning-based methods for feature extraction and attack detection, but it also opens up the possibility to experiment with feature selection techniques [116] and with techniques for combining simple classifiers, such as ensemble methods [3]. All these techniques have seen very limited application until now, because of the limitations that we previously discussed. However, they have already proven their efficacy in related tasks and are thus likely to provide favourable results also for the detection of COVID-19 phishing attacks.

Another challenge that we highlighted in the previous section is the difficulty at assessing the validity of the experimental results of phishing detectors. To this regard, another much needed direction of research is the one related to the development of systematic evaluation campaigns of the existing detectors. As it typically happens with many detection tasks [31], the majority of efforts are devoted to developing new detectors and only a small minority of works focus on evaluating and comparing the different detectors. With the foreseen increase in the development of state-of-the-art phishing detectors, the latter task will become even more important. Systematic evaluations of the existing detectors should not only involve comparisons between the detectors, but should also include experiments aimed at evaluating the generalizability of the different detectors – that is, their capacity to detect attacks for which they were not trained. The latter test in particular has proven valuable in other tasks for identifying detectors' generalization deficiencies and for estimating their capacity to thwart future and unforeseen attacks [111].

5.3 | Final remarks

COVID-19 has been one of the deadliest pandemics in the history of humanity and the first to occur in a massively digitized and hyperconnected world. Withstanding its spread and impact required drastic changes that gave rise to a plethora of problems. One of such problems – phishing attacks – has been the subject of this survey.

The long-term effects of the pandemic on our society are still unclear. However, it is already evident that some changes are bound to stay. As an example, the sudden shift to remote work represented a unique opportunity to reimagine and reorganise businesses, jobs and work habits. The world after COVID-19 will never be the same. Moreover, more and worse pandemics are expected to strike in the coming years [117].

What all of this means is that at least some of the problems that we faced during COVID-19 will remain for a long time and will probably reappear and intensify over and over again. Gunther Eysenbach – the father of infodemiology – stressed in 2009 the need to 'build tools now to manage future infodemics' [118]. In retrospect, we clearly see that his warning call went unheeded [119]. For all of these reasons, it is of the utmost importance to capitalize on the lessons learnt in this pandemic, for such experiences will be decisive to withstand the future infodemics and scamdemics.

6 | CONCLUSIONS

In this survey we focussed on the most frequent type of cyber-attack perpetrated during the COVID-19 pandemic: phishing. We systematically analysed and discussed both scientific studies, as well as reports by cybersecurity firms and governmental agencies that investigated phishing attacks or that proposed solutions against them.

Our analysis highlighted that many works investigated the drivers and the characteristics of phishing attacks. Instead, only a minority of scholars worked to build and share resources for the community (e.g., reference datasets) and to propose specific solutions against phishing. Moreover, the existing solutions are mostly based on traditional machine learning techniques, thus largely overlooking the state-of-the-art methods for both the classification and feature extraction steps.

Given this picture, the most favourable directions for future research and experimentation revolve around building and sharing resources to the community, such as large datasets and evaluation campaigns. Once more resources will be available, efforts should be directed towards applying state-of-the-art techniques, such as those based on deep learning, for the task of phishing detection. The lessons learnt from contrasting phishing and other cyber-attacks during the COVID-19 pandemic will be valuable for responding to the increasing cybersecurity concerns that are rising with each passing year.

ACKNOWLEDGEMENTS

The publication of this article was funded by the Qatar National Library (QNL), Doha, Qatar and partially supported by award QRLP10-G-1803022 from the Qatar National Research Fund (QNRF), member of Qatar Foundation.

