Analysis of Digital Competence in Handling Phishing Cases: Case Study at the Special Criminal Directorate of the Yogyakarta Regional Police

Benny Erwin, Universitas Gadjah Mada, Indonesia

The Kyoto Conference on Arts, Media & Culture 2025
Official Conference Proceedings

Abstract

This study examines the processes and digital competencies for handling online fraud cases (phishing) at the Directorate of Special Criminal Investigation (Ditreskrimsus) of the Regional Police of the Special Region of Yogyakarta (Polda DIY). Using a qualitative approach with a case study method, this study aims to analyze the handling process and identify the digital competencies required of police personnel. Data were collected through in-depth interviews with five members of Ditreskrimsus, observations of phishing case examination and filing activities, and analysis of investigation filing documents and phishing case handling reports carried out by the Polda DIY. This study adopted the DigComp 2.2 framework in data analysis. This framework identifies five areas of digital competency: information and data literacy, communication and collaboration, digital content creation, digital security, and problem-solving. The analysis indicates a gap in the digital competency area for Ditreskrimsus Polda DIY personnel. Through an analysis of the phishing handling process at Ditreskrimsus Polda DIY, this study highlights the importance of improving digital competency to increase the effectiveness of handling phishing cases in the dynamic digital era.

Keywords: phishing, cybercrime, digital competence, Polda DIY, cybersecurity

iafor
The International Academic Forum
www.iafor.org

Introduction

The digital era has brought significant changes to human life, including in the fields of security and law enforcement. The development of information and communication technology, while facilitating public activities, also opens opportunities for various new forms of crime that exploit security vulnerabilities in cyberspace. One such crime is cybercrime, which has become a global threat with increasing intensity. Cybercrime includes attacks such as phishing, malware, ransomware, social engineering, denial-of-service attacks, and disinformation (European Parliament, 2024). Among these various types, phishing is one of the most common and harmful attacks. Aleroud and Zhou (2017) define phishing as a social engineering–based attack that deceives victims by impersonating a trusted entity. The goal is to steal sensitive information such as credentials, financial data, or account access. This attack is typically carried out via email, text message, or fake websites designed to resemble legitimate ones, making victims unaware they are providing information to perpetrators. One common technique involves sending links to intentionally engineered spoofed websites that appear authentic (Ekayani et al., 2023).

Globally, losses from cybercrime are projected to reach 10.5 trillion USD by 2025 (Cybersecurity Ventures, 2020). The Anti-Phishing Working Group (APWG, 2023) reported 4.7 million phishing websites in 2022, with 1.35 million cases in the fourth quarter alone. These figures highlight the urgency of improving mitigation and investigative capabilities for phishing, including in Indonesia. In Indonesia, phishing attacks have increased alarmingly. The Indonesia Anti-Phishing Data Exchange (2023) reported that Indonesia ranked first globally in hosting phishing sites under the .id domain throughout 2023, followed by the United States.

Figure 1

Countries Hosting .id Domain Phishing Sites

Negara	Oktober	November	Desember
Indonesian	91.3%	85.89%	95.7%
United States	3.89%	3.93%	1.19%
Russia	3.11%	9.31%	3.0%
United Kingdom	0.11	0.06%	
Singapore	0.92%	0.17%	0.03%
Germany	0.32%	0.17%	
None	0.36%	0.46%	0.08%

Source: Indonesia Anti-Phishing Data Exchange (IDADX)

Throughout the year, 64,989 phishing attacks were reported, with a peak of 26,675 attacks in the first quarter. Targets included social media, financial institutions, e-commerce platforms, ISPs, and cryptocurrency exchanges. This vulnerability is exacerbated by the fact that 79.5% of Indonesia's population, which totals 221 million people, are internet users (APJII, 2024). However, public awareness regarding cybersecurity remains low; only 19.5% of users demonstrate a good understanding (Pratiwi et al., 2024). In addition to human factors, digital infrastructure also contributes to the rise in phishing attacks. Browsers and other software contain vulnerabilities that phishers can exploit (Chiew et al., 2018). Yurita et al. (2023)

emphasize that the large population of internet users, weak cybersecurity literacy, and gaps in digital infrastructure further worsen the situation.

