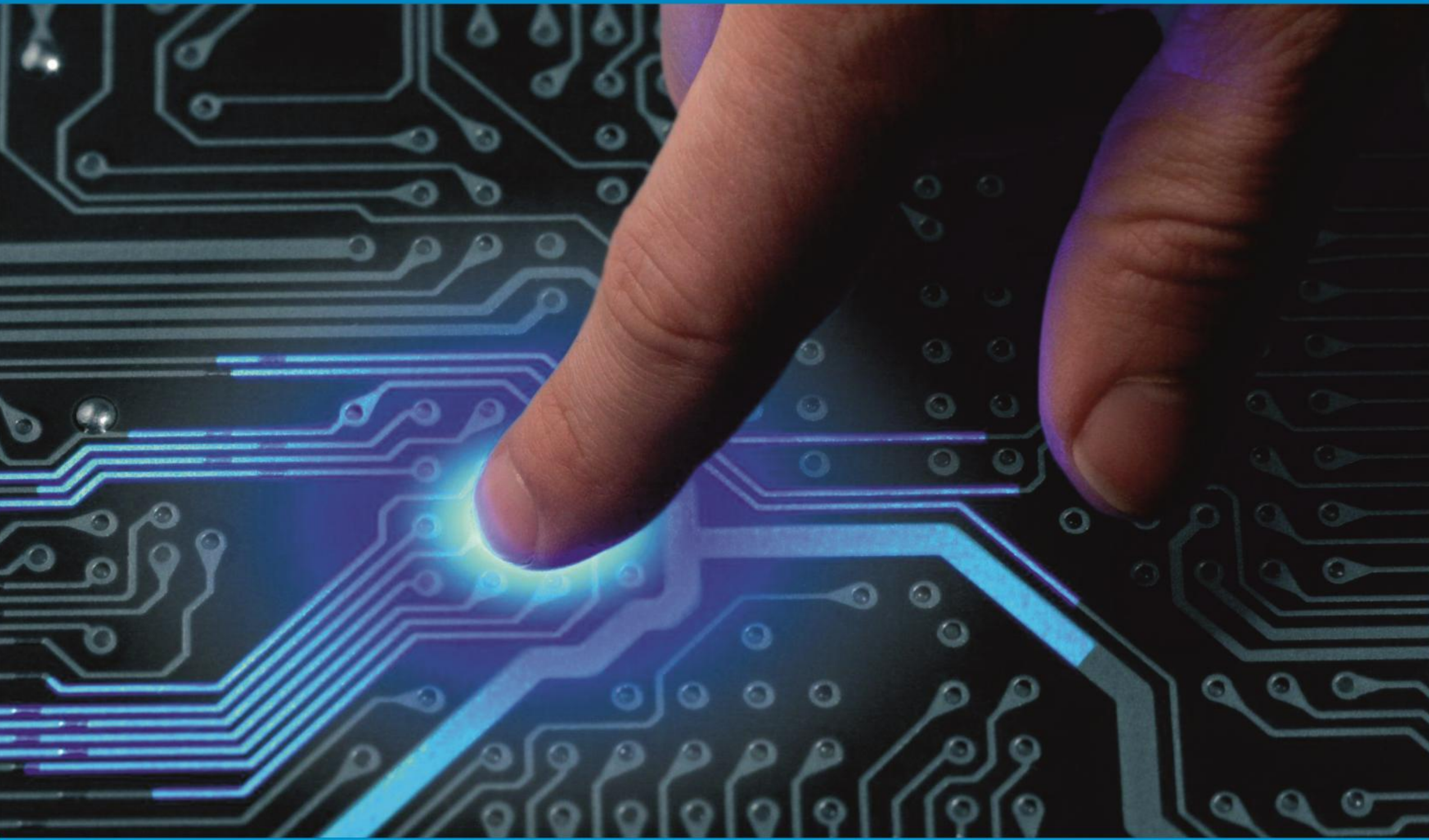
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 10, October 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

A Detailed Study on Various Kinds of Phishing Attacks on Android Devices

Dipti S. Dhankarghare

Student, Dept of I.T, B.K Birla College of Arts, Science and Commerce (Autonomous), Kalyan, India

