**Journal of Technology and Informatics (JoTI)**
Vol. 7, No. 2, October 2025
P-ISSN 2721-4842
E-ISSN 2686-6102

# Simulated Phishing Attack and Forensic Analysis Using the D4I Framework: A Case Study on Kredivo

**Muhammad Yusuf Halim[1*], Toto Raharjo[2], Rosi Rahmadi Syahputra[3], Erika Ramadhani[4]**
[1*,2,3]Master Program in Informatics, Universitas Islam Indonesia, Sleman, Yogyakarta, Indonesia
[4]Department of Informatics, Universitas Islam Indonesia, Sleman, Yogyakarta, Indonesia
e-mail: myusufhalim26@gmail.com[1*], etotoraha@gmail.com[2], rosirahmadisyahputra@gmail.com[3], erika@uii.ac.id[4]

**Article Information**

**Article History:**

| | |
|---|---|
| *Received* | : 11 Juni 2025 |
| *Revised* | : 26 Juni 2025 |
| *Accepted* | : 8 Juli 2025 |
| *Published* | : 30 Agustus 2025 |

***Correspondence:**
myusufhalim26@gmail.com

**Keywords:**
Cybersecurity, D4I Framework, Digital Forensics, Fintech Security, Phishing Attack

10.37802/joti.v7i2.1086

**Journal of Technology and Informatics (JoTI)**
P-ISSN 2721-4842
E-ISSN 2686-6102
https://e-journals.dinamika.ac.id/index.php/joti

**Abstract:**

Phishing is a form of cyberattack where attackers deceive users into revealing sensitive information such as credentials or financial data, often through fake communication channels or websites. This threat is particularly critical in the financial technology (fintech) sector, where services rely heavily on digital transactions and user trust. This study presents a simulated phishing case targeting Kredivo users to evaluate the effectiveness of the Digital Forensics framework for Reviewing and Investigating cyber-attacks (D4I) in digital forensic analysis. The Cyber Kill Chain (CKC) model was employed to trace attacker behavior across seven phases, from weaponization to actions on objectives. Forensic data was acquired using MOBILedit Forensic Express from two smartphones, namely an iPhone 11 (iOS 15.8.1) and a Vivo Y21 (Android 8.1.0), which served as simulated evidence devices. Using the D4I framework, the investigation successfully identified and correlated key digital artifacts such as phishing links, OTP transmissions, and unauthorized access logs. These findings were organized into a visual chain of artifacts to reconstruct the full attack lifecycle. The results demonstrate that the D4I framework is effective in guiding structured forensic investigations and understanding attack patterns, supporting the enhancement of fintech security strategies.

## INTRODUCTION

The rapid growth of financial technology services has revolutionized how users manage transactions, credit access, and personal finance through mobile platforms [1]. One such example is Kredivo, a widely used digital lending application in Indonesia that enables users to make purchases and repay later [2]. Despite the convenience offered by these services, their increasing popularity has also made them prime targets for cyberattacks, especially phishing [3]. Phishing is a deceptive practice in which cybercriminals impersonate legitimate entities to extract sensitive information such as usernames, passwords, and one-time passwords (OTPs)

[4], [5]. In December 2021, Kredivo users experienced a phishing campaign involving fake websites, fraudulent messages, and unauthorized access to user accounts [6]. This case revealed vulnerabilities in both user awareness and security infrastructure, necessitating a systematic approach to analyze phishing incidents [7].

Although various technical solutions have been introduced to detect and prevent phishing, many users remain vulnerable due to evolving attack patterns and sophisticated social engineering [8]. Several studies have explored this issue from different perspectives. Alkhalil et al. [9] developed a comprehensive phishing anatomy that outlines the entire lifecycle of phishing attacks. Sangha and Sulistiani [3] identified user ignorance and weak privacy practices as key factors behind successful phishing in fintech platforms. Athulya and Praveen [10] highlighted emerging evasion techniques used by attackers, including random URL generation and phishing kits. Carroll et al. [11] examined the impact of COVID-19 on user susceptibility to phishing, noting how attackers exploited public fear and remote work environments. Dimitriadis et al. [12] introduced the D4I (Digital Forensics for Reviewing and Investigating cyber-attacks) framework, offering structured guidance for analyzing incidents by mapping digital artifacts to the stages of the Cyber Kill Chain.

In the context of fintech, digital forensic investigations face unique challenges due to the use of encrypted communication channels, rapid data exchanges, and cloud-based infrastructures [13]. Fintech platforms often handle sensitive financial data across multiple devices and applications, making it difficult to isolate, collect, and preserve digital evidence without disrupting service availability or violating user privacy [14]. Additionally, attackers may exploit short-lived data sessions and obfuscation techniques, which complicate the timeline reconstruction and attribution process in forensic analysis [15], [16]. These challenges underscore the urgency for adaptable, structured, and platform-aware forensic frameworks that can support effective incident response in the fintech environment.

This study adopts the D4I framework, a Digital Forensics framework for Reviewing and Investigating cyber-attacks, to investigate phishing threats through a simulated real-world scenario. The research simulates a phishing campaign targeting Kredivo users by constructing a phishing website, distributing malicious links via the WhatsApp messaging platform, collecting user credentials, and analyzing digital artifacts extracted from two smartphones. The analysis is structured based on the seven phases of the Cyber Kill Chain (CKC), which provides a comprehensive model to trace attacker behavior from reconnaissance to actions on objectives [17]. By applying the D4I methodology in conjunction with CKC, the study reconstructs the forensic timeline and identifies key indicators of compromise throughout the attack lifecycle. This structured approach enables a deeper understanding of the attacker’s tactics and the forensic evidence left behind, offering valuable insights for improving fintech security and digital investigation strategies.

Unlike previous works that primarily focus on phishing detection or user education, this research contributes by demonstrating a complete phishing incident from attack simulation to forensic analysis. The integration of a real case study with a practical application of the D4I framework provides valuable insights into how phishing campaigns operate in the fintech landscape. The novelty of this study lies in its end-to-end methodology, which bridges the gap between theoretical cybersecurity frameworks and real-world implementation. The results are expected to assist cybersecurity analysts, developers, and digital forensics practitioners in enhancing their incident response capabilities and raising awareness among fintech users.