At the local level, Yogyakarta is one of the regions that faces significant phishing threats. Data from the Ditreskrimsus Polda DIY shows that in 2022, cybercrime was the most common case, accounting for 43 of 83 cases successfully handled (Harianjogja.com, 2023). As an educational city with an internet penetration rate of 88.73% (APJII, 2024), Yogyakarta has a large population of young and active internet users, making them prime targets for phishing perpetrators. The high level of digital penetration and students' online behavior patterns add complexity to the challenges faced by law enforcement.

In such conditions, the digital competence of law enforcement officers becomes a crucial factor. According to the DigComp framework (Carretero et al., 2017), digital competence includes the ability to use technology safely, critically, and creatively. Guillén-Gámez and Mayorga-Fernández (2020) emphasize that digital competence involves not only technical skills but also risk awareness and the application of protective practices against cyber threats. For police personnel, this competence is essential for detecting, analyzing, and resolving increasingly complex phishing cases.

However, several studies show that challenges related to officers' digital competence remain substantial. Previous research has identified obstacles such as limited resources, technical skill gaps, constraints in digital forensics, jurisdictional issues, and procedural approaches that do not adequately address digital competence (Aini & Lubis, 2024; Prakoso, 2022; Purwandari, 2024; Sitompul et al., 2024). These gaps indicate the need for more targeted research on police officers' digital competence in handling phishing cases, particularly at the regional level, such as Polda DIY. This study aims to analyze how the digital competence of Ditreskrimsus Polda DIY personnel contributes to the handling of phishing cases, while identifying the challenges and limitations they encounter. Using a qualitative case study method and the DigComp 2.2 framework, the study is expected to provide a comprehensive understanding of the digital capacity-building needs among law enforcement officers.

Beyond its academic contribution, this research also has practical relevance. The findings can serve as a foundation for the Indonesian National Police in designing more targeted training programs to strengthen personnel's technical and analytical capabilities in handling phishing cases. With the increasing prevalence of cybercrime in Indonesia, improving the digital competence of law enforcement officers has become an urgent necessity to protect the public and maintain the effectiveness of law enforcement in the digital era.

Literature Review

The development of digital technology has transformed how society interacts, creating a growing need for law enforcement officers to possess adequate digital competencies, particularly in handling cybercrimes such as phishing. This study employs digital literacy as its primary theoretical foundation, which is further elaborated into an operational digital competency framework.

Digital literacy, according to Gilster (1997), refers to the ability to understand and use information from various digital sources. Martin (2005) expands this definition by emphasizing the ability to access, manage, evaluate, analyze, and synthesize digital resources. Eshet-Alkalai (2004) adds five dimensions of digital literacy, including photo-visual,

reproduction, branching, information, and socio-emotional literacy. Meanwhile, Van Deursen and Van Dijk (2014) introduce six modern digital skill categories, ranging from operational skills to strategic skills.

For the operational framework, this study adopts DigComp 2.2 as the primary reference for assessing the digital competencies of police personnel. DigComp Framework (Vuorikari et al., 2022) includes five areas: (1) information and data literacy, (2) communication and collaboration, (3) digital content creation, (4) safety, and (5) problem solving. This framework was selected because it provides a comprehensive analytical structure suitable for evaluating digital competencies within a professional context.

DigComp 2.2 is used in this study to analyze the digital competencies of personnel at the Regional Police of the Special Region of Yogyakarta (Polda DIY) in two main aspects. First, to assess the digital competencies of Ditreskrimsus Polda DIY personnel in handling phishing cases based on the five competency areas. Second, to identify the strategies required for developing digital competencies to enhance the effectiveness of phishing case handling. By employing DigComp 2.2, this study is expected to provide a systematic overview of the digital competency readiness of police personnel and the relevant development needs in law enforcement related to cybercrime.

Method

This study employs a qualitative case study approach. According to Yin (2018), the case study method is appropriate for exploring contemporary phenomena within real-life contexts, especially when the boundaries between the phenomenon and its context are not clearly defined. A case study involves providing a detailed description of the case being examined. Essentially, case study research typically begins with “how” and “why” questions. In this research, the case study method enables an in-depth exploration of digital competencies in handling phishing cases at the Special Criminal Investigation Directorate (Ditreskrimsus) of Polda DIY. As explained by Stake (1995), this method helps gather rich contextual data through multiple sources. Although it has limitations in terms of generalizability and access to sensitive information, the depth of analysis produced can offer valuable insights for developing strategies to address phishing cases.

