information

MDPI

Article

Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks

Dania Aljeaid *, Amal Alzhrani, Mona Alrougi and Oroob Almalki

Department of Information System, Faculty of Computing and Information Technology, KingAbdulaziz University, Jeddah 21551, Saudi Arabia; aalzhrani0452@stu.kau.edu.sa (A.A.); malrougui0004@stu.kau.edu.sa (M.A.); oalmalki0032@stu.kau.edu.sa (O.A.)

* Correspondence: daljeaid@kau.edu.sa

Received: 8 October 2020; Accepted: 23 November 2020; Published: 25 November 2020

Abstract: Phishing attacks are cybersecurity threats that have become increasingly sophisticated. Phishing is a cyberattack that can be carried out using various approaches and techniques. Usually, an attacker uses trickery as well as fraudulent and disguised means to steal valuable personal information or to deceive the victim into running malicious code, thereby gaining access and controlling the victim's systems. This study focuses on evaluating the level of cybersecurity knowledge and cyber awareness in Saudi Arabia. It is aimed at assessing end-user susceptibility through three phishing attack simulations. Furthermore, we elaborate on some of the concepts related to phishing attacks and review the steps required to launch such attacks. Subsequently, we briefly discuss the tools and techniques associated with each attack simulation. Finally, a comprehensive analysis is conducted to assess and evaluate the results.

Keywords: cybersecurity; phishing attacks; attack simulation; cybersecurity awareness

1. Introduction

The utilisation of information and communications technologies has led to unprecedented advances in our daily lives and resulted in an increase in the usage and production of electronic devices. As the real world has shifted into the cyber world, a growing number of uncertainties related to the use of the digital environment have occurred, posing new digital security threats and challenges. Over the last decade, a dramatic increase in the number of cybercrimes has been witnessed worldwide. These crimes have been successfully committed through the Internet and include fraud, identity theft, scams, cyberstalking, and even cyber terrorism [1–3]. Such criminal acts can terrorise people as well as invade their privacy and jeopardise their wellbeing [2,3]. Furthermore, some cybercrimes are specifically designed to blackmail children and young people [4,5]. Several adult users are not fully aware and sufficiently knowledgeable to protect themselves against cyber threats and cyberattacks. Consequently, this adversely affects their role in protecting their children, who thus become an easy target for exploitation by cyber criminals.

Currently, a major concern is protecting end users from fraudulent websites and phishing attacks. One such measure is raising user awareness regarding the consequences of phishing attacks [5–8]. The Anti-phishing Working Group (APWG) defines phishing as "a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials" [9]. According to the Phishing Activity Trends Report published by the APWG in the third quarter of 2018, the number of detected phishing websites was 151,014, whereas the number of reported phishing e-mails by APWG consumers was 270,557, and the number of brands targeted by

the phishers was 777. Furthermore, the payment processes and bank sector were the industry sectors most targeted by criminals, with a rate of up to 38.2% [9].

Moreover, RiskIQ, which is a member of the APWG, conducted an analysis on a random sample consisting of 3378 approved phishing URLs reported to APWG. This analysis indicated that the most frequent domain names were legacy generic top-level domains (TLDs), such as .com, .org and .net., with a rate of 59.4% [9].

In this paper, we present three experimental methods according to the attack type: (1) We cloned a website and then observed end-user behaviour. (2) We crafted a phishing email to obtain sensitive information. (3) We launched a social networking phishing (SNP) attack. Finally, a comprehensive analysis was conducted to assess and evaluate the results of these attacks.

Contribution: The contributions of this study are as follows:

1. To the best of our knowledge, this is the third related study conducted in Saudi Arabia. In the experiment, three types of phishing attacks were performed: clone phishing, email phishing and SNP.
2. Each attack servers as model providing information about phishing and indicating possible preventive measures.
3. We systematically analyse each attack and discuss the impact factors from the victim's perspective. This analysis can facilitate the understanding of user behaviour and the development of security awareness.

Hypothesis: The experiment assumed that end users in Saudi Arabia are not sufficiently knowledgeable regarding cyberattacks. In addition, they lack the ability to protect themselves against various types of phishing attacks. To test this hypothesis, we simulate different phishing attacks to evaluate user behaviour.

Organisation: The rest of the paper is organised as follows: In Section 2, we review various types of phishing attacks. In Section 3, we present a complete cloning process to launch website phishing attacks, and we provide a comprehensive analysis after the simulated attack. In Section 4, we emulate domain spoofing through email phishing, and discuss the result of spear phishing for the selected target domain. In Section 5, we conduct a live SNP attack. We briefly discuss security evaluation and the factors that contributed to the success of the three attacks in Section 6. In Section 7, we review related works. Finally, conclusion is presented in Section 8.

2. Types of Phishing

Phishing attacks is an example of social engineering techniques. Phishing is not limited to emails, and various techniques and methods can be adopted to launch such attacks, for example, using SMS, websites and phone calls. It is crucial to differentiate the types of phishing attacks and understand their victims. Phishing attacks can be classified as follows:

- Spear phishing: Spear phishing aims to collect or expose sensitive information from a specific organization's employees or single person through E-mails that crafted carefully for this purpose. By contrast, traditional phishing targets millions of unknown users [10,11].
- SMS phishing (smishing): This involves writing text messages so that the phishers can persuade and deceive people to disclose their personal information. These messages request victims to call a specific phone number or log to legitimate-looking website [11].
- Vishing scams make use of the Voice-over-Internet Protocol: Vishing refers to phishing over voice mail or phone calls through which the caller (phisher) drives victims to make impulsive decisions that may lead them to divulge their personal or financial information [11,12].
- Whaling: There is a slight difference between whaling and spear phishing. Whaling is more specific regarding its target group, such as the executives in any organisation, that is, high-profile employees that own sensitive data [12,13].
- Clone phishing: Phishers imitate a legitimate website by cloning its design, layout, logos, and images. Usually, these websites ask a user to log into a system with the purpose of stealing

user information and breaching the security of the local computer by redirecting the user to pages infected with malware [13].

- Social networking-based phishing (SNP): By posing as a trustworthy person or legitimate organisation, a phisher uses social media (e.g., Twitter, LinkedIn, and Google Plus) as a means whereby a victim may be deceived and reveal valuable information [10,14,15].
- Watering hole attack (WHA): This attack usually conducted in conjunction with any type of phishing attacks and social engineering attacks. As the name implies, the attackers search for the most frequently visited websites of a specific victim or organisation. Then, they inject the vulnerable website with malicious code or drive-by download malvertisement. The key method is to direct victims to a cloned/vulnerable website that deliver a malicious payload or trick the victim to click on a link and run malicious scripts [16,17].

3. Website Phishing Attack Simulation

This phase of the experiment involves cloning a website. There are various available cloning tools, such as httrack, wget and serf-online, the purpose of which is to allow developers to easily establish a new website by using an existing website [18,19]. Unfortunately, attackers usually misuse these tools to serve their malicious intentions. That is, they use these tools to launch phishing attacks [4,16,20]. In this part of the experiment, we cloned the website of King Abdulaziz University (KAU) in Saudi Arabia. The fake website was designed and only exposed to the control group to avoid any attempts to denigrate the organisation. Then, a comprehensive analysis was conducted by examining the attack and assessing the results regarding the effect of visual signs in determining the legitimacy of phishing websites.

