Swinburne University Of Technology

School of Science, Computing, and Engineering Technologies

ASSIGNMENT AND PROJECT COVER SHEET

Unit Code: COS30015 Unit Title: IT SECURITY

Assignment number and title: RESEARCH REPORT- ASSIGNMENT 1

Due date: **24 SEPT 2024**

Lab Group: Tutor: Lecturer: FAIZAL ALIAS

Family name: KING Identity no: J23039507

Other names: JOSHUA SANJAY

To be completed if this is an INDIVIDUAL ASSIGNMENT

I declare that this assignment is my individual work. I have not worked collaboratively nor have I copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for me by another person.

Signature: JSK

To be completed if this is a GROUP ASSIGNMENT

We declare that this is a group assignment and that no part of this submission has been copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for us by another person.

ID Number	Name	Signature

HD Assignment - Phishing Activities Detection

Introduction

Phishing attacks has been a rampant and lucrative crime that has been around since the dawn of Internet. Over time, these attacks have become an alarming threat to an individual's, corporate sector and even government agencies. The definition of phishing is illegally obtaining and using somebody's detail (etc. credit card details, bank details, passwords) to steal money or using their identification to perform crimes on the attacker's behalf. The attackers, or also known as *phishers*, use social engineering tactics to trick their victims by designing websites similar to trusted and legitimate organisations and asking users to enter their credentials so that the phishers would be able to receive the victim's details and hack their personal accounts.

This paper aims to analyse the key research challenges being solved within the phishing detection space, highlighting major themes such as real-time detection, model adaptation, and the use of advanced machine learning techniques. Despite significant progress, several issues remain unsolved, particularly the difficulty in handling zero-day attacks and the limitations of training data. The role of data in these challenges is paramount, influencing both the accuracy of detection models and their adaptability to new threats.

Additionally, the impact of time on research methodologies and results will be explored, assessing how advances in phishing tactics necessitate changes in detection approaches. This paper will also examine whether these tasks can be fully automated or if a human analyst still plays a critical role. Finally, the essay will consider which machine learning techniques are best suited to address the phishing detection problem, evaluating both their effectiveness and limitations in this domain.

Key research themes within phishing detection space

It is crucial to note the importance of cybersecurity as phishing attacks in today's times have evolved and cost not only the privacy of the victims, but some even lose huge monetary value as according Microsoft Safer security Index's report in 2014, phishers has scammed a total of $5 billion dollars alone [1]. The detection and prevention of phishing attacks is an ongoing challenge in cybersecurity, and researchers are actively working to address various aspects of the problem. In this report, **phishing emails** will be discussed as it is the most common phishing method.

Phishing emails is an attack that relies heavily on social engineering tactics, convincing users to follow the provided instructions, often without noticing subtle red flags such as mismatched email addresses or suspicious links.To summarise the findings on the topic of spoofed emails *(Defending against phishing attacks: taxonomy of methods, current issues and future directions,2018)*, also known as phishing emails, are sent from phishers with the intention of tricking their potential victims into clicking URLs that are malicious and stealing their credentials. These emails typically disguise themselves as trusted organisations and request the victims to follow the instructions provided by them. [2]

"Phishing environments, techniques, and countermeasures: A survey" elaborates the elements of a typical malicious URL that would be found in phishing emails are: having bad domain names, shortened URLs, host name obfuscation, and encoded URL obfuscation [3]. As researchers found the common elements, they have developed a THEMIS model that improves email detection by analysing the structure of emails, its header and body, and characters. This model would be a good countermeasure as it would be able to detect suspicious and common patterns from the features of the emails [4].

In addition to standard spoofed emails, there are a few attacks related to phishing emails and in this paragraph onwards, the term **spear phishing** and **whaling** will be introduced. A key challenge in the phishing detection space is effectively identifying spear phishing and whaling attacks, which involve social engineering tactics. Spear fishing, another attack related to phishing emails, individually selects its victims such as employees or customers of a specific organisation. This attack uses the crafting of impersonating a trusted person or organisation with the intention of requesting readers to take action by clicking on a malicious link, downloading viruses or entering credentials for the sake of stealing sensitive information. Data from *"Going Spear Phishing: Exploring Embedded Training and Awareness"* shows the loss from this attack which can exceed beyond a $100 million. [5] This kind of attack is effective within a workplace

environment where vast volumes of emails are exchanged within a day and many would unknowingly fall prey to phishing attacks by clicking links or complying with instructions from impersonated profiles.