CONFLICT OF INTEREST

The authors declare that have no conflicts of interest.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Stefano Cresci https://orcid.org/0000-0003-0170-2445

REFERENCES

1. 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. 9, 7152–7169 (2021). https://doi.org/10.1109/access.2020.3048839
2. Di Pietro, R., et al.: New dimensions of information warfare. Adv Inf Sec, vol. 84. (2021)
3. Valiyaveedu, N., et al.: Survey and analysis on AI based phishing detection techniques. The 2021 International Conference on Communication, Control and Information Sciences (ICCISC'21), vol. 1, pp. 1–6. IEEE (2021)
4. Zarocostas, J.: How to fight an infodemic. Lancet. 395(10225), 676 (2020). https://doi.org/10.1016/s0140-6736(20)30461-x
5. Ferrara, E., Cresci, S., Luceri, L.: Misinformation, manipulation, and abuse on social media in the era of COVID-19. J Comput Soc Sci. 3(2), 271–277 (2020). https://doi.org/10.1007/s42001-020-00094-5
6. Szurdi, J., et al.: Studying how cybercriminals prey on the COVID-19 pandemic. Unit42 (2020)
7. Lallie, H.S., et al.: Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput. Secur. 105, 102248 (2021). https://doi.org/10.1016/j.cose.2021.102248
8. Jalali, M.S., et al.: Why employees (still) click on phishing links: investigation in hospitals. J. Med. Internet Res. 22(1), e16775 (2020). https://doi.org/10.2196/16775
9. Schneck, P.A.: Cybersecurity during COVID-19. IEEE Ann. Hist. Comput. 18(06), 4–5 (2020). https://doi.org/10.1109/msec.2020.3019678
10. He, Y., et al.: Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. J. Med. Internet Res. 23(4), e21747 (2021). https://doi.org/10.2196/21747
11. United Nations Department of Global Communications: UN Tackles infodemic of Misinformation and Cybercrime in COVID-19 Crisis (2020). https://www.un.org/en/un-coronavirus-communications-team/un-tackling-'infodemic'-misinformation-and-cybercrime-covid-19. Accessed 31 May 2022
12. Basit, A., et al.: A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommun. Syst. 76(1), 139–154 (2021). https://doi.org/10.1007/s11235-020-00733-2
13. Salloum, S., et al.: Phishing email detection using natural language processing techniques: a literature survey. Procedia Comput. Sci. 189, 19–28 (2021). https://doi.org/10.1016/j.procs.2021.05.077

