Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871

Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

Implementation and Analysis of QR Code Phishing Attacks on Indonesian Internet Banking Using Attack Tree and Time-Based Metrics

Shavira Eka Yuniati[1], Adityas Widjajarto*[2], Umar Yunan Kurnia Septo Hediyanto[3]

[1,2,3]Information System, Telkom University, Indonesia

Email: [2]adtwjrt@telkomuniversity.ac.id

Received : Jun 3, 2025; Revised : Jun 23, 2025; Accepted : Jun 25, 2025; Published : Feb 15, 2026

Abstract

The development of technology in Internet banking services facilitates customers' financial transactions. However, this can also create opportunities for cybercrime threats, including a quishing attack. A quishing attack is a type of phishing attack that uses a QR Code to redirect victims to a fake website to steal sensitive information. This research formulates an attack tree model for quishing attacks by combining OSINT, social engineering, and QR Code exploitation, structured using data flow diagrams and evaluated with time-based metrics. The attack was simulated as a Proof of Concept (PoC) to realistically depict the stages of exploitation. Results from the experiments show that the fastest attack path using the OSINT tool Truecaller, the social engineering tool SEToolkit, and the QR Code tool Qrencode takes 248.31 seconds. This path is considered more efficient, outperforming the second fastest combination, which uses the OSINT tool Find Mobile Number Location by 25.15 seconds, with a total time of 273.46 seconds. Truecaller's advantage lies in its ability to obtain data quickly without requiring a geographic location process like the Find Mobile Number Location tool. This approach shows that banking institutions can integrate time-based metric attack trees to assess vulnerability response times, simulate realistic threat scenarios, and develop more effective incident response strategies to prevent unauthorized access during quishing attacks.

Keywords : *Attack tree, Attack experiment, Quishing attack, Social engineering, Time metric*

1. INTRODUCTION

Information technology development has impacted various aspects of human life, especially in the financial or banking sector[1]. Internet banking is one of the banking services that makes it easier for customers to make online transactions. However, this development raises new challenges with the emergence of various cybercrime parties trying to take advantage of system weaknesses [2]. Cybercrime is a criminal act committed by utilizing the development of computer technology and the internet as the primary crime tools [3]. One form of cybercrime that is very commonly used is phishing, which aims to trick targets into sharing sensitive information such as account credentials, personal details, credit card and financial account information, etc [4]. This attack uses social engineering techniques, which utilize the target's weaknesses to obtain information, gain unauthorized access, and encourage the target to take specific actions [5].

Phishing incidents are rampant in online banking services at banks in Indonesia [6]. Phishing attacks may continue increasing and become a serious security threat to the banking sector. The impact of these attacks includes financial losses, resulting in leakage of sensitive customer data and a decline in reputation that can reduce customer confidence in the security and integrity of banking services [7]. Currently, there is a new type of cybercrime known as quishing. This attack combines phishing techniques with QR (Quick Response) technology to steal user information [8]. QR Code is a two-dimensional bar code capable of encoding various data types, such as binary, numeric, and alphanumeric, in digital images [9]. QR codes are becoming increasingly popular in sales and marketing

Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

activities. When a user scans a QR Code on billboards and banners, the smartphone will redirect the user to a website [10]. Along with the development of QR codes, criminals take advantage of security gaps to carry out QR code-based phishing attacks or quishing. In a quishing attack, a malicious QR Code redirects users to a fake website or app resembling a genuine site to acquire sensitive data, such as the user's personal information and login credentials [11].

To analyze quishing attacks, a structured threat modeling approach is required. Threat modeling is the process of using theoretical and practical security scenarios, system diagrams, methods, and testing tools to assess asset security and possible weaknesses, as well as the procedures used to discover potential vulnerabilities before they become system threats and suggest corrective actions and policies [12][13]. This research uses threat modeling to create an attack tree, a visual representation of a branching hierarchical diagram used to map various attack scenarios [14]. Each node in the attack tree depicts the steps or attack vectors required to achieve the goal of a threat [15]. By integrating time metrics at each stage, the duration of completion of each stage of the attack can be measured, and the time efficiency at each stage can be analyzed. Time metrics also allow the determination of the total duration of the attack as well as the time sequence in which the attack occurred [16].

Although various threat modeling methods have been developed and widely used to analyze cyber threats to systems such as STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN, each of these methods has a different focus, such as threat classification, risk assessment, or privacy compliance [12]. However, attack tree approaches that integrate time metrics are rarely applied, especially in quishing attacks. Research conducted by Naik et al. (2022) shows that a combination of attack trees and risk matrices can be used to evaluated potential attacks against Self-Sovereign Identity (SSI) systems, including identity faking attacks, identity theft, and Distributed Denial of Service (DDoS) attacks [17]. Although this approach is considered efficient and systematic, its application is still limited and has not been widely developed for quishing attack scenarios.

On the other hand, existing research on quishing is generally limited to the success rate of attacks and their impact on users without considering the temporal aspect. For example, Sharevski et al. (2022) showed that in a fake COVID-19 digital registration scenario using a QR code, 67% of users submitted their Google or Facebook account credentials, 18.5% created a new account, and only 14.5% did not register [18]. Research conducted by Marie et al. shows that quishing attacks against employees are as effective as conventional phishing but harder to detect. In contrast, based on LLM and OSINT data, email phishing gets 30% of employees to open links and 10% to hand over their credentials [19]. Another research by Putu et al. showed that social engineering tools such as SEToolkit successfully obtained Facebook account login data (email and password) with high accuracy[20]. However, these studies have not measured execution time to assess the efficiency of each attack stage, so there is still a gap in time-based threat modeling in the case of quishing.

Therefore, security testing is needed to protect data in public banking institutions against quishing attacks. The Open-Source Intelligence (OSINT) method finds vulnerabilities by obtaining public data [21]. In addition, it utilizes social engineering attacks to manipulate the target through a QR Code that is designed in such a way that it looks legitimate. The implemented QR Code will act as a link to direct the target to a fake website that is made to look like legitimate and authorized internet banking. The testing phase will be organized using a data flow diagram. A data flow diagram is a graphical representation that describes data flow through an information system and presents the business processes and data shared and exchanged between processes within the system and external entities [22][23]. By designing threat modeling using an attack tree, the quishing attacks can be evaluated by comparing test results and metrics [24].