## METHOD

### Research Design

This study adopts a qualitative experimental approach using a simulation of a phishing attack scenario targeting Kredivo users. The objective is to analyze the incident using the D4I (Digital Forensics for Reviewing and Investigating cyber-attacks) framework, which integrates the Cyber Kill Chain (CKC) model as a core analytical structure. The research combines a practical demonstration of a phishing scheme with digital forensic investigation, enabling an end-to-end view of how cybercriminals operate and how forensic analysts can reconstruct the sequence of compromise.

Theoretically, CKC is a conceptual model developed to describe the stages of a cyberattack, focusing on the offensive strategies of threat actors across seven phases, from reconnaissance to actions on objectives [18]. In contrast, D4I is a forensic methodology that emphasizes how investigators can review and analyze digital attacks by identifying, correlating, and interpreting forensic artifacts left behind during these phases [12]. While CKC serves as a temporal blueprint of attacker behavior, D4I provides structured investigative steps to reconstruct that behavior using digital evidence. Thus, D4I uses CKC as a reference for aligning forensic findings with the attacker's operational sequence.

### Produce and Framework

The D4I framework is structured around the seven phases of the Cyber Kill Chain (CKC): Reconnaissance (R), Weaponization (W), Delivery (D), Exploitation (E), Installation (I), Command and Control (C2), and Actions on Objectives (A). These phases represent the chronological steps typically followed by attackers in a successful cyberattack [19]. The sequential phases of a cyberattack, as conceptualized in the Cyber Kill Chain (CKC) model, are illustrated in Figure 1.

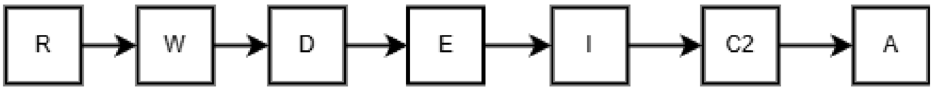


Figure 1. the CKC Phases [20]

Figure 1 illustrates the CKC phases. The first phase, Reconnaissance (R), involves the attacker scanning the internet to collect intelligence about the target. In the Weaponization (W) phase, a seemingly harmless file or link is prepared and embedded with a tailored malicious payload. During the Delivery (D) phase, this file is sent to the victim, often through emails or messaging platforms. Once the file is opened, the attack progresses to the Exploitation (E) phase, where system vulnerabilities are exploited to execute the payload. The next stage, Installation (I), establishes persistence by embedding malware into the victim's system. In the Command and Control (C2) phase, the malware opens a covert communication channel to the attacker's server. Finally, in Actions on Objectives (A), the attacker achieves their goal, such as stealing data, financial fraud, or gaining unauthorized system access. This model allows analysts to segment attacks for targeted investigation and response.

To operationalize CKC in digital forensic investigations, D4I introduces a systematic step-by-step procedure aligned with Indicators of Compromise (IoCs). This can be seen in Figure 2.

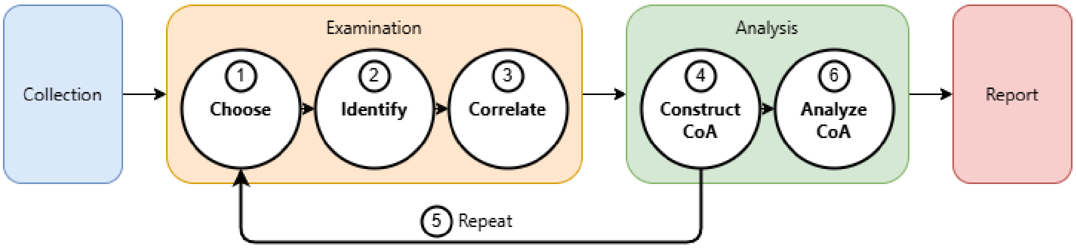


Figure 2. D4I Step by Step Instruction Method [12]

Figure 2 depicts this six-step method. First, the Chose step involves selecting the CKC phase where an IoC has been discovered. Then, in the Identify step, all digital artifacts related to that phase are identified based on the proposed classification. The third step, Correlate, examines the relationships among artifacts found within the same or adjacent CKC phases using NIST-compliant methods. After correlations are established, the Construct Chain of Artifacts (CoA) step builds a chronological artifact chain that forms a narrative of the attack. These four steps are then repeated (Repeat) across all CKC phases to ensure thorough examination. Finally, in the Analyze CoA step, the artifact chain is evaluated to determine if it represents a systematic cyberattack. The assumption here is that if a sequence of CKC phases can be reconstructed from artifacts, then a complete or partial attack occurred [20].

This procedure bridges the gap between abstract models and practical investigation by offering actionable steps based on observable evidence. While CKC provides a theoretical attack lifecycle, D4I enriches this with concrete guidelines for analysis and evidence correlation.

### Testing and Scenario Simulation

To validate the application of the D4I framework, a phishing scenario was simulated to replicate a realistic cyberattack targeting Kredivo users. The simulated attack follows the stages of the CKC, beginning from reconnaissance and ending with data exfiltration. The flow of the attack is illustrated in Figure 3.