14. Alkhalil, Z., et al.: Phishing attacks: recent comprehensive study and a new anatomy. Front. Comput. Sci. 3, 6 (2021). https://doi.org/10.3389/fcomp.2021.563060
15. Hakak, S., et al.: Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. IEEE Access. 8, 124134–124144 (2020). https://doi.org/10.1109/access.2020.3006172
16. Korkmaz, M., Sahingoz, O.K., Diri, B.: Feature selections for the classification of webpages to detect phishing attacks: a survey. In: The 2nd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA'20), pp. 1–9. IEEE (2020)
17. Ghafir, I., Prenosil, V.: Advanced persistent threat attack detection: an overview. Int J Adv Comput Networks Secur. 4(4), 5054 (2014)
18. Ahmad, A., et al.: Strategically-motivated advanced persistent threat: definition, process, tactics and a disinformation model of counterattack. Comput. Secur. 86, 402–418 (2019). https://doi.org/10.1016/j.cose.2019.07.001
19. Kumaran, N., Lugani, S.: Protecting Businesses against Cyber Threats during COVID-19 and beyond, Google Cloud - Identity and Security (2020)
20. Williams, C.M., Chaturvedi, R., Chakravarthy, K.: Cybersecurity risks in a pandemic. J. Med. Internet Res. 22(9), e23692 (2020). https://doi.org/10.2196/23692
21. Boddy, A., et al.: A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures. In: The 1st International Conference on Internet of Things and Machine Learning (IML'17), pp. 1–7. ACM (2017)
22. Offner, K., et al.: Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. Intell. Natl. Secur. 35(4), 556–585 (2020). https://doi.org/10.1080/02684527.2020.1752459
23. Ronquillo, J.G., et al.: Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. JAMIA Open. 1(1), 15–19 (2018). https://doi.org/10.1093/jamiaopen/ooy019
24. Weil, T., Murugesan, S.: IT risk and resilience—cybersecurity response to COVID-19. IT Prof. 22(3), 4–10 (2020). https://doi.org/10.1109/mitp.2020.2988330
25. Sardi, A., et al.: Cyber risk in health facilities: a systematic literature review. Sustainability. 12(17), 7002 (2020). https://doi.org/10.3390/su12177002
26. Kim, D.-w., Choi, J.-y., Han, K.-h.: Risk management-based security evaluation model for telemedicine systems. BMC Med. Inf. Decis. Making. 20(1), 1–14 (2020). https://doi.org/10.1186/s12911-020-01145-7
27. Naidoo, R.: A multi-level influence model of COVID-19 themed cybercrime. Eur. J. Inf. Syst. 29(3), 306–321 (2020). https://doi.org/10.1080/0960085x.2020.1771222
28. Da San Martino, G., et al.: A survey on computational propaganda detection. In: The 29th International Joint Conference on Artificial Intelligence, pp. 4826–4832. IJCAI'20 (2020)
29. Iuga, C., Nurse, J.R., Erola, A.: Baiting the hook: factors impacting susceptibility to phishing attacks. Human-centric Comput Inf Sci. 6(1), 1–20 (2016). https://doi.org/10.1186/s13673-016-0065-2
30. MalwareBytes, Cybercriminals impersonate World Health Organization to Distribute Fake Coronavirus E-Book (2020). https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/. Accessed 31 May 2022
31. Cresci, S.: A decade of social bot detection. Commun. ACM. 63(10), 72–83 (2020). https://doi.org/10.1145/3409116
32. The Daily Mail: Cyber criminals create a spoof copy of the NHS website in the midst of the coronavirus pandemic to trick users into downloading dangerous malware that can steal their passwords and credit card data. https://www.dailymail.co.uk/sciencetech/article-8250737/Kaspersky-detects-fake-NHS-site-steals-credit-card-data.html (2020). Accessed 31 May 2022
33. Krebs on Security.: Live coronavirus map used to spread malware. https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/ (2020). Accessed 31 May 2022
34. Xia, P., et al.: Identifying and characterizing COVID-19 themed malicious domain campaigns. In: The 11th ACM Conference on Data and Application Security and Privacy, pp. 209–220. CODASPY'21 (2021)