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

2. METHOD

2.1. Framework Research

This research is systematically designed to analyze quishing attacks on Internet banking through attack tree modeling based on time metrics. To explain the methodology used, Figure 1 presents a research framework that illustrates the stages of problem-solving from the initial to the final stage.

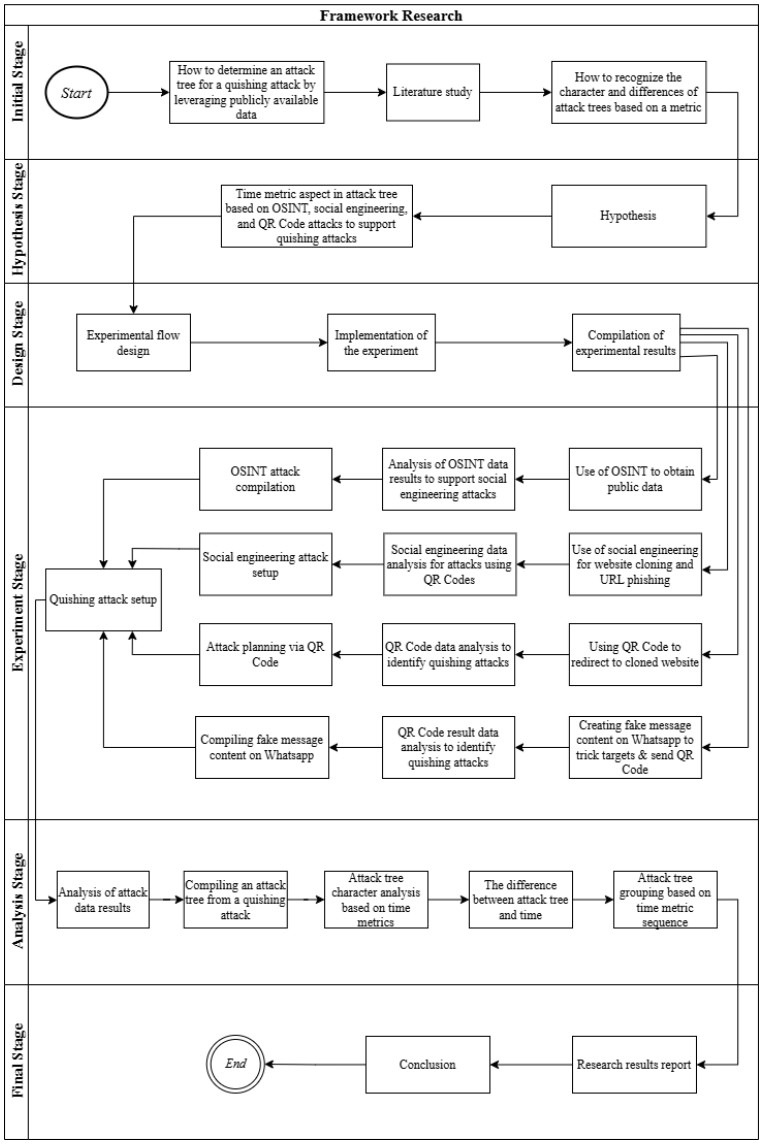


Figure 1. Research Framework

Figure 1 illustrates the research framework, which is divided into several stages:

1. **Initial Stage**
   The research begins by identifying how to determine the attack tree for quishing attacks by utilizing available public data. A literature study is conducted to understand the basic theories and concepts relevant to the research problem. Then, the characteristics and differences of attack trees based on time metrics are introduced through experiments**.**
2. **Hypothesis Stage**
   In the hypothesis stage, testable assumptions are formulated based on applying time metrics in attack trees for OSINT, social engineering, and QR Code attacks.

Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

3. **Design Stage**
   The design stage focuses on developing experimental scenarios for each OSINT, social engineering, and QR Code tool, followed by implementation to understand how each works. The resulting experimental data is then collected into tables and analyzed further.
4. **Experiment Stage**
   The experimental stage uses OSINT, social engineering, and QR Code tools to conduct quishing attack experiments. Data from each tool is then analyzed to assess the effectiveness of the attacks.
5. **Analysis Stage**
   The analysis stage begins by reviewing the experimental data to formulate an attack tree for each scenario. Each attack tree is analyzed using time metrics, then compared and ranked based on the difference in attack duration at each stage to determine its efficiency level. Time metrics are classified into Real, User, and System. In this research, the analysis is limited to the Real category, as it is representative of the other two categories.
6. **Final Stage**
   The final stage aims to compile a research report that concludes with findings from the experiments and analysis, along with suggestions for future research development.

2.2. Experiment Flow

The experimental flow outlines structured steps to collect and analyze data from simulated quishing attacks. The experiment flow consists of the following:

a. Experiment Flow Using OSINT Tool Truecaller

At this stage, verifying the target phone number has a WhatsApp account using Truecaller starts with accessing the tool and scanning the target phone number until the data identity and validation of the target Whatsapp account are obtained. Figure 2 presents an explanation of the experimental scenario using Truecaller in the form of a flowchart diagram.

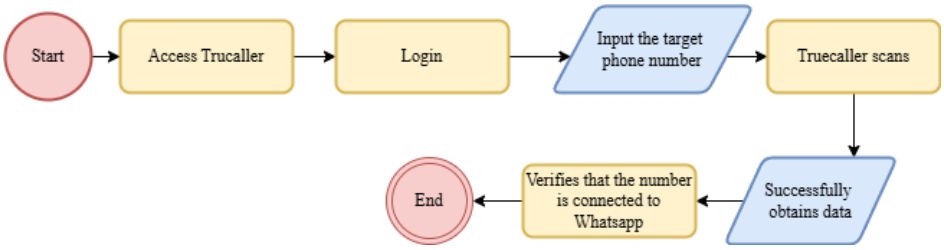


Figure 2. Experiment Flow Using OSINT Tool Truecaller

Overall, this experimental scenario allows the verification of whether a phone number is connected to the Whatsapp application with the OSINT tool Truecaller. The process will end after a successful connection with the Whatsapp account is obtained.

b. Experiment Flow Using OSINT Tool Find Mobile Number Location

At this stage, verifying that the target phone number has a WhatsApp account is done using Find Mobile Number Location, which is used from accessing the tool until data is obtained and the target WhatsApp account is validated. Figure 3 presents an explanation of the experimental scenario using Find Mobile Number Location in the form of a flowchart diagram.

