QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing)

Godwin Awuah Amoah
Department of Computer Science
Kwame Nkrumah University of Science & Technology
Kumasi, Ghana

Hayfron-Acquah J.B.
Department of Computer Science
Kwame Nkrumah University of Science & Technology
Kumasi, Ghana

ABSTRACT
To accommodate new technologies and communication methods, cybersecurity must advance. For security experts, especially those working in fields like digital forensics, new technologies provide both opportunities and challenges. New technologies like smartphones and new ways of disseminating information, like social media, might provide difficulties. Use of QR (Quick Response) codes is one of the rapidly expanding interface technologies. This paper explores privacy issues that might arise with QR codes and other information security-harming technologies. Additionally, it emphasizes the necessity for experts in the field to solve security concerns raised by the increasing use of QR codes. Each URL's words were extracted using a count vectorizer, and the URLs that were part of the QR code were used to obtain features. To distinguish between legitimate and phishing URLs, traits and words were tokenized, and naive Bayesian machine learning classification techniques were used in a recursive loop alongside logistic regression. A very accurate model was created, aiding in the reduction of quishing behaviour.

General Terms
QR Code Phishing Detection

Keywords
Quick Response Code, Naïve Bayes, Natural Language Processing, Logistic Regression, Machine Learning, Feature Extraction, True Positive, True Negative, False Positive, False Negative

1. INTRODUCTION
Information security is focused on defending computer systems from possible dangers. Information security is often measured by three criteria: confidentiality, integrity, and availability (CIA). Information security professionals are driven by the desire to protect the information systems they are responsible for. Information security entails making sure systems are trustworthy and secure and that the right people always have access to information. IT and information security professionals must stay current to remain relevant in a digital world that is becoming more interconnected. QR codes, a social interaction technology that is quickly growing, are often used as tangible shortcuts to online services. In 1994, DensoWave, a Toyota company, invented the QR code, a matrix barcode for identifying vehicle parts. Although this technology is open and free to use in accordance with ISO and JIS standards. QR Code is a trademark of DensoWave Incorporated [5]. Due to their ease of use and simplicity, QR codes are becoming more and more popular in sales and marketing. When a smartphone is used to scan QR codes on billboards and banners, it directs the user to a website.


Fig 1: Sample QR Code

They may be found in TV advertisement, print media, periodicals, and even business cards. People often use the cameras on their smart phones to quickly scan QR codes to access a website. Customers request and submit personal information along with product information. While the machine reading of QR codes offers convenience (no customer input), it also raises security concerns. This is addressed by these two recommendations; JIS 0521 and ISO/IEC 18004 [5]. Systems, vendors, and different development technologies all have variable degrees of implementation difficulty (especially web-based). Usually, inconsistency results in platform or device compromise. Users, vendors, and security testers all expect user data, applications, and privacy to be handled uniformly and securely. This problem is not solved by the unpredictable nature of the software that decodes QR codes. Using a simple online or offline code generator, anybody or any organization may create their own QR code by converting text into a distinctive QR code representation. The most well-known website redirect provider now generates a QR code for each website automatically. QR code is typically 50 characters long, but the new, denser format allows for up to 1264 characters. You may add longer URLs than the QR code version allows for, as well as details about the QR code's position (such where the poster is located), by using URL shortening services. As previously mentioned, the authenticity of visited websites is compromised by the invalidity of QR data. Link destination URLs are becoming more complicated as a result of the growing popularity of shortened URL providers. These worries undermine trust in manually entering website URLs. UI manipulation attack, may be carried out by a malicious actor who secretly sent traffic to websites, tricked users into clicking on things they didn't want to. Users run the risk of unintentionally disclosing personal information or engaging in online transactions.

2. GOALS AND IMPLICATIONS
The goal of the paper was to investigate current defenses against QR code phishing attacks, describe the weaknesses exploited by phishers to exploit QR codes, and propose an algorithm to stop phishing attacks on QR codes that employ false URLs.

2.1 The research's major goals were to

To emphasize the security risks that using QR codes may poseto users, as well as potential methods that attackers may use to change legitimate QR codes. To propose a solution to these security risks by creating a machine learning model that can foretell and identify phishing in QR codes.