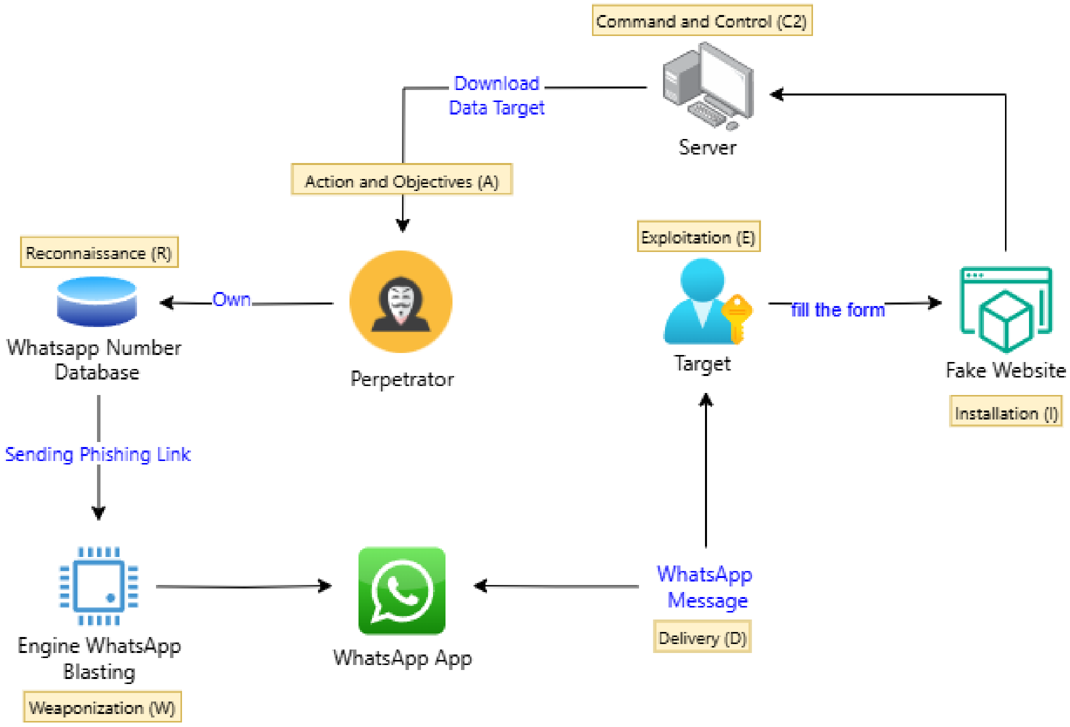


Figure 3. Phishing Attack Scenarios

To validate the application of the D4I framework, a phishing scenario was simulated to replicate a realistic cyberattack targeting Kredivo users. The simulated attack follows the stages of the CKC, beginning from reconnaissance and ending with data exfiltration. The flow of the attack is illustrated in Figure 3. The attack begins with the perpetrator owning or gaining access to a database of WhatsApp numbers through reconnaissance activities. These numbers are collected as potential targets for the phishing campaign. In the weaponization phase, the attacker configures a WhatsApp message blasting engine, which is programmed to distribute malicious links to victims via the WhatsApp platform. These links lead to a fake website that visually imitates the official Kredivo login page. Once the engine is active, the delivery phase is executed through the WhatsApp App, which sends out phishing messages containing a deceptive link. The target receives the message and, believing it to be legitimate, opens the link. In the exploitation phase, the victim is persuaded to fill out a web form on the fake site, providing sensitive information such as login credentials and a one-time password (OTP). This data is silently collected and stored.

In the installation phase, the fake website acts as a persistent phishing interface, ready to capture further data from future victims. Upon submission of credentials and OTP, the attacker gains unauthorized access to the victim’s Kredivo account. In the command and control (C2) phase, the stolen data is transmitted to a remote server controlled by the attacker. Finally, in the actions on objectives phase, the perpetrator downloads the exfiltrated data and proceeds with malicious actions, such as initiating fraudulent transactions or selling the harvested credentials.

This scenario demonstrates the complete lifecycle of a phishing attack mapped to the CKC model, which can then be forensically reconstructed using the D4I framework. Artifacts such as phishing messages, form data, browser logs, and server communication records are identified and correlated across CKC phases. The simulation provides a comprehensive case for validating the effectiveness of D4I in understanding, analyzing, and responding to phishing-based cyberattacks in a fintech context.

## RESULTS AND DISCUSSION

### Analysis of CKC Phases in the Simulated Attack

This study simulated a phishing attack targeting Kredivo users using the D4I framework to analyze and reconstruct cyberattacks through the Cyber Kill Chain (CKC). The simulation encompassed all CKC phases, from Reconnaissance to Actions on Objectives, and was reconstructed using forensic data extracted from two smartphone devices. The smartphones served as evidence containers for the simulated victim interactions and were examined to uncover digital traces related to the attack. The forensic acquisition and analysis processes were carried out using MOBILedit Forensic Express PRO version 7.4.0.20393, which facilitated the extraction of chat histories, browser records, and application data. A summary of the tools and materials used in this study is presented in Table 1.

Table 1. Tools and Materials Used in the Simulation and Forensic Analysis

| Category | Specification/Description |
|---|---|
| Smartphone Evidence #1 | iPhone 11, iOS version 15.8.1 |
| Smartphone Evidence #2 | Vivo Y21, Android version 8.1.0 |
| Forensic Tool | MOBILedit Forensic Express PRO v7.4.0.20393 |
| Phishing Infrastructure | Phishing domain: kredivo.desylo-santicho.my.id<br>Server with SSL, Port 80 enabled |

Table 2. Continued: Tools and Materials Used in the Simulation and Forensic Analysis

| Category | Specification/Description |
|---|---|
| Messaging Platform | WhatsApp-based message blasting engine using wwebjs.dev |
| Delivery Medium | WhatsApp chat messages with embedded phishing links |
| Scripting & Web Hosting | Custom HTML/CSS/JavaScript frontend; backend logging server |

This setup provided a controlled environment to replicate the attack and trace every action taken by the simulated attacker and victim. All artifacts recovered during this simulation were categorized into their respective CKC phases and served as the basis for further analysis using the D4I framework.

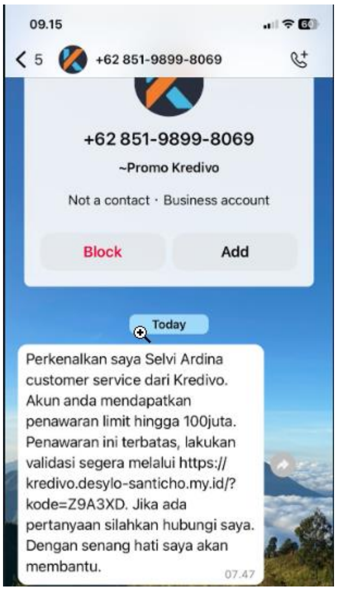
**Testing and Scenario Simulation**

This study simulated a phishing attack scenario based on a real-world case involving Kredivo. The simulation was constructed to follow all seven stages of the CKC, beginning specifically from Reconnaissance and proceeding sequentially to Actions on Objectives. This order reflects the structure and flow of the actual attacker's operations, which started from phishing content preparation rather than intelligence gathering.

The simulation began at the Reconnaissance stage. In the Reconnaissance phase, the attacker conducted initial information gathering to identify potential victims. This included researching user behavior, online presence, and publicly available contact data. The attacker also monitored Kredivo's official website to replicate its design and contents for use in a phishing website. Tools used in this phase included publicly available information sources and a custom WhatsApp automation library (https://wwebjs.dev) to scan and manage target numbers. The gathered intelligence enabled the attacker to craft realistic phishing emails and messages, increasing the likelihood of success in later phases.

