Comparative Analysis of Phishing Tools on Social Media Sites

Putu Candra Ariani[1], I Gede Bagastia Widi Atmaja[2], Kadek Sukma Jayanti[3], I Gusti Agung Ayu Ananda Dewi[4], Gede Arna Jude Saskara[5], I Made Edy Listartha[6]

[1,2,3,4,5,6]Faculty of Engineering and Vocational, Ganesha University of Education, Singaraja, Indonesia

[1]candra.ariani@undiksha.ac.id, [2]bagastia.widi@undiksha.ac.id, [3]sukma.jayanti@undiksha.ac.id, [4]agung.ayu.ananda@undiksha.ac.id, [5]jude.saskara@undiksha.ac.id , [6]listartha@gmail.com

Accepted 09 December 2022
Approved 29 December 2022

***Abstract*— Social networks, often referred to as social media are a form of information technology development. Social networks are used by society in obtaining information, being a means of long-distance communication, as well as distributing information. However, behind the development of social media which has experienced significant developments, there are problems related to information security. Vulnerable to leakage of credential data and fraud becomes a negative impact due to the development of social media, one of the scams that often occurs on social media is phishing. Such scams are attempts to obtain, steal, or dig into someone's data through emails, text messages, and social media posts. Social media accounts are targeted by phishing criminals because they consist of sensitive data of social media users, one of the social media accounts that can be affected by phishing attacks is Facebook. The problem studied in this study is the way criminals use three different types of phishing tools to carry out attacks. This study aims to compare three phishing tools used in committing information crimes on social media sites in terms of features, accuracy, and ease of installation each of these phishing tools. With this research, readers can understand the comparison of these phishing tools used by hackers to access social media accounts.**

***Index Terms*— accounts; information security; phishing; phishing tools; social media**.

I. INTRODUCTION

Social media is an important part of people's daily life. In general, information needs to encourage people to use social media as a means of communication, obtaining information, and entertainment. The most common examples of social media are Instagram, TikTok, Facebook, Twitter, and YouTube [1]. Social media is a medium that allows a person to socialize by sharing content, news, and photos with others or can be a tool to promote as well as work [2]. Web dictionaries define social media (nouns) simply as, "Websites and applications used for social networks". It is noted that a total of 160 million people in Indonesia use social media descriptions with a percentage of smartphone use at 62%, computers at 16%, and tabs at 6% [3]. Facebook is one of the social media platforms where people can share statuses, moments, and photos and sell something there, this platform stores a lot of users' personal information and can be a risk if security does not work. One interesting aspect of Facebook is the use of apps and third-party interactions. This means that each Facebook page now acts as a web page, blog, instant messaging, email system, and third-party applications that enable real-time functionality [4]. On the Facebook site, there is a statistic on the number of Facebook users which states that active Facebook users have reached more than 300 million users. Even in Indonesia, the number of Facebook users is increasing every year and the percentage of Facebook users is 2997.3% in just 1 year [5].

The rapid development of social media and providing benefits to society is one of the positive impacts of technological advances, but the use of social media is also detrimental to society. Information security threats are negative impacts arising from the development of social media, various cases of information security threats often occur on social media accounts [6]. This can happen due to the negligence of social media users, and service providers, or the deliberate negligence of information criminals. Therefore, people who use social media must have been exposed to the risks of social media itself [7]. Crime attacks on social media have many types of attacks, one of which is phishing, these attacks are scams against social media users because the perpetrator will trick the victim into obtaining and digging someone's data through emails, or uploads on social media [8]. Phishing is in many ways an evolutionary threat, phishing can become bigger and worst if hackers get personal information [9].

Hackers usually do phishing to steal the victim's personal information, or simply try their expertise in Web Security (white hackers), phishing can be done on a Facebook account by duplicating a login site, and using the link to make the victim believe and logging in via a link. The existence of a phishing tool can make it easier for perpetrators to phish the victim's account because this phishing tool can be downloaded for free so it allows the perpetrator to carry out fraud attacks freely without any obstacles.