This study uses the DigComp 2.2 framework to analyze the digital competencies of Polda DIY personnel in handling phishing cases. Five competency areas are used as analytical indicators, including: (1) information and data literacy, namely the ability to analyze digital evidence and data related to phishing; (2) communication and collaboration, namely coordination across units and with relevant stakeholders; (3) digital content creation, namely digital case documentation and content development in handling phishing cases; (4) digital safety, namely understanding aspects of cybersecurity; and (5) problem solving, namely the ability to overcome technical issues encountered during investigations.

This research aims to thoroughly uncover the factors influencing the digital competencies of Polda DIY personnel in handling phishing cases in Yogyakarta. The research subjects are police personnel serving within the Cyber Sub-Directorate (Subdit Siber) of Ditreskrimsus Polda DIY, particularly those directly involved in handling phishing cases. Selecting Polda DIY personnel as research subjects is highly relevant since they are directly responsible for investigating and responding to phishing cases in the Yogyakarta region. The criteria determined by the researcher to obtain sufficiently in-depth and valid information include: (1)

Police personnel who have served for at least six months in the Cyber Sub-Directorate of Ditreskrimsus Polda DIY to ensure sufficient understanding of procedures and variations of phishing cases; and (2) personnel with direct experience in handling phishing cases. Research subjects are selected using a purposive sampling procedure. According to Sugiyono (2016), purposive sampling is a technique for selecting data sources based on specific considerations. The reason for using purposive sampling is that not all potential samples meet the required criteria for the phenomenon being studied.

The researcher collects data through in-depth interviews with five personnel from Subdit V Cyber of Ditreskrimsus Polda DIY who meet the predetermined criteria, as well as through observations and document analysis. The interviews focus on personnel's experiences in handling phishing cases across the five competency areas of DigComp 2.2. Observations are conducted on the case-handling process to identify the application of digital competencies in practice. Document analysis includes investigation files and standard operating procedures that indicate the required digital competencies. Validity testing is conducted through early-stage triangulation by comparing results from these three sources to validate findings on digital competencies based on the DigComp 2.2 framework. This triangulation process involves using diverse perceptions to clarify meaning and assess the likelihood of repeating specific observations or interpretations. Triangulation techniques can also be used to clarify meaning by identifying different perspectives on various phenomena (Flick, 1992, in Denzin and Lincoln, 2009).

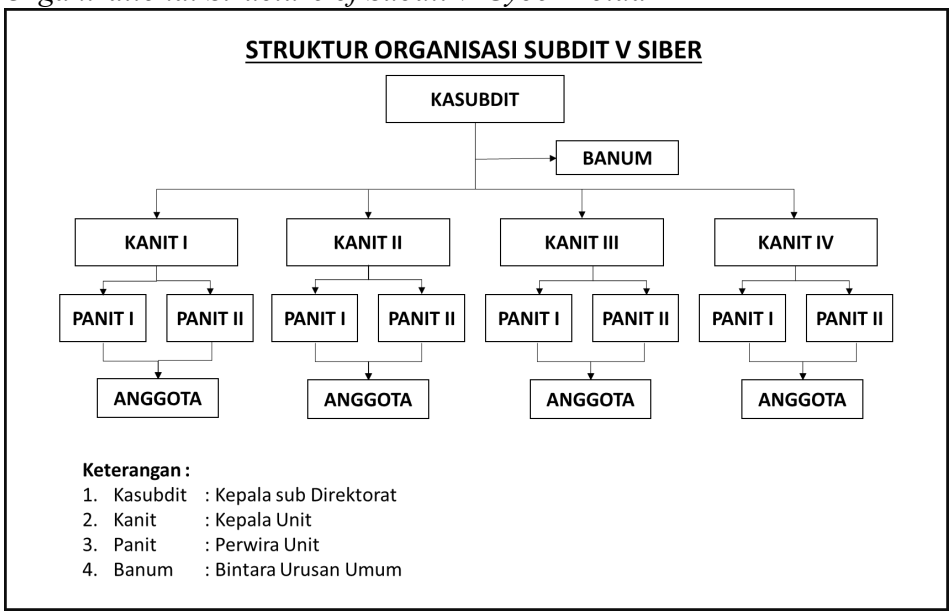
Discussion

The analysis of the digital competencies of Ditreskrimsus Polda DIY personnel in handling phishing cases reveals several important findings based on the DigComp 2.2 framework. Through interviews, observations, and document analysis, this study identifies patterns of capabilities and implementation challenges across the five core areas of digital competence.