During the Weaponization phase, the attacker created a professional-looking phishing website hosted at kredivo.desylo-santicho.my.id. The phishing infrastructure included SSL encryption and a message blasting engine designed to resemble Kredivo's interface. The attacker embedded social engineering tactics into the phishing content, persuading victims to enter detailed personal information such as WhatsApp number, gender, occupation, email, address, and national ID number [21]. This process aimed to maximize credibility and effectiveness of the phishing attempt by mimicking legitimate Kredivo communication channels.

The Delivery phase involved sending phishing messages to the identified targets via WhatsApp. These messages contained the malicious link crafted during the Weaponization phase and were distributed using an automated message-blasting tool. The message content was designed to appear as if it came from Kredivo, often including urgency (e.g., promo expiration or account warnings) to induce user action. This stage is captured in Figure 4, showing the dissemination of phishing links through the messaging platform.



09.15

5 +62 851-9899-8069

+62 851-9899-8069

~Promo Kredivo

Not a contact · Business account

Block Add

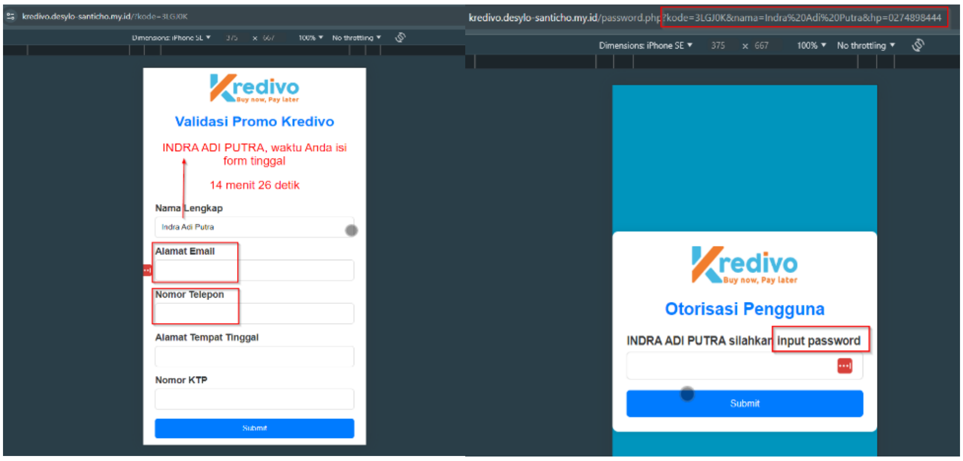
Today

Perkenalkan saya Selvi Ardina customer service dari Kredivo. Akun anda mendapatkan penawaran limit hingga 100juta. Penawaran ini terbatas, lakukan validasi segera melalui https://kredivo.desylo-santicho.my.id/?kode=Z9A3XD. Jika ada pertanyaan silahkan hubungi saya. Dengan senang hati saya akan membantu. 07.47

Figure 4. Sending phishing links using WhatsApp

The Delivery phase involved sending phishing messages to the identified targets via WhatsApp. These messages contained the malicious link crafted during the Weaponization phase and were distributed using an automated message-blasting tool. The message content was designed to appear as if it came from Kredivo, often including urgency (e.g., promo expiration or account warnings) to induce user action. This stage is captured in Figure 4, showing the dissemination of phishing links through the messaging platform.

Once a user clicked the link, the Exploitation phase was triggered. Victims were redirected to the fake Kredivo login page and prompted to input sensitive information such as their email, ID number, and OTP. This information was silently collected by backend scripts and stored in the attacker's server. Three visuals support this phase: Figure 5 shows the entry of personal data, Figure 6 illustrates the victim receiving the OTP via SMS, and Figure 7 captures the OTP being submitted into the phishing form.



kredivo.desylo-santicho.my.id/?kode=3LGJ0K

Dimensions: iPhone SE ▾ 375 × 667 100% ▾ No throttling ▾

Kredivo Buy now, Pay later

Validasi Promo Kredivo

INDRA ADI PUTRA, waktu Anda isi form tinggal

14 menit 26 detik

Nama Lengkap: Indra Adi Putra

Alamat Email

Nomor Telepon

Alamat Tempat Tinggal

Nomor KTP

Submit

kredivo.desylo-santicho.my.id/password.php?kode=3LGJ0K&nama=Indra%20Adi%20Putra&hp=0274898444