3. LIMITATIONS AND SCOPE

To identify QR code phishing, this study employs a frequently used machine learning technique. This research utilizes machine learning to categorize data using Naive Bayes and logistic regression algorithms. Record characteristics are carefully picked from hundreds of labels based on URL phishing hosts and language structure.Recommended phishing detection solutions may not be proven against zero-day phishing assaults. Phishing URLs don't persist long since browsers and search engines routinely identify them and alert users. The PhishTank database and other comparable datasets labelled with phishing URLs supplied the dataset for this investigation. The processing capability of the simulation PC influences the detection speed and execution duration of the phishing algorithm.

4. RELATED WORK

Although they offer numerous benefits, attack vectors are already being exploited with QR codes [6]. The attackers have either encrypted the broken links that send visitors to phishing sites, or the code is erroneously performed. The primary disadvantage of QR codes is that they are not produced by people.According to experts, using QR codes to spread malware and conduct phishing attacks is quite effective. Humans are unable to distinguish between good and bad code since only a computer can interpret it. Malicious QR codes may be distinguished from legitimate ones. Users may feel better knowing that reputable companies are using their QR code for advertising [7]. More and more financial fraud use QR codes. According to a recent report, phishers allegedly stole 13 million US dollars in the United States, while in China there was a loss of about 900,000 Yuan roughly [13]. When a customer scans the original version of the seller's QR code, which has been illegally altered, it may lead to loss of personal information. APWG recorded 384,291 attacks in March 2022. As shown to Figure 2, this is the highest monthly total in the group's reporting history. APWG discovered 1,025,968 phishing attempts in Q1 2022. This quarter was the worst for APWG ever, with the quarterly total finally reaching 1 million. 2021's fourth quarter saw a record-breaking 888,585 attacks. Phishing attempts have escalated since the beginning of 2020, when the APWG recorded 68,000–94,000 attacks monthly [2].

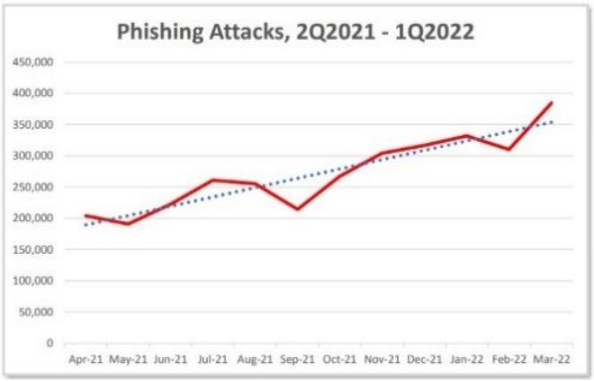


Fig. 2: APWG report on phishing attacks globally for the first quarter of 2022

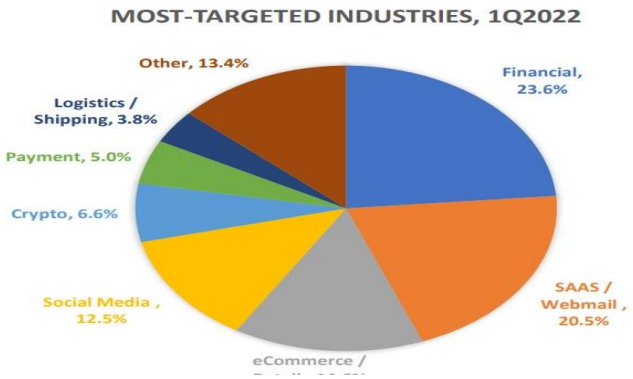


Fig. 3: APWG chart for sectors their attack distribution

Banks were the target of 23.6% of all phishing attempts in Q1 2022, according to OpSec Security, a founding member of the APWG. As shown in Fig 3. There was obviously an issue right away. Attacks on retail and e-commerce websites dropped from 17.3% to 14.6% over the holiday season, although they continued to often target webmail and software as a service (SAAS) providers. As a proportion of all attacks, phishing attacks on social media platforms climbed from 8.5% in Q4 2021 to 12.5% in Q1 2022.

