"Proximity" an All-in-One Automated Phishing Attack Tool with Built in Anonymous Mass Mailer

Lingeshvaaran Linganathar[1,*], Vinesha Selvarajah[2]

[1,2]*Asia Pacific University of Technology & Innovation (APU), Malaysia*
[*]*Corresponding author. Email: TP046116@mail.apu.edu.my*

ABSTRACT
Phishing is a rapidly rising threat in the cyber world, costing internet users billions of dollars per year. It is an illicit operation that requires the use of a mixture of social engineering and technologies to gather personal information from Internet users. Many cyber-attacks are distributed through mechanisms that leverage end-user vulnerabilities, rendering end-users the weakest link in the security chain. Phishing techniques can be performed in various methods; however, email is the most popular medium. This paper explores why users need to understand phishing and the need for a system that demonstrates how real-world phishing attacks are conducted. The developed system is a Linux Based python tool named "Proximity" an All-in-One Automated Phishing Attack Tool with a built-in Anonymous Mass Mailer.

***Keywords**: Phishing, Ethical Hacking, Cyber Security, Anonymous Email.*

1. INTRODUCTION

The definition of phishing describes the act of cybercrime in which a person impersonates a genuine entity and then proceeds to contact the victim or target by email, phone, or text message to persuade them to provide private information such as personal information, and confidential information such as bank number and passwords [1] [13-15]. The information is then utilized to get access to sensitive accounts, which can result in identity theft and financial harm [1] [8-12].

In the past, several phishing attempts were delivered in bulk to a vast number of users at the same time, resulting in impersonal greetings. The emails will often use familiar words like "customer," "employee," or "patient" to address the client [2]. According to a new FBI survey, phishing scams are the most prevalent form of Internet crime today. The same report highlights that people lost more than $57.8 million in 2019 because of phishing, which includes over 114,000 victims in the United States [2].

As phishing gets more profitable, hackers are becoming more proficient in the ways they employ to obtain credentials, according to Tanmay Ganacharya, a principal director of Microsoft's Computer Security team [3]. In some situations, a hacker can spoof an executive's email address and send a letter to workers warning them that they have been laid off and instructing them to log into the network as soon as possible to fill out a form to collect their severance pay [4]. Employees then click on a malicious link to their company's network and enter their usernames and passwords without understanding it is a fake.

However, in the background, the attacker captures all the employee's credentials which he can then proceed to do many malicious things [4]. Hackers are constantly researching company's employees and discovering their communication behaviour through email before spoofing them. They will collect sensitive information from executives' or their family members' social media pages and learn, for example, that they are about to go on holiday [4] [16-19].

With all these worrying reports, statistics, and anecdotes, it is necessary that a modern phishing tool is developed that is equipped with modern functionality that reflect current and real-world phishing attacks.In this project, the proposed tool will be able:

- To perform a variety of real-world online phishing attacks on user accounts as well as an added unique functionality of sending anonymous mass emails.

- To allow users to customize their phishing link.
- To help educate students and the average computer user on how phishing attacks are conducted in real life.
- To help security professionals test the security awareness of their employees.

2. MATERIALS AND METHODS

To develop the project, the materials and method will be explained in the subsections below.

2.1 Materials

For the development of the project, there are several materials required. It is important to choose an appropriate programming language for the development of the system. The developer has chosen Python as the programming language for system development because it is easy to learn and has extensive support of libraries. The IDE chosen for this project is PyCharm because it is one of the best and dedicated IDE for Python. The developer will utilize the ngrok module for this project. The Operating System that will be used is Parrot OS.

2.2 Software Development Methodology

The developer has decided to choose the Rapid Application Development (RAD) model as the methodology to develop the All-in-one phishing tool with an anonymous mass mailer. Due to the project duration being 3 months, this model is useful for developing systems in a short period. Besides that, the requirements of the project can be altered or changed right up to the 3rd phase of the model, till the requirements are fulfilled by both the developer and FYP supervisor. This model allows the supervisor to give feedback on what is needed to be implemented to the system, while the development of the system is undergoing. Moreover, this model helps to reduce the project risk due to the flexibility and adaptability of changing the requirements. Compared to the waterfall model, adjustments can only be made at the start, and once made, they cannot be altered anymore. Therefore, Rapid Application Development (RAD) is the model that will be chosen to develop the All-in-one phishing tool with an anonymous mass mailer, as it encourages and prioritizes customer feedback, requirements can be altered any time, and the development time is short compared to other models. The phases of RAD are requirements planning, user design, rapid construction, and transition. The Requirements Planning stage is like a project scoping session. Although the preparation stage is simplified relative to other methodologies in project management [5]. Developers, consumers (software users) and team members collaborate at this point to decide the priorities and objectives for the project, as well as actual and future challenges that should be resolved during development [5].