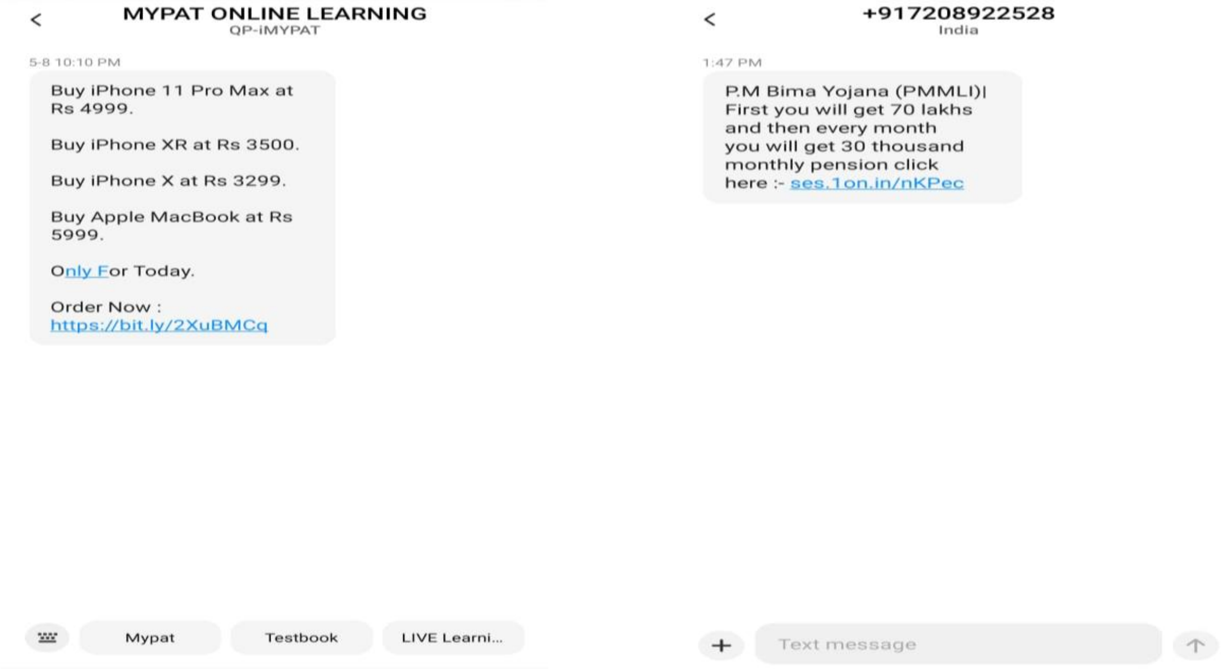
ABSTRACT: Phishing is basically a cyber-crime in which victims is contacted by email, telephone, or text message or by trickling people by calling and threatening them by someone posing as a legitimate institution to lure individuals into providing sensitive and important data like personally identifiable information, banking, and Mastercard details and passwords. In this paper, we have explained about Smishing. Smishing is essentially a security attack during which the user is tricked (sometimes confused or annoyingly) into downloading an epidemic, or other malware onto his telephone or other mobile devices. Smishing is short for "SMS phishing." Banks and anti-fraud agencies around the world warn that fraudulent text messages are becoming more numerous and sophisticated, although statistics to confirm these claims are hard to come by. But then too there are many attacks happening all over the globe various measures and actions need to be taken against this. Smishing remains the problem that continues to increase with growing years, attackers are more innovative and always finds loopholes in the security to attack victim. The best way to tackle this attack is to train and aware people of this attack through podcasts, seminars, public announcements, etc. In this paper, we discuss in detail these attacks.

KEYWORDS: Smishing, Vishing, Instant apps, Cyber-crime, SMS, URL

I. INTRODUCTION

A vast development in Information Technology and related filed has influenced us to connect to the internet and increase smartphone usage. These smartphones are becoming more lavish and there's an increase in smartphone usage. Many big companies like Facebook, Amazon, Google, Microsoft are endeavoring to make the internet a more fascinating utility. Due to its popularity and lack of security Smartphones are becoming an effortless target for attackers. As everything is getting digitalized people to keep their crucial information like a debit card and credit card details in their devices due to this user privacy is becoming an important issue in Android. Mobile devices are more prone to such attacks due to reasons like lack of awareness to user about the that they might face as a result of adopting less secure behaviors or user not able to check the legitimacy of a message or webpage (due to small display) or habit of entering credentials whenever asked without checking the legality of that page etc. There are various kinds of phishing attacks like email phishing, spear phishing, whaling, smishing, vishing, angler phishing. In this paper, we mainly focus on smishing (SMS phishing) and vishing (attacks via phone calls) attacks on Android devices.