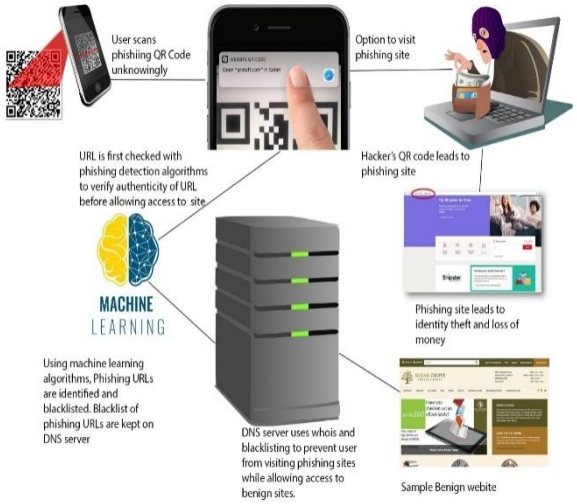


Fig 4: QR code phishing attack and proposed remedy

As shown in fig 5, this can be phishing using a QR code. Without permission, the attacker starts a client-side QR session and copies the login QR code to the phishing website. The victim might be given access to a well-crafted phishing website with a fake QR code of it. The attacker sends the victim the link to the phishing website. The victim uses a smartphone app that has been particularly designed to scan the QR code. The victim's account finally belongs to the attacker after signing in into the fake site or creating an account. This service transmits all of the victim's data to the session of the attacker.

5. QR CODE PHISHING DETECTION

In contrast to traditional phishing, there isn't a lot of information accessible on how to identify phishing attacks utilizing QR codes. There has previously been research done on the acceptability and dangers of technology. An example of how to spot QR code fraud using Google Safe browsing and PhishTank was highlighted. Using the Google Safe Browsing API, the app can examine URLs for malware and

phishing. A thorough blacklist of phishing URLs is available from a database called PhishTank. This strategy is unsuccessful against zero-day phishing attempts because of its instability and susceptibility to API upgrades. This report does not discuss the outcomes of the proposed method for determining the QR code phishing detection rate or its comparison with outcomes from other prior studies. But that wasn't the study's objective. Instead, in light of prior user notification research, the efficacy of this approach was assessed. A website extractor that uses a crawling URL matcher technique was developed [11]. Researchers were unable to confirm the presence of potentially dangerous QR codes because of the brief lifetime of phishing websites. The extent of fraud that may be uncovered using this method is uncertain due to the absence of a baseline research and a dataset for QR code phishing. [10] proposed using digital signatures and wet paper codes to identify tampered QR codes. Encrypt data using a private key. Encrypted data is hidden by the QR code. If the message has been changed, use the recipient's public key to decrypt it. No result was tracked. Because of this, this response was not rated. It also ignores the importance of the technology.Through code construction, authentication, and data integrity, [12] isolate potentially dangerous QR codes using DSA symmetric key encryption and SHA1. The QR code also has to be produced and confirmed. The suggested solution seeks to generate and read QR codes on secure systems. Due to the complexity of time and space, this recommended approach may not be able to identify zero-day QR code phishing attempts. Public data included no references to QR code phishing. According to a study by [7], the following criteria need to be applied:

Improve QR codes and lessen code changes. He suggested strengthening the QR code's legitimacy by adding a digital signature. Instead of QR code localization, the focus is on QR code production. In order to increase data security while communicating data via QR codes, [3] developed a technique. The information marked as a "secret" (QR code) is divided into pieces (multiple QR codes), and it is expected that some or all users will combine the pieces into one message, with unknown private key sent to a number of people. Data security is instead given priority over phishing prevention in this covert strategy for sharing QR codes. Researchers [4] have created a safe mobile payment method that makes use of 2D barcodes and QR codes. The QR code's validity is not checked before using this method to protect transactions using QR codes. There are some less sophisticated methods for increasing awareness of QR code security that should not be overlooked in addition to [8] technical approach. He had the brilliant idea to embellish his QR codes with illustrative features like logos. As a result, it is difficult for others to discern between the colors and copy his QR code.

