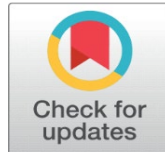


FORENSIC ANALYSIS OF WEB PHISHING AND SOCIAL ENGINEERING USING THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY METHOD CASE STUDY OF FACEBOOK ACCOUNT DATA THEFT

Rahmat Hidayat¹  , Nuril Anwar²  

^{1,2} Informatics Study Program, Universitas Ahmad Dahlan, Bantul Regency, Special Region of Yogyakarta 55191, Indonesia



Received 05 May 2024
Accepted 15 June 2024
Published 30 July 2024

Corresponding Author

Rahmat Hidayat,
rohmatmingil@gmail.com

DOI
[10.29121/DigiSecForensics.v1.i1.2024.14](https://doi.org/10.29121/DigiSecForensics.v1.i1.2024.14)

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Copyright: © 2024 The Author(s). This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

With the license CC-BY, authors retain the copyright, allowing anyone to download, reuse, re-print, modify, distribute, and/or copy their contribution. The work must be properly attributed to its author.



ABSTRACT

Modern society heavily relies on digital technology and the internet, particularly on social media platforms like Facebook, which, despite their benefits, also pose security risks. In Q4 2023, a total of 8,161 phishing URLs were detected across 53 different domains, including id, my.id, biz.id, ac.id, and web.id. Criminals employ phishing techniques and social engineering to steal personal information by creating fake websites that resemble Facebook. This research adopts the National Institute of Standards and Technology (NIST) methodology involving the stages of collection, examination, analysis, and reporting to uncover Facebook account data theft. Using Wireshark, the study successfully captured the activities of both phishing perpetrators and victims, revealing evidence such as email messages containing social engineering tactics, victim account data, and information stored in the phishing perpetrators' databases. These findings underscore the importance of public education and awareness enhancement to mitigate increasingly sophisticated phishing attacks.

Keywords: Digital Forensics, NIST, Social Engineering, Web Phishing

1. INTRODUCTION

Modern society today heavily relies on the advancements in digital technology and the internet. These developments provide widespread access to knowledge, news, and information, making it easily and swiftly accessible to the public. One significant aspect of this digital landscape is social media, which has become a primary priority for society. Engaging in social media activities has become a daily routine for many, involving interactions, seeking and sharing information,

expanding networks, building brands, entertainment, increasing knowledge, and even conducting business transactions. Social media serves various purposes such as communication, work tools, transaction platforms, learning aids, and entertainment [Dwijayanti et al. \(2022\)](#). One of the commonly used social media platforms is Facebook.

Facebook is an online platform that enables users to establish digital friendships and share information in discussion forums or communication channels. It also facilitates connections with family, friends, and other Facebook users [Ryansyah et al. \(2023\)](#). Facebook was created by Mark Zuckerberg, a student at Harvard University, in February 2004. Initially, it was used by Zuckerberg and his friends to stay connected and share information. However, Facebook quickly gained popularity among students at various universities across the United States. As a result, Facebook expanded its access to people worldwide, a trend that continues to this day [Hermanto et al. \(2023\)](#).

HTTPS is a protocol that ensures high security levels, making it possible for phishing perpetrators to exploit its security to create mirror Facebook sites and deceive victims into believing that the accessed site is the genuine one [Nofiyah & Mushlihudin \(2020\)](#). Facebook account data thieves also utilize fake domains that closely resemble the original, aiming to convince victims that they are on a secure website. This technique is a form of social engineering, which is one of the easiest hacking techniques to perform because it exploits human weaknesses. Consequently, phishing perpetrators can easily deceive victims and steal their crucial data [Tias Darmaningrat et al. \(2022\)](#).

Facebook is highly popular and used for various activities. However, many users neglect account security by using easily guessed passwords, making them vulnerable to cybercrime. Additionally, Facebook is often used for sales and promotions of goods that are not always safe. Sometimes, promotional links or advertisements contain malware that can steal user data [Yanti et al. \(2021\)](#).

It is important to note that cybercrime is not a representation of technological advancement itself, but rather the wrongful behavior of individuals or groups who exploit it in ways that can harm others [Hidayah \(2020\)](#). Therefore, as social media users, it is essential to be cautious of cybercrime activities to protect personal privacy and increase awareness about social media security.

Preventing cybercrime needs to be emphasized as it can help in maintaining personal privacy [Muria et al. \(2022\)](#). In the case of Facebook account data theft by sending messages via email using the modus operandi of "Facebook curiosity", the evidence in this case includes a fake login website and social engineering methods obtained from the emails sent by the perpetrator to the victim. These elements can be used to verify the authenticity of the Facebook account theft.