Thus, to examine the problems that have been previously presented, the phishing tools in this study consist of three types, namely Social Engineering Toolkit (Setoolkit), SocialFish, and HiddenEye. These three tools have uses to carry out various kinds of attacks, but the focus of this research is on the use of these tools in carrying out phishing attacks on target accounts. Testing on all three phishing tools will be carried out on the Kali Linux operating system and the social media account to be tested is a Facebook account. With this test, the public knows the performance of phishing tools in manipulating social media accounts to obtain the personal data of the account owner concerned. The tools will be tested and then analyzed for a comparison of the performance contained in each tool.

II. Methodology

A. Research Methods

In this test, the researcher uses a qualitative comparative method, which means that the researcher will compare the results of this test. Qualitative research includes research that explains research using analysis and is descriptive, while comparative is comparative research.

Qualitative methods are generally defined as "a collection of methods and rules followed in science or discipline"[10]. Qualitative methods have been widely used in research in Indonesian journals. Meanwhile, comparative research is research that focuses on the research subject group, then continues by focusing on the study of variables in the comparative group [11]. Comparative research is ex post facto, which means data is collected after all the events to be studied have occurred.

B. Research Design

In these tests, the results are created based on each tool’s data and test objectives. The tools used by the Tester are the Social Engineering Toolkit (Setoolkit), SocialFish, and HiddenEye which have been tested on Kali Linux OS. The purpose of this test is to compare and analyze the differences between each tool. Testers install each tool first on a computer with Kali Linux OS and perform phishing tests on each tool. The comparison of each tool is accurate, the features, and the effectiveness of each tool, and get a valid conclusion.

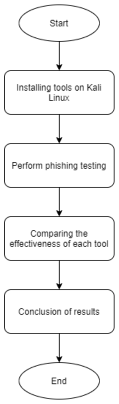

Start
Installing tools on Kali Linux
Perform phishing testing
Comparing the effectiveness of each tool
Conclusion of results
End

Fig. 1. Testing the Design Flowchart

III. Results and Discussion

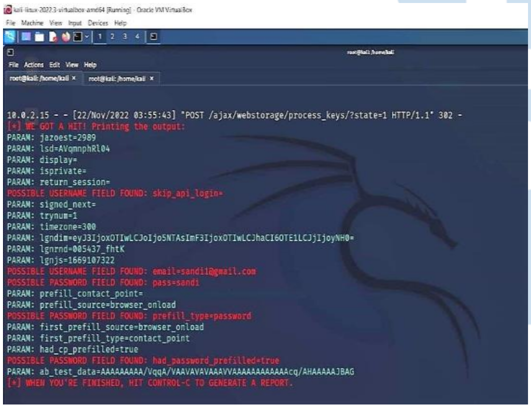
A. Setoolkit (Social Engineering Toolkit)

Social Engineering Toolkit or called Setoolkit is a tool that uses phishing methods and serves as manipulation of login pages on a site, the main purpose of this tool is to get information about the target account, especially in the password section [12]. Setoolkit can also be mentioned as an integrated set of tools specifically designed to carry out follow-up attacks on the human element [13]. These tools are used to find information on emails or find social media account passwords. By using the phishing method, the hacker must make the target click on a fake link that has been created by the hacker, usually, the hacker will approach the target by sending a link along with an attractive image that aims to make the target fall into a trap. The way Setoolkit works starts with hackers sending fake links through social media like email and so on. After the target clicks on the link that the hacker has sent, the target will be directed to a fake site, and on the site, there is a login form with the same appearance accompanied by convincing words so that the target will not realize that the site is just a clone. All information in the form of a username or Email and password that the target enters into the form such as login will be automatically saved to the hacker's PC. Therefore, the hacker will know the password and username of the target account so that the hacker can immediately change the password of the target account and get the hang of it.