However, using well-known online tools is not advised since both hackers and normal people may easily add logos and modify the color of standard QR codes. Some individuals would believe that his QR code, which has excellent attributes, originates from a reliable source, which is plausible. According to [7], the complexity of recreating QR codes depends on their color scheme. To make the QR code simpler to notice, it also makes use of attractive color palettes throughout the advertising campaign. It also stresses the use of digital signatures to reveal who created the QR code and how to do so. QR codes are protected using two of the newly created cryptographic approaches. To safeguard the data, one utilizes symmetric encryption and the other, asymmetric encryption.

AES is recommended as an encryption method for symmetric QR codes since it uses a secret key that both the reader and the writer share. The asymmetric technique encrypts symmetric keys that might be connected to communications using RSA technology. [9] suggests employing a digital signature to verify the source first. QR code security is a very secure identification method since it uses several bits to identify the signer's public key. Given that it takes up a significant amount of space in the QR code, the key can only be used to a limited extent. The best course of action in this situation may not be to use RSA technology on portable devices. Therefore, it is preferable to adopt a strict minimum public key in order to reduce computational expenses.

Another study suggested that the detection of QR code phishing using machine learning was effecive. In this study, machine learning including Naive Bayes were both used for categorization. Record features were explicitly picked based on lexical structure and URL phishing host. The use of CNNs, which automatically learn features from datasets, is a more effective alternative to manually selecting attributes in many phishing attack situations. The search did not turn up all records involving QR code phishing. Ways to identify fake QR codes were identified. The highest detection rate of 88.33% indicates that further investigation is required to recognize phishing that uses phony QR codes. The phishing URLs included in this white paper came from one of the top three open access phishing databases. These websites include MalwareURLs, Openphish, and Phishtank. As a result, scientists could trust their conclusions. However, no record of the displayed QR code was made. The focus of this research is on cognitive tools rather than cognitive paradigms [14].

6. METHODOLOGY

Methodology employed for this was that a collection of data about phishing and benign URLs is given to the framework, which is then preprocessed for informative extraction that may be employed for investigation objectives. About 10 features of phishing URLs were revealed, which may be used to separate them from legal ones. Count vectorization was done on these URLs to extract words and then tokenize these words. Subsequently, the extracted features and tokenized words are run recursively through machine learning to identify phishing from legitimate URLs.

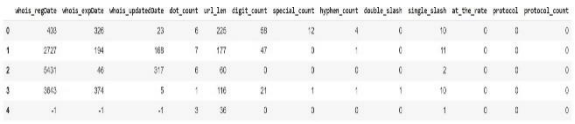
7. DATASET

The research website of Aalto University was where the initial data came from. Figure 6 displays specifics of the complete phishing detection procedure. Data extraction and data fitting to the machine learning model should come first. The key stages were as follows:

When disassembling machine learning (ML) models, remove zeros and duplicate data, the URL and Label columns are the only ones remaining after superfluous columns have been eliminated. To generate the final feature extraction dataset, 500,000 unbalanced URLs from each of the Whois-approved good and bad URL samples were included. The preprocessed data were separated into phishing sample groups and benign sample groups for Whois verification. In order to ensure that the ML model wasn't running amok,the system independently verified the Whois reachability of these two sample words and made sure that no functions unrelated to the function data were imported. TheML model was trained with the obtained functions to prepare the model to classify URLs.

8. EXTRACTION AND IMPLEMENTATION OF FEATURES

To perform Whois actions, we use the Python Whois module. A plethora of information about URLs is available through the Whois Python program. The establishment, renewal, and expiry dates for the domain name, registrar, whois server, name servers, and emails were crucial details because of the following things: For the most secure URLs, the creation date is verified. A URL becomes more likely to be secure over time. The majority of internet criminals don't maintain their domains for very long. This is why expiration dates are important. The validity of a URL may be proven using the creation date, expiration date, and update date. The majority of URLs—both good and bad—returned nulls for extra variables like postcodes and addresses that might have been utilized for classification in the datasets under investigation. Extracted feature count sample is displayed in figure 5.



	whois_regDate	whois_expDate	whois_updatedDate	dot_count	url_len	digit_count	special_count	hyphen_count	double_slash	single_slash	at_the_rate	protocol	protocol_count
0	438	326	23	6	226	68	12	4	0	10	0	0	0
1	2727	194	169	7	177	47	9	1	0	11	0	0	0
2	5431	46	317	6	60	0	9	0	0	2	0	0	0
3	3843	374	5	1	116	21	1	1	1	10	0	0	0
4	-1	-1	-1	3	36	0	0	0	0	1	0	0	0