Digital forensic investigation will assist in addressing Facebook account data theft committed by creating a mirrored Facebook login and using social engineering methods. The application of forensic investigation can aid in finding evidence in cases of Facebook account data theft, with the aim of uncovering hidden information, whether conducted by individuals, groups, state, or private entities.

The flow of this research will use the National Institute of Standards and Technology (NIST) method. In this method, there are several stages to be conducted: collection, examination, analysis, and reporting. The National Institute of Standards and Technology (NIST) is a method from the United States Department of Commerce. This method is a non-regulatory national body. The mission of this non-regulatory national body is to promote and create measurements, standards, and

technologies to improve productivity and quality of life for everyone [Nofiyah & Mushlihudin \(2020\)](#). The application of digital forensics will obtain digital evidence of Facebook messages between the perpetrator and the victim using tools, and it will be able to expose the phishing website and social engineering methods.

In Q4 2023, a total of 8,161 phishing URLs were detected, originating from 53 different domains. Some of the second-level domains (SLDs) targeted in phishing included id, my.id, biz.id, ac.id, and web.id. The phishing report for the year 2023 showed varying numbers, peaking in February 2023 with 15,050 reports and reaching its lowest in November 2023 with 1,729 reports [Indonesia Anti-Phishing Data Exchange. \(2024\)](#).

The government's anticipation of phishing crimes typically involves socialization and education to the public about the signs and ways to avoid phishing. However, increasing public awareness is very difficult, hence continuous emphasis on the dangers and losses from phishing is necessary. From the perspective of software developers, they usually implement various security layers such as complex password requirements and two-factor authentication (2FA). However, phishing attacks often involve fake login pages that are beyond the control of the original application developers, so users must remain vigilant.

Phishing is not only limited to platforms like Facebook but also targets other platforms such as Apple, Netflix, Yahoo, WhatsApp, PayPal, Chase, Facebook, Microsoft, eBay, and Amazon with the goal of stealing sensitive and critical data, such as social media credentials and bank account information [Alkhalil et al. \(2021\)](#). As an example of Facebook account data theft through phishing websites, attackers create fake sites that mimic the Facebook login page. They employ social engineering techniques to lure users into revealing their login information, which can then be exploited for malicious purposes. Below is an example URL of a phishing site targeting Facebook
 “https://sites.google.com/view/65tgesbh?fbclid=IwAR0Qs6UEEBSExoHAL_p4MSyt7yUGzAbCigcclHG2_00Hq-wB1FuShbGw_7g”,

2. RESEARCH METHOD

The research focuses on the theft of Facebook account data and social engineering techniques used by hackers through web phishing. This study aims to delve deeper into the methods and techniques attackers use to steal sensitive user data via fake websites that mimic the authentic Facebook interface. Additionally, the research will explore various tactics employed in social engineering, where attackers manipulate human emotions and vulnerabilities to obtain confidential information

2.1. SCENARIO

The scenario of Facebook account data theft using phishing websites and social engineering can be explained in three stages: before the incident, during the incident, and after the incident. The Facebook account theft scenario can be seen in [Figure 1](#).