Whaling is a form of spear phishing which targets the individual with the highest authority in an organisation and use social engineering tactics to deceive victims into revealing sensitive information such as employee or bank credentials. An example of a life real occurrence happened in 2015, where Hillary Clinton's presidential campaign chairman was hacked by a phishing email sent to his personal email which tricked him into entering his login credentials [6].

These attacks have been made clear that it is dangerous, as described in the paper *"Fighting Against Phishing Attacks: State of Art and Future Challenges"* [7]. Addressing these challenges requires advanced detection methods that would be able to capture features of common phishing. There have been various countermeasures developed to counteract phishing emails**. Authentication-based** can be considered an effective countermeasure according to *"A Survey of Phishing Email Filtering Techniques"*, as these methods help verify if the email was sent from a claimed sender, which reduces the risk of being phished. In addition, authentication mechanisms, especially digital signatures have a low probability of being replicated by attackers [8].

Another countermeasure discussed in the report *"Systematization of Knowledge (SoK): A Systematic Review of Software-Based Web Phishing Detection",* implemented **filtering techniques in email servers** such as URL-based lexical features examine the URL links contained in emails analyses the URL length, the number of subdomains and the use of HTTPS to determine phishing content. Having this tool can reduce phishing attacks as it prevents users from ever clicking the links in the first place [9].

Key research themes within phishing detection space that remain unsolved

Cybersecurity has been evolving and it had been noted that researchers developed various measures to prevent phishing emails and to a certain extent it has successfully diverted the consequences, however there is still unsolved issues in phishing detection space meaning there isn't a cure to this epidemic. As a result, phishing will continue to affect its victims. In this section, numerous issues will be discussed.

The first issue that will be examined is **zero-day phishing**. *"A Survey of Phishing Email Filtering Techniques"* provides a clear definition of this attack, explaining that this phishing attack has not been trained on old data samples and is able to bypass detection systems [8]. In addition, the report: *"Machine learning based phishing detection from URLs"* provide features of this attack: firstly, these phishing attacks are evolving rapidly, and it is difficult for detection systems to keep up as phishers use techniques like changing IP addresses and obfuscating URLs. To elaborate on the point of obfuscating URLs, PhishIntention wouldn't be able to detect it uses a computer vision model rather than relying on the HTML code. In addition, it should be noted that these machine learning systems for detection don't rely on up-to-date datasets therefore not being able to new phishing tactics employed [10]. Studies in "*Phishing Environments, Techniques, and Countermeasures: A Survey"* highlights that less than 20% of detection systems were able to stop zero-day phishing that was developed in the first day and it can take as long as 12 hours for over 50% of these phishing sites to be added to the blacklist which leaves many people vulnerable to zero-day attack [3].

Another issue is **evasion techniques** that prevent real-time detection. A report *"Inferring Phishing Intention via Webpage Appearance and Dynamics"* provides a well-rounded summary of issues with real time detection. The report explains that a detection model called PhishIntention analyses web pages appearance, logos and credential-taking intentions however this model would face challenges which leaves vulnerabilities open to potential victims. Phishing websites often employ CAPTCHA, a tool to prevent bot attacks, which blocks automated systems like PhishIntention from proceeding. In addition, phishing pages may shut down before the detection system can interact as the current systems sometimes causes delay, limiting the effectiveness of real-time detection. Attackers exploit these weaknesses as there isn't a model that is able to detect zero-day phishing immediately [11].

AI has recently been a great tool for improving the defences of phishing however AI also have the capabilities to be weaponised and can be a great tool for hackers and even criminals who have limited knowledge on technology, and in addition, AI has the ability to learn and adapt in real-time, which would be able to bypass detection systems that rely on old data. The report *"Weaponized AI for Cyber Attacks"* explores how AI can be misused and the threats it poses to the cybersecurity space. An experiment within the report was conducted to test the phishing skills of AI and it was able to produce a realistic looking phishing website. Furthermore, it was able to produce content fake content that bypasses detection systems that use old data. The report also highlights the risk of AI being involved with military systems with can improve the quality of them cyberattack which could lead to an amplified consequence [12]. Another report detailing the weaponised AI *"Social Engineering with ChatGPT"* shows that CHATGPT was able to detect malicious intentions requested from the user however these warnings were not able to stop attackers from proceeding with their intentions [13].It should be noted that AI nowadays is accessible to the public and it can be fed with malicious data which can be used as a weapon in the wrong hands.