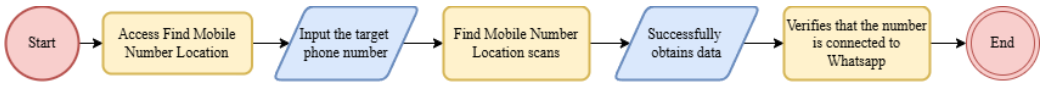


Figure 3. Experiment Flow Using OSINT Tool Find Mobile Number Location

Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

Overall, this experimental scenario allows verification of whether the phone number is connected to the Whatsapp application with the OSINT tool Find Mobile Number Location. The process will end after confirmation of a successful connection with a Whatsapp account is obtained.

c. Experiment Flow Using the Social Engineering Tool SeToolkit

At this stage, a cloned website is created using SeToolkit until a phishing URL is obtained that can trick the target and obtain the credential data entered by the target. Figure 4 presents an explanation of the experiment scenario using SEToolkit in the form of a flowchart diagram.

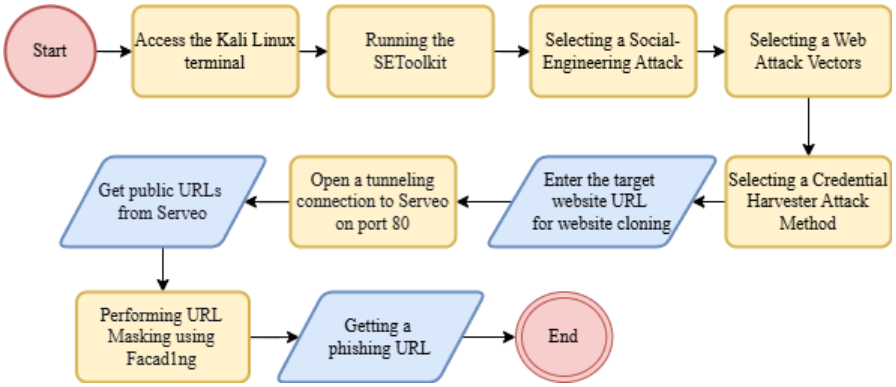


Figure 4. Experiment Flow Using Social Engineering Tool SEToolkit

Overall, the process of this experimental scenario allows the creation of cloned websites to obtain phishing URLs with social engineering attacks using SEToolkit. The process will end after SEToolkit generates an official-looking phishing URL that can be used to continue the attack.

d. Experiment Flow Using the Social Engineering Tool Dark-Phish

At this stage, a cloned website using Dark-Phish is created until a phishing URL can trick the target and obtain the credential data entered by the target. Figure 5 presents an explanation of the experimental scenario using Dark-Phish in the form of a flowchart diagram.

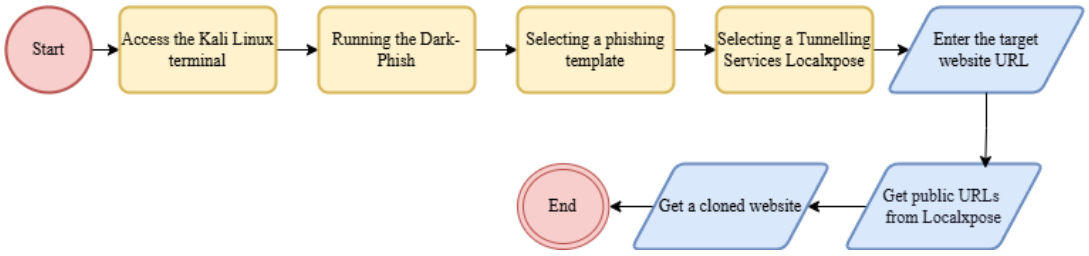


Figure 5. Experiment Flow Using Social Engineering Tool Dark-Phish

Overall, this experimental scenario allows for the creation of cloned websites to obtain phishing URLs with social engineering attacks using Dark-Phish. The process will end after Dark-Phish generates a cloned website that looks official and is used to continue the attack. However, the experimental scenario on Dark-Phish encountered a problem when it was run, which caused it to fail to continue the attack with Dark-Phish social engineering.

e. Experiment Flow Using QR Code Tool Qrencode

At this stage, the process of creating a QR Code using Qrencode is carried out until a QR Code can be obtained that can be used as a phishing attack medium. Figure 6 presents an explanation of the experimental scenario using the QR Code Tool in the form of a flowchart diagram.

Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

Figure 6. Experiment Flow Using QR Code Tool Qrencode

Overall, this experimental scenario allows for the generation of a QR Code containing the phishing URL obtained from the previous attack using Qrencode. The process will end after Qrencode generates a QR Code, which is used to continue the attack.

f. Experiment Flow of Quishing Attack Based on The Content of Fake Messages on WhatsApp

At this stage, the quishing attack process uses a QR Code with WhatsApp message content against customers until the target credential data is obtained. Figure 7 shows a flowchart diagram explaining the quishing attack experiment scenario based on fake WhatsApp content.

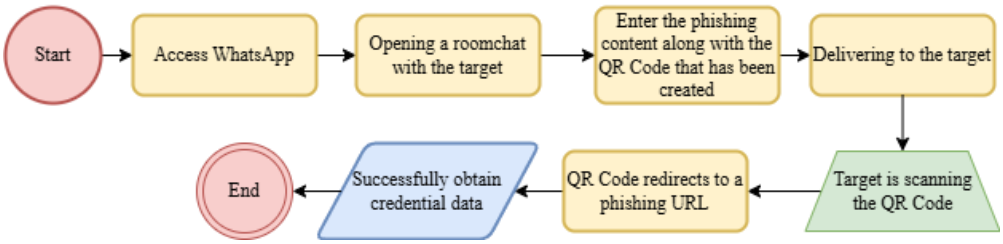


Figure 7. Experiment Flow of Quishing Attack Based on The Content of Fake Messages on WhatsApp

This quishing attack experiment scenario is limited to Proof of Concept (PoC), which means that it does not directly attack the target.