1) Testing

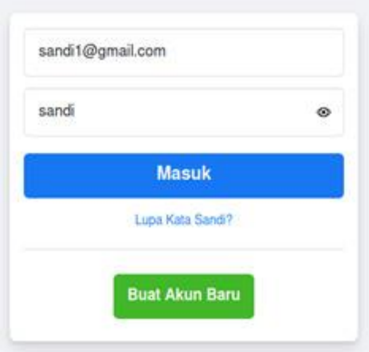
- In the first step, open the Kali Linux command terminal.
- Then write the command 'sudo su' and the password that was pre-created in Kali Linux in the terminal.
- Next, open the Social Engineering Toolkit that has been installed with the 'setoolkit' command.
- After that, choose option number 1 Social Engineering Attack.

- Then, select option number 2 Website Attack Vector.
- Select option number 3 of the Credential Harvester Attack Method.
- Select option number 2 in the Site Cloner section.
- Then create a new terminal file to get the IP address, with the same command as the previous terminal, write 'sudo su' and enter the password.
- Write the command 'ifconfig' to get the IP address then copy the selection.
- Paste the IP address selection on the first terminal.
- Enter the Facebook URL www.facebook.com.
- Copy the IP address and paste it into a browser on Kali Linux OS, for example, Firefox.
- The Facebook login menu will appear, it is a manipulated version of the phishing IP address.
- Targets enter their email and password, for example, using an email sandi1@gmail.com and password: password.
- After entering the email and password then click the login button and the tools will read the previous input data and appear in the terminal as a result of phishing (email and password).