Figure 1

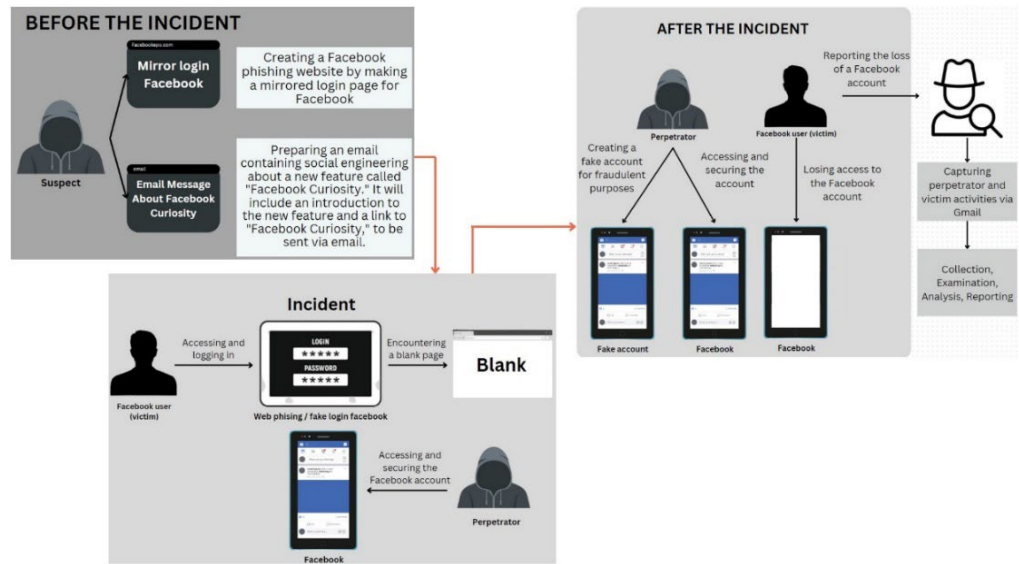


Figure 1 Criminal Scenario

The perpetrator meticulously prepares a phishing attack by creating a fake login site resembling Facebook and disseminating emails containing links to this site. The email promotes a new feature named "Facebook Curiosity" which claims to reveal who has been viewing the user's profile. When the victim becomes interested and clicks the link, they are directed to the fake login site and unwittingly provide their credentials. The perpetrator then steals the victim's username and password, accesses their Facebook account, and changes the credentials to secure control of the account. After the incident, the victim is unable to access their account, which has been altered to become a fake account by the perpetrator. Investigators use tools such as Wireshark to capture activity and gather evidence to trace the perpetrator and recover the victim's account.

2.2. RESEARCH PHASES

This research will involve several phases to achieve its objectives. The initial phase involves conducting a literature review to find relevant references to support the research. Next, a data survey will be conducted to determine how many people have been victims of data loss from Facebook accounts in theft scenarios simulated as described. Additionally, to provide a more detailed description of the Facebook account data theft scenario, a phishing website in the form of a fake login will be created. The user flow of the fake login occurring in Figure 2 is as follows.

Figure 2

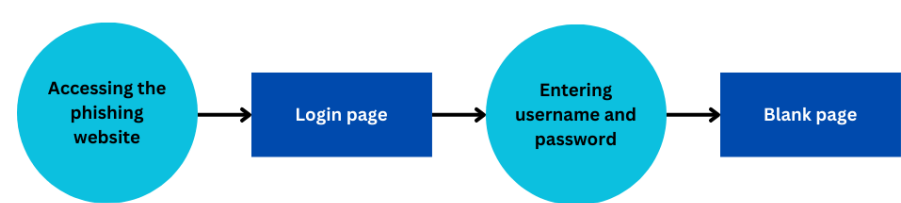


Figure 2 User Flow Fake Login

The research begins with a literature review, data survey, scenario design, creation of a phishing site resembling Facebook login page, and drafting email messages to be sent to targets. Following this, the research follows NIST methods involving evidence collection (DNS, server and destination IP, perpetrator and victim email identities), evidence examination using various tools, data analysis to identify attack patterns, and reporting findings as crime evidence based on the steps and processes conducted. The research phases can be seen in [Figure 3](#).

Figure 3

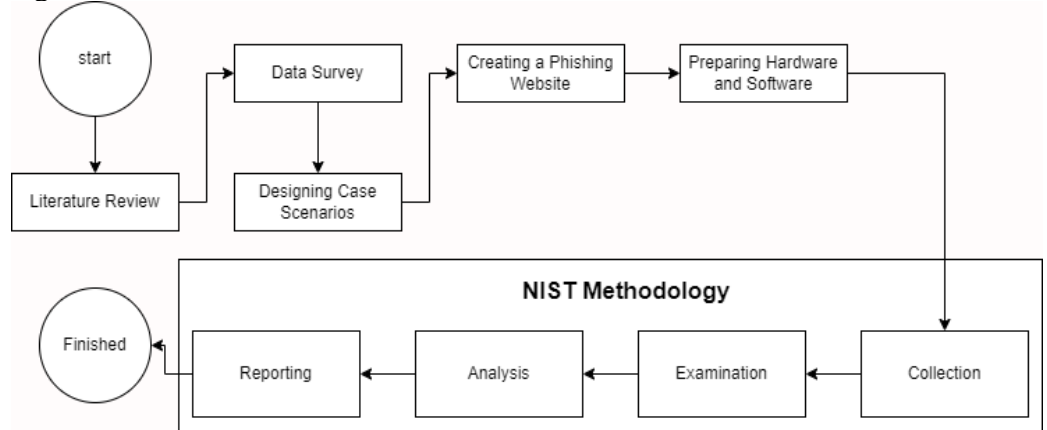


Figure 3 Research Phases

[Figure 3](#) depicts the flowchart of the research phases to be conducted, utilizing the National Institute of Standards and Technology (NIST) methodology.