Dimensions: iPhone SE ▾ 375 × 667 100% ▾ No throttling ▾

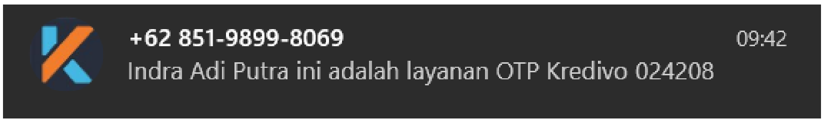
Kredivo Buy now, Pay later

Otorisasi Pengguna

INDRA ADI PUTRA silahkan input password

Submit

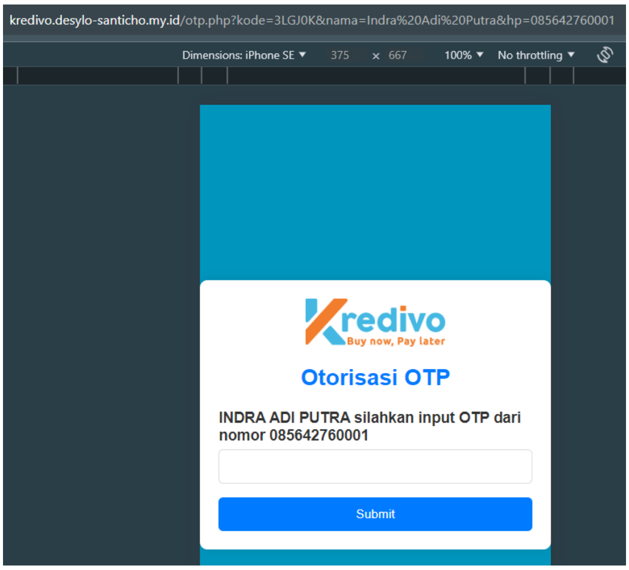
Figure 5. Personal Data Entry



+62 851-9899-8069 09:42

Indra Adi Putra ini adalah layanan OTP Kredivo 024208

Figure 6. Credivo OTP Received

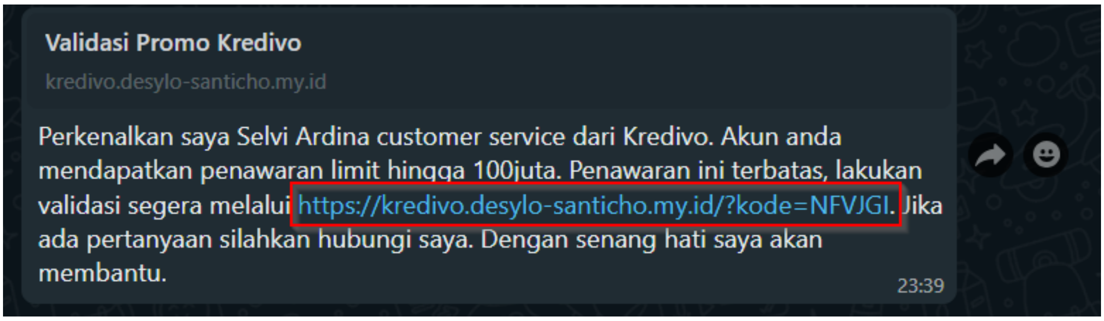

kredivo.desylo-santicho.my.id/otp.php?kode=3LGJ0K&nama=Indra%20Adi%20Putra&hp=085642760001

Otorisasi OTP

INDRA ADI PUTRA silahkan input OTP dari nomor 085642760001

Figure 7. OTP Input on Phishing Link

In the Installation phase, the phishing site delivered the entered data to the attacker in real time. Although no malware was directly installed in this case, the attacker's infrastructure functioned as a persistent data collector, maintaining access to stolen credentials and possibly preparing for further exploitation. As shown in Figure 8, the phishing infrastructure remained active, allowing multiple victims to interact with it over time.


Validasi Promo Kredivo

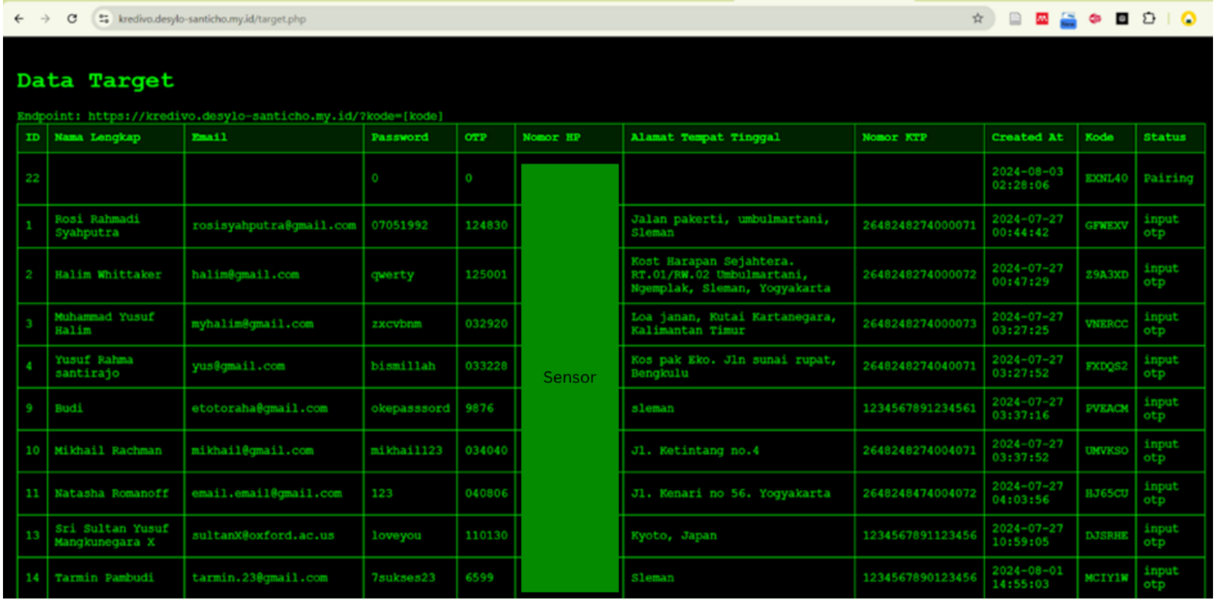
kredivo.desylo-santicho.my.id

Perkenalkan saya Selvi Ardina customer service dari Kredivo. Akun anda mendapatkan penawaran limit hingga 100juta. Penawaran ini terbatas, lakukan validasi segera melalui https://kredivo.desylo-santicho.my.id/?kode=NFVJGI. Jika ada pertanyaan silahkan hubungi saya. Dengan senang hati saya akan membantu.

23:39

Figure 8. Link Sending Using WhatsApp

The Command and Control (C2) phase was marked by the attacker's real-time interaction with the stolen data via a backend server. This infrastructure handled the reception of credentials, managed session control, and allowed the attacker to prepare or trigger unauthorized actions on behalf of the victim. Server logs and system behavior confirmed this ongoing link between victim activity and attacker control. Figure 9 illustrates the attacker's monitoring dashboard and command infrastructure.