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali
root@kali: /home/kali

```
10.0.2.15 - - [22/Nov/2022 03:55:43] "POST /ajax/webstorage/process_keys/?state=1 HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2989
PARAM: lsd=AVqmnphRl04
PARAM: display=
PARAM: isprivate=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=300
PARAM: lgndim=eyJ3IjoxOTIwLCJoIjo5NTAsImF3IjoxOTIwLCJhaCI6OTE1LCJjIjoyNH0=
PARAM: lgnrnd=005437_fhtK
PARAM: lgnjs=1669107322
POSSIBLE USERNAME FIELD FOUND: email=sandi1@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=sandi
PARAM: prefill_contact_point=
PARAM: prefill_source=browser_onload
POSSIBLE PASSWORD FIELD FOUND: prefill_type=password
PARAM: first_prefill_source=browser_onload
PARAM: first_prefill_type=contact_point
PARAM: had_cp_prefilled=true
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=true
PARAM: ab_test_data=AAAAAAAAA/VqqA/VAAVAVAVAAAVVAAAAAAAAAAAAAcq/AHAAAAAJBAG
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Fig. 2. Testing on Setoolkit


sandi1@gmail.com

sandi

Fig. 3. Setoolkit Phishing Results

The testing steps are said to be successful by gathering real evidence. A little review in the seventh step because the hacker will phish the Facebook account so that the option in no. 2, namely the cloner site, functions so that it can enter the official website of the Facebook account, namely www.facebook.com.

2) Result

Setoolkit can phish a Facebook account at any Linux time using a pre-customized Ip address according to the one in the terminal. But in experiments, there are errors caused by signal interference. However, if you want to phish in Linux times with a device such as a different laptop, the network or localhost must be the same as this can be the cause of the error.

B. SocialFish

In the world of social engineering, SocialFish is a tool that many hackers use to carry out phishing, especially email fraud. SocialFish is one of the Kali Linux tools that offer to phish on social media such as Facebook, Twitter, and Instagram as a feature [14]. With SocialFish it is necessary to get the target to click on the link to cheat the email. SocialFhis is one of the third-party tools outside of Linux, in contrast to the Social Engineering Toolkit or Setoolkit. SocialFhis must be installed first. In addition, the third version of the Python programming language needs to be installed for the tool to be used smoothly. In running SocialFish it is necessary to create a net to capture the target to be targeted. It is intended for users of the tool to create URLs http://0.0.0.0:5000 the address of this URL is used to trap the intended target. Most tools in general have provided the URL address of phishing attacks, for example, Facebook, Instagram, Twitter, and others. SocialFish is more flexible, so in using SocialFish users only copy links that will be the target of phishing, then the links will be duplicated into fake links which later the duplicate links previously had a http://0.0.0.0:5000 URL address. So, internet users who open fake links enter their login data so that it will appear in the SocialFish tool.

1) Testing

Testing the security of www.facebook.com pages from phishing attacks using one of the tools, called SocialFish v3, this tool is a third-party tool from the Linux operating system times. Here's how to test the security of www.facebook.com pages using the SocialFish v3 tool.

- SocialFish is a third-party phishing tool so it is necessary to download then install it to the directory, using the git clone command https://github.com/UndeadSec/SocialFish then wait until the installation process is complete.
- Run the pip install -r requirements.txt command to install the SocialFish requirements.
- Create a username and password that will be used to log in to the SocialFish web tool. With

the python3 command SocialFish.py username password.

- Next, go to the http://0.0.0.0:5000/neptune link then enter the username and password that have been created earlier.
- Then in the cloning and redirection column fill in the Facebook social media web link. Then refresh the http://0.0.0.0:5000 link then the link will become a fake link from Facebook.
- The features provided by the SocialFish tool don't have many advantages. The use of these tools is done completely manually without providing significant features. Users of this tool are required to enter the Facebook website address into the cloning and redirection field which will then be duplicated into a fake site that resembles a real URL.
- Next, the test is carried out ten times to obtain an accurate result. The first test was carried out to find out the accuracy of the "space" key on the keyboard because it was known that the "space" key can be entered into the password. A second test is performed to find out the standard rule on email, whether users can enter email addresses randomly. A third test was conducted to find out the standard rules on passwords because Facebook passwords are known to have at least eight characters. The fourth test is carried out in violation of the standard rules for both (email and password). The fifth test was carried out without entering an email address and password at all. And the sixth to tenth tests repeat the previous test from the first test to the fifth test to get the correct data accurate.

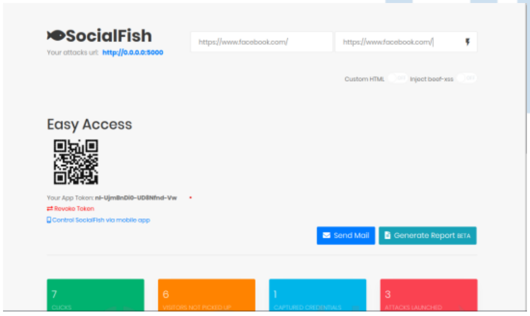
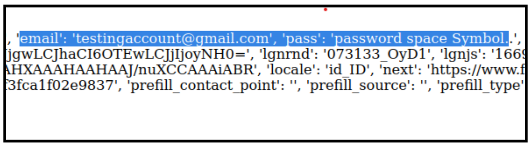

SocialFish
Your attacks url: http://0.0.0.0:5000
https://www.facebook.com/
https://www.facebook.com/
Custom HTML
Inject beef-xss
Easy Access
Your App Token: nl-UjmBnDI0-UD8Nfnd-Vw
Revoke Token
Control SocialFish via mobile app
Send Mail
Generate Report BETA
7
CLICKS
6
VISITORS NOT PICKED UP
1
CAPTURED CREDENTIALS
3
ATTACKS LAUNCHED

Fig. 4. Testing on SocialFish

2) *Result*