2.2.1. COLLECTION

The steps taken in this stage include collecting data related to the account data theft case, involving identification, collection, extraction, and recording of evidence. In this research phase, the initial process involves capturing data packets from emails and phishing websites using forensic tools such as Wireshark.

2.2.2. EXAMINATION

In this stage, the collected evidence is explored using the captured files that have been successfully collected. The exploration process is conducted using Wireshark tools to analyze the contents of these captured files. During the exploration, various pieces of evidence are discovered, such as email messages and URLs leading to phishing sites or other malicious websites.

2.2.3. ANALYSIS

After the evidence is collected and acquired, investigators conduct an analysis to gather evidence related to the case. The examination includes evidence of email messages from the Facebook account theft perpetrator, DNS used by the perpetrator, server IP address, destination IP address, victim's email, perpetrator's email, victim's data, and all data successfully transmitted to the phishing perpetrator.

2.2.4. REPORTING

The final stage involves creating a report on the investigation findings and disclosing the data obtained from the inquiry. The report includes the identification results of captured data from the email messages of the account theft perpetrator and phishing URLs as evidence.

3. ANALYSIS AND RESULTS

In this chapter, we discuss the analysis and discussion of the case study on Facebook account data theft using phishing and social engineering attacks. Through the application of the NIST methodology, forensic analysis is conducted to deeply understand how the attack was carried out and its impact on data security. The results of this analysis will be presented in the form of key findings, including the techniques used by the attacker, methods of attack distribution, and exploited system vulnerabilities.

3.1. COLLECTION

The first piece of evidence is a phishing email sent on Thursday, May 30, 2024, at 00:56, accessed from the victim's Gmail account "matsnews07@gmail.com" with the password "Karlina071802@". This email contains information used for phishing attacks aimed at stealing personal data. The second piece of evidence is the phishing site found in the link within the email, designed to mimic the legitimate site to deceive victims into entering their usernames and passwords.

Figure 4

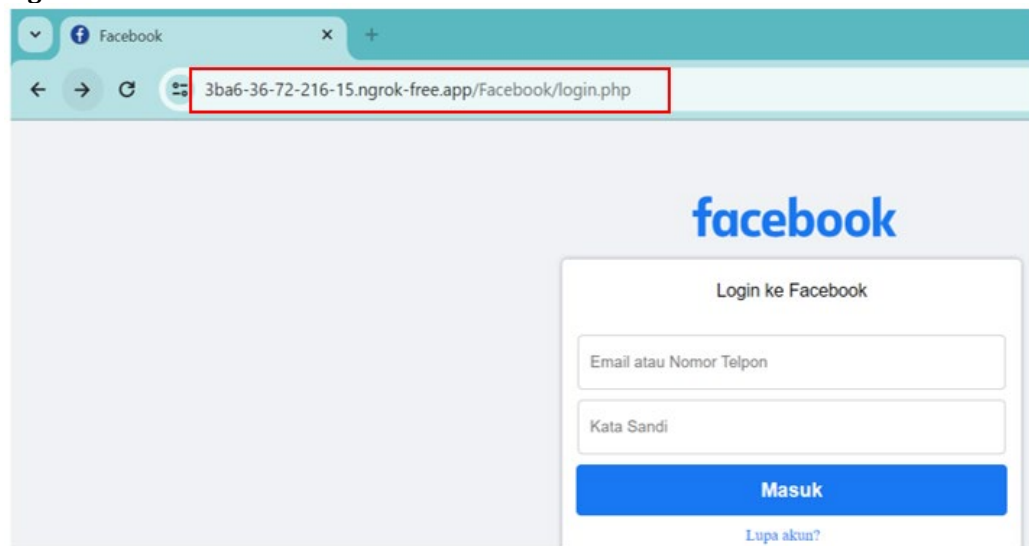





Figure 4 Mirror login Facebook

Information gathering using Wireshark tools to collect all relevant data from network activities, including traffic between the perpetrator and the victim. From the activities of the perpetrator and the victim, 3 captured files (*.pcapng) were obtained, as shown in [Figure 5](#).