Lastly**, user education** is the key factor that can prevent phishing attacks as these attacks are socially engineered tactics aimed to exploit the vulnerabilities of humans and not systems. There have measures to raise awareness and educate users on the topic however despite these attempts, phishing could never be fully prevented. For reference, *"Phishing Detection: A Literature Survey"* highlights the unresolved issues on the matter. In a study, 29 % of users who were trained by the best awareness groups had been undetectably phished. This shows that training alone is not sufficient as users may not be able retain their knowledge to apply in real-life situations. Phishing detection detections still heavily rely on users to act correctly by recognising phishing emails or reporting them however users would frequently ignore these warnings and undermine the effectiveness of user education [14].

Relevance of data being used in real-world phishing attacks

The effectiveness of phishing detection systems largely relies on the quality and relevance of data being used. Phishing tactics are constantly evolving to exploit new vulnerabilities and avoiding detection. Therefore, up-to-date data is crucial for ensuring that new emerging threats would not be able to bypass the detection systems. The lack of relevant data is the reason behind the unresolved or ongoing issues in the cybersecurity detection space, leaving users vulnerable to the current attacks. In this section, the importance of real-world and current data will be analysed with examples from recent studies showing the effectiveness of detection systems equipped with relevant data.

A prime example is from the authors *"Catching Phishers by Their Bait: Investigating the Dutch Phishing Landscape through Phishing Kit Detection",* where the researchers had **collected real-world data** from a phishing live campaign in the Dutch financial sector. The data collected included 70 phishing kits and 10 different phishing kit families. In addition, the study had successfully monitored 1,363 phishing domains between September 2020 and January 2021. This real-time monitoring had help detect the attacks and the researchers had also TLS certificates from the phishing domains to identify and track malicious domains as they emerge, which shows that detection is far more effective when current time data is acquired by cybersecurity analyst and detection systems. [15].

Another research *"Sunrise to Sunset: Analysing the End-to-End Life Cycle and Effectiveness of Phishing Attacks at Scale"* **monitored over 400,000 phishing websites and recorded that 4.8 million victims were affected**. These phishing attacks are short-lived with an average campaign lasting 21 hours and strongly effective. Detection by anti-phishing systems typically occurs 9 hours after its first victim visit, leaving attackers a time opportunity window known as “golden hours” to scam their victims. Moreover, the research found that just 10 % of most successful phishing sites are responsible for more than 80% of phishing victims. This highlights the importance of having real time data as using outdated data is less effective in combating the phishing space. If detection is delayed, the attack would have moved on and affect victims [16].

The paper *"Inferring Phishing Intention via Webpage Appearance and Dynamics"* elaborates on phishing detection methods that detects phishing pages using fake logos, credential forms and layout. **Data needs to be highly relevant to real-world attacks so that detection would be easier**. One of the experiments conducted was a two-month duration with the purpose of detecting emerging phishing sites and discovered over 1,942 phishing sites. To summarise the effectiveness of relevant data from the paper, the paper

highlights that phishing detection systems must continuously adapt to the tacts of attacks and will need current time data highly relevant to the real-world attacks. Real-time monitoring and detection had been an effective way of acquiring current data as researchers can see the new evolving tactics within the phishing detection space [11].

In the paper *"CrawlPhish: Large-scale Analysis of Client-side Cloaking Techniques in Phishing*", the relevance of the data to real-world phishing attacks is emphasized by **the large-scale collection and analysis** of 112,0005 phishing websites from 2018 to 2019. The dataset includes phishing kits, client-side cloaking techniques, and the evolution of sophisticated phishing tactics. The research collected real-time phishing data which allowed an effective countermeasure developed as researchers could detect and analyse the evasion techniques equipped by attackers. The paper demonstrates the critical need for continuous data collection to stay updated on real-world phishing tactics and tackle evasion techniques, making the research data relevant to the ongoing unsolved cybersecurity challenges [17].

In conclusion, the relevance of having up-to-date data in the phishing detection space is highly crucial as phishing techniques continue to evolve. The examples provided had shown that detection models are far more effective when real-time data from monitoring and collecting phishing kits used from the live phishing campaigns.