3.1. Launching Website Phishing Attack through Cloning

Initially, the legitimate website of KAU was downloaded using HTTrack website copier 3.49-2 [19]. The required modification to the HTML code of the website was applied to avoid prosecution. That is, all portal pages that require users to enter their credentials, such usernames and passwords, were removed and replaced with a warning page, as discussed later. All the details of the electronic services page of the KAU website were authentically cloned, as shown in Figures 1 and 2. The cloned website reflected the capability of the Httrack tool.

Figure 1. Legitimate page of KAU website.

Figure 2. Fake page of KAU website.

The next step we used domain squatting abuse technique [21]. We purchased a combosquatting domain name http://eservice-kau.com/ which is close to the legitimate website https://eservices.kau.edu.sa. Combosquatting involves combining trademarks of the legitimate DNS with additional words to lure the victims [21]. The legitimate page (https://eservices.kau.edu.sa) is considered the main portal for KAU students, faculty members, and employees, through which all electronic systems and services can be accessed. On the fake KAU website, if users click on any portal to the electronic systems, they are directed immediately to a warning page, where they are asked to fill in a questionnaire. This questionnaire enquires the victims about their demographic information, visual signs that attract their attention when they determine the legitimacy of fake websites, knowledge level regarding information security, and whether this experiment method was helpful in increasing their degree of awareness regarding phishing (shown in Figure 3).

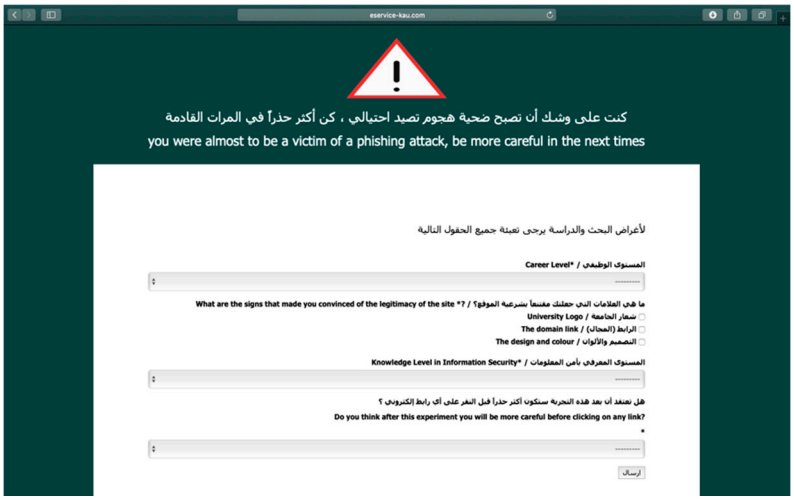

Figure 3. Warning page for the cloned KAU Website.

After the form was completed, the awareness page appeared to clarify why the electronic services page of the KAU website was a phishing attack, and to indicate the countermeasures that should be taken to prevent unsafe browsing (shown in Figure 4). The warning and awareness pages were modified by PyCharm and linked to an SQLight database through the Django framework.

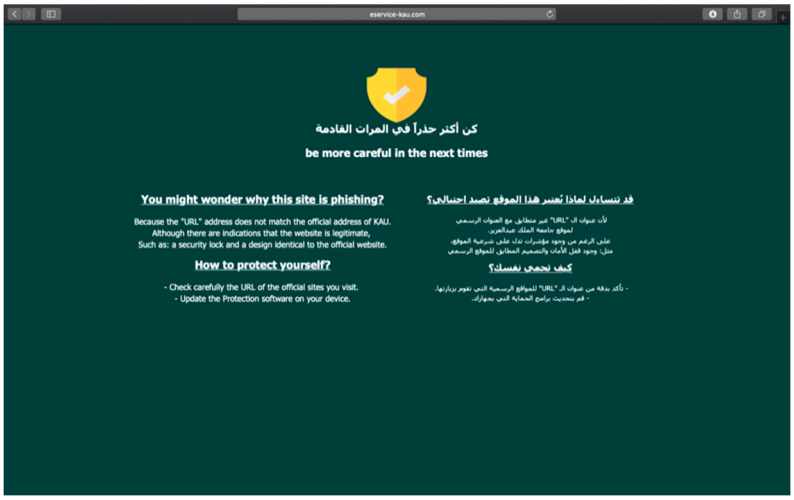

Figure 4. Awareness page for the fake KAU website.

3.2. Under-Control Group

In this cloning approach, the experiment targeted King Abdulaziz University students, faculty members and employees. The total number of participants was 66 and they were randomly selected from different faculties. The participants were briefed on the idea of phishing attacks and how phishers use persuasion tactics to evoke sensitive information by impersonating a trustworthy third party. Then, the participants were tested to observe the cloned page and decide whether it was a legitimate page or a forgery. If they were truly convinced of the legitimacy of the cloned website, they were asked to login. Once they clicked on the portal, they were directed immediately to the warning page.

3.3. Analysis of the Warning Page Form

The warning page informed the participants about the phishing attack status and requested them to answer some questions that were used to achieve our research objectives, as shown in Figure 5.

- Q1: Occupation. Occupation was classified as follows: Students, faculty members and employees. This classification was used to determine the correlation between occupation and cyber risk exposure, and accordingly provide precise recommendations to increase security awareness. Figure 5 shows the number of participants who were tested in this experiment according to their occupation.
- Q2: Visual signs used to determine the legitimacy of phishing websites (multiple answers). This question provides different choices regarding the overall appearance and visual signs through which the participants determined the legitimacy of the website: design and colours, fonts, domain link, or the university logo. The answers can be used to raise the participants' awareness of the most critical visual signs through which legitimate and phishing sites can be distinguished. The finding demonstrated that 76% of the victims agreed that they were deceived by the design, colours of the site, and the university logo. Those signs were the principal factors for determining the legitimacy of the site, whereas the domain link was ignored.
- Q3: Knowledge level in information security. This was categorised as follows: high, moderate, little, and no knowledge. The percentage of participants with little knowledge reached 47%, whereas the percentage corresponding to moderate knowledge was 39%.

- Q4: Do you think after this experiment you will be more careful before clicking on any link? (Yes/No answers) This question measured the effectiveness of the experiment in increasing the participants' awareness of a phishing attack. All participants agreed that they would be more careful before visiting any website.

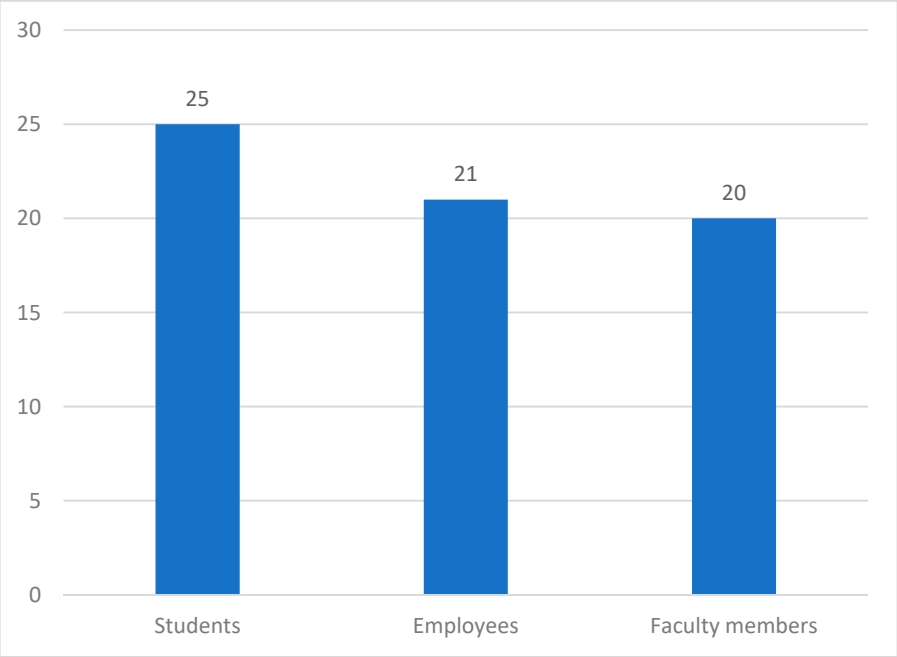

Figure 5. Number of participants according to their occupation.