 Capture Web Phishing	30/05/2024 01:10	Wireshark capture file	971 KB
 Pesan Phishing	30/05/2024 01:00	Wireshark capture file	9.553 KB
 Web Phishing	30/05/2024 01:04	Wireshark capture file	2.329 KB

Resan Phishing.pcapng

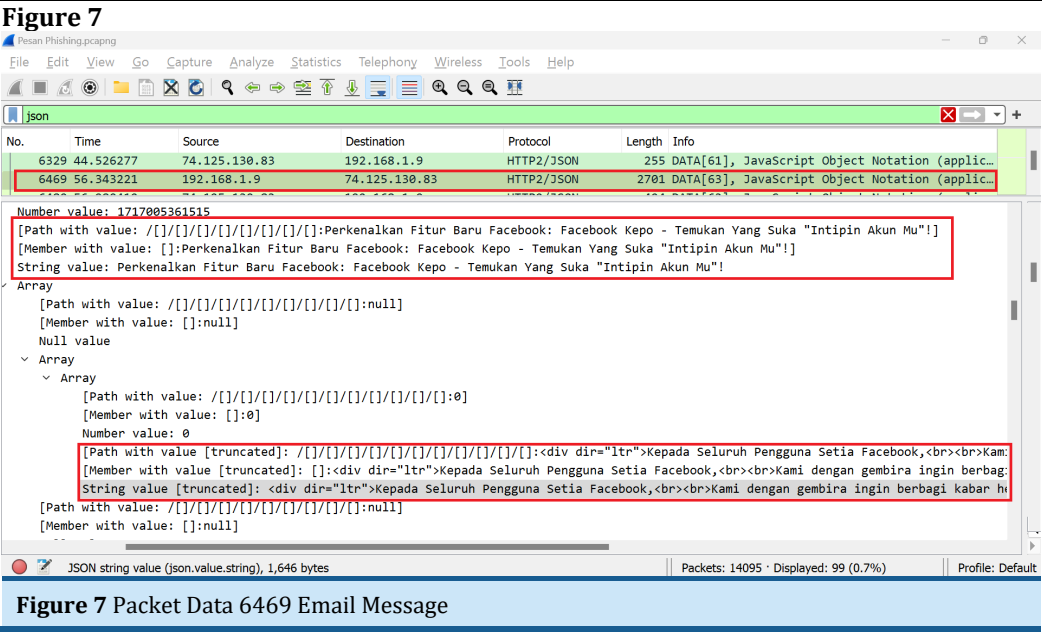


Figure 7 Packet Data 6469 Email Message

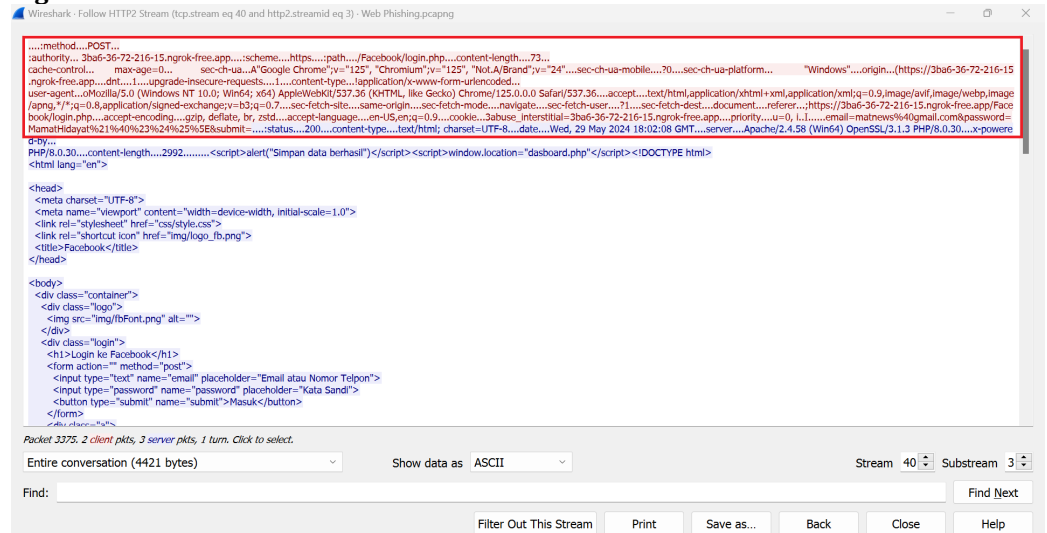
In packet number 6469, the complete email message sent by the phishing perpetrator to the victim is displayed. The message not only explains about the new feature called 'Facebook Curiosity', but also invites the victim to use this new feature by providing a link that directs to the phishing web page. This message reflects the careful strategy of the phishing perpetrator to lure the victim with the promise of a new feature, while actually aiming to conduct phishing.