35. O'Donnell, L.: Skype Phishing Attack Targets Remote Workers' Passwords (2020). https://threatpost.com/skype-phishing-attack-targets-remote-workers-passwords/155068/. Accessed 31 May 2022
36. Rodger, J.: The school meals coronavirus text scam which could trick parents out of thousands. https://www.birminghammail.co.uk/news/midlands-news/school-meals-coronavirus-text-scam-17975311 (2020). Accessed 31 May 2022
37. Pilkey, A.: Coronavirus Email Attacks Evolving as Outbreak Spreads (2020). https://blog.f-secure.com/coronavirus-email-attacks-evolving-as-outbreak-spreads/. Accessed 31 May 2022
38. Patranobis, S.: Indian hackers targeting Chinese medical institutes amid coronavirus outbreak, says report (2020). https://www.hindustantimes.com/world-news/indian-hackers-targetting-chinese-medical-institutes-amid-coronavirus-outbreak-says-report/story-piDHQeY4UfTVy8BWa2GG3O.html. Accessed 31 May 2022
39. Vergelis, M.: Phishers Are Using the Wuhan Coronavirus as Bait, Trying to Hook E-Mail Credentials (2020). https://www.kaspersky.com/blog/coronavirus-phishing/32395/. Accessed 31 May 2022
40. Walter, J.: Threat Intel Cyber Attacks Leveraging the COVID-19/coronavirus Pandemic (2020). https://www.sentinelone.com/labs/threat-intel-cyber-attacks-leveraging-the-covid-19-coronavirus-pandemic/. Accessed 31 May 2022
41. Doffman, Z.: Chinese Hackers 'weaponize' Coronavirus Data for New Cyber Attack: Here's what They Did (2020). https://www.forbes.com/sites/zakdoffman/2020/03/12/chinese-hackers-weaponized-coronavirus-data-to-launch-this-new-cyber-attack. Accessed 31 May 2022
42. Henderson, S., et al.: Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage (2020). https://www.mandiant.com/resources/apt32-targeting-chinese-government-in-covid-19-related-espionage. Accessed 31 May 2022
43. Del Rosso, K.: New Threat Discovery Shows Commercial Surveillanceware Operators Latest to Exploit COVID-19 (2020). https://www.lookout.com/blog/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19. Accessed 31 May 2022
44. Greig, J.: Global Shipping Industry Attacked by Coronavirus-Themed Malware (2020). https://www.techrepublic.com/article/global-shipping-industry-attacked-by-coronavirus-themed-malware/. Accessed 31 May 2022
45. Smithers, R.: Fraudsters Use Bogus NHS Contacttracing App in Phishing Scam (2020). https://www.theguardian.com/world/2020/may/13/fraudsters-use-bogus-nhs-contact-tracing-app-in-phishing-scam. Accessed 31 May 2022
46. Nurse, J.R.: Cybercrime and you: how criminals attack and the human factors that they seek to exploit. In: The Oxford Handbook of Cyberpsychology, pp. 663–690. Oxford University Press (2019)
47. Check Point: Coronavirus Cyber-Attacks Update: Beware of the Phish (2020). https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/. Accessed 31 May 2022
48. Williams, E.J., Polage, D.: How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. Behav. Inf. Technol. 38(2), 184–197 (2019). https://doi.org/10.1080/0144929x.2018.1519599
49. Pletinckx, S., et al.: Cash for the register? Capturing rationales of early COVID-19 domain registrations at Internet-scale. In: The 12th International Conference on Information and Communication Systems (ICICS'21), pp. 41–48. IEEE (2021)
50. Krebs on Security: Sipping from the Coronavirus Domain Firehose (2020). https://krebsonsecurity.com/2020/04/sipping-from-the-coronavirus-domain-firehose/. Accessed 31 May 2022
51. BAE Systems: The COVID Crime Index 2021 (2021). https://www.baesystems.com/en-financialservices/insights/the-covid-crime-index. Accessed 31 May 2022
52. Pritom, M.M.A., et al.: Characterizing the landscape of COVID-19 themed cyberattacks and defenses. In: The 18th IEEE International