Based on field observations, Sub-Directorate V Cybercrime (Subdit V Siber) of Ditreskrimsus Polda DIY is responsible for investigating and prosecuting cybercrimes, including phishing. The unit consists of investigators, cyber analysts, and digital forensic personnel; however, a significant technical competence gap was observed. Of 37 personnel, only three hold digital forensic certification, which poses a challenge in addressing the growing complexity of cybercrime cases.

The organizational structure of Subdit V Cybercrime, as illustrated in the figure, is arranged with a clear hierarchy. The Sub-Director leads the entire unit, which is divided into four operational units (Unit Heads I–IV), each supported by Section Heads (Panit) and several staff members. Additionally, there is a Banum (Administrative Officer) who supports administrative functions. While this structure allows for a clear division of tasks, gaps in digital competence can hinder operational effectiveness, particularly in investigations and case preparation.

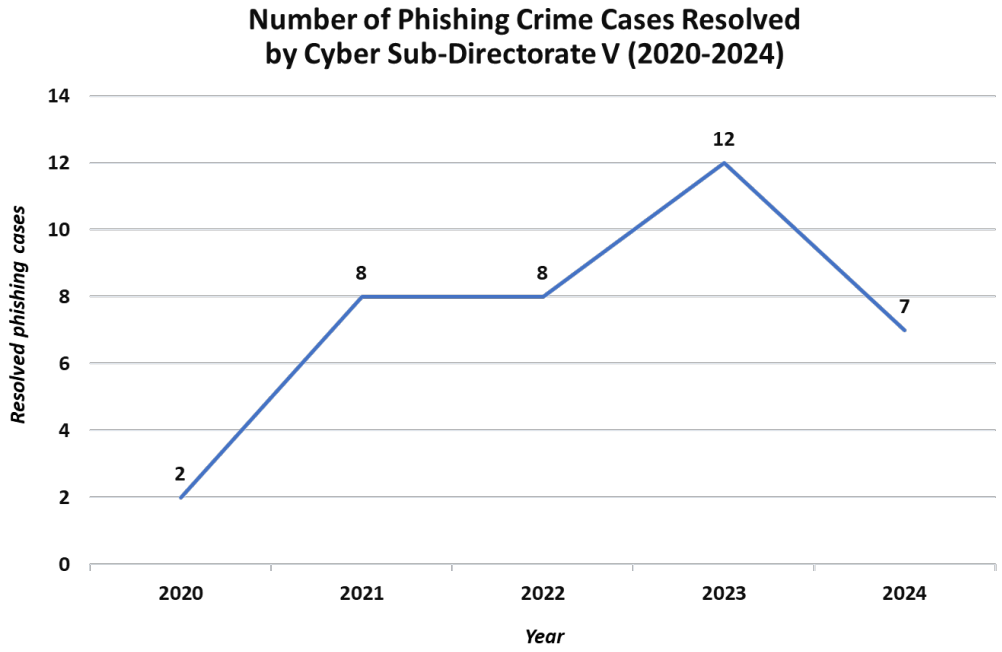
Figure 2
Organizational Structure of Subdit V Cyber Polda DIY



In practice, phishing cases are handled through a systematic procedure: the report is received at the Integrated Police Service Center (SPKT), followed by investigation, case conferences, elevation to a full investigation, and, finally, case file preparation before submission to the Public Prosecutor. This workflow reflects an organized mechanism, although the success of each stage remains dependent on the technical competencies of the personnel involved.

An analysis of phishing case trends handled by Subdit V Cybercrime from 2020 to 2024 shows notable fluctuations (Figure 3). In 2020, only two phishing cases were completed, marking the lowest level in the five years, likely influenced by COVID-19 pandemic-related restrictions on activity. In 2021, the number increased significantly to eight cases, with similar figures observed in 2022. The highest number of case completions occurred in 2023, reaching twelve cases, indicating an improvement in the unit's handling capacity compared to previous years. However, the number decreased again in 2024 to 7 cases, reflecting fluctuations in the region's phishing case-handling trends.

Figure 3
Number of Phishing Cases Handled by Subdit V Cybercrime, Polda DIY (2019–2024)



These fluctuations indicate that phishing remains a significant threat in Yogyakarta, with a recent upward trend in case resolution despite a decline in 2024. The decrease may be attributed to the growing adoption of digital technologies and increasingly complex cybercrime techniques. Amid these challenges, Ditreskrimsus Polda DIY continues efforts to strengthen personnel's digital competencies despite resource limitations and the high demand for technological adaptation.