3.4. Discussion

This experiment showed that 77% of the participants fell victim to this attack, and majority of the victims were students (41%) as shown in Table 1. We used the chi-square statistic, which is a statistical test, to determine whether there is a relationship between the categorical variables "occupation" and "exposure to phishing attack". The result was obtained by using the statistical program IBM SPSS Statistics v22 [22].

Table 1. Chi-square technique.

			Occupation			Total
			Employees	Faculty Members	Students	
Exposure	**Exposed**	**Count**	16	14	21	51
		Expected Count	16.2	15.5	19.3	51.0
		% within exposed	31%	28%	41%	100%
	Not Exposed	Count	5	6	4	15
		Expected Count	4.8	4.5	5.7	15.0
		% within not exposed	33%	40%	27%	100%
Total		Count	21	20	25	66
		Expected Count	21.0	20.0	25.0	66.0

This test was used to investigate if occupation is independent of the probability of exposure to a phishing attack, which represents the null hypothesis (H_0). Initially, the observed and expected frequencies were calculated as shown in Table 1. Then, the chi-square values were calculated as follows:

(1) X-squared =

$$x^2 = \sum \frac{(Observed - Expected)^2}{Expected}$$

$$x^2(chi - square) = \frac{(16-16.2)^2}{16.2} + \frac{(14-15.5)^2}{15.5} + \frac{(21-19.3)^2}{19.3} + \frac{(21-19.3)^2}{19.3} + \frac{(5-4.8)^2}{4.8} + \frac{(6-4.5)^2}{4.5} + \frac{(4-5.7)^2}{5.7} = 1.31$$

(2) Degrees of freedom =

$$df = (rows - 1)(columns - 1) = (2-1)(3-1) = 2$$

(3) Alpha = 0.05 (standard).

(4) Probability value = 5.991, as shown in Table 2.

Table 2. Probability level (alpha).

d.f.	0.995	0.99	0.975	0.95	0.9	0.1	0.05	0.025	0.01
1	0.00	0.00	0.00	0.00	0.02	2.71	3.84	5.02	6.63
2	0.01	0.02	0.05	0.10	0.21	4.61	5.99	7.38	9.21
3	0.07	0.11	0.22	0.35	0.58	6.25	7.81	9.35	11.34
4	0.21	0.30	0.48	0.71	1.06	7.78	9.49	11.14	13.28
5	0.41	0.55	0.83	1.15	1.61	9.24	11.07	12.83	15.09
6	0.68	0.87	1,24	1.64	2.20	10.64	12.59	14.45	16.81
7	0.99	1.24	1.69	2.17	2.83	12.02	14.07	16.01	18.48
8	1.34	1.65	2.18	2.73	3.49	13.36	15.51	17.53	20.09
9	1.73	2.09	2.70	3.33	4.17	14.68	16.92	19.02	21.67
10	2.16	2.56	3.25	3.94	4.87	15.99	18.31	20.48	23.21
11	2.60	3.05	3.82	4.57	5.58	17.28	19.68	21.92	24.72
12	3.07	3.57	4.40	5.23	6.30	18.55	21.03	23.34	26.22
13	3.57	4.11	5.01	5.89	7.04	19.81	22.36	24.74	27.69
14	4.07	4.66	5.63	6.57	7.79	21.06	23.68	26.12	29.14

Here, the X-squared value is less than the probability value 5.991, and thus the null hypothesis H_0 is accepted. This implies that occupation and the probability of exposure to a phishing attack are uncorrelated.

4. Domain Spoofing through Email Phishing

In 2012, Aramco was exposed to the worst cyberattack in its history, resulting in the serious malfunction of approximately 35,000 computers. Forensic investigations revealed that the cause of this incident was a spear-phishing attack. Apparently, a technician with Aramco opened a phishing email that seemed authentic and clicked on the attached malicious link. Following this behaviour, the 'Shamoon' malware was automatically installed on the victim's machine, thus allowing the attacker to control the machine, spread the attack, and escalate privileges [23]. Currently, most phishers send e-mails that appear as if they were sent from a legitimate organisation, a friend, or any other trustworthy source. This induces the victims to trust the masquerade sender and open the email, whereas, in fact, the victims are used to spread malware or obtain sensitive information. In this section, we describe an experiment that was conducted to assess the response of the target group to incoming messages that mimic messages from trusted organisations so that an active education method may be implemented. We hope that this can increase awareness in the field of phishing emails. The attack simulation was conducted using email phishing techniques. It targeted students in King Abdulaziz University who expected to graduate in 2020 at the Faculty of Computers and Information Technology (FCIT). It is worth mentioning that this experiment was conducted in an ethical manner, and sensitive information

was not collected. The content of the email was reviewed and approved by the research committee of the faculty. We used 165 email addresses, which were collected from FCIT department supervisors.

4.1. Structure of the Phishing Email

This attack simulation has two objectives: (1) To assess the students' initial judgemental and determine whether they would fall victim to this type of attack; and (2) to measure their understanding of the attack and the ability to spot any phishing indicators, that is, FROM header (King Abdulaziz University), content, and design. Initially, the generic account *studentsamba.kau@gmail.com* was generated. This spoofed email was crafted to appear as a legitimate email composed by the IT deanship. Then, we constructed the email content, which was a request from a bank to urgently update account information to prevent halting monthly payments. In addition, the phishing email contained a fabricated link, on which the students were required to click to update their information. Accessing this link would direct the students immediately to the awareness page (Figure 6). It is important to note that the email was designed to appear similar to the actual design by adopting the same footer and format used by the Information Technology Deanship; specifically, by altering some information included in the footer, selecting similar colours to those usually used in university emails, and putting the university logo in the header, as shown in Figure 7.

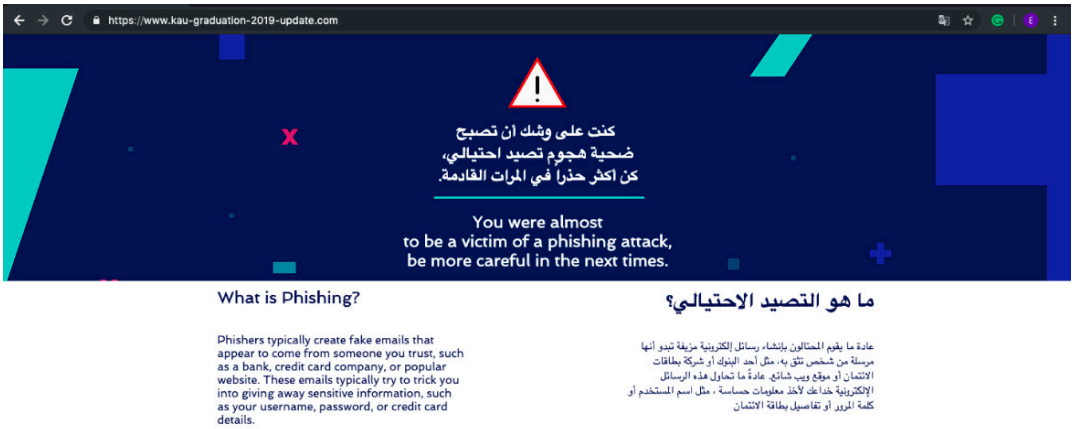

Figure 6. Awareness page for e-mail phishing.