The User Design stage is a critical component of the RAD methodology, and it is what distinguishes it from other project management approaches. During this phase, clients work closely with developers to ensure that their demands are met at all stages of the design process [5]. The Rapid Construction stage takes from the design stage the prototypes and beta structure and transforms them into the operating model [5]. Because many of the concerns and changes were resolved through the complete iterative design phase, developers may create the final operational model faster than they could by using a traditional project management strategy. This phase breaks down into coding and unit, integration, and system testing [5]. The final phase, transition, is where the finished system is launched into their environment.

2.3 Research Methods

The research method aims to help the developer have a better understanding of the target users concerning the proposed tool through data gathering. There are two types of research methods that will be used by the developer which are qualitative and quantitative method.

Qualitative analysis gathers knowledge about previous experiences, feelings, or behaviours, as well as the meanings that people assign to them. The aim is to help the developer acquire a better understanding of how cultures interact within society and their interactions. This research approach is useful for evaluating how or why things occur [6].

Quantitative research is applied to measure or quantify the problem by generating numerical data and produce a statistic from the data gathered [6]. The developer can quantify the opinions or generalize the results from the respondents about the proposed system.

For the project “Proximity” an All-in-One Automated Phishing Attack Tool with a built-in Anonymous Mass Mailer, the developer has chosen a questionnaire as the research method. A questionnaire is a research method that is made up of open-ended questions or closed-ended question. The questionnaire aims to gather appropriate data from the respondents which can be used for research purposes [7]. The developer will gather the primary research on the respondent’s level of understanding of phishing and what features that can be added to reflect the results.

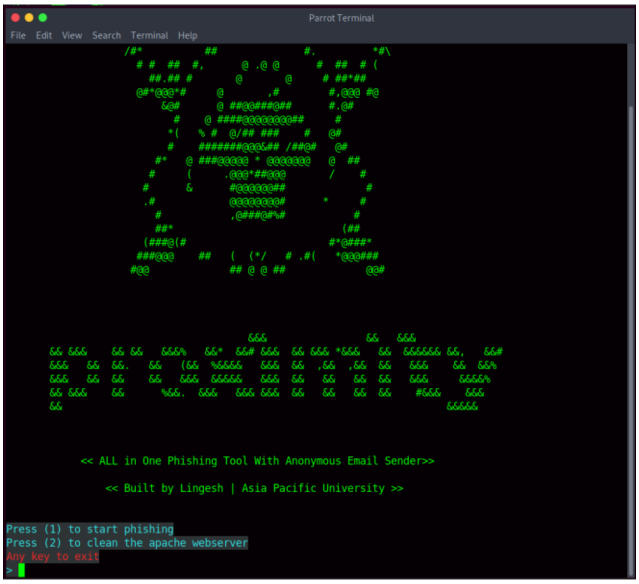
3. RESULTS AND DISCUSSION

By performing the questionnaire, the statistics and data have been collected from the 30 respondents assisted the developer significantly to develop the proposed tool. Besides that, the results from the questionnaire help the developer to determine the features that can be included in the All-in-One Automated Phishing Attack Tool with a built-in Anonymous Mass Mailer. The majority of the respondents have heard of the term "phishing", however, many of them unable to detect or identify a phishing email, thus giving a positive reply to the development of this tool. The questionnaire is a suitable research method for this project. The questionnaire helped in identifying knowledge and perception of phishing of computer users, of different age and educational background.

4. DEVELOPED TOOL

Below are screenshots and an explanation of each page of the developed tool.

4.1 Homepage

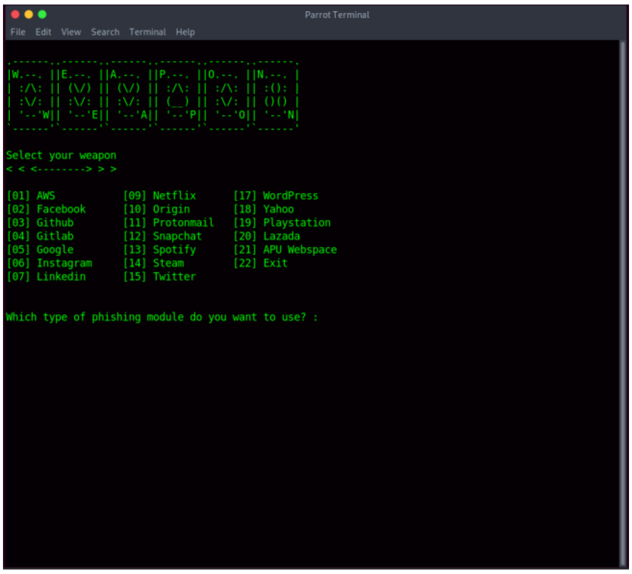


```
        << ALL in One Phishing Tool With Anonymous Email Sender>>

            << Built by Lingesh | Asia Pacific University >>


Press (1) to start phishing
Press (2) to clean the apache webserver
Any key to exit
>
```