Fig 5: Sample extracted featurecount

Table 1.Lexical features extracted

S/N	Feature
1	Dot Count
2	Single Slash Count
3	Double Slash Count
4	Protocols Count
5	@Sign Count
6	Hyphen Count
7	Special Character Count
8	Digit Count
9	Dot Count
10	URL length

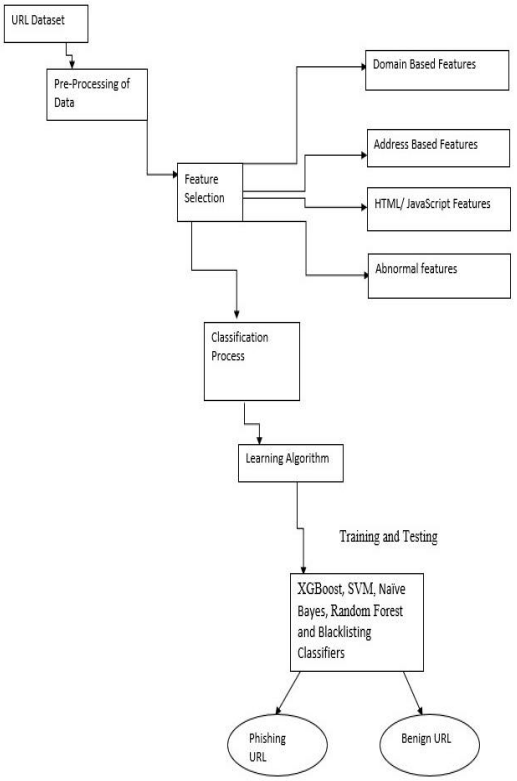


Fig 6: Proposed system architecture diagram

These phishing websites could request customers' credit card details. Furthermore, we are aware that different phishing URLs use different protocols. This query string will redirect you to another malicious website. Having this knowledge was important. It is a series of recommendations that prior studies overlooked. These URL components were collected by examining the lexical content of each URL. The resulting lexical traits are shown in Table 1.

8.1 CountVectorization

Vectorizing URLs was made feasible by translating a collection of texts from URL records into a matrix of token counts. As a result, the tokenizer extracts words from the URL. As shown in fig 7.

	domain	label	text_tokenized	text_stemmed
94495	hiddenway.tripod.com/hero/	0	[hiddenway, tripod, com, hero]	[hiddenway, tripod, com, hero]
24900	yourleadssource.com/cgi-bin/config.php?check=3	1	[yourleadssource, com, cgi, bin, config, php, ...	[yourleadssourc, com, cgi, bin, config, php, c...
18984	operator.juplo.com/it/cmd_logi.php	1	[operator, juplo, com, it, cmd, logi, php]	[oper, juplo, com, it, cmd, logi, php]
32400	zarabotok-vinternet.ru/wp-content/plugins/wp_c...	1	[zarabotok, vinternet, ru, wp, content, plugin...	[zarabotok, vinternet, ru, wp, content, plugin...
2258	petrepes.net/GRcntrlde/webscr.php?cmd_=session...	1	[petrepes, net, GRcntrlde, webscr, php, cmd, s...	[petrep, net, grcntrlde, webscr, php, cmd, ses...

Fig 7: Sample extracted words using tokenization and stemming

8.2 SnowballStemmer

This approach is also used in the extraction of words from URLs. Snowball, a basic string processing language, is used to generate root words. As shown in fig 7.