Conference on Intelligence and Security Informatics (ISI'20), pp. 1–6. IEEE (2020)

53. Pols, P.: Tech. rep. In: The Unified Kill Chain. Leiden University (2017)
54. Eian, I.C., et al.: Cyber Attacks in the Era of COVID-19 and Possible Solution DomainsPreprints (2020). https://doi.org/10.20944/preprints202009.0630.v1
55. Plachkinova, M.: Exploring the shift from physical to cybercrime at the onset of the COVID-19 pandemic. Int J Cyber Forensics Adv Threat Invest. 2(1), 50–62 (2021). https://doi.org/10.46386/ijcfati.v2i1.29
56. Khan, N.A., Brohi, S.N., Zaman, N.: Ten Deadly Cyber Security Threats amid COVID-19 Pandemic. TechRxiv (2020). https://doi.org/10.36227/techrxiv.12278792.v1
57. Parani, S., Raikwar, M.: A study on phishing attack during the COVID-19 lockdown. Int. J. Comput. Appl. 174(21), 50–54 (2021). https://doi.org/10.5120/ijca2021921086
58. Malecki, F.: Overcoming the security risks of remote working. Comput. Fraud Secur. (7), 10–12 (2020). https://doi.org/10.1016/s1361-3723(20)30074-9
59. Sarginson, N.: Securing your remote workforce against new phishing attacks. Comput. Fraud Secur. 2020(9), 9–12 (2020). https://doi.org/10.1016/s1361-3723(20)30096-8
60. Ahmad, T.: Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity
61. Pranggono, B., Arabo, A.: COVID-19 pandemic cybersecurity issues. Internet Technol Lett. 4(2), e247 (2021). https://doi.org/10.1002/itl2.247
62. Başeskioğlu, M.Ö., Tepecik, A.: Cybersecurity, computer networks phishing, malware, ransomware, and social engineering anti-piracy reviews. In: The 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA'21), pp. 1–5. IEEE (2021)
63. Mathew, A.R.: Cybersecurity pros warn–COVID-19 pandemic as a tool. Int. J. Eng. Adv. Technol. 9(4), 2441–2443. https://doi.org/10.35940/ijeat.d8305.049420
64. Furnell, S., Shah, J.N.: Home working and cyber security–an outbreak of unpreparedness. Comput. Fraud Secur. 2020(8), 6–12 (2020). https://doi.org/10.1016/s1361-3723(20)30084-1
65. Škiljić, A.: Cybersecurity and remote working: Croatia's (non-) response to increased cyber threats. Int Cybersecur Law Rev. 1(1), 51–61 (2020). https://doi.org/10.1365/s43439-020-00014-3
66. Amarullah, A.H., Runturambi, A.J.S., Widiawan, B.: Analyzing cyber crimes during COVID-19 time in Indonesia. In: The 3rd International Conference on Computer Communication and the Internet (ICCCI'21), pp. 78–83. IEEE (2021)
67. Chapman, P.: Are your IT staff ready for the pandemic-driven insider threat. Netw. Secur. (4), 8–11 (2020). https://doi.org/10.1016/s1353-4858(20)30042-8
68. Bitaab, M., et al.: Scam pandemic: how attackers exploit public fear through phishing. In: The 2020 Symposium on Electronic Crime Research (eCrime'20), pp. 1–10. APWG (2020)
69. Akdemir, N., Yenal, S.: How phishers exploit the coronavirus pandemic: a content analysis of COVID-19 themed phishing emails. Sage Open. 11(3), 21582440211031879 (2021). https://doi.org/10.1177/21582440211031879
70. Wang, L., et al.: Beyond the virus: a first look at coronavirus-themed Android malware. Empir. Software Eng. 26(4), 1–38 (2021). https://doi.org/10.1007/s10664-021-09974-4
71. Xia, P., et al.: Don't Fish in Troubled Waters! Characterizing Coronavirus-Themed Cryptocurrency Scams. arXiv preprint arXiv:2007.13639
72. Nizzoli, L., et al.: Charting the landscape of online cryptocurrency manipulation. IEEE Access. 8, 113230–113245 (2020). https://doi.org/10.1109/access.2020.3003370
73. Mihailović, A., et al.: COVID-19 and beyond: employee perceptions of the efficiency of teleworking and its cybersecurity implications. Sustainability. 13(12), 6750 (2021). https://doi.org/10.3390/su13126750
74. Pearl, J.: Causal inference in statistics: an overview. Stat. Surv. 3(none), 96–146 (2009). https://doi.org/10.1214/09-ss057