Figure 7. Phishing e-mail.

4.2. Structure of the 'Awareness Page' of the Phishing Website

The link in the email was https://www.kau-graduation-2019-update.com/, and it can be noticed that the keywords were intentionally selected to deceive the victims regarding the authenticity of the link. The domain name was purchased from *wix.com* for the awareness page. The purpose of the awareness page was to briefly explain to the victims the situation. As can be seen in Figure 8, the page was constructed as an educational infographic to indicate that this e-mail should be considered a phishing attack. The page contained the definition of a phishing attack (Figure 6), and the instructions were labelled in the fake e-mail, so that the recognition process for phishing emails can be easily demonstrated. Moreover, one of the reasons for selecting *wix.com* is that it provides analytics applications with useful features, such as website traffic statistics and visitor behaviour analytics. These tools assisted in analysing the daily website visitors and counting the number of victims who clicked on the fake link.

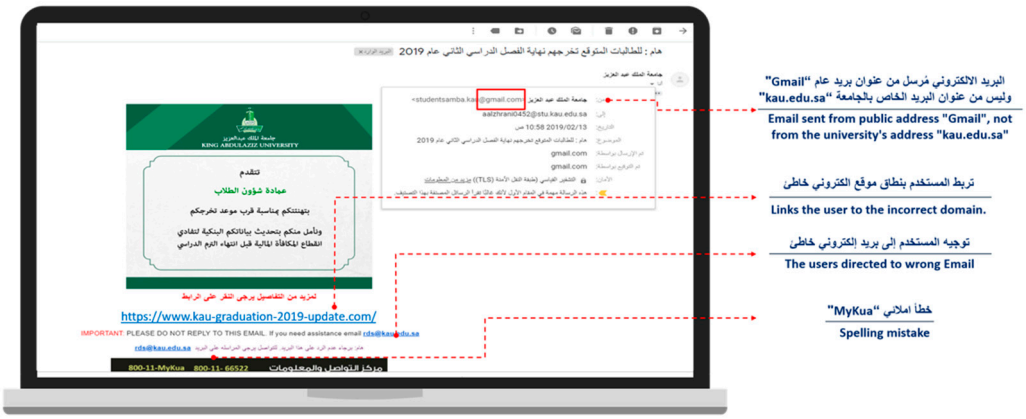

Figure 8. Educational infographic in the awareness page.

4.3. Result of Spear-Phishing Email

This experiment was launched on Sunday 26th March 2020 at 01:36 pm with a duration of four days. The total number of clicks on the fake link on the first day reached 36 (27% of the 165 students), whereas the total number of victims for the other days decreased gradually (i.e., on the second, third, and fourth day, it was 20, 10 and 3, respectively), as shown in Figure 9. It is important to emphasise that no information was collected or compromised in this experiment; on the contrary, this experiment increased the participants' knowledge and awareness regarding e-mail phishing attacks.

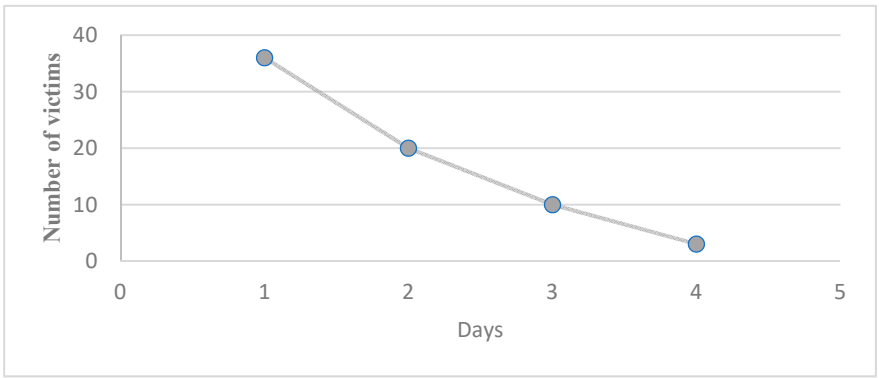

Figure 9. Number of victims per day.

5. Social Networking-Based Phishing Attack Simulation

Web 2.0 technologies have revolutionised the Internet. Recently, phishers have taken advantage of these technologies and deployed their attacks through social media such as Twitter, Instagram,

WhatsApp and LinkedIn. Typically, they claim to be trustworthy people or legitimate businesses so that they can steal valuable information from users, such as national ID numbers, credit card numbers, login IDs, and passwords. This scam is called social networking-based phishing, SNP for short. [14,15,24].

Steps of Social-Networking Phishing Simulation

This experiment simulates the phisher' steps to launch SNP attack. The purpose of this simulation is not to forge a legitimate website; rather, we set up a scam website for a non-existent car company called '*Madar*'. We ensured that there was no official car company in Saudi Arabia by that name. The website template was customised and designed through the *Wix* website builder, and the domain https://www.madarcarrental.com/ was used for this simulation. Furthermore, we added a desirable security feature, namely, the SSL green lock icon, to the URL bar. This technique was used to improve the authenticity of the website and to gain the victims' trust.

The SSL/TLS and HTTPS protocols have been recognised as an essential part of digital security. The goal of these protocols is to ensure the authenticity and confidentiality of TCP connections and provide encryption for secure communication [20,23,24]. A major misconception among end users is that a website is considered trustworthy if the HTTPS or SSL lock icons appear. However, the existence of the HTTPS and SSL locks are not sufficient indicators of website legitimacy. In fact, they only indicate that the transmitted data between the users' web browser and the website are encrypted to prevent a third party from accessing and eavesdropping on the channel. In this case, the website could be malicious and pose threats [25–28]. Unfortunately, 49.4% of the phishing sites in the third quarter of 2018 were using HTTPS, representing an increase by 35% from the previous quarter according to the PhishLabs study, as shown in Figure 10 [29]. Nevertheless, one of the motivations of this simulation is to measure this type of user knowledge.

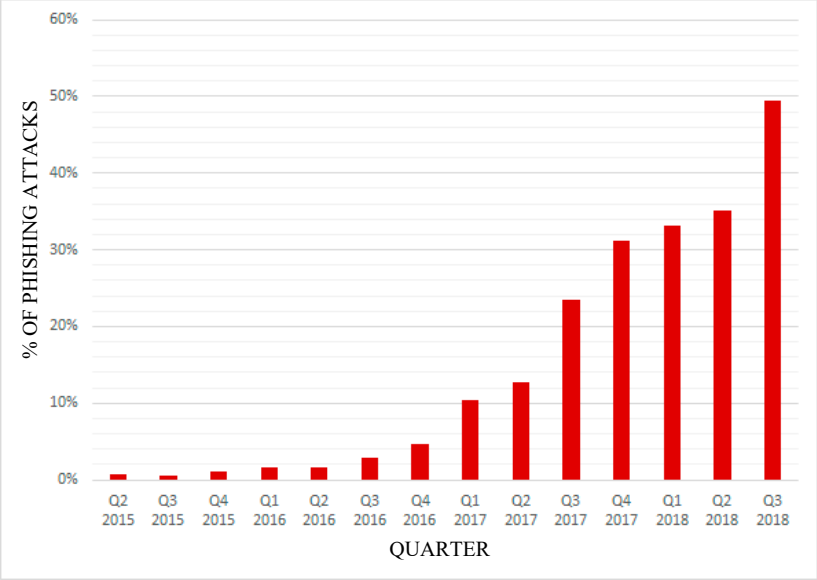

Figure 10. Percentage of phishing sites that use HTTPS.