9. RESULTS

Table 2. Summary of the pipelined logistic regression model results

	Precision	**Recall**	**F1-Score**	**Support**
Bad	0.88	0.96	0.92	26048
Good	0.99	0.96	0.95	100751
Accuracy			0.96	126799
Macro	0.93	0.96	0.95	126799

Average				
Weighted Average	0.97	0.96	0.97	126799

Training Accuracy: 97.89%

Testing Accuracy: 96.47%

Table 3. Summary of Performance for the selected Classifiers

Algorithm	Accuracy	False Positives	False Negatives	No. of Used Features
XGBoost	89%	1951	13760	18
Naïve Bayes	96%	1951	3276	18
Logistic Regression	96.47%	1951	3276	18

The outcomes of several categorization algorithms in decreasing order of accuracy is presented in table 2. This information makes it quite evident that of the tested classifiers, Naive Bayes and Logistic Regression have the two highest scores. With an accuracy rate of 96.47% presented in table 3, logistic regression produced the best results. Out of 10,000 predicted URLs, only 5227 were misclassified. However, the outcomes of the two best algorithms are almost equal and do not vary much (96% or more).

Fig 9 Heatmap of the Confusion Report for Pipelined Logistic Regression Model

As shown in fig 8, True Positive (TP) = 25390 shows that the model correctly classified 25390 URL points as being in the positive category. True Negative (TN) = 96182 means that the model correctly identified 96182 URL entries in the negative class. False positive (FP) = 1951 implies that the model misidentified positive authentic URLs as negative URLs in 1951. False Negatives (FN) = 3276 means that the model mistook 3276 positive class data items for negative class data items. The logistic regression model outperformed the others on the confusion matrix.

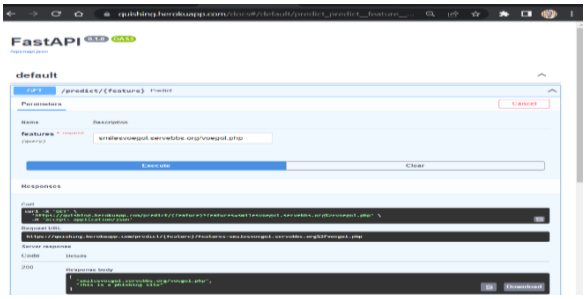


Fig 10: FastAPI testing of the model on the URL "smilesvoegol.servebbs.org/voegol.php"

9.1 Implementing Fastapi to Make the Model Available Worldwide

For developers who wish to add security checks to their Android and web apps, the machine learning model's API was hosted on Heroku servers. Screenshots of the test results are shown above in fig 10. A set of model API tests utilizing the Android QR code reader are shown in Figures 11 and 12. With 97% accurate predictions, 300000 safe URLs and 20000 phishing URLs in the QR code were evaluated. When the predict button is pushed, the Heroku server's API receives the URL decoded from the QR code and use machine learning to determine which class the URL belongs to. Output serves as the user's form of feedback. The secure QR code may be accessed by responding with the phrase "This is a legitimate website." Conversely, you should stay away from websites that pose as phishing sites since they are risky.

Fig. 11 Android QR code scanner implementation or API using URL " servciosbys.com/paypal.cgi.bin.get-"

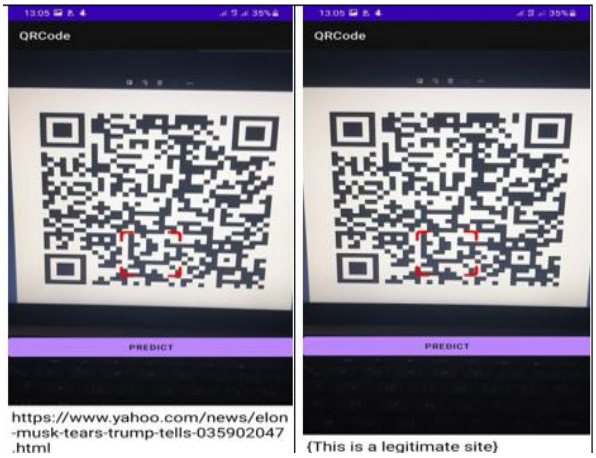


Fig. 12 Android QR code scanner implementation or API using URL:https://www.yahoo.com/newa/elon-musk-tears-trump-tells-035902047.htm