3.3. ANALYSIS

After digital evidence is found, investigators proceed with a deeper analysis to substantiate the authenticity of the evidence related to the case. The examination includes evidence of email messages from the Facebook account theft perpetrator, DNS used by the perpetrator, server IP address, destination IP address, victim's email, and perpetrator's email.

In this analysis stage, evidence data from the 'Phishing Message', 'Phishing Website', and 'Phishing Web Capture' files are used with Wireshark tools for analysis and evidence collection. Investigators use the sslkeylog.log file to assist in decrypting HTTP2, TLSv1.2, and encrypted TCP, although not all data from the capture files can be decrypted due to HTTPS security using SSL (Secure Socket Layer) or TLS (Transport Layer Security). The data packets to be analyzed are selected using filtering techniques to speed up and facilitate packet identification. Several keywords are used to search for data packets related to Gmail to find HTTP2 email messages. Using JSON filtering, it was found that packet number 6469 contains a complete message sent by the phishing perpetrator to the victim. This complete message is crucial as it contains information that can reveal the tactics and strategies used by the phishing perpetrator.

From the analysis of the perpetrator's message, it appears that there indeed was a URL directing users to a phishing site. This URL led users to a page resembling the Facebook login interface. After the victim entered their login information, they did not receive the promised information from the message. Instead, they encountered an empty page.

Figure 8**Figure 8** Packet Number 3375: Phishing Website

Analysis of packet number 3375 reveals an HTTP POST transmission to the URL <https://3ba6-36-72-216-15.ngrok-free.app/Facebook/login.php>. This packet is part of the HTTP/2 protocol, identified via the HTTP/2 Stream.

1) Method and URL Request:

- HTTP Method: POST
- URL Request: <https://3ba6-36-72-216-15.ngrok-free.app/Facebook/login.php>

2) Main Headers:

- Method: POST
- Authority: 3ba6-36-72-216-15.ngrok-free.app
- Scheme: https
- Path: /Facebook/login.php
- Content-Length: 73
- Cache-Control: max-age=0
- Sec-Ch-Ua: "Google Chrome";v="125", "Chromium";v="125", "Not.A/Brand";v="24"
- Sec-Ch-Ua-Mobile: ?0
- Sec-Ch-Ua-Platform: "Windows"
- Origin: <https://3ba6-36-72-216-15.ngrok-free.app>
- DNT: 1
- Upgrade-Insecure-Requests: 1
- Content-Type: application/x-www-form-urlencoded
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

age/webp,image/apng,;q=0.8,application/signed-exchange;v=b3;q=0.7

- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: navigate
- Sec-Fetch-User: ?1
- Sec-Fetch-Dest: document
- Referer: <https://3ba6-36-72-216-15.ngrok-free.app/Facebook/login.php>
- Accept-Encoding: gzip, deflate, br, zstd
- Accept-Language: en-US,en;q=0.9
- Cookie: 3abuse_interstitial=3ba6-36-72-216-15.ngrok-free.app
- Priority: u=0, i

3) Payload (Data Sent):

- Content:
email=matnews%40gmail.com&password=MamatHidayat%21%40%23%24%25%5E&submit=
- Email: matnews@gmail.com
- Password: MamatHidayat!@#\$\$%^

4) Server Response:

- Status: 200
- Content-Type: text/html; charset=UTF-8
- Date: Wed, 29 May 2024 18:02:08 GMT
- Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
- X-Powered-By: PHP/8.0.30
- Content-Length: 2992

5) HTML Response:

- Script executed: `<script> alert ("Data saved successfully") </script>`
`<script>window.location="dashboard.php"</script>`

After the stage of sending data to the phishing server, the analysis continues at the stage of data extraction from the database carried out by the phisher. Phishing perpetrators have prepared a hidden directory, namely <https://3ba6-36-72-216-15.ngrok-free.app/Facebook/extract.php>. At this stage, the data that has been successfully recorded from the phishing victim will be saved into a database for the purpose of further misuse, including the victim's account data, the extract.php page can be seen in [Figure 9](#).