1. Smishing: It involves se sending venomous SMS to the user using which the user is supposed to send his information. Smishing may contain activities like embedding malicious code to victim's profile, sometimes it may download a .apk file in victim's devices which turns to be malware. It is necessary to mark the authenticity of a message sometimes it may be spam too. Some methods are also used that can detect phishing text messages but though they are not so accurate. A code analyzer that inspects the legitimacy of the source code can also be used to detect such malicious messages. Fig 1: examples of smishing messages.



MYPAT ONLINE LEARNING
QP-iMYPAT

5-8 10:10 PM

Buy iPhone 11 Pro Max at Rs 4999.

Buy iPhone XR at Rs 3500.

Buy iPhone X at Rs 3299.

Buy Apple MacBook at Rs 5999.

Only For Today.

Order Now : https://bit.ly/2XuBMCq

+917208922528
India

1:47 PM

P.M Bima Yojana (PMMLI)| First you will get 70 lakhs and then every month you will get 30 thousand monthly pension click here :- ses.1on.in/nKPec

Fig 1. Examples of smishing messages

2. Vishing: Vishing attack is conducted through voice email, VoIP (voice over internet protocol), landlines, or cellular phones i.e. android devices. By spoofing a legitimate call number, attackers make the victim believe that call is legitimate. In this paper, we propose made use of various algorithms to analyze SMS content and URL behavior the false-positive results

II. Types of Smishing Attacks

Smishing (SMS + phishing), which was named by McAfee, an online security company, occurs when an internet site link is shipped via text messaging to a sensible phone user [6]. When the user connects to the online site whose link (URL) was present in the SMS, a Trojan virus is inserted on the smartphone, allowing it to be controlled by a 3rd party.

The first type is where the attacker sends a message which contains a malicious URL that will redirect the user to the fake website. As the user clicks the URL and immediately connects to the website then the malicious or harmful code is inserted into his/her android device. Hence the user's device is infected with malicious code that may harm the device and collect sensitive information. As the user makes any payment or online transaction the malicious code interrupt and steals all the information and that information is saved to the attacker's datab ase. The attacker further sends another SMS that the user finds attractive without getting any doubt. After the user opens the message and clicks the URL, the smartphone is infected by malicious code or some .Apk package. Fig 2. Shows the diagrammatic representation of smishing attack