3. RESULT

3.1. Design and Preparation

Design and preparation are important initial steps before conducting experiments and attacks on targets. At this stage, hardware and software are required as supporting elements in this research to achieve the research objectives of the quishing attack experiment using OSINT techniques, social engineering, and QR codes.

3.1.1. Experimental Platform

The experimental platform aims to identify and describe the tools used in OSINT, social engineering, and QR Code attack experiments against targets.

Figure 8 illustrates the experimental platform that includes the Internet, Main OS, Mobile Device, and Kali Linux Virtual Machine as an attacker. The target in this experiment is the domain, and the target telephone number is the research object. The attacker uses a Mobile Device to run OSINT attacks and Kali Linux with IP Address 192.168.24.131/24 to run social engineering attacks and QR codes. On the Main OS, the attacker uses Windows 11 with IP Address 192.168.1.29/24. The attack is carried out through tunneling on port 80, which aims to connect the sending of a QR Code and phishing URL so that it can be accessed publicly on the internet.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

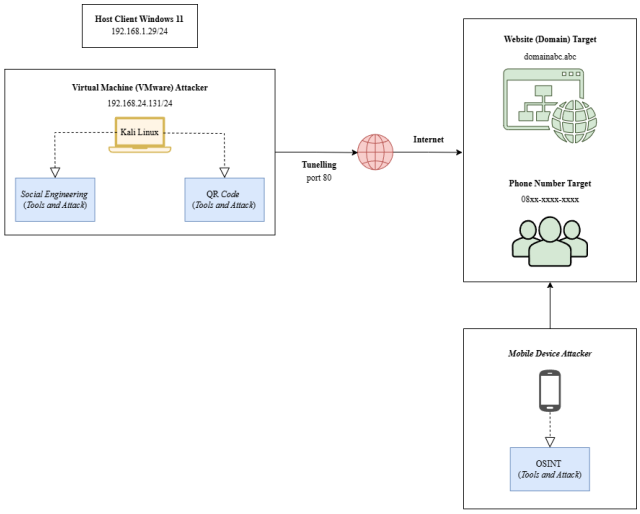


Figure 8. Experimental Platform

3.1.2. Software Spesifications

The software used in this research was selected to support each stage of the simulated quishing attack: target information collection, creating a cloned website, and distributing fake message content and fake QR Codes via WhatsApp. The details are presented in Table 1.

Table 1. Software Specifications

Type	Software
Operating System	Kali Linux
OSINT Tools	Truecaller Find Mobile Number Location
Social Engineering Tools	SEToolkit Dark-Phish
URL Masking Tools	Facad1ng
QR Code Generator	Qrencode
Tunneling Service	Serveo Localxpose

The selection of tools presented in Table 1 corresponds to the designed experimental flow and was evaluated based on their functional effectiveness during the experiment. Among the tools tested, eight tools were not used successfully due to various issues, such as limited data and errors during execution. Not successfully used tools were Get Contact, Whocalld, Spokeo, Spydialer, Number Finder, Emobile Tracker, Py.Pisher, and BlackEye.

3.2. Experiment Result Data

Experiment result data aims to present a table containing input and output data during the experimental process. The output data obtained will then be analyzed to identify which data is used to perform the quishing attack.

1. Experiment Result in Data Using OSINT Tool Truecaller

Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

The experimental results data using the Truecaller OSINT tool, which shows the input and output generated in the experimental process, are shown in Table 2.

Table 2. Experiment Result Data Using Truecaller OSINT Tool

Input	Output				
	Name	**Phone Number**	**WhatsApp Account**	**Address**	**Email**
08**-****-****	M***	08**-****-****	Connected and Valid	I*****a	m***@xx.yy.zz

Based on the data in Table 2, it can be concluded that the experimental data were obtained using the OSINT tool Truecaller, starting with the scanning process, which includes input data in the form of the target's phone number. The output data obtained is in the form of the target's name, phone number, email, address, and WhatsApp account, which is used in the quishing attack.

2. Experiment Result in Data Using OSINT Tool Find Mobile Number Location
   The experimental data using the OSINT tool Find Mobile Number Location, which shows the inputs and outputs generated in the experimental process, are shown in Table 3.

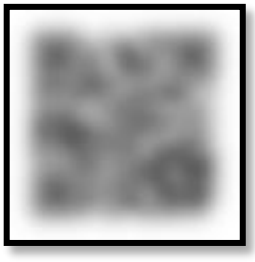
Table 3. Experiment Result Data Using OSINT Tool Find Mobile Number Location

Input	Output	
	Location	**WhatsApp Account**
08**-****-****	I******	Connected and Valid

Based on the data in Table 3, it can be concluded that the experimental data using Find Mobile Number Location started with a scanning process that included input data in the form of a target phone number. The output data obtained is the location and WhatsApp account of the target, which is used in the quishing attack.

3. Experiment Result in Data Using Social Engineering Tool SEToolkit
   After the SEToolkit social engineering experimentation process is successfully carried out, it will produce an output in the form of a cloned website like the original target website.
4. Experiment Result in Data Using Social Engineering Tool Dark-Phish
   After successfully carrying out the Dark-Phish social engineering experiment, it will produce output as a cloned website, unlike the original target website.
5. Experiment Result in Data Using QR Code Tool Qrencode
   The experimental data using the QR Code tool, which shows the inputs and outputs generated in the experimentation process, is shown in Table 4.

Table 4. Experiment Result Data Using QR Code Tool Qrencode

Input	Output
https://bank*****.co.id-account-login@xx.yy.zz	

Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

Based on the data in Table 4, it can be concluded that the experimental data used Qrencode with input data in the form of a phishing URL. The URL is then converted into a QR Code. The resulting QR Code can be sent to the target and scanned to access the phishing URL that has been created.

6. Experiment Result in Data Quishing Attack Using QR Code Containing SEToolkit Phishing URL Based on Fake Message Content on WhatsApp
   The experimental results of quishing attacks based on fake message content on WhatsApp targeting customers, including the inputs and outputs generated during the experiment process, are shown in Table 5.

Table 5. Experiment Results Data Quishing Attack Using QR Code Containing SEToolkit Phishing URL Based on Fake Message Content on WhatsApp

Input	Output	
	User Id	**Password**
Fake message content QR Code contains phishing URL	s******	2******

Based on the data in Table 5, it can be concluded that the results of the quishing attack experiment used fake message content on WhatsApp and QR codes as input data. This experiment was conducted by creating a fake message on WhatsApp designed to manipulate the target to scan the QR Code containing the phishing URL. Login credential data in the form of a user ID and target password will be recorded and visible on the terminal from SEToolkit.