75. Georgiadou, A., Mouzakitis, S., Askounis, D.: Working from home during COVID-19 crisis: a cyber security culture assessment survey. Secur. J. 35(2), 1–20 (2021). https://doi.org/10.1057/s41284-021-00286-2
76. Turner, C., Turner, C.B., Shen, Y.: Cybersecurity concerns & teleworking in the COVID-19 era: a socio-cybersecurity analysis of organizational behavior. J Adv Res Soc Sci. 3(2), 22–30 (2020). https://doi.org/10.33422/jarss.v3i2.502
77. Schutt, R.K.: Investigating the Social World: The Process and Practice of Research. SAGE publications (2018)
78. Baryshevtsev, M., McGlynn, J.: Persuasive appeals predict credibility judgments of phishing messages. Cyberpsychol Behav. Soc. Netw. 23(5), 297–302 (2020). https://doi.org/10.1089/cyber.2019.0592
79. Hawdon, J., Parti, K., Dearden, T.E.: Cybercrime in America amid COVID-19: the initial results from a natural experiment. Am. J. Crim. Justice. 45(4), 546–562 (2020). https://doi.org/10.1007/s12103-020-09534-4
80. Daengsi, T., et al.: A comparative study of cybersecurity awareness on phishing among employees from different departments in an organization. In: The 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE'21), pp. 102–106. IEEE (2021)
81. Gordon, W.J., et al.: Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. J. Am. Med. Inf. Assoc. 26(6), 547–552 (2019). https://doi.org/10.1093/jamia/ocz005
82. Mishra, S., Soni, D.: DSmishSMS-A system to detect smishing SMS. Neural Comput. Appl., 1–18 (2021). https://doi.org/10.1007/s00521-021-06305-y
83. Almeida, T.A., Hidalgo, J.M.G., Yamakami, A.: Contributions to the study of SMS spam filtering: new collection and results. In: The 11th ACM Symposium on Document Engineering, pp. 259–262. DocEng'11 (2011)
84. Biswal, S.: Real-time intelligent vishing prediction and awareness model (RIVPAM). In: The 7th International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA'21), pp. 1–2. IEEE (2021)
85. Jones, K.S., et al.: How social engineers use persuasion principles during vishing attacks. Inf.Comput. Secur. 29(2), 314–331 (2020). https://doi.org/10.1108/ics-07-2020-0113
86. Wu, P., Guo, H., Holmes: An Efficient and Lightweight Semantic Based Anomalous Email Detector. arXiv preprint arXiv:2104.08044
87. Sarma, D., et al.: Comparative analysis of machine learning algorithms for phishing website detection. In: Inventive Computation and Information Technologies, pp. 883–896. Springer (2021)
88. Mukhopadhyay, A., Prajwal, A.: Edith - a robust framework for prevention of cyber attacks in the COVID era. In: The 2nd International Conference for Emerging Technology (INCET'21), pp. 1–8. IEEE (2021)
89. Ispahany, J., Islam, R.: Detecting malicious COVID-19 URLs using machine learning techniques. In: The 19th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM'21 Workshops), pp. 718–723. IEEE (2021)
90. Tawalbeh, L., et al.: Predicting and preventing cyber attacks during COVID-19 time using data analysis and proposed secure IoT layered model. In: The 4th International Conference on Multimedia Computing, Networking and Applications (MCNA'20), pp. 113–118. IEEE (2020)
91. Saha, I., et al.: Phishing attacks detection using deep learning approach. In: The 3rd International Conference on Smart Systems and Inventive Technology (ICSSIT'20), pp. 1180–1185. IEEE (2020)
92. Basit, A., et al.: A novel ensemble machine learning method to detect phishing attack. In: The 23rd International Multitopic Conference (INMIC'20), pp. 1–5. IEEE (2020)
93. Pritom, M.M.A., et al.: Data-driven characterization and detection of COVID-19 themed malicious websites. In: The 18th IEEE International Conference on Intelligence and Security Informatics (ISI'20), pp. 1–6. IEEE (2020)