The effectiveness involvement of human analyst in the phishing detection space

The phishing attacks have not only been evolving into more challenging attacks for analyst and detection system, but it has been growing rapidly at an exponential speed and there is no doubt that the cybersecurity challenges can be tackled solely by human interventions.

The large scale of phishing attacks makes it impossible for human analyst to tackle the ongoing cybersecurity issue. The research*," Catching Phishers by Their Bait: Investigating the Dutch Phishing Landscape through Phishing Kit Detection"* gathered a large dataset of phishing attacks which would make it highly challenging for human analysis due to the large and sophisticated attacks. The paper explains automated systems, such as real-time monitoring of TLS certificates and crawling suspected phishing domains, are essential for detecting and precenting phishing threats effectively and quickly. In addition, some phishing campaigns only last 24 hours, making it incompatible for human dependency [15].

To further the argument **that humans are incapable of assessing large scale attacks**, *"A Survey of Phishing Email Filtering Techniques"* elaborates that many phishing emails contain various complex evading techniques such as zero-day and deceptive phishing, making manual detection by human analyst highly impractical. The paper outlines a complex machine-learning model (SVM), k-nearest neighbour (k-NN), and neural networks are trained on extensive datasets which is unrealistic for human analyst to match the speed and accuracy of these systems for reviewing a large scale of emails [8].

Due to the introduction of **AI being weaponised***, "Social Engineering with ChatGPT"* demonstrates attackers are able to leverage ChatGPT to create phishing websites, generate code and make realistic and convincing emails within a matter of minutes. Given this speed, attacks would increase exponentially and human analyst would struggle with the scale, and speed required to detect phishing attacks. Therefore, using automated systems for detecting AI attacks would be effective as automated systems are known for handling large scale of data and complexity found within the attacks [13].

Another point to take in consideration is that **human analysts are prone to make mistakes in the detection process**. The report *"Inferring Phishing Intention via Webpage Appearance and Dynamics: A Deep Vision Based Approach"* highlights the issue that human analyst would face in terms of accuracy. Phishing detection involves extracting features of a website such as layout components, recognizing logos and determining the credential-taking intentions of webpages which are time consuming and requires extensive attention to detail. Human analyst would struggle with these tasks like identifying subtle visual cues and identifying credential login pages. Furthermore, these tasks done by humans are also prone to errors as they would be processing large volumes of information quickly to be able to detect phishing sites before its short duration expires [11]. Additionally, the report *"Fighting against phishing attacks: state of the art and future challenges"* describes the complexity of these tasks as phishing detection models like

PhishIntention must interact dynamically with web pages and crawl through various of page redirections. The process of these tasks also involves handling adversarial attacks like obfuscation and require deep vision models that are robust against such adversarial input [7]. Furthermore, another report titled "*Phishpedia: A Hybrid Deep Learning Based Approach to Visually Identify Phishing Webpages"* explains that detection model Phishpedia have far more effective approaches to counteract phishing attacks. Firstly, Phishpedia is able to analyse large volumes of URLs such as 1,704 phishing sites which is difficult for human analyst to accomplish. Secondly, Phishpedia also has more accuracy uses object detection models and Siamese neural networks to identify logos for precision purposes and match them with a set of known brands. Lastly, the detection model is able to process URLs and webpage screenshots in less than 0.2 seconds, which is greatly appreciated in the detection space as speed is crucial and the speed cannot be matched by human analysis [18].

In conclusion, the rapid evolution and increasing complexity of phishing attacks have made it clear that relying solely on human analysis is not sufficient to address these cybersecurity challenges. The use of AI in phishing campaigns has made human analysis difficult and detection systems are more reliable as they can process large scale of data quickly and accurately. Research shows that automated systems like Phishpedia and machine learning models are more effective in countering phishing attacks in real time. These systems are equipped to handle and have the speed to counteract modern phishing attacks.

The Important features of data used for solving key research challenges

In cybersecurity, identifying phishing attacks remains as a critical challenge as these attacks have its own uniqueness and tactics to avoid detection. Extracting and analysing key features from websites and emails is an essential approach to determine whether they are legitimate or phishing attempts. This section of the report will explore key data features that can be used from extracting websites to determine its integrity and explain why these features are so impactful in solving the research challenges in the phishing detection space.