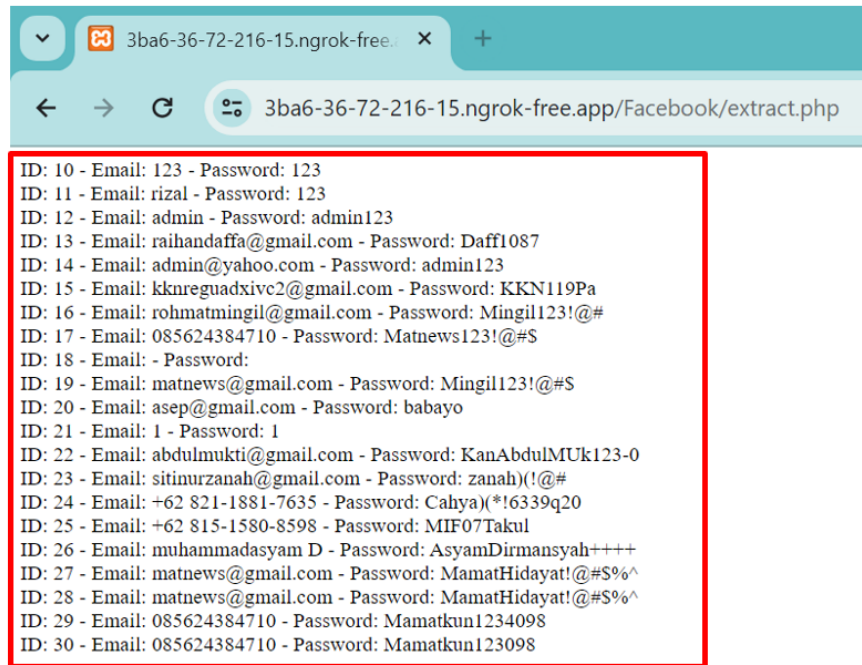
Figure 9**Figure 9** View of Hidden Directory (Extract.php)

Figure 9 shows the extract.php page, which contains all the data successfully entered into the phishing website by victims. The perpetrator created a hidden directory named extract.php, where they can view all the data submitted to the phishing website. This allows the perpetrator to access all the collected data without having to access the database directly.

3.4. REPORTING

The reporting stage of this investigation reports the results of the analysis of evidence related to the email messages of the perpetrators of theft of Facebook web phishing account data. From the results of the capture file, the analysis results are obtained. Reporting of the results of the analysis that has been carried out and presented in a data package in a bookmark which is exported in pdf form.

Figure 10

No	Time	Source	Destination	Protocol	Length	Info
3375	41.162.998	192.168.1.9	18.141.129.246	HTTP2	255	HEADERS[3]: POST /Facebook/login.php
3377	41.163.238	192.168.1.9	18.141.129.246	HTTP2	158	DATA[3] (application/x-www-form-urlencoded)
3407	41.236.250	18.141.129.246	192.168.1.9	HTTP2	85	DATA[3] (text/html)
3414	43.406.107	192.168.1.9	18.141.129.246	HTTP2	126	HEADERS[5]: GET /Facebook/dashboard.php
3677	66.002.111	192.168.1.9	18.141.129.246	HTTP2	124	HEADERS[7]: GET /Facebook/login.php

Figure 10 HTTP Web Phishing

In **Figure 10**, there is a capture file which shows a data packet containing an HTTP POST request sent by the client to the server with 3ba6-36-72-216-15.ngrok-free.app via the HTTPS protocol. Packages marked in red contain login information in the form of a username and password. The login details captured are email matnews@gmail.com and password MamatHidayat!@#S%^ The server response indicates successful data saving by displaying the message "Save data successfully" and directing the user to the dashboard page. The total data packages recorded

regarding the phishing website were 5 data packages, including data package 3377 which contained the victim's account.

Based on the results of further analysis regarding phishing websites, data was found resulting from theft carried out by phishing perpetrators in a hidden directory with the location <https://3ba6-36-72-216-15.ngrok-free.app/Facebook/extract.php>. A total of 30 accounts were identified as phishing victims, including victim accounts marked in red.

Then the results of the analysis regarding the phishing web used by the perpetrator include the DNS used by the perpetrator, server IP address, destination IP address, email of the victim and the perpetrator can be seen in [Table 1](#).

Table 1

Table 1 Phishing Web Analysis Results		
No	Types of Evidence	Findings
1	Phishing Website URL	https://3ba6-36-72-216-15.ngrok-free.app/Facebook/login.php (https://web.facebook.com)
2	IP address destination	192.168.1.9
3	Server	3ba6-36-72-216-15.ngrok-free.app
4	Server IP address	18.141.129.246
5	Server Software	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30

In [Table 1](#), the domain, destination IP address, and server IP address used can vary. This is because using the free ngrok service has its limitations. When the ngrok client is turned off, the domain and IP address provided will become inactive. Upon restarting the ngrok client, new domain and IP addresses will be assigned, which will differ from the previous ones. Therefore, the evidence findings reflect the conditions at the time of data collection and may change when the ngrok service is restarted.