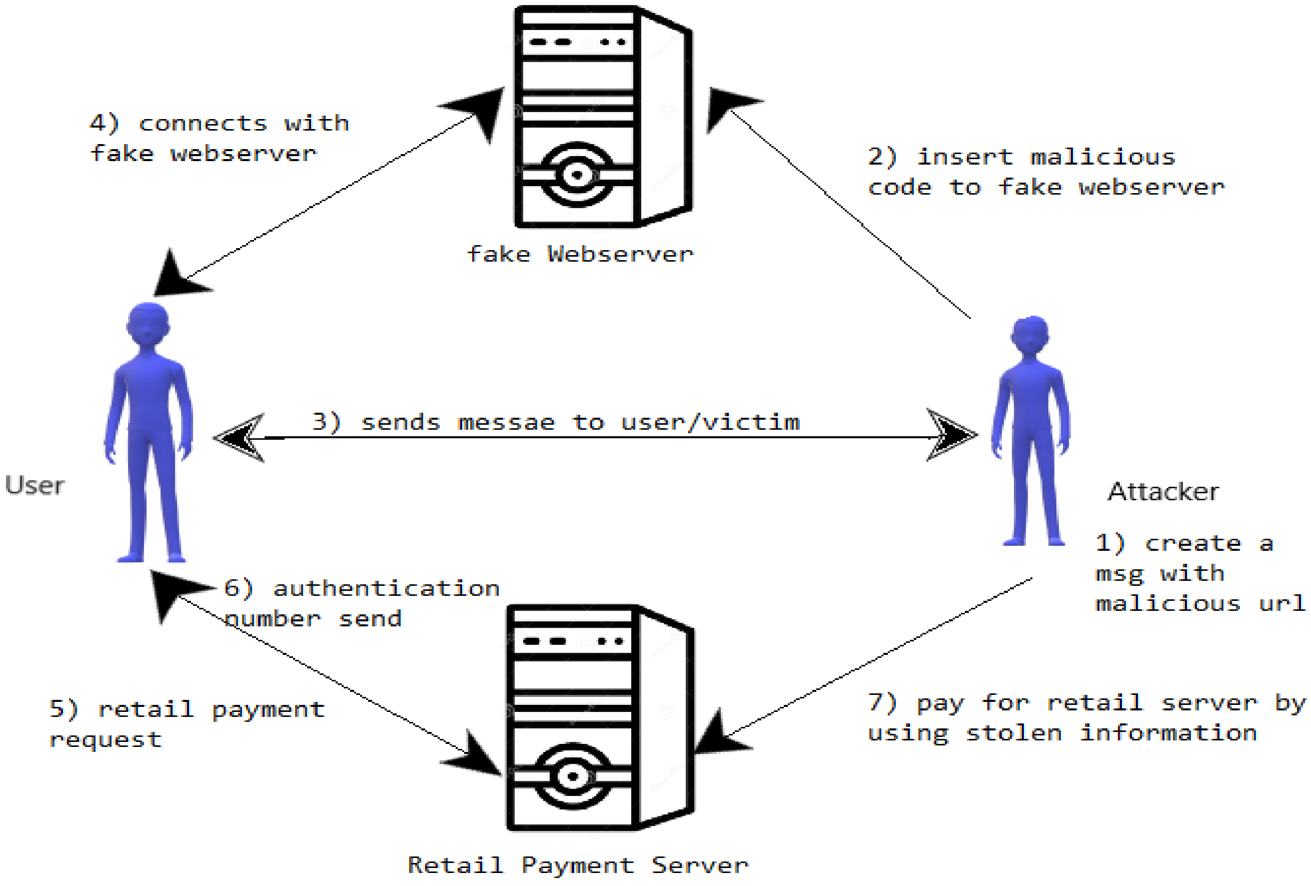

4) connects with fake webserver
fake Webserver
2) insert malicious code to fake webserver
3) sends messae to user/victim
User
Attacker
1) create a msg with malicious url
6) authentication number send
5) retail payment request
7) pay for retail server by using stolen information
Retail Payment Server

Fig 2. Smishing attack flow

The second type is where the message seems to be from very official sites like bank messages. This type of message may contain some alerting information like your account has been debited by some Rs. XXXX or to change some PIN etc. and they will be providing a link that will redirect the user to a fake bank website which will look the same as the legitimate one. When u enter your details like credit card or debit card number and CVV or pin all the information will be passed to the attacker. The attacker can further use your sensitive details and steal all your money.

III. Security Considerations for Android Devices

In this part, we explain about security considerations required for android devices for tackling smishing messages. We use the URL Validation Test or URL validation technique here to check whether the URL present in the message is spam or legitimate.

URL Validation Test:
this test helps to know the validity of the URL present in the message. This test performs a comparison among the URL present in the message using a smartphone application. This test works according to the following steps:

Step1: The attacker sends a message to the victim which include the URL
Step2: The application checks the presence of a URL. If the URL does not present then the message is directly sent to the message box.
Step3: The URL is inspected thoroughly by the application. If the URL is legitimate then it is moved to the message box.
Step4: If the URL is not authentic then a warning is given to the user and the message is flagged as dangerous.

The above steps are represented diagrammatically in fig 3. Where Y and N represent yes and no respectively. And the arrow shows the flow of the diagram.

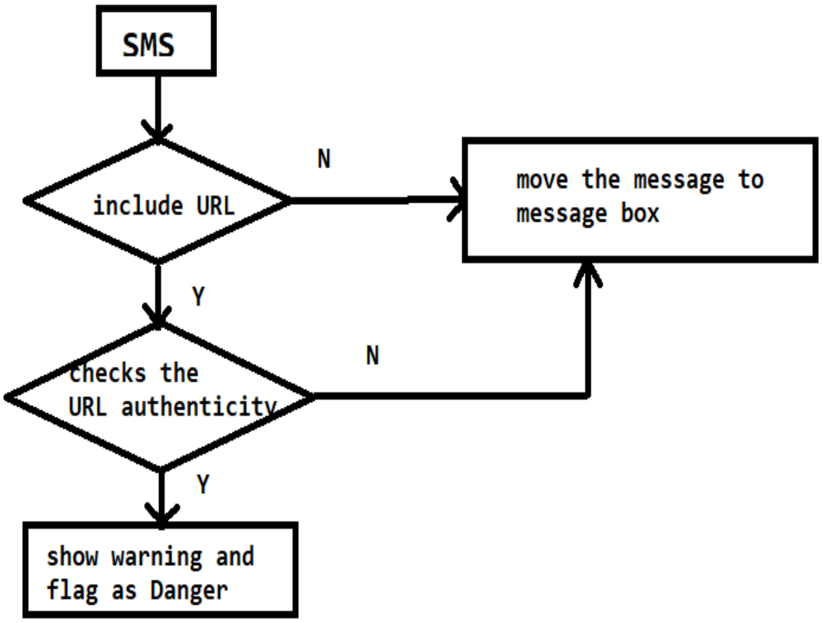

SMS
include URL
N
move the message to message box
Y
checks the URL authenticity
N
Y
show warning and flag as Danger