```
, 'email': 'testingaccount@gmail.com', 'pass': 'password space Symbol..',
jgwLCJhaCI6OTEwLCJjIjoyNH0=', 'lgnrnd': '073133_OyD1', 'lgnjs': '1669
AHXAAAHAAHAAJ/nuXCCAAAiABR', 'locale': 'id_ID', 'next': 'https://www.f
f3fca1f02e9837', 'prefill_contact_point': '', 'prefill_source': '', 'prefill_type'
```

Fig. 5. SocialFish Phishing Results

Setoolkit can phish a Facebook account at any Based on the results of ten tests, the first accuracy test found that the username testingaccount@gmail.com and with a password named Symb0l password space ... not fully stated to be accurate. This is because the password cannot record "space" on the keyboard, has only one space spacing, and cannot be more than one space. In the second test, the result was that the standard and non-standard formats in E-mail and passwords could be recorded well. Then the third test had the result that passwords that were less than eight characters could be recorded in this tool. Please note that the results obtained are not only recorded results, but this tool does not have some kind of feature to recognize the standard format in E-mail and password of Facebook users. Although the results of some tests say that the results are indeed all well-recorded. However, there is one problem that is said to be less accurate, that is, the "space" button is not recorded properly as is usually done by users, that is, it can create a password with just the "space" button.

C. *HiddenEye*

HiddenEye is a highly effective Social Engineering tool that can be used to collect user credentials, and miscellaneous information [15]. This tool can be a great asset in an Enterprise-level Penetration Test or any other engagement. HiddenEye is included as a third-party tool that provides the most menu features in carrying out phishing attacks. Unlike the previous tools, HiddenEye has provided a phishing menu feature so that users only use these tools. These phishing tools are used by testers to phish the target's Facebook account, but there are other features in it such as Instagram or Twitter phishing. This feature is only for certain reasons and should not be used for illegal activities. HiddenEye does not exist by default in Kali Linux, so to use this tool the user needs to download it twice, namely on Kali Linux devices and operating systems. To use this tool, users only need to select the phishing menu provided by HiddenEye. For example, a tool user wants to use the menu feature on the Facebook page site, and in using the Facebook phishing feature, a URL will be given which is used as a medium in launching phishing attacks on the target to be targeted. Just like phishing tools in general, to use the HiddenEye tool the user simply copies or clones the original site. For example, on https://www.facebook.com site copy the URL https//127.0.0.1:1028. If the target enters a copied or fake URL, login data such as the Email and Password of the target will be sent to the HiddenEye tools so that the login data can be seen by the user of the HiddenEye tool.

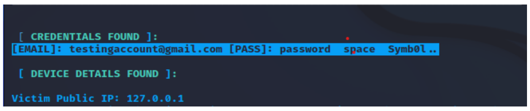
1) *Testing*

The security testing on the www.facebok.com website using the HiddenEye tool is:

- The first thing that needs to be done is to download the HiddenEye tools using the git clone https://github.com/Morsmalleo/HiddenEye command and then wait for the installation process to complete.

- To enter the directory by performing the cd HiddenEye command. Next, download the Requirements file with the pip3 install -r requirements.txt command and wait for the installation process to complete.
- Run the tool from HiddenEye by using the python3 HiddenEye.py -h command.
- HiddenEye is designed to perform phishing attacks completely with a variety of features. There are several menu features options for carrying out phishing attacks, such as Facebook, Instagram, Netflix, Google, and others. And this test only focuses on the Facebook website.
- Inside the Facebook website attack menu feature. There are sub-features such as standard phishing methods, phishing sub-features using polling methods, phishing sub-features with methods of providing fake security information messages to users, and phishing sub-features through fake trust messages. But basically, these tools use the same methods to capture user information, but the feature aims to create different attack methods so that phishing attacks are much more effective and have minimal failures.
- Then, this test uses a local server with the URL address already provided by HiddenEye with the URL address http//127.0.0.1:1028/. URLs are used as a medium to launch phishing attacks or in other words URLs that match the original site so that the URLs look similar.
- Furthermore, at this stage using ten tests can produce maximum tool accuracy data. The first test was carried out to find out the accuracy of the "SPACE" key on the keyboard because it became known that the "SPACE" key can be entered in the password. The second test is performed to find out the standard rules in email and whether it is possible to select any Email for the user to enter. A third test was conducted to find out the standard password rules because it was known that the Facebook password has at least eight characters. The Fourth Test is performed by violating the standard rules of both (Email and Password). The fifth test was done by not entering the Email and Password at all. And the sixth to tenth tests repeat the previous test from test one to the fifth test to get the correct accurate data.

2) *Result*