3.3. Data Flow Diagram Based on Quishing Attack

The formulation of the attack aims to understand the scope and limitations of the successful experiment. The attacks carried out include OSINT attacks to collect target data, social engineering attacks that successfully cloned websites and generated phishing URLs, and limited QR Code attacks as Proof of Concept (PoC) using WhatsApp message content. The success of each attack can be identified through the formulation in the form of a data flow diagram.

a. Data Flow Diagram on using OSINT Truecaller, Social Engineering SEToolkit, and QR Code Qrencode Attacks
   In this formulation, a data flow diagram is created to map quishing attacks based on OSINT attacks with Truecaller, Social Engineering attacks with SEToolkit, and QR Code attacks with Qrencode, which will describe the data scenario in the implementation of quishing attacks. The process that occurs until the quishing attack is presented and explained in Figure 9.
b. Data Flow Diagram on using OSINT Find Mobile Number Location, Social Engineering SEToolkit, and QR Code Qrencode Attacks
   In this formulation, a data flow diagram is created to map quishing attacks based on OSINT attacks with Find Mobile Number Location, Social Engineering with SEToolkit, and QR Code with Qrencode, which will describe the data scenario in the implementation of quishing attacks. The process that occurs until the quishing attack is presented and explained in Figure 10.
c. Data Flow Diagram on using OSINT Truecaller and Social Engineering Dark-Phish Attacks**.**
   In this formulation, a data flow diagram is created to map the quishing attack based on OSINT attacks with Truecaller and Social Engineering with Dark-Phish, which will describe the data scenario in the implementation of the quishing attack. The process that occurs up to the quishing attack is presented and explained in Figure 11.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

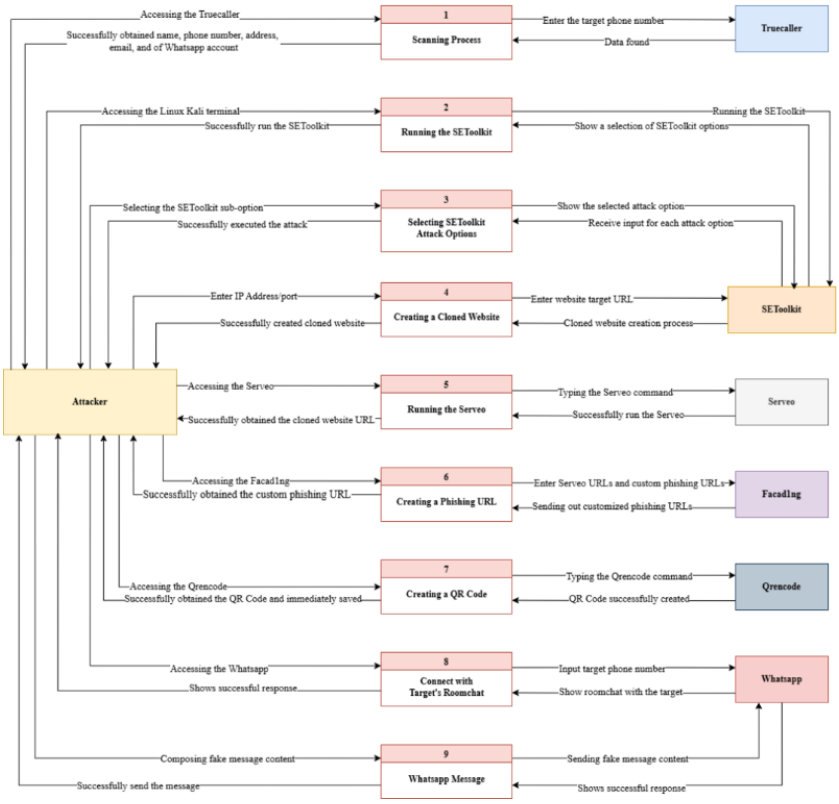


Figure 9. Data Flow Diagram on using OSINT Truecaller, Social Engineering SEToolkit, and QR Code Qrencode

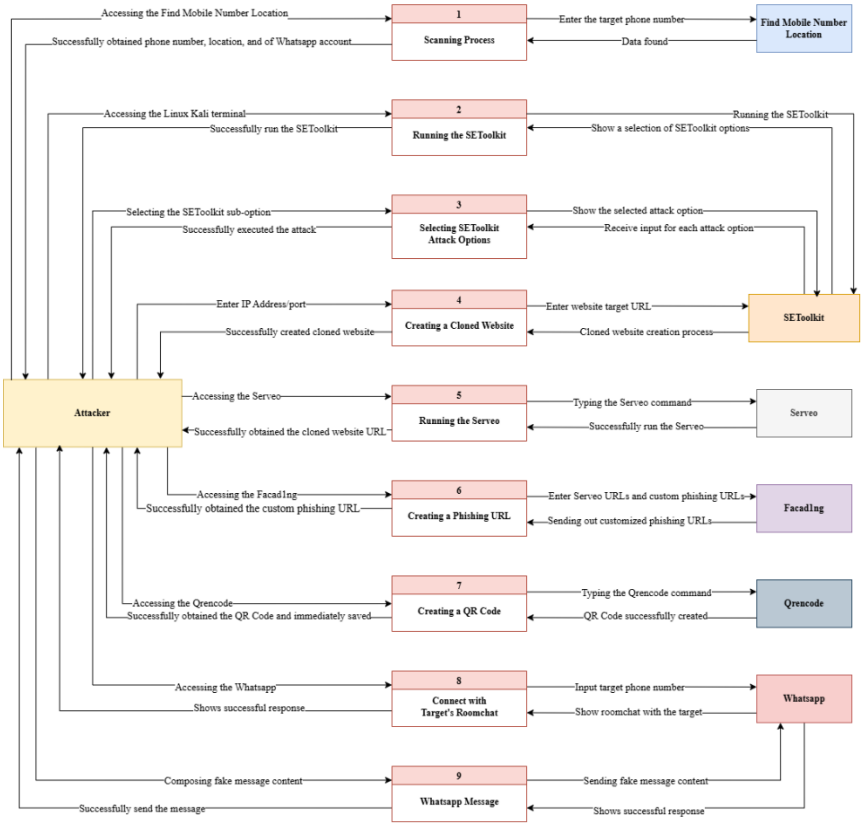


Figure 10. Data Flow Diagram on using OSINT Find Mobile Number Location, Social Engineering SEToolkit, and QR Code Qrencode Attacks

Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

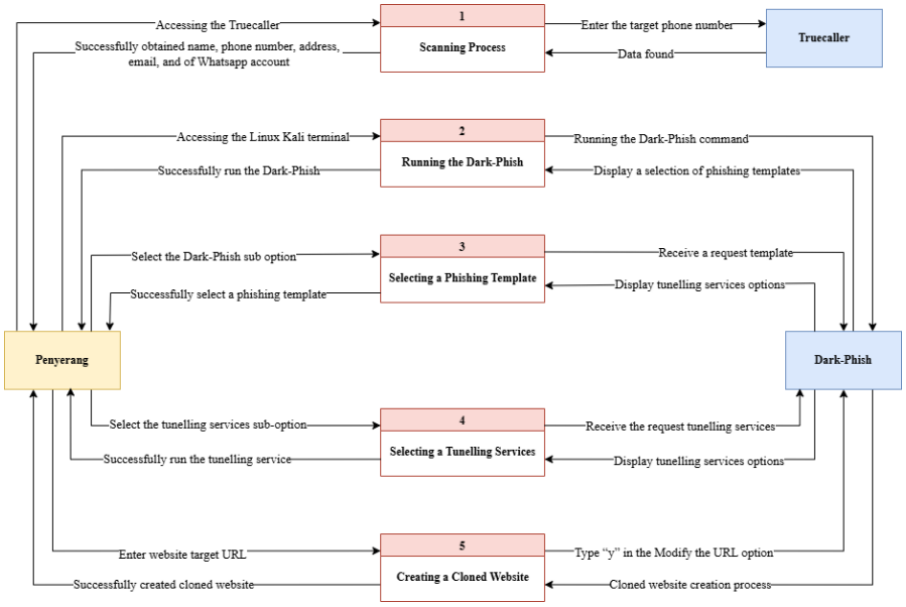


Figure 11. Data Flow Diagram on using OSINT Truecaller and Social Engineering Dark-Phish Attacks

The use of the Dark-Phish tool was not fully successful because the cloned website created was not completely similar and and recording target credential data was limited. This prevented the process of compiling the data flow diagram from being carried out thoroughly until the target credential data stage was obtained.

3.4. Time Measurement in Quishing Attack

Time metric measurement aims to identify, measure, and record the amount of time required in the quishing attack process or stage. Measurements are performed automatically using the $ time command on the Linux terminal to record the total duration in one execution or manually using a stopwatch tool.

1. Time Measurement Results Using OSINT Truecaller, Social Engineering SEToolkit, and QR Code Qrencode

Based on Table 6, the measurement results of the time of the quishing attack based on the OSINT Truecaller, social engineering SEToolkit, and QR Code Qrencode attacks, the total average attack time was 248.31. The OSINT attack involved manual search and data collection using a stopwatch, resulting in a total duration of 16.94 seconds. For the social engineering attack, the total time required was 83.76 seconds. This process includes the creation of a cloned website and phishing URL. The QR Code attack stage took the longest at 147.61 seconds because the process from composing the message to accessing the phishing URL was measured manually with a stopwatch.

Table 6. Time Measurement Results of Quishing Attacks Using OSINT Truecaller, Social Engineering SEToolkit, and QR Code Qrencode

No	Step	Real-time
	OSINT Attacks	
1	Phone Number Scanning	12.91
2	Collect Data	04.03
Total Real-time OSINT Attack		**16.94**

Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

	Social Engineering Attacks	
3	Select Attack Method	19.90
4	Input Target Website URL	20.12
5	Get Cloned Website	09.08
6	Run Serveo Service	04.45
7	Get Serveo URL	03.58
8	Input Serveo URL	03.91
9	Input Custom URL Phishing	07.24
10	Get URL Phishing	15.48
Total Real-time Social Engineering Attack		**83.76**
	QR Code Attacks	
11	Input URL Phishing	20.93
12	Get QR Code	0,01
13	Input Phone Number Target	08.81
14	Create Message Content	93.95
15	Send Message and QR Code	02.38
16	Target Scan QR Code	06.27
17	Target Accessing URL Phishing	11.48
18	Get Credential Data	03.78
Total Real-time QR Code Attack		**147.61**
Total Real-time		**248.31**

2. Time Measurement Using OSINT Find Mobile Number Location, Social Engineering SEToolkit, and QR Code Qrencode

Table 7. Time Measurement Results of Quishing Attacks Using OSINT Find Mobile Number Location, Social Engineering SEToolkit, and QR Code Qrencode

No	Step	Real-time
	OSINT attacks	
1	Phone Number Scanning	36.95
2	Collect Data	05.14
Total Real-time OSINT attack		**42.09**
	Social Engineering Attacks	
3	Select Attack Method	19.90
4	Input Target Website URL	20.12
5	Get Cloned Website	09.08
6	Run Serveo Service	04.45
7	Get Serveo URL	03.58
8	Input Serveo URL	03.91
9	Input Custom URL Phishing	07.24
10	Get URL Phishing	15.48
Total Real-time Social Engineering Attack		**83.76**

Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

	QR Code Attacks	
11	Input URL Phishing	20.93
12	Get QR Code	0.01
13	Input Phone Number Target	08.81
14	Create Message Content	93.95
15	Send Message and QR Code	02.38
16	Target Scan QR Code	06.27
17	Target Accessing URL Phishing	11.48
18	Get Credential Data	03.78
Total Real-time QR Code Attack		**147.61**
Total Real-time		**273.46**

Based on Table 7, the measurement results of the time of the quishing attack based on the OSINT Find Mobile Number Location, social engineering SEToolkit, and QR Code Qrencode attacks, the total average attack time was 273.46. The OSINT attack involved manual search and data collection using a stopwatch, resulting in a total duration of 42.09 seconds. For the social engineering attack, the total time required was 83.76 seconds. This process includes the creation of a cloned website and phishing URL. The QR Code attack stage took the longest at 147.61 seconds because the process from composing the message to accessing the phishing URL was measured manually with a stopwatch.