94. Ahmad, H., Erdodi, L.: Overview of phishing landscape and homographs in Arabic domain names. Secur.Priv. 4(4), e159 (2021). https://doi.org/10.1002/spy2.159
95. Montañez, R., Golob, E., Xu, S.: Human cognition through the lens of social engineering cyberattacks. Front. Psychol. 11, 1755 (2020). https://doi.org/10.3389/fpsyg.2020.01755
96. Guitton, M.J.: Cyberpsychology research and COVID-19. Comput. Hum. Behav. 111, 106357 (2020). https://doi.org/10.1016/j.chb.2020.106357
97. Cockburn, A., et al.: Threats of a replication crisis in empirical computer science. Commun. ACM. 63(8), 70–79 (2020). https://doi.org/10.1145/3360311
98. Assenmacher, D., et al.: Benchmarking crisis in social media analytics: a solution for the data sharing problem. Soc. Sci. Comput. Rev. https://doi.org/10.1177/08944393211012268
99. Domingos, P.: A few useful things to know about machine learning. Commun. ACM. 55(10), 78–87 (2012). https://doi.org/10.1145/2347736.2347755
100. Alam, F., et al.: A Survey on Multimodal Disinformation Detection. arXiv preprint arXiv:2103.12541
101. Liu, X., et al.: Multi-task deep neural networks for natural language understanding. In: The 57th Annual Meeting of the Association for Computational Linguistics, pp. 4487–4496. ACL'19 (2019)
102. Al-Turkistani, H.F., Ali, H.: Enhancing users wireless network cyber security and privacy concerns during COVID-19. In: The 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA'21), pp. 284–285. IEEE (2021)
103. Kott, A., Linkov, I.: To improve cyber resilience, measure it. Computer. 54(2), 80–85 (2021). https://doi.org/10.1109/mc.2020.3038411
104. Groenendaal, J., Helsloot, I.: Cyber resilience during the COVID-19 pandemic crisis: a case study. J. Contingencies Crisis Manag. 29(4), 439–444 (2021). https://doi.org/10.1111/1468-5973.12360
105. Hollnagel, E.: RAG – Resilience Analysis Grid, Introduction to the Resilience Analysis Grid (RAG)
106. Cresci, S., et al.: From reaction to proaction: unexplored ways to the detection of evolving spambots. In: The Web Conference 2018 (WWW'18 Companion), pp. 1469–1470 (2018)
107. Hyslip, T.S.: Cybercrime-as-a-Service Operations, pp. 815–846. The Palgrave Handbook of International Cybercrime and Cyberdeviance (2020)
108. Arshey, M., Viji, K.A.: Thwarting cyber crime and phishing attacks with machine learning: a study. In: The 7th International Conference on Advanced Computing and Communication Systems (ICACCS'21), vol. 1, pp. 353–357. IEEE (2021)
109. Verma, R., Das, A.: What's in a URL: fast feature extraction and malicious URL detection. In: The 3rd ACM International Workshop on Security and Privacy Analytics, pp. 55–63. IWSPA'17 (2017)
110. Patil, D.R., Patil, J.B.: Malicious URLs detection using decision tree classifiers and majority voting technique. Cybern. Inf. Technol. 18(1), 11–29 (2018). https://doi.org/10.2478/cait-2018-0002
111. Echeverrìa, J., et al.: LOBO: evaluation of generalization deficiencies in Twitter bot classifiers. In: The 34th Annual Computer Security Applications Conference (ACSAC'18), pp. 137–146. ACM (2018)
112. Yi, P., et al.: Web phishing detection using a deep learning framework. Wireless Commun. Mobile Comput., 1–9 (2018). https://doi.org/10.1155/2018/4678746
113. Yang, P., Zhao, G., Zeng, P.: Phishing website detection based on multidimensional features driven by deep learning. IEEE Access. 7, 15196–15209 (2019). https://doi.org/10.1109/access.2019.2892066
114. Sun, C., et al.: Revisiting unreasonable effectiveness of data in deep learning era. In: The 15th IEEE International Conference on Computer Vision, pp. 843–852 (2017)
115. Trujillo, A., Cresci, S.: Make Reddit Great Again: Assessing Community Effects of Moderation Interventions on r/The_Donald. arXiv: 2201.06455
116. Gandotra, E., Gupta, D.: An efficient approach for phishing detection using machine learning. In: Multimedia Security, pp. 239–253. Springer (2021)
117. Intergovernmental science-policy platform on biodiversity and ecosystem services, IPBES workshop report on biodiversity and pandemics. Tech. Rep. (2020)
118. Eysenbach, G.: Infodemiology and infoveillance: framework for an emerging set of public health informatics methods to analyze search, communication and publication behavior on the internet. J. Med. Internet Res. 11(1), e1157 (2009). https://doi.org/10.2196/jmir.1157
119. Cinelli, M., et al.: The COVID-19 social media infodemic. Sci. Rep. 10(1), 1–10 (2020)

How to cite this article: Al-Qahtani, A.F., Cresci, S.: The COVID-19 scamdemic: a survey of phishing attacks and their countermeasures during COVID-19. IET Inf. Secur. 16(5), 324–345 (2022). https://doi.org/10.1049/ise2.12073