Figure 1 Homepage

The user will be directed to this page if he/she answered "Y" on the disclaimer page. There are two options on this page which are (1) start phishing and (2) to clean the apache webserver. If the user answers "1" the user can begin selecting their phishing page. If the user answers "2", the user can clean their apache webserver.

4.2 Select Phishing Page

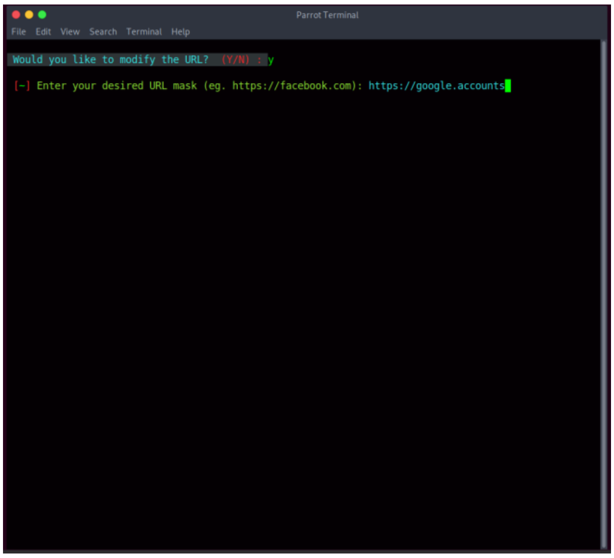


```
.------.,------.,------.,------.,------.,------.
|W.--. ||E.--. ||A.--. ||P.--. ||O.--. ||N.--. |
| :/\: || (\/) || (\/) || :/\: || :/\: || :(): |
| :\/: || :\/: || :\/: || (__) || :\/: || ()() |
| '--'W|| '--'E|| '--'A|| '--'P|| '--'O|| '--'N|
`------'`------'`------'`------'`------'`------'

Select your weapon
< < <--------> > >

[01] AWS          [09] Netflix      [17] WordPress
[02] Facebook     [10] Origin       [18] Yahoo
[03] Github       [11] Protonmail   [19] Playstation
[04] Gitlab       [12] Snapchat     [20] Lazada
[05] Google       [13] Spotify      [21] APU Webspace
[06] Instagram    [14] Steam        [22] Exit
[07] Linkedin     [15] Twitter


Which type of phishing module do you want to use? :
```

Figure 2 Select Phishing Page

When the user answered "1" on the homepage, this the page he/she will be directed to. On this page, the user can select any of the 19 phishing pages available as their phishing module. The user can select their desired phishing module by simply clicking the number associated with it.

4.3 Customize URL Phishing Link Page

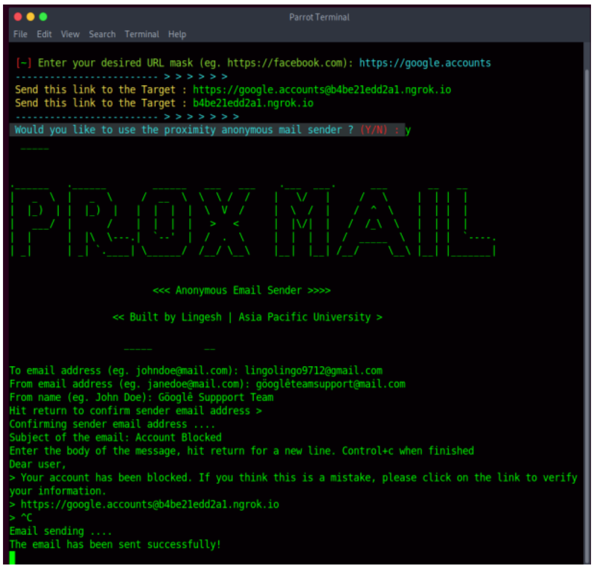


```
Would you like to modify the URL?  (Y/N) : y

[-] Enter your desired URL mask (eg. https://facebook.com): https://google.accounts
```

Figure 3 Customize Phishing URL Link

Once the user has clicked on their desired phishing module, he/she will be directed to this page. On this page, the user is given an option to customize the URL of their phishing link. The user can type their desired URL in the command line prompt.