The phishing attack life cycle used in this simulation is shown in Figure 11. The steps were adopted from [30], but some significant modifications were applied to adapt to the context of the present experiment.

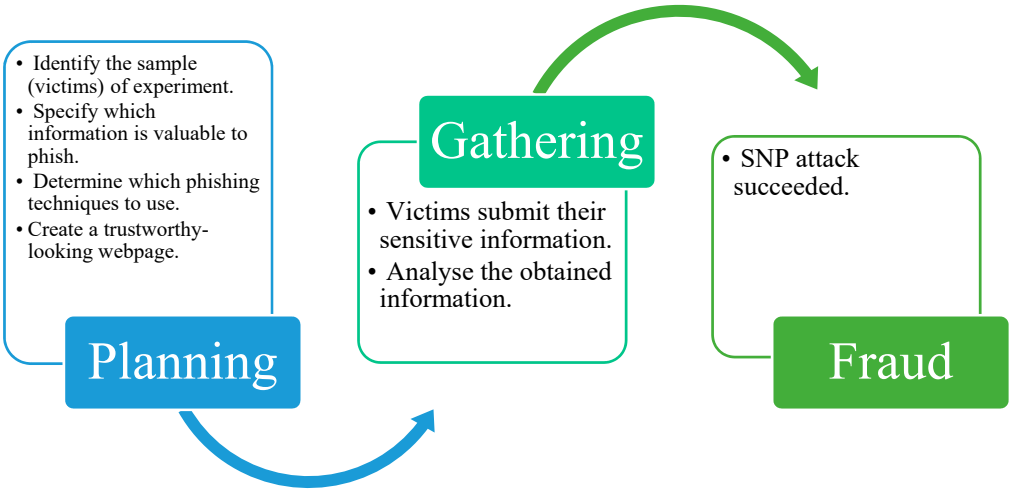

Figure 11. Methodology of the SNP experiment.

Planning: The target sample for this attack simulation was randomly selected by publishing the scam website on social networking platforms. The scenario for this phishing attack is to attract visitors' attention by claiming that *Madar* was founded in 1969 and has gained the reputation of providing reliable service. On the occasion of its anniversary, the company wishes to celebrate by organizing a grand prize drawing. To participate, the visitors were requested to fill in and submit the following information (Figure 12):

- Full name
- Contact number
- National ID or Iqama Number
- City
- Occupation

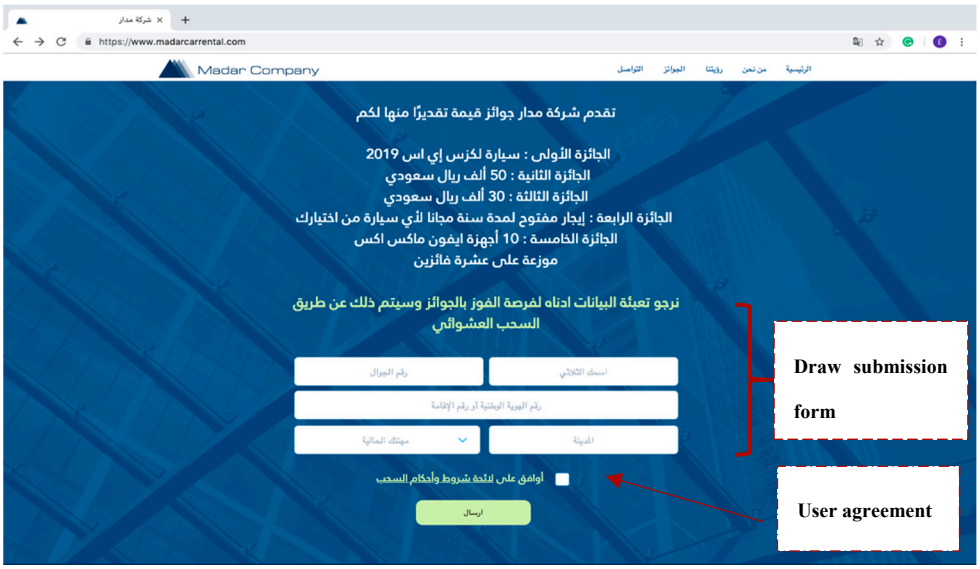

Figure 12. Grand prize drawing page of the 'Madar' website.

To conduct this experiment in an ethical manner, the visitors must agree to the listed terms and conditions before they submit the requested information. An important condition is that "I agree to providing my personal information, and after submission, I waive any rights regarding this

information". In addition, the national ID numbers are masked and removed from the database immediately. Once visitors click on the submit button, a warning page appears to inform them that the website is a phishing attack, and the Madar company does not exist. Then, we explain preventing measures against this attack, as shown in Figure 13.

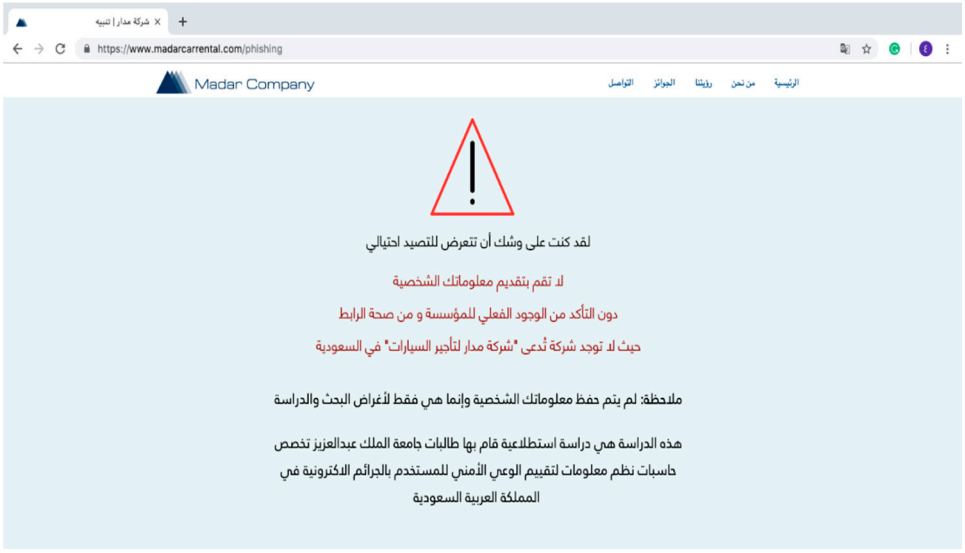

Figure 13. Warning page for the 'Madar' website.

Gathering: We first crafted a scam message containing the URL of the Madar website. This message was subsequently distributed to WhatsApp and Telegram groups, and on Facebook on 3 March 2020. Data collection terminated on 12 March 2020. The number of visitors during this period was 342. As the number of victims was 160, 47% of the visitors were exposed to the phishing attack. Most victims were higher-education students, at a rate of 37%, as shown in Figure 14.