Fig 3. URL validator diagrammatic representation

IV. VISHING

Vishing is the social engineering attack intended for the victim to provide some personal data for financial fraud. Vishing is primarily based on Voice over Internet Protocol, or VOIP. Most of the attackers fix their strategy to trigger human emotions like fear, sympathy, and greed to accomplish their goals. Sometimes vishers pretend to call from a bank number and ask the victim to punch their Credit Card, Debit Card, and CVV or PIN. Further, they record all this information and use it for doing some unauthorized transactions through their bank account. Sometimes the attacker calls the victim and sends them some message and asks the user to open it and click on the link, and when the user's click on it malicious code is installed to his device.

Some common vishing attacks:

1. "compromised" Bank account: The person on the other end will always pretend that there is any issue with your bank account or with any of the payment apps you use. They will always ask for your bank details or card details.
2. Investment & Loan offers: Here the person on other hand will give you information about some loan with a very low-interest rate or sometimes these people seduce you to buy some stocks or shares which never exist. In short, they scam making you invest in some fake sites.
3. Tax Scam: sometimes you get a call and the person pretend to be from some income tax department and tells you that you have not paid the tax or your tax has been increased warrant is issued and you will be arrested. It also tells you don't call back if something goes wrong with your tax. The main aim here is to fear the victim and ask for his details.
4. Medical Care: Here most of the victims are elderly people. The attacker calls the victim and gives a too good to be a true offer to people regarding medicare enrollment and then asks for financial details or bank account numbers.

Preventing of Vishing attacks:

Most of the times the vishing attackers have offer which is too good to be true so we must always be alert if such offer comes to us easily. Following steps can be followed to tackle the same:

- Block the caller
- Use apps which identifies unknown numbers (e.g. Truecaller)
- Hang up the call
- Gather information about the caller and details for which he called you.

V. CONCLUSION

Phishing is a malicious cybercrime by which victim's crucial data is gathered with the help of victim only. In this paper discusses kinds of smishing attacks. Further, we discuss security considerations for android devices against smishing attacks using an URL validator test which checks the legitimacy of the message. We also discussed various types of these smishing attacks and measures of how to prevent them. Vishing is a cybercrime that takes place via phone calls. In vishing attacks mostly negative human emotions are triggered. Types of such vishing attacks are also discussed and some preventive measures are also listed which can prevent such attacks. This attack continues as long as we are not aware of it and know the preventive measures to prevent such attacks. So, the best way is to learn about this and make people aware.

VI. FUTURE WORK

In the future, more techniques should be proposed to prevent more versatile threat methods. Our current systems are lacking security in ensuring the legitimacy of the application, URLs, messages, etc. Hence, to ensure application security, we must plan to insert a Malware detector to identify malicious apps in our future work. This will focus on more research work to provide security against personal information leakage and to detect malicious applications downloaded. Also, a method can be created where the biometric method (eye recognition, fingerprint recognition, etc.) is mandatory to use before logging or making any transactions from crucial sites like bank websites, etc.

VII. ACKNOWLEDGEMENT

The author is sincerely thankful to B.K. Birla College of Arts, Science, and Commerce for providing the platform and opportunity to write a research paper on behalf of the department. The research is partially supported by **Prof. Swapna Augustine Nikale** for Supervision & review of the paper. The author would also like to thank the anonymous reviewers for their valuable comments and support.