Visual element analysis is one of the most important elements employed in phishing detection. The detection model Phishpedia which is studied from the report "*Phishpedia: A Hybrid Deep Learning Based Approach to Visually Identify Phishing Webpages"* analyses visual cues such as brand logos to determine a website's legitimacy. Phishing websites frequently use logos to trick consumers into trusting their websites as it would be the feature that victims would notice before proceeding. The detection model analyses logos from pages flagged for phishing with legitimate logos from a trusted dataset. As a result, using logo detection makes it easier to identify phishing sites which makes it a useful feature for increasing detection accuracy [18].

Apart from logos, another crucial visual feature in phishing detection is **identifying layout and spelling inconsistencies**. Phishing websites frequently make small but noticeable mistakes in imitating legitimate websites. Misspellings or incorrect formatting in the layout can serve as strong indicator of phishing, making this feature impactful because legitimate websites are professionally designed and less likely contain these kinds of errors. Phishers often create quick, unpolished copies of trusted sites, and detection systems can take advantage of this by flagging websites that exhibit such inconsistencies [18]. In addition to visual elements, **input fields (which require login credentials) and buttons are essential for phishing detection**. Phishing sites typically use forms to obtain sensitive user data, which is their main objective. Phishpedia uses this feature to examine how users interact within the websites, highlighting buttons and input fields that ask for sensitive information like passwords and usernames. Phishing detection systems can effectively detect phishing websites by focusing on these essential interaction features.

There are several important data features that helps the process of detection that had been discussed in the report titled "Tutorial and Critical Analysis of Phishing Websites. The usage of IP addresses in URLs, unusual URLs and DNS records are strong indicators of a phishing website. In addition, features that allow attackers to gain credential information such as redirect pages, onMouseOver events and server handles are analysed as phishing websites would employ these features in attempt of learning how users interact within the page and stealing their victims' data [19].

Natural Language Processing (NLP) features as elaborated by the report “phishGILLNET—phishing detection methodology using probabilistic latent semantic analysis, AdaBoost, and co-training” are paired with a detection model phishGILLNET to handle details such as synonyms, polysemy, and intentional misspellings in phishing emails. These features are impactful because phishing emails often have spelling or grammar mistakes to evade detection methods of traditional keywords. Furthermore, the detection model phishGILLNET analyses hyperlinks embedded in emails and the system uses a Term Document Frequency (TDF) matrix for the analysation of words in hyperlinks. Precise detection and analysis of URLs allow the detection system to determine phishing attempts before users can even click on malicious links [20].

In conclusion, the effectiveness of phishing detection system heavily relies on the extraction and analysis of data features from websites and emails. Visual elements such as brand logos, interaction component such as input fields and buttons, URL structures and redirect pages are key features of indicating phishing behaviour. Using NLP techniques allows analysing of embedded hyperlinks which provides an advanced layer of protection against phishing emails. Together, these features assist detection systems and address unique tactics employed by phishers.

Proposal for phishing attacks

Phishing attacks are evolving continuously at the volume of attacks as well as complexity and uniqueness. Researchers have made progress to counteract these attacks however there are still significant gaps in the detection space such as zero-day phishing, spear phishing and whaling. The main issues that highlight the challenges in the current phishing detection systems are lack of real time adaption to emerging phishing techniques and also not having an up-to-date dataset. Furthermore, user awareness and education alone has not been effective to completely prevent phishing attacks due to the phishing attacks being more sophisticated.

This proposal presents solutions focused on **deep monitoring campaigns, AI-based authentication mechanisms and real time verification systems** to strengthen phishing detection capabilities and reduce vulnerabilities.

Findings from “Catching Phishers by Their Bait” had proven that **automated deep monitoring bots** have been impactful as these bots would scan websites and email continuously, gathering real-time data on new phishing domains, websites and email servers. The use of AI bots can expand the scope of phishing detection and prevent phishing sites the moment they go online. The system suggested would also use AI-powered data crawlers that are capable of analysing visual and structural features of the websites and flagging suspicious elements found [15].

To combat sophisticated phishing techniques such as spear phishing and whaling, **stronger AI-based email authentication mechanisms should be developed**. This mechanism would utilise digital signatures and AI-based verification and must be able to work effectively throughout every email server regardless. Besides that, AI-based system would examine content, sender identity, and context in real time to prevent phishing emails from reaching users. By analysing the semantic content of emails and verifying the sender’s identity with AI, these systems would be able to detect even complex phishing attempts. In addition, multi-factor authentication (MFA) could be integrated to provide an extra layer of security.