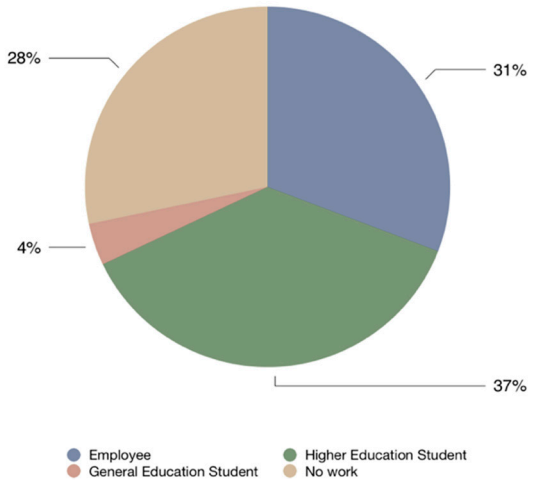

Figure 14. Distribution of victims' occupation.

Ten days after the attack was launched, there was a significant decrease in the daily number of visitors and victims, as shown in Figure 15. The reason for this decline reflects the victims' behaviour in social media, where the victims warned others from checking this website.

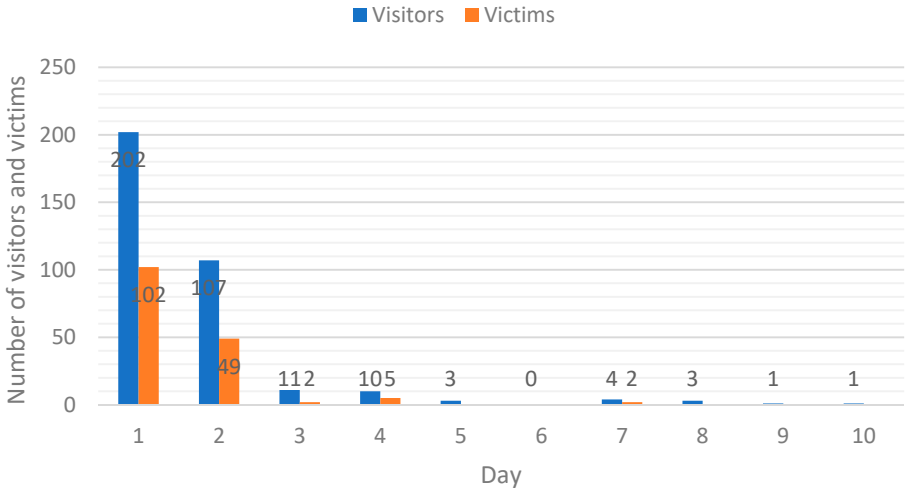

Figure 15. Number of visitors and victims during the attack.

Fraud: The phishing attack simulation was a successful experiment, as the attack affected different areas in Saudi Arabia, as shown in the map in Figure 16. The spread pattern clearly demonstrates that social media can contribute to the rapidly spreading of messages. In the fraud phase, we observed how the phishers can achieve their goals simply by deceiving the victims to willingly submit their credentials or sensitive information. This illegal action allows the phisher to commit criminal offences, such as false impersonation and selling the victims' sensitive information in black markets.

Figure 16. Spreading of the attack in Saudi Arabia.

6. Discussion

The experiment was designed to test and evaluate the assumption that end users in Saudi Arabia do not have sufficient knowledge and lack the ability to protect themselves against cyberattacks. In the attack simulation phase, we conducted a phishing attack through three experiments: clone phishing, spear-phishing, and SNP. Also, we applied different types of influence techniques to persuade the victims. In the clone phishing experiment (cloned KAU website), the simulation revealed that 77% of the participants fell victim to this attack. Most of the victims were students. In addition, occupation and the probability of exposure to a phishing attack are uncorrelated. In spear phishing, the phishing email was sent to 165 students. Forty-five students (27%) clicked on the attached link. Finally, in SNP (Madar website), the attack simulation indicated that 47% of the visitors disclosed sensitive personal information even though most of them had a higher education degree. We developed a systematic approach for different attack techniques to validate this hypothesis. Based on the results obtained from the three attack simulations, we were able to confirm the need to improve cybersecurity knowledge and establish that cybersecurity awareness programs are indeed crucial. We live in an era in which

technologies take over our lives. Thus, it is essential to ensure that individuals are fully aware of security risks, and this is more likely to occur after their privacy is violated.

When launching phishing attacks, cyber criminals usually attempt to tempt their victims either by using influence techniques to attract their attention or by presenting a context that appears feasible and realistic. According to Lawson et al. [31], there are various persuasion principles and strategies that can be employed to persuade a target. The most effective influence techniques used in phishing attacks are [31,32]:

- *Commitment/consistency*: the concept of completing an action you previously initiated.
- *Liking*: trust due to a prior interaction or familiarity, such as for a largely recognizable brand.
- *Authority*: an authority figure mandating an action, with consequences for failing to comply.
- *Scarcity*: a short and specific time frame to complete an action.

Thus, cyber criminals have a tendency to opt for personalised rather than generic attacks. Table 3 summarises the three attack simulations according to phishing type, technical approaches, type of influence technique, authenticity features and the real impact of other cyberattacks if the phishing attacks were successful.

Table 3. Summary of phishing attack simulations.

Experiment	Phishing Type	Techniques	Type of Influence Technique	Authenticity Features	Other Cyber Threats Associated with Phishing Attack
Attack simulation 1	Website forgery	Cloning tools Domain squatting	Invoke a sense of Commitment and liking	Authentic appearance Presence of SSL	Man-in-the-middle (MITM) Watering hole attack (WHA) Cross-site scripting (XSS) Data breach
Attack simulation 2	Spear email phishing	Domain squatting	Invoke a sense of urgency and scarcity	Authentic appearance Presence of SSL	Botnets Watering hole attack (WHA) Dynamic malware Data breach
Attack simulation 3	Social networking phishing	NA	Promising monetary/prize reward	Presence of SSL	Cross-site scripting (XSS) Watering hole attack (WHA) Dynamic malware Blend malicious code Data breach

The past decade has seen the rapid development of anti-phishing approaches based on artificial intelligent and machine learning-based detection systems. The most widely deployed anti-phishing solutions focus on the phishing detection system accuracy by proposing novel features or optimising classification algorithms [33,34]. For example, Sahingoz et al. [35] proposed a real-time anti-phishing system, which uses seven different classification algorithms and natural language processing (NLP) based features. Another approach was developed by Jain and Gupta [36] that can detect phishing websites using the hyperlink information present in the source code of the website, while other studies focused on exploit state of the art machine learning algorithms to build models using indicators to detect phishing activities [37] and apply data-driven intelligent decision making for protecting the systems from cyber-attacks [38].

To conclude, end users would fall victim to phishing attacks if they do not have adequate security knowledge and security awareness regardless of their educational background, qualifications, occupation, age, or gender. One of the misconceptions that we noted was that the behaviour of end users is often related to the presence of technical safeguards. For example, they trust that keeping anti-virus software up to date and using SSL/HTTPS can prevent cyber attackers. Unfortunately, technology alone cannot withstand cyberattacks. The impacts of successful phishing attacks can be

serious. These attacks could lead to data loss, credential and account compromise, financial loss and fraud and malware infection.

7. Related Works

In this section, we review the recent phishing attack experiments that are based on real attack simulations such as spear phishing attacks and email phishing attacks. Most of related works associated with this literature indicates the users are prone to phishing attacks and the degree varies depending on the user's background and behaviours.