4.4 Proximity Anonymous Mailer Page



```
Parrot Terminal
File  Edit  View  Search  Terminal  Help

[-] Enter your desired URL mask (eg. https://facebook.com): https://google.accounts
------------------------- > > > > > >
Send this link to the Target : https://google.accounts@b4be21edd2a1.ngrok.io
Send this link to the Target : b4be21edd2a1.ngrok.io
------------------------- > > > > > > >
Would you like to use the proximity anonymous mail sender ? (Y/N) : y
  _____


.______   .______      ______  ___   ___   .___  ___.      ___      __   __
|   _  \  |   _  \    /  __  \ \  \ /  /   |   \/   |     /   \    |  | |  |
|  |_)  | |  |_)  |  |  |  |  | \  V  /    |  \  /  |    /  ^  \   |  | |  |
|   ___/  |      /   |  |  |  |  >   <     |  |\/|  |   /  /_\  \  |  | |  |
|  |      |  |\  \----.|  `--'  | /  .  \    |  |  |  |  /  _____  \ |  | |  `----.
| _|      | _| `._____| \______/ /__/ \__\   |__|  |__| /__/     \__\|__| |_______|


                    <<< Anonymous Email Sender >>>>

               << Built by Lingesh | Asia Pacific University >

                    _____         __

To email address (eg. johndoe@mail.com): lingolingo9712@gmail.com
From email address (eg. janedoe@mail.com): gööglêteamsupport@mail.com
From name (eg. John Doe): Gööglê Suppport Team
Hit return to confirm sender email address >
Confirming sender email address ....
Subject of the email: Account Blocked
Enter the body of the message, hit return for a new line. Control+c when finished
Dear user,
> Your account has been blocked. If you think this is a mistake, please click on the link to verify
your information.
> https://google.accounts@b4be21edd2a1.ngrok.io
> ^C
Email sending ....
The email has been sent successfully!
```

Figure 4 Proximity Anonymous Mailer Page

Once the link has been given, the user will have the option to use the proximity anonymous mailer. If the user answers “N” the user will be directed to another page where he/she can view the capture credentials. If the user answers “Y” the user can begin to use the proximity anonymous mailer. Here the user can type in the recipient email address, their desired email address and sender name, subject and message.

5. CONCLUSION

The development of “Proximity” an All-in-One Automated Phishing Attack Tool with built-in Anonymous Mass Mailer has overall been a success. The developer has fulfilled all the project aim, objectives, and deliverables stated at the start of the project. The response towards the system has been positive as the users find it incredibly useful in understanding how phishing is conducted and how emails can be spoofed to appear legitimate.

Even though the proposed system provides significant benefits to many computer users, there are several limitations to be accessed and evaluated before deploying the project to the public. One of the major challenges that may occur upon the deployment of this system is, firstly due to the project being open-source, finding end-users that will use the system and programmers that can contribute to the source code of it will be the first task. It cannot be denied that students or security professionals in the field of cybersecurity will be quite sceptical upon hearing of this project due to reasons being that the system might be malicious or if that they do not know what the project is all about. Therefore, detailed and comprehensive documentation on what the system is about and the functionalities of it would need to be prepared and distributed to the users to ensure that they understand what the system offers and guarantee no security risks. In addition, the codes that were used in this project would need to be transparent for public viewing so the project can gain trust among the ethical hacker community, removing all suspicions of any malicious intentions.

In the end, the developer has improved his time management and has exhausted his coding knowledge in developing “Proximity” an All-in-One Automated Phishing Attack Tool with a built-in Anonymous Mass Mailer. The help of the developer’s supervisor has given motivation and confidence in developing the project despite the tough situation that was faced by many regarding COVID-19 and online schooling.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my university supervisor DR. Vinesha A/P Selvarajah for the guidance and support she provided to me throughout the development of my FYP including both the system and final documentation. Besides that, I would like to thank my friends for the stimulating discussions that resulted in many new and innovative ideas. Lastly, I would like to thank my family for supporting me throughout my life.

REFERENCES

[1] C. Armada, "What is Phishing - Cyber Armada," 24 July 2019.[Online].Available:https://www.cyber-armada.com/phishing.

[2] A. Gendre, "Phishing Awareness Training: 8 Things Your Employees Should Understand," 16 May 2019. [Online].