From this research, it can be seen that phishing websites can harm many parties by stealing sensitive information such as usernames and passwords. Therefore, it is important to understand what phishing is so that we can anticipate it and be more cautious when engaging online, especially when accessing services like Facebook. Here are several ways to recognize phishing websites.

Phishing websites often use URLs that resemble legitimate sites but are different, such as replacing the letter "O" with the number "0" or adding extra words to the domain. Ensuring the URL matches the official domain is crucial. One way to detect phishing is to try logging in with incorrect usernames and passwords; if the login is successful, it indicates a phishing site. Phishing sites typically only feature a login option without the ability to register for a new account, as their main goal is to steal login information. Additionally, even though the site's appearance may be similar, there are small differences such as logos, layouts, or inaccurate text, as well as spelling or grammatical errors. Pay attention to these elements to avoid phishing.

Knowing the characteristics of a phishing website is the first step to protecting yourself from phishing attacks, and it is also important to take anticipatory steps. Some precautions include always checking the URL to ensure it matches the official domain before entering personal or login information, avoiding clicking on suspicious links sent via email, text message, or social media by manually typing the URL in the browser, using two-factor authentication (2FA) to add an additional

layer of security to your account, and keep your software and browser updated to the latest versions that include important security fixes.

4. CONCLUSION

The results of research on forensic analysis of web phishing and social engineering indicate that investigations and digital forensics have successfully uncovered evidence related to the theft of Facebook account data. The NIST method is used to identify critical data such as email addresses, email messages with social engineering elements, and phishing websites used by perpetrators. Analysis of phishing emails shows the use of social engineering tactics with false claims about the "Facebook Kepo" feature to create urgency and steal login information. Data packet analysis reveals an HTTP POST transmission to a malicious URL containing a payload with email and password, followed by a server response redirecting the user to a dashboard page after authentication, indicating a successful data theft process.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

- Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, 1–23. <https://doi.org/10.3389/fcomp.2021.563060>
- Dwijayanti, A., Komalasari, R., Harto, B., Pramesti, P., & Alfaridzi, M. W. (2022). Efektivitas Penggunaan Media Sosial Sebagai Sarana Promosi dan Pemasaran pada UMKM Sablon Anggi Screen di Era Digital. *Ikra-Ith Abdimas*, 6(2), 68–75. <https://doi.org/10.37817/ikra-ithabdimas.v6i2.2408>
- Hermanto, M. N., Martanto, & Iin. (2023). Analisis Forensic Berbasis Web Phising Menggunakan Metode National Institute of Standards and Technology, *Jurnal Informasi dan Komputer*, 11(1), 116–123. <https://doi.org/10.35959/jik.v11i01.311>
- Hidayah, I. R. (2020). Representasi Social Engineering Dalam Tindak Kejahatan Dunia Maya (Analisis Semiotika Pada Film Firewall). *Tibannndaru: Jurnal Ilmu Perpustakaan Dan Informasi*, 4(1), 30. <https://doi.org/10.30742/tb.v4i1.905>
- Indonesia Anti-Phishing Data Exchange. (2024). Phishing Activity Report - 4th Quarter 2023.
- Muria, R. M., Muntasa, A., Yusuf, M., & Hamzah, A. (2022). Studi Litelatur: Peningkatan Kinerja Digital Forensik Dan Pencegahan Cyber Crime. *Jurnal Aplikasi Teknologi Informasi Dan Manajemen (JATIM)*, 3(1), 12–20. <https://doi.org/10.31102/jatim.v3i1.1422>
- Nofiyah, A., & Mushlihudin, M. (2020). Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards And Technology (NIST). *JSTIE (Jurnal Sarjana Teknik Informatika) (E-Journal)*, 8(2), 53. <https://doi.org/10.12928/jstie.v8i2.16697>

- Ryansyah, E., Maulana, R., Rozikin, C., Informatika, P. S., & Karawang, U. S. (2023). Survei Tingkat Pemahaman Mahasiswa Mengenai Ancaman Keamanan Sistem Pada Facebook, 7(3). <http://dx.doi.org/10.30998/string.v7i3.15090>
- Tyas Darmaningrat, E. W., Noor Ali, A. H., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi. Sewagati, 6(2). <https://doi.org/10.12962/j26139960.v6i2.92>
- Yanti, L.P.F., Suandi, I.N., & Sudiana, I.N. (2021). Analisis Kesantunan Berbahasa Warganet Pada Kolom Komentar Berita Di Media Sosial Facebook. Jurnal Pendidikan Dan Pembelajaran Bahasa Indonesia, 10(1), 139–150. https://doi.org/10.23887/jurnal_bahasa.v10i1.405