10. CONCLUSION AND FUTURE WORK

According to the findings, users should exercise extreme caution while scanning QR codes supplied by adverts and payment options. It is recommended to scan QR codes only from reliable sources. Scanning the code for the sake of curiosity is not advised. Viewpoint's QR code must be reviewed on a regular basis by suppliers and businesses to identify any changes or substitution of authentic QR code with a fake. Software developers are invited to incorporate the

suggested model APIs into their web and mobile applications. While this technology has many benefits, it may be hampered by financial, network, and access concerns. It may take some years before the remedy is generally embraced. However, there are so many opportunities to integrate technology into this method in security-critical circumstances that the advantages are seen to exceed the risks. It may be deduced from the findings that logistic regression offered the greatest baseline accuracy for future comparisons. This study lacked up-to-date, confirmed information concerning phishing URLs. As a consequence, it was found throughout the analysis that, the vast majority of the URLs used were obsolete records and could not be accessed by the DNS resolver (nslookup) or the WhoisPython module. As a consequence, the feature could not be recorded. In the future, using larger datasets to create a better Whois/DNS resolution Python module that can successfully extract more vital properties and analyze them using different machine learning classifiers will be adopted.

10. ACKNOWLEDGMENT

This research would not have been possible without the support of Professor J.B. Hayfron-Acquah whose guidance and directions made this work possible.

11. REFERENCES

[1] "Aalto University". [Online]. Available: https://research.aalto.fi/portal/en/. [Accessed 20 04 2022].

[2] Anti-Phishing Working Group, 2022. Phishing Activity Trends Report (4 th Quarter 2022). Unifying the Global Response To Cybercrime. [online] APWG. Available at: <http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf> [Accessed 14 August 2022].

[3] Chuang, J.C., Hu, Y.C., Ko, H.J. (2010). A Novel Secret Sharing Technique Using QRCode. International Journal of Image Processing (IJIP) 4(5) 468-475

[4] Gao, J., Kulkarni, V., Ranavat, H., Chang, L., Mei, H. (2009). A 2D Barcode-Based Mobile Payment System. In: Multimedia and Ubiquitous Engineering, 2009. MUE'09. Third International Conference on, IEEE 320-329

[5] ISO/IEC 18004:2000. (2000).Ínformation technology-Automatic identification and data capture techniques – Bar Code symbology-QR Code ".

[6] Kharraz, A., Kirda, E., Robertson, W., Balzarotti, D., &Francillon, A. A. (2014). Optical delusions: A study ofmalicious QR codes in the wild. Proceedings - 44th AnnualIEEE/IFIP International Conference on DependableSystems and Networks, DSN 2014, (December), 192–203.https://doi.org/10.1109/DSN.2014.103

[7] Krombholz, K., Fr¨uhwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., Weippl, E. (2014). QR Code Security: A Survey of Attacks and Challenges for Usable Security. In: International Conference on Human Aspects of Information Security, Privacy, and Trust, Springer 79-90

[8] Narayanan, A.S. (2012). QR Codes and Security Solutions. International Journal of Computer Science and Telecommunications 3(7) 69-71

[9] Peng, K., Sanabria, H., Wu, D., Zhu, C. (2014). Security Overview of QR Codes. Student project in the MIT course 6.857,'14

[10] T. Ishihara and M. Niimi, "Compatible 2D-Code HavingTamper Detection System with QR-Code," (2014). TenthInternational Conference on Intelligent Information Hiding andMultimedia Signal Processing, Kitakyushu, 2014, pp. 493-496.DOI: 10.1109/IIH-MSP.2014.129

[11] Yao, H., & Shin, D. (2013). Towards preventing QR code-based attacks on android phones using security warnings.Proceedings of the 8th ACM SIGSAC Symposium onInformation, Computer, and Communications Security -ASIA CCS '13, 341.https://doi.org/10.1145/2484313.2484357

[12] Banu, M. N., & Banu, S. M. (2013). A Comprehensive Study of Phishing Attacks. International Journal of ComputerScience and Information Technologies, 4(6), 783 786.Retrievedfromhttp://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.643.766&rep=rep1&type=pdf

[13] Tao, L. (2017). QR code scams rise in China, putting epayment security in spotlight | South China Morning Post. South China Morning Post. Retrieved from http://www.scmp.com/business/china business/article/2080841/rise-qr-code-scams-china-putsOnline-payment-security.

[14] Shaikh, A. N., Shabut, A. M., & Hossain, M. A. (2017). Aliterature review on phishing crime, prevention review andinvestigation of gaps. SKIMA 2016 - 2016 10th International Conference on Software, Knowledge, Information Management and Application.