Available:https://www.vadesecure.com/en/phishing-awareness-training-8-things-employees-understand/.

[3] A. Holmes, "Hackers are getting better at tricking people into handing over passwords," 24 July 2020. [Online]. Available:https://www.businessinsider.co.za/phishing-scams-getting-more-sophisticated-what-to-look-out-for-2020-2-2.

[4] Ryan and Kevin, "Phishing Is Getting More Sophisticated. Here's What to Look Out For," 17 January 2020. [Online]. Available:https://www.inc.com/kevin-j-ryan/cybersecurity-data-breaches-hacks-how-ceo-use-tech-survey.html.

[5] Lucidchart, "4 Phases of Rapid Application Development Methodology,"2020.[Online].Available: https://www.lucidchart.com/blog/rapid-application-development-methodology.

[6] Libguides, "Research Methods: What are research methods?,"2017.[Online].Available: https://libguides.newcastle.edu.au/researchmethods.

[7] QuestionPro, "The ultimate guide to great questionnaires," 2018.[Online].Available: https://www.questionpro.com/blog/what-is-a-questionnaire/.

[8] Subramani, P., Al-Turjman, F., Kumar, R., Kannan, A. and Loganthan, A., 2021. Improving medical communication process using recurrent networks and wearable antenna s11 variation with harmonic suppressions. Personal and Ubiquitous Computing, pp.1-13.

[9] Prabu, S., Velan, B., Jayasudha, F.V., Visu, P. and Janarthanan, K., 2020. Mobile technologies for contact tracing and prevention of COVID-19 positive cases: a cross-sectional study. International Journal of Pervasive Computing and Communications.

[10] Sujan, L.J.L., Telagadi, V.D., Raghavendra, C.G., Srujan, B.M.J., Prasad, R.V., Parameshachari, B.D. and Hemalatha, K.L., 2021. Joint Reduction of Sidelobe and PMEPR in Multicarrier Radar Signal. In Cognitive Informatics and Soft Computing (pp. 457-464). Springer, Singapore.

[11] Ashish, D., Raghavendra, C.G., Prajwal, B.R., Parameshachari, B.D. and Hemalatha, K.L., 2021. Reduction of PMEPR in Multicarrier Signals Using CBC Approach. In Cognitive Informatics and Soft Computing (pp. 669-683). Springer, Singapore.

[12] Kumar, M.K., Parameshachari, B.D., Prabu, S. and liberata Ullo, S., 2020, September. Comparative Analysis to Identify Efficient Technique for Interfacing BCI System. In IOP Conference Series: Materials Science and Engineering (Vol. 925, No. 1, p. 012062). IOP Publishing.

[13] Shahriar, Md Rakib, SM Nahian Al Sunny, Xiaoqing Liu, Ming C. Leu, Liwen Hu, and Ngoc-Tu Nguyen. "MTComm based virtualization and integration of physical machine operations with digital-twins in cyber-physical manufacturing cloud." In 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 46-51. IEEE, 2018.

[14] Nguyen, N.T. and Liu, B.H., 2018. The mobile sensor deployment problem and the target coverage problem in mobile wireless sensor networks are NP-hard. IEEE Systems Journal, 13(2), pp.1312-1315.

[15] Pham, D.V., Nguyen, G.L., Nguyen, T.N., Pham, C.V. and Nguyen, A.V., 2020. Multi-topic misinformation blocking with budget constraint on online social networks. IEEE Access, 8, pp.78879-78889.

[16] L. Tan, K. Yu, F. Ming, X. Cheng, G. Srivastava, “Secure and Resilient Artificial Intelligence of Things: a HoneyNet Approach for Threat Detection and Situational Awareness”, IEEE Consumer Electronics Magazine, 2021, doi: 10.1109/MCE.2021.3081874.

[17] Z. Guo, K. Yu, A. Jolfaei, A. K. Bashir, A. O. Almagrabi, and N. Kumar, “A Fuzzy Detection System for Rumors through Explainable Adaptive Learning”, IEEE Transactions on Fuzzy Systems, doi: 10.1109/TFUZZ.2021.3052109.

[18] C. Feng et al., "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," IEEE Network, vol. 35, no. 1, pp. 130-137, January/February 2021, doi: 10.1109/MNET.011.2000223.

[19] Z. Guo, L. Tang, T. Guo, K. Yu, M. Alazab, A. Shalaginov, “Deep Graph Neural Network-based Spammer Detection Under the Perspective of Heterogeneous Cyberspace”, Future Generation Computer Systems, https://doi.org/10.1016/j.future.2020.11.028.