Alseadoon et al. [39] conducted a study to investigate whether users in Saudi Arabia are more vulnerable to phishing attacks. The experiment targeted undergraduate students within the 18−25 age group using phishing email. The idea of the phishing email was to inform the students that it has been a technical issue with the university system that caused disruption and loss of data. Whoever received this email, they were affected, and they must act fast and provide their information either by accessing the link or replying to the email sender. Finally, the fabricated email was signed by an authentic IT specialist along with university logo. The researchers divided the collected sample into two groups based on the participants' action, click or reply. The experiment revealed 7% of students responded to the attack by replying to the email with the requested information whereas the majority 86% clicked on the link attached to the phishing email. Another experiment conducted by Alghazo and Kazimi [40] targeting 200 university students in the Eastern Province of Saudi Arabia within the 18−25 age group. The researchers constructed a fake eBay webpage and hosted it in a local server and post shortcut icon on the desktop. The attack was carried out in a controlled computer lab where the students were asked to click on the fake eBay and provide their credentials for login. Once the participants trusted the webpage and entered their username and password, their credentials were saved in the database and the participant were redirected to the authentic eBay website. This attack performed in the experiment was a man-in-the-middle phishing attack. Afterwards, the participants were asked to fill in a survey to analyse their behaviours. The survey focused on two main concerns: (1) the general appearance of the website, which includes website authenticity, graphics and fonts quality, and the validity of the URL; (2) the sudden URL forwarding, which involves understanding participants' judgement when URL redirecting to the original website. The finding shows that more than 90% of participants believed that the fake eBay was genuine even though it contained low quality graphics, the overall appearance was slightly different than the original, and the URL was incorrect. With regard to being redirected again to the original eBay website after successfully attempting login to the phishing website, around 60% responded that this occurred due to a server error while the rest thought the process seemed suspicious.

Hwartfield et al. [41] studied the feasibility of predicting user susceptibility using deception-based attacks. The researchers conducted two experiments, each consisting a survey and an exhibit-based test, asking participants to distinguish between attack and non-attack exhibit. Using the data collected from both experiments, they discovered practical predictors of users' susceptibility against semantic attacks by employing a logistic regression and a random forest prediction model. They indicated that users are able to detect deception attempts with security training. Moreover, they emphasized that other features can contribute as well such as computer literacy, familiarity and frequency of access to a specific platform. Williams et al. [42] explored employee susceptibility of spear phishing in the UK using a mixed methods approach. The experiment conducted nine spear phishing simulation emails sent to 62,000 employees over a six-week period. All emails contained the following information: (1) addressing the individual recipient by the first name (e.g., 'Dear John'); (2) a corresponding logo related to the fictitious organization; (3) a link; and (4) a message to provoke a response using authority or urgency cues. If recipients clicked on the link, they were automatically directed to an internal educational material. The results demonstrated that the presence of authority, urgency, offering a reward, or threating has significant impact susceptibility to phishing attacks. [42,43] Chatchalermpun et al. [44] conducted a pilot study about cybersecurity drill tests within a large financial services company in Thailand using phishing emails. The simulation attack was sent to more than 21,000 users nationwide

including executives and employees. Two types of phishing employed in the cybersecurity drill, spear phishing targeting employees and whaling targeting executives. The result revealed that 73% of executives and 77% of employees ignored the phishing emails, whereas, 12% of executives and 15% of employees opened, clicked and filled-in the password.

The only works on phishing attack simulation in Saudi Arabia other than this paper are Alseadoon et al. [39] and Alghazo et al. [40]. Table 4 demonstrated a brief comparison of phishing attack simulations conducted in Saudi Arabia.

Table 4. Comparison of phishing attack simulations conducted in Saudi Arabia.

		Sample Size	Gender	Age Group	Type of Phishing	Authentic Appearance	DNS Squatting	SSL
Alseadoon et al. (2012)		200	-	18–25	Spear email phishing	Yes	Yes	No
Alghazo et al. (2013)		200	Male	18–25	Website forgery	Yes, but with low quality graphics	Yes	No
Our experiment	Simulation 1	66	Female	17>	Website forgery	Yes	Yes	Yes
	Simulation 2	165	Female	18–25	Spear email phishing	Yes	Yes	Yes
	Simulation 3	342	Both	all	Social networking phishing	NA	NA	Yes

8. Conclusions

We presented an experiment conducted in Saudi Arabia to assess and measure the security awareness of end users in Saudi Arabia. Three types of phishing attacks were carefully selected based on the attack types most commonly used in Saudi Arabia: clone phishing, email phishing, and SNP. Subsequently, we described and analysed these attacks through simulation using appropriate tools and techniques. Results indicate that the presence of authentic design and the type of influence technique employed can significantly affect the users' judgments. In addition, we demonstrated that users can easily fall victim to such attacks if they are not sufficiently knowledgeable to make good judgments in cyberspace. This is due to the lack of cybersecurity awareness and education as well as to relying on technical safeguards. Security awareness should become a new culture and must be taught at a very young age to improve cyber awareness and develop sustainable safe cyber behaviour. Passive awareness through, for example, emails, newsletters, and SMS notifications is not sufficient. Moreover, integrated proactive training programmes targeted at different age groups are necessary, which can be taught in schools, universities, and organizations. It is essential to conduct a thorough understanding of the combination of different technical approaches to help developing a more effective anti-phishing technique.

Author Contributions: Conceptualization, D.A.; formal analysis, D.A., A.A., M.A. and O.A.; investigation, D.A., A.A., M.A. and O.A.; software, A.A., M.A. and O.A.; supervision, D.A.; writing—original draft, D.A., A.A., M.A. and O.A.; writing—review & editing, D.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: A sincere thank you to all the reviewers for their constructive review and comments. The reviews are detailed and helpful to improve and finalize the manuscript. The authors are highly grateful to them.