kredivo.desylo-santicho.my.id/target.php

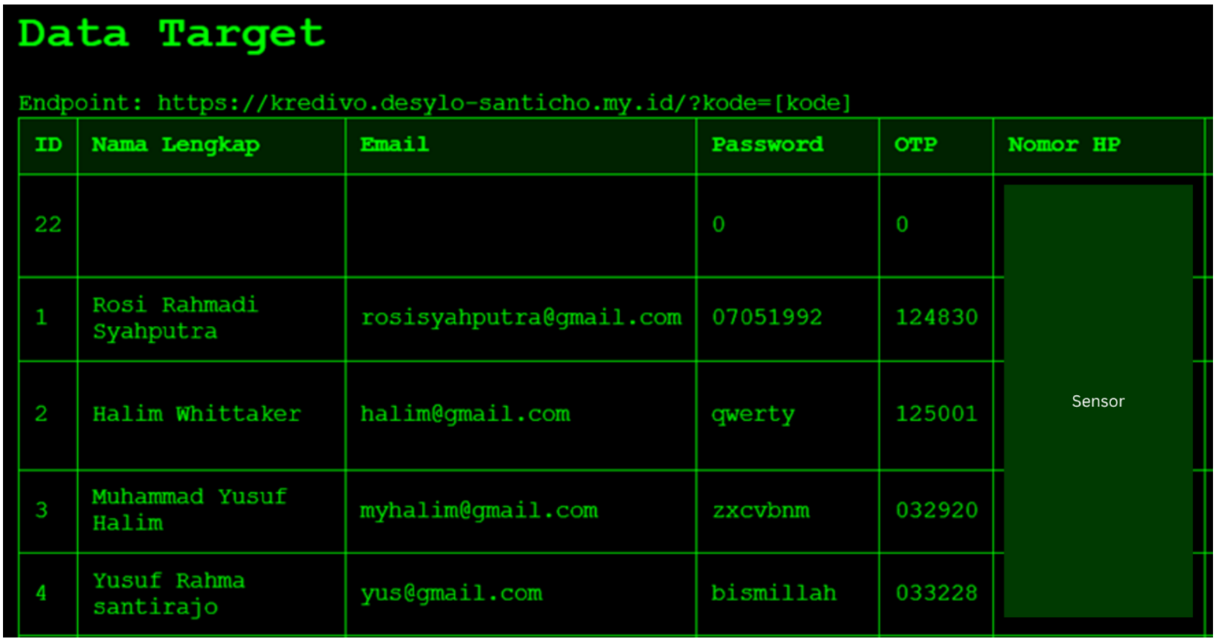
Data Target

Endpoint: https://kredivo.desylo-santicho.my.id/?kode=[kode]

| ID | Nama Lengkap | Email | Password | OTP | Nomor HP | Alamat Tempat Tinggal | Nomor KTP | Created At | Kode | Status |
|---|---|---|---|---|---|---|---|---|---|---|
| 22 | | | 0 | 0 | Sensor | | | 2024-08-03 02:28:06 | EXNL40 | Pairing |
| 1 | Rosi Rahmadi Syahputra | rosisyahputra@gmail.com | 07051992 | 124830 | | Jalan pakerti, umbulmartani, Sleman | 2648248274000071 | 2024-07-27 00:44:42 | GFWEXV | input otp |
| 2 | Halim Whittaker | halim@gmail.com | qwerty | 125001 | | Kost Harapan Sejahtera. RT.01/RW.02 Umbulmartani, Ngemplak, Sleman, Yogyakarta | 2648248274000072 | 2024-07-27 00:47:29 | Z9A3XD | input otp |
| 3 | Muhammad Yusuf Halim | myhalim@gmail.com | zxcvbnm | 032920 | | Loa janan, Kutai Kartanegara, Kalimantan Timur | 2648248274000073 | 2024-07-27 03:27:25 | VNERCC | input otp |
| 4 | Yusuf Rahma santirajo | yus@gmail.com | bismillah | 033228 | | Kos pak Eko. Jln sunai rupat, Bengkulu | 2648248274040071 | 2024-07-27 03:27:52 | FXDQS2 | input otp |
| 9 | Budi | etotoraha@gmail.com | okepasssord | 9876 | | sleman | 1234567891234561 | 2024-07-27 03:37:16 | PVEACM | input otp |
| 10 | Mikhail Rachman | mikhail@gmail.com | mikhail123 | 034040 | | Jl. Ketintang no.4 | 2648248274004071 | 2024-07-27 03:37:52 | UMVKSO | input otp |
| 11 | Natasha Romanoff | email.email@gmail.com | 123 | 040806 | | Jl. Kenari no 56. Yogyakarta | 2648248474004072 | 2024-07-27 04:03:56 | HJ65CU | input otp |
| 13 | Sri Sultan Yusuf Mangkunegara X | sultanX@oxford.ac.us | loveyou | 110130 | | Kyoto, Japan | 1234567891123456 | 2024-07-27 10:59:05 | DJSRHE | input otp |
| 14 | Tarmin Pambudi | tarmin.23@gmail.com | 7sukses23 | 6599 | | Sleman | 1234567890123456 | 2024-08-01 14:55:03 | MCIY1W | input otp |

Figure 9. Target Data Control

The attack culminated in the Actions on Objectives phase, where the attacker used the stolen credentials and OTP to gain unauthorized access to the victim's Kredivo account. Once inside, the attacker could view financial details, initiate fraudulent transactions, or steal identity data. This final phase demonstrates the completion of the phishing lifecycle and validates the attacker's success. Figure 10 captures the final stage, showing victim data processed and stored in the attacker's system.



Data Target

Endpoint: https://kredivo.desylo-santicho.my.id/?kode=[kode]

| ID | Nama Lengkap | Email | Password | OTP | Nomor HP |
|---|---|---|---|---|---|
| 22 | | | 0 | 0 | Sensor |
| 1 | Rosi Rahmadi Syahputra | rosisyahputra@gmail.com | 07051992 | 124830 | |
| 2 | Halim Whittaker | halim@gmail.com | qwerty | 125001 | |
| 3 | Muhammad Yusuf Halim | myhalim@gmail.com | zxcvbnm | 032920 | |
| 4 | Yusuf Rahma santirajo | yus@gmail.com | bismillah | 033228 | |

Figure 10. Target Data That Has Beent Inputted by the Victim

This simulation not only recreated a realistic phishing attack with all CKC stages but also generated a rich dataset of digital artifacts. These artifacts were used in the following sections to construct a Chain of Artifacts (CoA) analyze the attack through the D4I forensic lens.

### Construction and Analysis of the Chain of Artifacts

The Chain of Artifacts (CoA) is a chronological mapping of evidence that demonstrates the transition of attacker activity across CKC phases. Each artifact, from the initial message sent to the user to the final unauthorized login was documented and timestamped. Browser history, WhatsApp logs, OTP metadata, server access logs, and phishing form submissions were used to link actions between phases. By analyzing this chain, organizations can identify critical intervention points. For instance, if phishing messages are intercepted during delivery, the subsequent phases can be disrupted. Similarly, if unusual C2 behavior is detected, systems can be isolated before any damage is done.

Understanding the attacker's timeline enables organizations not only to respond to incidents effectively, but also to build proactive defense strategies tailored to each CKC phase, such as privacy protection during reconnaissance, advanced phishing detection during delivery, and user training to combat exploitation.