REFERENCES

1. Aonzo, S. (2018). Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 1788–1807. https://doi.org/10.1145/3243734
2. Baykara, M., & Gurel, Z. Z. (2018). Detection of phishing attacks. 2018 6th International Symposium on Digital Forensic and Security (ISDFS), 1. https://doi.org/10.1109/isdfs.2018.8355389
3. Darwish, A., Zarka, A. E., & Aloul, F. (2012). Towards understanding phishing victims' profile. 2012 International Conference on Computer Systems and Industrial Informatics, 0. https://doi.org/10.1109/iccsii.2012.6454454
4. Sreelekha, B., Harika, B., & Sujihelen, M. (2019). Detecting phishing website using Pattern Mining. IOP Conference Series: Materials Science and Engineering, 590, 012024. https://doi.org/10.1088/1757-899x/590/1/012024
5. cui, Q. I. A. N., Jourdan, G.-V., Bochmann, G. V., Courturier, R., & Onut, L.-V. (2017). Tracking Phishing Attacks Over Time. WWW '17: 26th International World Wide Web Conference, 667–676. https://dl.acm.org/doi/10.1145/3038912.3052654
6. Kang, A., Dong Lee, J., Kang, W. M., Barolli, L., & Park, J. H. (2014b). Security Considerations for Smart Phone Smishing Attacks. Lecture Notes in Electrical Engineering, 467–473. https://doi.org/10.1007/978-3-642-41674-3_66
7. Jain, A. K., & Gupta, B. B. (2018b). Rule-Based Framework for Detection of Smishing Messages in Mobile Environment. Procedia Computer Science, 125, 617–623. https://doi.org/10.1016/j.procs.2017.12.079
8. Jain, A. K., Yadav, S. K., & Choudhary, N. (2020b). A Novel Approach to Detect Spam and Smishing SMS using Machine Learning Techniques. International Journal of E-Services and Mobile Applications, 12(1), 21–38. https://doi.org/10.4018/ijesma.2020010102
9. Balim, C., & Gunal, E. S. (2019b). Automatic Detection of Smishing Attacks by Machine Learning Methods. 2019 1st International Informatics and Software Engineering Conference (UBMYK), 1. https://doi.org/10.1109/ubmyk48245.2019.8965429
10. Mishra, S., & Soni, D. (2019b). SMS Phishing and Mitigation Approaches. 2019 Twelfth International Conference on Contemporary Computing (IC3), 1. https://doi.org/10.1109/ic3.2019.8844920
11. Mishra, S., & Soni, D. (2020). Smishing Detector: A security model to detect Smishing through SMS content analysis and URL behavior analysis. Future Generation Computer Systems, 108, 803–815. https://doi.org/10.1016/j.future.2020.03.021

12. Abdelhamid, M. (2020). The Role of Health Concerns in Phishing Susceptibility: Survey Design Study. Journal of Medical Internet Research, 22(5), e18394. https://doi.org/10.2196/18394

13. Hiremath, R., Malle, M., & Patil, P. (2016). Cellular Network Fraud & Security, Jamming Attack and Defenses. Procedia Computer Science, 78, 233–240. https://doi.org/10.1016/j.procs.2016.02.038

14. A.A. Ojugo, and O. Otakore, “Mitigating Social Engineering Menace in Nigerian Universities.” Journal of Computer Sciences and Applications, vol. 6, no. 2 (2018): 64-68. doi: 10.12691/jcsa-6-2-2

15. Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing Detection: A Literature Survey. IEEE Communications Surveys & Tutorials, 15(4), 2091–2121. https://doi.org/10.1109/surv.2013.032213.00009

16. Sharif, O., Hoque, M. M., Kayes, A. S. M., Nowrozy, R., & Sarker, I. H. (2020). Detecting Suspicious Texts Using Machine Learning Techniques. -, 1. https://doi.org/10.20944/preprints202008.0033.v1

17. Sonowal, G., Kuppusamy, K. S., & Kumar, A. (2017). Usability evaluation of active anti-phishing browser extensions for persons with visual impairments. 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 1. https://doi.org/10.1109/icaccs.2017.8014654

18. collection of spam message dataset retrieved from - https://www.kaggle.com/uciml/sms-spam-collection-dataset

19. Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. Computers & Security, 26(1), 73–80. https://doi.org/10.1016/j.cose.2006.10.009

20. collection of messages dataset retrieved from - https://www.kaggle.com/akashkr/phishing-website-dataset

21. collection of other messages dataset retrieved from - https://www.kaggle.com/shravan3273/sms-spam

22. Jamil, A., Asif, K., Ghulam, Z., Nazir, M. K., Mudassar Alam, S., & Ashraf, R. (2018). MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook. 2018 IEEE International Conference on Big Data (Big Data), 1. https://doi.org/10.1109/bigdata.2018.8622505

23. Chen, X., Liu, X., Zhang, L., & Tang, C. (2019). Optimal Defense Strategy Selection for Spear-Phishing Attack Based on a Multistage Signaling Game. IEEE Access, 7, 19907–19921. https://doi.org/10.1109/access.2019.2897724

24. Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI ’06, 1. https://doi.org/10.1145/1124772.1124863

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com