The availability of AI to the public have increased phishing attacks as it is easier for attackers as AI is capable of creating convincing emails, identical replications of trusted websites and even creating a plan designed for the purposes for the attackers. **Recommendation of AI-based pattern recognition would be implemented to monitor request histories, checking signs of potential misuse such as generating malicious in AI platforms** such as ChatGPT. This system would continuously learn and adapt to new patterns of phishing behaviour and flagging requests that align with known phishing or hacking behaviours for further investigation by human analyst.

In conclusion, phishing attacks are growing more complex and frequent, as issues such as zero-day, spear phishing and whaling. Outdated or lack of real-time data have proven to be the reason for ineffective

phishing detective systems. This proposal recommends AI-driven deep monitoring, real-time verification and stronger authentication mechanism to enhance phishing detection.

References

[1] news.biharprabha.com, “20% Indians are victims of Online phishing attacks: Microsoft.,” 2014.

[2] B. B. G. ·. N. A. G. A. ·. K. E. Psannis3, “Defending against phishing attacks: taxonomy of methods, current,” https://doi.org/10.1007/s11235-017-0334-z, 2018.

[3] L. Z. Ahmed Aleroud a, “Phishing environments, techniques, and countermeasures: A survey,” 2017.

[4] C. Z. C. H. ,. L. L. A. Y. Y. YONG FANG, “Phishing Email Detection Using Improved RCNN Model With Multilevel Vectors,” 2019.

[5] S. L. P. e. J. D. F. E. J. Deanna D. Caputo, “Going Spear Phishing: Exploring Embedded Training and Awareness”.

[6] G. &. K. T. (. C. N. Krieg, “T. (2016). CNN News, Is this the email that hacked John Podesta's account?,” CNN, 2016.

[7] B. B. G. •. A. T. •. A. K. J. •. D. P. Agrawal, “Fighting Against Phishing Attacks: State of the Art and Future Challenges,” Neural Comput & Applic, 2017.

[8] B. B. G. S. A. A. M. a. E. A. Ammar Almomani, “A Survey of Phishing Email Filtering Techniques,” 2013.

[9] S. M. I. I. K. M. I. A. K. M. I. Zuochao Dou, “Systematization of Knowledge (SoK): A Systematic Review of Software-Based Web Phishing Detection,” 2017.

[10] E. B. O. D. D. Ozgur Koray Sahingoz, “Machine learning based phishing detection from URLs,” 2019.

[11] Y. L. X. Y. a. S. H. N. Ruofan Liu, “Inferring Phishing Intention via Webpage Appearance and Dynamics,” 2022.

[12] M. U. H. U. B. K. Muhammad Mudassar Yamin a, “Weaponized AI for Cyber Attacks,” 2021.

[13] I. D. Dijana Vukovic Grbic, “Social Engineering with ChatGPT,” 2023.

[14] Y. I. S. M. I. a. A. J. Mahmoud Khonji, “Phishing Detection: A Literature Survey,” 2013.

[15] T. B. A. S. A. N. R. v. W. Hugo Bijmans, “Catching Phispher by Their Bait: Investigating the Dutch Phishing Landscape through Phishing Kit Detection,” 2021.

[16] J. B. Z. ,. K. T. A. D.-J. A. Eric Nunes, “Sunrise to Sunset: Analysing the End-to-End Life Cycle and Effectiveness of Phishing Attacks at Scale”.

[17] A. O. H. C. S. J. B. W. S. K. B. R. W. S. D.-J. A. Penghui Zhang, “CrawlPhish: Large-scale Analysis of cloaking techniques in phishing,” 2021.

[18] R. L. M. D. Y. N. Q. Z. C. L. S. Z. S. D. Yun Lin, “Phishpedia: A Hybrid Deep Learning Based Approach to Visually Identify,” 2021.

[19] F. T. M. Rami M. Mohammad, “Tutorial and Critical Analysis of Phishing Websites,” 2015.

[20] V. R. a. H. Wechsler, “phishGILLNET—phishing detection methodology using probabilistic latent semantic analysis, AdaBoost, and co-training,” 2012.

Marker's comments:

Total Mark:

Extension certification:

This assignment has been given an extension and is now due on

Signature of Convener: Date: /2023