4. DISCUSSIONS

This section discusses the efficiency of quashing attacks based on time metrics with a combination of OSINT, social engineering, and QR Code attacks, as well as the implications of using time-based attack tree models in improving information security responses, especially in the banking sector.

The attack tree model in Figure 12 depicts a systematic quishing attack, starting from information gathering through OSINT, followed by social engineering and sending QR codes to obtain target data credentials. Each node in the attack tree indicates a specific attack stage and is equipped with a time metric to measure the efficiency of each attack path combination. Based on the attack tree results, Table 8 presents the results of ranking the quishing attack paths based on time metrics, from the fastest to the slowest.

The results in Table 8 show the ranking of quishing attacks based on time metrics, from the fastest to the slowest execution. The attack tree combined Truecaller OSINT attacks, social engineering using SEToolkit, and QR Code from Qrencode, which was recorded as the fastest at 248.31 seconds. This combination proved to be the most efficient in collecting target data, thus ranking first. In contrast, the combination of OSINT Find Mobile Number Location with the SEToolkit and Qrencode methods recorded the longest time, namely 273.46 seconds, or a difference of 25.15 seconds. Although it took a little longer, this combination efficiently completed all attack stages.

Combining attacks with OSINT Truecaller proved to be the fastest and most efficient way to obtain target credentials. Truecaller has the advantage of scanning data without requiring a geographic location tracking process, as in the Find Mobile Number Location tool. Martina Nobili's (2023) research reinforces this finding, showing that Truecaller is one of the most effective OSINT tools for identifying cross-border phone number users, with a 77% success rate in linking numbers to user identities. [25].

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

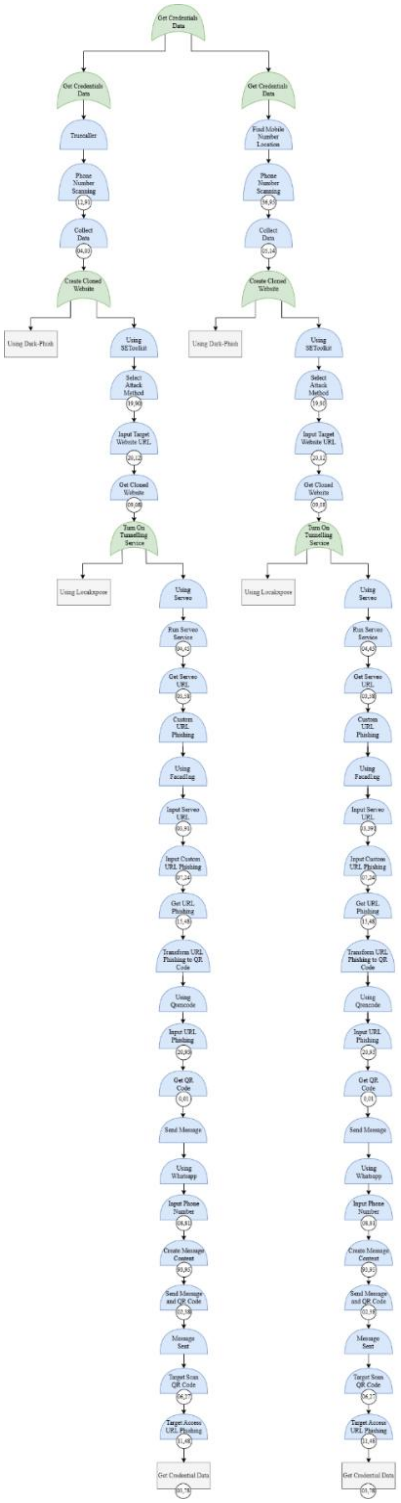


Figure 12. Attack Tree of Quishing Attack along with Time Metric Measurement

Table 8. Results of The Quishing Attack Ranking Based on The Time Metric

Quishing Attack	Real-time
OSINT Truecaller, Social Engineering SEToolkit, dan QR Code Qrencode Attacks	248.31
OSINT Find Mobile Number Location, Social Engineering SEToolkit, dan QR Code Qrencode Attacks	273.46

Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

This time-metric attack tree approach offers practical benefits, especially for banking institutions. This method can assess the speed of response to vulnerabilities by mapping the path of quishing attacks to adjust incident response strategies more effectively. This approach also allows for a more realistic simulation of attack scenarios, allowing banks to improve user preparedness through cybersecurity training and strengthening authentication systems to prevent unauthorized access before an incident occurs.

5. CONCLUSION

Quishing attacks can be modeled through threat modeling as an attack tree based on the formulation of data flow diagrams of each OSINT attack, social engineering attack, and QR Code attack to obtain target data credentials. The attack tree is organized based on time metrics to measure the duration of each attack stage at each node in the attack tree. Based on the results of the time metric measurement, the sequence of attack combinations with the fastest duration that shows efficiency in achieving the attack objectives is obtained, namely the OSINT Truecaller, social engineering SEToolkit, and QR Code Qrencode attacks of 248.31 seconds. This combination is superior to OSINT Find Mobile Number Location, social engineering SEToolkit, and QR Code Qrencode attacks, which total 273.46 seconds. This approach can help banking institutions assess response time to vulnerabilities by systematically identifying quishing attack paths so that incident handling strategies can be adjusted more effectively. Furthermore, this research can be extended by analyzing other metrics, such as probability or frequency metrics, to see the success rate and frequency of quishing attacks.

REFERENCES

[1] B. Novendra and S. S. Aulianisa, "Konsep dan Perbandingan Buy Now, Pay Later dengan Kredit Perbankan di Indonesia : Sebuah Keniscayaan di Era Digital dan Teknologi," *J. Rechts Vinding*, vol. 9, no. 2, pp. 183–201, 2020, doi: https://dx.doi.org/10.33331/rechtsvinding.v9i2.444.

[2] A. Muftiadi, T. P. M. Agustina, and M. Evi, "Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phising terhadap Layanan Online Banking," *Hexatech J. Ilm. Tek.*, vol. 1, no. 2, pp. 60–65, 2022, doi: 10.55904/hexatech.v1i2.346.