### Visualization of D4I Findings

The visualization in Figure 11 presents the D4I framework in action, mapping the artifacts and attack flow across the CKC phases. Each black dot represents a detected artifact in that phase, while red dashed lines represent cross-phase connections, together visualizing the modus operandi and attack signature of the attacker.

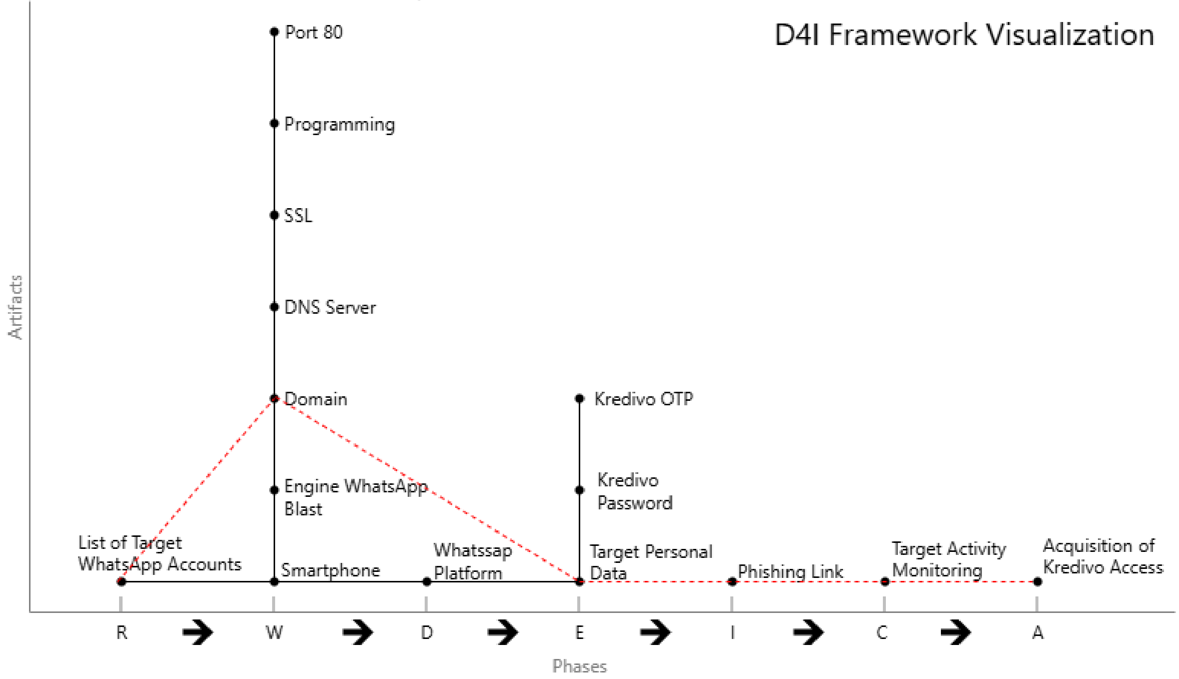


Figure 11. D4I Framework Visualization of the Phishing Attack Simulation

Figure 11 diagram illustrates the attacker's artifacts per CKC phase and highlights inter-phase connections that reflect the attack's progression. The highest concentration of artifacts appears in the Weaponization phase, emphasizing the attacker's investment in infrastructure setup, domain, SSL, scripting, and WhatsApp engine. From Reconnaissance to Exploitation, the artifacts illustrate the operational flow, with key data inputs and OTP logs confirming victim interaction. The red lines reflect the coherence and causality between phases, making it easier to understand the attacker's logic. This form of visualization enhances the utility of the D4I framework by providing investigators and stakeholders with a clear, visual summary of the attack lifecycle.

### Discussion

The D4I framework offers several strengths, particularly in its deep focus on the Examination and Analysis phases of forensic investigation. Its structured methodology enables investigators to map, correlate, and visualize complex attacks with clarity and precision. In the Kredivo case, D4I helped trace digital footprints, ranging from phishing messages to final account access by organizing evidence into logical sequences. The process is also iterative, allowing investigators to revisit earlier phases if new insights emerge, enhancing both accuracy and completeness. In addition, D4I supports investigative logic through the 5W1H approach (Who, What, When, Where, Why, How), helping explain not only how the attack occurred, but also why it succeeded.

However, D4I also exhibits limitations. It does not explicitly address the Collection and Reporting phases of the forensic process, both of which are crucial in real-world investigations. Without proper guidance on evidence collection, key artifacts may be overlooked or mishandled, potentially rendering them inadmissible in legal proceedings. Similarly, the absence of a formal reporting structure can hinder communication of findings, especially in cross-functional or legal environments. While D4I's visualization (e.g., Figure 11) offers a helpful overview, it is not a substitute for a full, standardized forensic report.

These gaps represent opportunities for further development of the D4I framework. Future research could enhance D4I by integrating systematic collection protocols and standardized reporting modules to provide a more comprehensive and court-ready forensic methodology.

## CONCLUSIONS AND SUGGESTIONS

This research has demonstrated the applicability of the D4I framework in analyzing phishing attacks through a simulated case involving Kredivo users. By following the seven phases of the Cyber Kill Chain, the study successfully identified and correlated digital artifacts from the weaponization phase to the final actions on objectives. The attack scenario, which involved social engineering techniques, phishing websites, and OTP harvesting via WhatsApp messages, was effectively reconstructed using D4I. The framework proved valuable in supporting detailed post-incident analysis through its pillars of detection, deterrence, disruption, and information. Furthermore, the structured visualization of artifacts across phases enabled a clear understanding of the attack flow. However, the findings also revealed that D4I lacks several critical components such as procedures for digital evidence collection, file imaging, and standardized reporting. These omissions limit its forensic completeness and legal applicability in real-world investigations.

To improve the effectiveness of D4I in future implementations, it is recommended that the framework be expanded to include a dedicated phase for evidence collection along with clear guidelines for forensic imaging and acquisition. Future researchers should also consider integrating formal reporting mechanisms to ensure investigative results are well-documented and usable in legal or organizational contexts. From a broader perspective, service providers such as Kredivo are encouraged to enhance their security controls and continuously educate users to recognize and avoid phishing attempts. At the user level, maintaining awareness of online threats and avoiding the disclosure of personal information through untrusted sources are essential practices. These recommendations are intended to strengthen the application of forensic frameworks and promote a more resilient and informed digital environment.