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

References

1. Al-Khater, W.A.; Al-Maadeed, S.; Ahmed, A.A.; Sadiq, A.S.; Khan, M.K. Comprehensive Review of Cybercrime Detection Techniques. *IEEE Access* **2020**, *8*, 137293–137311. [CrossRef]
2. Joseph, D.P.; Norman, J. An analysis of digital forensics in cyber security. In *First International Conference on Artificial Intelligence and Cognitive Computing*; Springer: Singapore, 2019; pp. 701–708.
3. Hakar, H.K.; Joshi, R.A.; Dobariya, A. An Analysis on Scope of Cyber Security. In Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 13–15 March 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 612–615.
4. Leukfeldt, R.; Holt, T.J. (Eds.) *The Human Factor of Cybercrime*; Routledge: Abingdon, UK, 2019.
5. Kahimise, J.; Shava, F.B. An analysis of children's online activities and behaviours that expose them to cybercrimes. In Proceedings of the 2019 27th Telecommunications Forum (TELFOR), Belgrade, Serbia, 26–27 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–4.
6. Arora, B. Exploring and analyzing internet crimes and their behaviours. *Perspect. Sci.* **2016**, *8*, 540–542. [CrossRef]
7. Surwade, A.U. Phishing e-mail is an increasing menace. *Int. J. Inf. Technol.* **2020**, *12*, 611–617. [CrossRef]
8. Furnell, S.; Millet, K.; Papadaki, M. Fifteen years of phishing: Can technology save us? *Comput. Fraud. Secur.* **2019**, *2019*, 11–16. [CrossRef]
9. APWG. Phishing Activity Trends Report: 3rd Quarter 2017. Anti-Phishing Working Group, Retrieved 30 April 2018. p. 2018. Available online: https://docs.apwg.org//reports/apwg_trends_report_q3_2017.pdf (accessed on 24 November 2020).
10. Vijayalakshmi, M.; Shalinie, S.M.; Yang, M.H. Web phishing detection techniques: A survey on the state-of-the-art, taxonomy and future directions. *IET Netw.* **2020**, *9*, 235–246. [CrossRef]
11. Banu, M.N.; Banu, S.M. A comprehensive study of phishing attacks. *Int. J. Comput. Sci. Inf. Technol.* **2013**, *4*, 783–786.
12. Ozkaya, E. *Learn Social Engineering: Learn the Art of Human Hacking with an Internationally Renowned Expert*; Packt Publishing Ltd.: Birmingham, UK, 2018.
13. Bossetta, M. The weaponization of social media: Spear phishing and cyberattacks on democracy. *J. Int. Aff.* **2018**, *71*, 97–106.
14. Bhavsar, V.; Kadlak, A.; Sharma, S. Study on phishing attacks. *Int. J. Comput. Appl.* **2018**, *182*, 27–29. [CrossRef]
15. Vishwanath, A. Getting phished on social media. *Decis. Support Syst.* **2017**, *103*, 70–81. [CrossRef]
16. Anson, S. *Applied Incident Response*; John Wiley & Sons: Hoboken, NJ, USA, 2020.
17. Allen, J.; Yang, Z.; Landen, M.; Bhat, R.; Grover, H.; Chang, A.; Ji, Y.; Perdisci, R.; Lee, W. Mnemosyne: An Effective and Efficient Postmortem Watering Hole Attack Investigation System. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, 9–13 November 2020; pp. 787–802.
18. O'Leary, D.E. What phishing e-mails reveal: An exploratory analysis of phishing attempts using text analysis. *J. Inf. Syst.* **2019**, *33*, 285–307. [CrossRef]
19. HTTrack. HTTrack Website Copier. 2017. Available online: https://www.httrack.com/ (accessed on 2 April 2020).
20. Alsharnouby, M.; Alaca, F.; Chiasson, S. Why phishing still works: User strategies for combating phishing attacks. *Int. J. Hum. Comput. Stud.* **2015**, *82*, 69–82. [CrossRef]
21. Kintis, P.; Miramirkhani, N.; Lever, C.; Chen, Y.; Romero-Gómez, R.; Pitropakis, N.; Nikiforakis, N.; Antonakakis, M. Hiding in plain sight: A longitudinal study of combosquatting abuse. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 569–586.
22. Statistics Solutions. Using Chi-Square Statistic in Research. 2019. Available online: https://www.statisticssolutions.com/using-chi-square-statistic-in-research/ (accessed on 2 April 2020).
23. Pagliery, J. The Inside Story of the Biggest Hack in History. 2015. Available online: https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html (accessed on 27 January 2019).
24. Yacowenia, A. Social Networking Sites: The Malicious Use. Ph.D. Thesis, Utica College, New York, NY, USA, 2020.
25. Naylor, D.; Finamore, A.; Leontiadis, I.; Grunenberger, Y.; Mellia, M.; Munafò, M.; Papagiannaki, K.; Steenkiste, P. The cost of the "s" in https. In Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies, Sydney, Australia, 2 December 2014; pp. 133–140.

26. Maimon, D.; Wu, Y.; McGuire, M.; Stubler, N.; Qui, Z. SSL/TLS Certificates and Their Prevalence on the Dark Web (First Report). 2019. Available online: https://www.venafi.com/sites/default/files/2019-02/Dark-Web-WP.pdf (accessed on 25 November 2020).
27. Xiao, C.; Zhang, L.; Liu, W.; Bergmann, N.; Xie, Y. Energy-efficient crypto acceleration with HW/SW co-design for HTTPS. *Future Gener. Comput. Syst.* **2019**, *96*, 336–347. [CrossRef]
28. Kraus, L.; Ukrop, M.; Matyas, V.; Fiebig, T. Evolution of SSL/TLS Indicators and Warnings in Web Browsers. In *Security Protocols XXVII. Security Protocols 2019. Lecture Notes in Computer Science*; Anderson, J., Stajano, F., Christianson, B., Matyáš, V., Eds.; Springer: Cham, Switzerland, 2020; Volume 12287.
29. Volkman, E. 49 Percent of Phishing Sites Now Use HTTPS. 2018. Available online: https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https (accessed on 25 November 2020).
30. Mohammad, R.M.; Thabtah, F.; McCluskey, L. Tutorial and critical analysis of phishing websites methods. *Comput. Sci. Rev.* **2015**, *17*, 1–24. [CrossRef]
31. Lawson, P.; Pearson, C.J.; Crowson, A.; Mayhorn, C.B. Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Appl. Ergon.* **2020**, *86*, 103084. [CrossRef] [PubMed]
32. Cialdini, R.B. *Influence: The Psychology of Persuasion*; Collins: New York, NY, USA, 2007; Volume 55, p. 339.
33. Mohammad, R.M.; Thabtah, F.; McCluskey, L. An assessment of features related to phishing websites using an automated technique. In Proceedings of the 2012 International Conference for Internet Technology and Secured Transactions, London, UK, 10–12 December 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 492–497.
34. Chiew, K.L.; Tan, C.L.; Wong, K.; Yong, K.S.; Tiong, W.K. A new hybrid ensemble feature selection framework for machine learning-based phishing detection system. *Inf. Sci.* **2019**, *484*, 153–166. [CrossRef]
35. Sahingoz, O.K.; Buber, E.; Demir, O.; Diri, B. Machine learning based phishing detection from URLs. *Expert Syst. Appl.* **2019**, *117*, 345–357. [CrossRef]
36. Jain, A.K.; Gupta, B.B. A machine learning based approach for phishing detection using hyperlinks information. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 2015–2028. [CrossRef]
37. Cuzzocrea, A.; Martinelli, F.; Mercaldo, F. Applying Machine Learning Techniques to Detect and Analyze Web Phishing Attacks. In Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services, Yogyakarta, Indonesia, 19–21 November 2018; pp. 355–359.
38. Sarker, I.H.; Kayes, A.S.M.; Badsha, S.; Alqahtani, H.; Watters, P.; Ng, A. Cybersecurity data science: An overview from machine learning perspective. *J. Big Data* **2020**, *7*, 41. [CrossRef]
39. Alseadoon, I.; Chan, T.; Foo, E.; Gonzalez Nieto, J. Who is More Susceptible to Phishing Emails? A Saudi Arabian Study. In Proceedings of the 23rd Australasian Conference on Information Systems, Geelong, Australia, 3–5 December 2012.
40. Alghazo, J.M.; Kazimi, Z. Social Engineering in Phishing Attacks in the Eastern Province of Saudi Arabia. *Asian J. Inf. Technol.* **2013**, *12*, 91–98.
41. Heartfield, R.; Loukas, G.; Gan, D. You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks. *IEEE Access* **2016**, *4*, 6910–6928. [CrossRef]
42. Williams, E.J.; Hinds, J.; Joinson, A.N. Exploring susceptibility to phishing in the workplace. *Int. J. Hum. Comput. Stud.* **2018**, *120*, 1–13. [CrossRef]
43. 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.* **2019**, *38*, 184–197. [CrossRef]
44. Chatchalermpun, S.; Wuttidittachotti, P.; Daengsi, T. Cybersecurity Drill Test Using Phishing Attack: A Pilot Study of a Large Financial Services Firm in Thailand. In Proceedings of the 2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE), Malaysia, 18–19 April 2020. [CrossRef]