[3] T. Nugraheni, A. Sinurat, and D. A. Kian, "Analisis Yuridis Penerapan Perlindungan Hukum dalam Melindungi Pengguna Layanan Internet Banking dari Cyber Crime," *J. Hukum, Polit. dan Ilmu Sos.*, vol. 3, no. 2, 2024, doi: https://doi.org/10.55606/jhpis.v3i2.3715.

[4] T. Rains, *Cybersecurity Threats, Malware Trends, and Strategies*. 2020.

[5] I. R. Hidayah, "Representasi Social Engineering Dalam Tindak Kejahatan Dunia Maya (Analisis Semiotika Pada Film Firewall)," *Tibanndaru J. Ilmu Perpust. dan Inf.*, vol. 4, no. 1, p. 30, 2020, doi: 10.30742/tb.v4i1.905.

[6] E. J. Pranata and L. Ependi, "Phishing terhadap Website Bank BCA," *J. Trends*, vol. 01, no. 01, pp. 34–40, 2023, doi: https://doi.org/10.56772/trends.v1i1.293.

[7] B. Wibowo and T. Hidayat, "Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ," *J. Pengabdi. Masy. Sultan Indones.*, vol. 2, no. 1, pp. 1–9, 2024, doi: 10.58291/abdisultan.v2i1.294.

[8] Fridayani and B. Cuaca, "Transaksi Keuangan Digital Menggunakan QRIS Ditinjau dari Aspek Hukum," *Teach. Learn. J. Mandalika*, vol. 4, no. 2, pp. 164–174, 2023, [Online]. Available: http://ojs.cahayamandalika.com/index.php/teacher

[9] A. R. H. Martawireja, R. Ridwan, A. P. Hafidzin, and M. Taufik, "Proteksi Keamanan Data pada Quick Response (QR) Code," *J. Teknol. dan Rekayasa Manufaktur*, vol. 3, no. 2, pp. 99–110, 2021, doi: 10.48182/jtrm.v3i2.58.

[10] G. A. Amoah and H.-A. J.B., "QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing)," *Int. J. Comput. Appl.*, vol. 184, no. 33, pp. 34–39, 2022, doi: 10.5120/ijca2022922425.

[11] D. Njuguna and J. Ndia, "Quick Response Code Security Attacks and Countermeasures : A Systematic Literature Review," *J. Cyber Secur.*, 2025, doi: 10.32604/jcs.2025.059398.

Vol. 7, No. 1, February 2026, Page. 44-59
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.1.4819

[12] N. Naik, P. Jenkins, P. Grace, D. Naik, S. Prajapat, and J. Song, "A Comparative Analysis of Threat Modelling Methods : STRIDE, DREAD, VAS , PASTA, OCTAVE, and LINDDUN," 2024, doi: https://doi.org/10.1007/978-3-031-74443-3_16.

[13] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies," *Cyber-Physical Energy Syst. Secur.*, vol. 9, pp. 29775–29818, 2021, doi: 10.1109/ACCESS.2021.3058403.

[14] M. Tatam, B. Shanmugam, S. Azam, and K. Kannoorpatti, "A Review of Threat Modelling Approaches for APT-Style Attacks," *Heliyon*, vol. 7, no. 1, p. e05969, 2021, doi: 10.1016/j.heliyon.2021.e05969.

[15] S. Chlup, K. Christl, C. Schmittner, M. A. Shaaban, S. Schauer, and M. Latzenhofer, "THREATGET : Towards Automated Attack Tree Analysis for Automotive Cybersecurity," *J. Inf.*, vol. 14, no. 14, pp. 1–28, 2023, doi: https://doi.org/10.3390/info14010014.

[16] L. Kuipers, "Analysis of Attack Trees : Fast Algorithms for Subclasses," 2020.

[17] N. Naik, P. Grace, P. Jenkins, K. Naik, and J. Song, "An Evaluation of Potential Attack Surfaces Based on Attack Tree Modelling and Risk Matrix Applied to Self-Sovereign Identity," *Comput. Secur.*, vol. 120, p. 102808, 2022, doi: 10.1016/j.cose.2022.102808.

[18] F. Sharevski, A. Devine, E. Pieroni, and P. Jachim, "Phishing with Malicious QR Codes," *ACM Int. Conf. Proceeding Ser.*, pp. 160–171, 2022, doi: 10.1145/3549015.3554172.

[19] M. Weinz, N. Zannone, L. Allodi, and G. Apruzzese, *The Impact of Emerging Phishing Threats : Assessing Quishing and LLM-generated Phishing Emails against Organizations*, vol. 1, no. 1. arXiv, 2025. doi: 10.1145/3708821.3736195.

[20] P. C. Ariani *et al.*, "Comparative Analysis of Phishing Tools on Social Media Sites," *Ultim. J. Tek. Inform.*, vol. 15, no. 1, pp. 22–27, 2023, doi: https://doi.org/10.31937/ti.v15i1.2920.

[21] Yusuf Raharja, "Implementasi Metode OSINT untuk Mengidentifikasi Serangan Judi Online pada Website," *J. Inform. Polinema*, vol. 10, no. 3, pp. 359–364, 2024, doi: 10.33795/jip.v10i3.4847.

[22] R. Ganesh and G. Prabu, "Determination of Internet Banking Usage and Purpose with Explanation of Data Flow Diagram and Use Case Diagram," *Int. J. Manag. Humanit.*, vol. 0913, no. 7, pp. 52–58, 2020, doi: 10.35940/ijmh.G0674.034720.

[23] A. Y. Aleryani, "Analyzing Data Flow: A Comparison between Data Flow Diagrams (DFD) and User Case Diagrams (UCD) in Information Systems Development," *Eur. Mod. Stud. J.*, vol. 8, no. 1, pp. 313–320, 2024, doi: 10.59573/emsj.8(1).2024.28.

[24] A. W. Pratiwi, A. Widjajarto, and A. Budiyono, "Pemodelan Attack Tree Pada Spear Phishing Attack di Instansi Publik dengan Metrik Granularitas Data," *J. Inf. Syst. Res.*, vol. 6, no. 1, pp. 76–86, 2024, doi: 10.47065/josh.v6i1.5876.

[25] M. Nobili, "Review OSINT Tool for Social Engineering," vol. 6, 2023, doi: 10.3389/fdata.2023.1169636.