## REFERENCES

[1] M. F. Naseri, Q. A. Frugh, and Q. Shamsi, "Challenge and Opportunity of Mobile Banking in Afghanistan," *Journal of Technology and Informatics (JoTI)*, vol. 7, no. 1, Art. no. 1, Apr. 2025, doi: 10.37802/joti.v7i1.896.

[2] I. A. G. Y. S. Putri, N. M. Estiyanti, and L. Yupita, "Analysis of Factors Affecting Borrowes' Interest in Using Kredivo Fintech Peer-to-peer Lending Services During the COVID-19 Pandemic in Denpasar City," *JurnalTAM*, vol. 14, no. 1, p. 120, Jul. 2023, doi: 10.56327/jurnaltam.v14i1.1398.

[3] Z. K. Sangha and H. Sulistiani, "Risk Analysis of Computer Network Security Focusing on Phishing Attacks in Fintech Platform," in *The 5th International Conference on Information Technology and Security*, IC-ITECHS, Dec. 2024, pp. 1028–1034. doi: 10.32664/ic-itechs.v5i1.1687.

[4] R. Lohiya and A. Thakkar, "A Compendium on Risk Assessment of Phishing Attack Using Attack Modeling Techniques," *Procedia Computer Science*, vol. 235, pp. 1105–1114, 2024, doi: 10.1016/j.procs.2024.04.105.

[5] M. K. Mehmood, H. Arshad, M. Alawida, and A. Mehmood, "Enhancing Smishing Detection: A Deep Learning Approach for Improved Accuracy and Reduced False Positives," *IEEE Access*, vol. 12, pp. 137176–137193, 2024, doi: 10.1109/ACCESS.2024.3463871.

[6] A. C. Banjarnahor and P. Priyana, "Analisis Yuridis Cybercrime Terhadap Penanganan Kasus Phising Kredivo," *HERMENEUTIKA: Jurnal Ilmu Hukum*, vol. 6, no. 1, pp. 32–36, Feb. 2022, doi: 10.33603/hermeneutika.v6i1.6754.

[7] N. Ilany-Tzur and L. Fink, "Device and risk-avoidance behavior in the context of cybersecurity phishing attacks," *International Journal of Information Management*, vol. 84, p. 102919, Oct. 2025, doi: 10.1016/j.ijinfomgt.2025.102919.

[8] S. K. Birthriya, P. Ahlawat, and A. K. Jain, "A Comprehensive Survey of Social Engineering Attacks: Taxonomy of Attacks, Prevention, and Mitigation Strategies," *Journal of Applied Security Research*, vol. 20, no. 2, pp. 244–292, Apr. 2025, doi: 10.1080/19361610.2024.2372986.

[9] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Front. Comput. Sci.*, vol. 3, p. 563060, Mar. 2021, doi: 10.3389/fcomp.2021.563060.

[10] A. A. A. and P. K., "Towards the Detection of Phishing Attacks: A Survey, Taxonomy, and Open Research Challenges," in *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India: IEEE, 2020, pp. 337–343. doi: 10.1109/ICOEI48184.2020.9142967.

[11] F. Carroll, J. A. Adejobi, and R. Montasari, "How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society," *SN Computer Science*, vol. 3, no. 2, p. 170, Mar. 2022, doi: 10.1007/s42979-022-01069-1.

[12] A. Dimitriadis, N. Ivezic, B. Kulvatunyou, and I. Mavridis, "D4I - Digital forensics framework for reviewing and investigating cyber attacks," *Array*, vol. 5, p. 100015, 2020, doi: 10.1016/j.array.2019.100015.

[13] M. M. Mirza, A. Ozer, and U. Karabiyik, "Mobile Cyber Forensic Investigations of Web3 Wallets on Android and iOS," *Applied Sciences*, vol. 12, no. 21, p. 11180, Nov. 2022, doi: 10.3390/app122111180.

[14] S. Mehrban *et al.*, "Towards Secure FinTech: A Survey, Taxonomy, and Open Research Challenges," *IEEE Access*, vol. 8, pp. 23391–23406, 2020, doi: 10.1109/ACCESS.2020.2970430.

[15] J. A. Jafri, S. I. M. Amin, A. Abdul Rahman, and S. M. Nor, "A systematic literature review of the role of trust and security on Fintech adoption in banking," *Heliyon*, vol. 10, no. 1, p. e22980, Jan. 2024, doi: 10.1016/j.heliyon.2023.e22980.

[16] N. Sirenko, I. Atamanyuk, Y. Volosyuk, A. Poltorak, O. Melnyk, and P. Fenenko, "Paradigm Changes that Strengthen the Financial Security of the State through FINTECH Development," in *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine: IEEE, May 2020, pp. 110–116. doi: 10.1109/DESSERT50317.2020.9125026.

[17] Y. Ahmed, A. T. Asyhari, and M. A. Rahman, "A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats," *Comput. Mater. Contin.*, vol. 67, no. 2, pp. 2497–2513, 2021, doi: 10.32604/cmc.2021.014223.

[18] K. Haga, P. H. Meland, and G. Sindre, "Breaking the Cyber Kill Chain by Modelling Resource Costs," in *Graphical Models for Security*, H. Eades III and O. Gadyatskaya, Eds., Cham: Springer International Publishing, 2020, pp. 111–126. doi: 10.1007/978-3-030-62230-5_6.

[19] M. Kazimierczak, N. Habib, J. H. Chan, and T. Thanapattheerakul, "Impact of AI on the Cyber Kill Chain: A Systematic Review," *Heliyon*, vol. 10, no. 24, p. e40699, Dec. 2024, doi: 10.1016/j.heliyon.2024.e40699.

[20] M. M. Yamin, M. Ullah, H. Ullah, B. Katt, M. Hijji, and K. Muhammad, "Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security," *Mathematics*, vol. 10, no. 12, p. 2054, Jun. 2022, doi: 10.3390/math10122054.

[21] I. Stylianou, P. Bountakas, A. Zarras, and C. Xenakis, "Suspicious minds: Psychological techniques correlated with online phishing attacks," *Computers in Human Behavior Reports*, vol. 19, p. 100694, Aug. 2025, doi: 10.1016/j.chbr.2025.100694.