```
 [ CREDENTIALS FOUND ]:
[EMAIL]: testingaccount@gmail.com [PASS]: password  space  Symb0l..

 [ DEVICE DETAILS FOUND ]:

Victim Public IP: 127.0.0.1
```

Fig. 6. HiddenEye Phishing Results

The results of the ten tests above are known that the first test by entering the username testingaccount@gmail.com and password: password space Symb0l... Get the test results that this tool has good accuracy to capture passwords from Facebook users because the "space" button is recorded on the password in the first test. Then the second test got the result that not all standard formats in E-mail can be recorded. It is accurate, but this tool cannot tell if the email has a standard format or just the text is recorded. In the third test, Facebook's rule was known that passwords must have at least eight characters to be declared valid. However, this tool only captures the user's password even if there is only one character in the password. And the fifth test got the result that, if the user does not enter the data into the tool, the tool will automatically record even though they did not enter the E-mail and Password. In other words, this accuracy test is said to be accurate, since every recorded data result entered by the user will be recorded as a whole. Although this tool cannot figure out how to format the standard email and password of Facebook users.

D. *Comparative Analysis*

Here is a comparison of the tests performed on the three phishing tools.

TABLE I. COMPARISON BY FEATURE

No.	Tools	Feature
1.	Setoolkit	The available features are easy to implement and the error problems are minimal, when phishing Facebook users there are no problems. The instructions for using the Setoolkit tools are clear and simple
2.	SocialFish	SocialFish does not have any superior features that are effective for carrying out phishing attacks. The features provided by SocialFish are limited to generating fake URLs only and no direct attack features are provided
3.	HiddenEye	HiddenEye features a social media menu to carry out phishing attacks directly. This feature is useful for carrying out phishing attacks without having to enter a URL which is then spoofed

TABLE II. COMPARISON BASED-ON ACCURACY

No.	Tools	Feature
1.	Setoolkit	Setoolkit cannot record "spaces" on the keyboard, this is inaccurate if the target enters a password that has spaces
2.	SocialFish	SocialFish is inaccurate in phishing because the "space" button is not recorded correctly, it is only recorded once and is not recorded more than twice the space in the character
3.	HiddenEye	The accuracy of HiddenEye tool is very accurate, login data such as Emails and passwords are well recorded even if they use "spaces". Because "space" can be used as a password in an account. Therefore the HiddenEye tool is accurate and effective in phishing

TABLE III. COMPARISON BASED-ON EASE OF INSTALLATION

No.	Tools	Feature
1.	Setoolkit	Setoolkit is available by default in Kali Linux operating systems. Users do not need to download the installation package from third parties and users can use it directly and easily
2.	SocialFish	SocialFish needs to be downloaded from a third party. The user must copy the original URL to the fake URL as a phishing site, then the fake URL can record the user's login data
3.	HiddenEye	HiddenEye requires downloading installation packages from third parties. The menu feature has been provided by HiddenEye. Users only use the available menu and do not need to create a new URL to launch a phishing attack

IV. CONCLUSIONS

Based on the results of a comparison of Setoolkit, HiddenEye, and SocialFish tools conducted ten tests, it can be concluded that:

1. The three tools tested are phishing tools that can be used on the Kali Linux operating system and have the same function, which can phish emails along with the password of the intended account. Despite the differences in how it works, the output remains the same.
2. In phishing, the three tools have their advantages and disadvantages which can be seen from the comparison between the features, accuracy, and convenience offered by each of these tools, such as the features provided by the HiddenEye tools have various features compared to the Setoolkit and SocialFish tools. The accuracy rate of the HiddenEye and Setoolkit tools is higher than that of the SocialFish tool. And the Setoolkit tool is easier to use compared to the other two tools because the tool users do not need to download the Setoolkit tool from third parties.
3. With this test, Facebook social media users know how phishing is done by hackers working on the target Facebook account so that users can be more vigilant and always maintain account security which can be done by downloading the information security guard application.

ACKNOWLEDGMENT

The researcher would like to thank Mr. Gede Arna Jude Saskara and Mr. I Made Edy Listartha as teaching lecturers at the Ganesha University of Education who have supported and helped in guiding researchers to make articles well.

REFERENCES

[1] E. Dwi and S. Watie, "Communication and Social Media," *Journal of The Messenger*, vol. 3, no. 2, pp. 69–74, March 2016.

[2] V. Taprial and P. Kanwar, "Classification of Social Media," *Understanding Social Media*, pp. 30, 2012.

[3] P. Study Ilmu Komunikasi, "TREN PENGGUNAAN MEDIA SOSIAL SELAMA PANDEMI DI INDONESIA," 2020.

[4] S. Leitch and M. Warren, "Security Issues Challenging Facebook Security Issues Challenging Facebook Security Issues Challenging Facebook," 2009, doi: 10.4225/75/57b4188730df5.

[5] M. Hanafi, "PENGARUH PENGGUNAAN MEDIA SOSIAL FACEBOOK TERHADAP MOTIVASI BELAJAR MAHASISWA FISIP UNIVERSITAS RIAU," 2016.

[6] M. Betty Yel and M. K. M Nasution, "SECURITY OF PERSONAL DATA INFORMATION ON SOCIAL MEDIA," *JIK)*, VOL. 6, NO. 1, 2022.

[7] "Social Media Security: Leveraging Social Networking While Mitigating Risk – Michael Cross – Google Books."

[8] N. Vadila and A. R. Pratama, "Analisis Kesadaran Keamanan Terhadap Ancaman Phishing," *Automata*, vol. 2, pp 14-17, 2021.

[9] Z. Ramzan, "Phishing Attacks and Countermeasures," *Handbook of Information and Communication Security*, pp. 433-448, 2010.

[10] G. R. Somantri, "Memahami Metode Kualitatif," *Makara Human Behavior Studies in Asia*, vol. 9, no. 2, pp. 57 – 65, Dec. 2005, doi: 10.7454/mssh.v9i2.122.

[11] A. B. Sesuai, Dengan, ASI ttry, and R. Nur Sasongko, "PENELITIAN KOMPARATIF," 2009.

[12] S. Wahyuni, I. M. Raazi, and D. I. Dwitawati, "Analisis Teknik Penyerangan Phishing Pada Social Engineering Terhadap Keamanan Informasi di Media Sosial Profesional Menggunakan Kombinasi Black Eye dan Setoolkit," *Jurnal Nasional Komputasi dan Teknologi Informasi*, vol. 5, no. 1, 2022.

[13] N. Pavković and L. Perkov, "Social Engineering Toolkit — A systematic approach to social engineering," 2011 Proceedings of the 34th International Convention MIPRO, 2011, pp. 1485-1489.

[14] N. Helminen, K. Tero, and K. Sampo, "Description Information and communication technology," 2021.

[15] "John J Hacking." https://johnjhacking.com/blog/hiddeneye/ (accessed Nov. 15, 2022).

[16] UndeadSec, "UndeadSec SocialFish," June 11, 2022. https://github.com/UndeadSec/SocialFish (accessed November 15, 2022).

[17] Morshmalleo, "Morshmalleo HiddenEye," Sept. 06, 2022. https://github.com/Morsmalleo/HiddenEye (accessed November 19, 2022).