To provide a comprehensive analysis, the discussion is divided into two parts: first, an assessment of personnel digital competencies based on the five areas of DigComp 2.2; and second, an identification of competency gaps and development needs to enhance the effectiveness of phishing case handling in Ditreskrimsus Polda DIY.

This DigComp 2.2-based analysis offers an in-depth overview of the capabilities and limitations of personnel in managing phishing cases across each competency area.

1. *Information and Data Literacy*

The analysis of the information and data literacy competency area at Ditreskrimsus Polda DIY reveals varying levels of capability in handling phishing cases. According to the DigComp 2.2 framework (Vuorikari et al., 2022), information and data literacy encompasses three main competency dimensions: the ability to articulate information needs and to locate and retrieve digital data; the ability to evaluate the relevance and reliability of sources and their content; and the ability to store, manage, and organize digital data. These competencies are fundamental in cybercrime investigations, as they involve handling complex digital data.

In the first dimension, namely the ability to articulate information needs and conduct digital data searches, Ditreskrimsus Polda DIY has implemented standard procedures for the collection of digital evidence. As the informants explained, each phishing case requires digital forensic analysis of the victim's devices to understand the takeover process. The team uses various forensic tools, including Cellebrite, Magnet Axiom, and Oxygen, for data extraction and analysis. Wireshark complements the use of these tools for network analysis, Autopsy for digital forensics, and multiple OSINT tools to obtain comprehensive data.

In the second dimension, the ability to evaluate the relevance of data sources and content, the team applies ISO standards in assessing digital evidence. Informants stated that the unit uses ISO 27037 for evidence collection, preservation, and identification, and ISO 27042 for analysis and reporting. Data verification involves several techniques, including hash verification, digital signature analysis, and timestamp verification. For email-related evidence, the team performs DMARC, SPF, and DKIM checks to verify email authenticity. Despite these efforts, a significant limitation remains: of the 37 personnel in the cyber unit, only three hold digital forensic certification.

The third dimension, the ability to store, manage, and organize digital data, is implemented through the Laboratory Information Management Forensic System (LIMFS). This system stores and manages request documents, police reports, seizure warrants, case summaries, and original copies of digital evidence. The unit conducts automatic daily backups to a redundant system and performs long-term archiving using structured classification and indexing. However, storage capacity limitations restrict the unit to processing only around 75 requests per month.

The analysis indicates that although Ditreskrimsus Polda DIY has established standard procedures and utilizes adequate tools across the three aspects of information and data literacy, several key challenges remain. First, the limited number of personnel with digital forensic certification, with only three out of 37. Second, storage capacity and infrastructure limitations that restrict the number of cases that can be handled. Third, the need to enhance competencies in the use of advanced forensic tools to keep pace with evolving cybercrime modus operandi. Fourth, the need to standardize data analysis procedures across units to improve case-handling effectiveness.

2. Communication and Collaboration

The analysis of communication and collaboration competencies at Ditreskrimsus Polda DIY shows structured coordination in handling phishing cases. In the DigComp 2.2 framework (Vuorikari et al., 2022), this area includes communicating and collaborating through digital technologies, participating in digital services, and managing digital presence.

First, the ability to communicate and collaborate digitally while considering cultural diversity is demonstrated through a structured internal coordination system. As stated by an informant, "Coordination is carried out through an integrated system and regular coordination meetings. We have a dedicated WhatsApp group for rapid communication between units. For sharing digital evidence, we use a secure internal system." The unit has developed standard digital documentation systems and secure information-sharing protocols, including encryption and layered access controls to protect data integrity.

Internal coordination is further strengthened through routine coordination meetings and a forensic analysis request management system.

Second, regarding participation in public or private digital services, the study identifies coordination mechanisms involving various actors across the digital and financial ecosystem. An informant described the scope of this coordination: “We definitely work with relevant institutions. Banking, telecommunications operators, and e-commerce platforms. Sometimes we also coordinate with the Ministry of Communication and Informatics.” However, this coordination process faces structural constraints, particularly related to data access and regulatory limitations. The informant further explained the complexity of coordinating with international platforms: “Indonesia is only a user of the platform… When we talk about legal regulations, the regulations that apply are those of the country where the platform is based.”

Third, in the area of managing digital identity and reputation, Ditreskrimsus Polda DIY has developed various cyber awareness and educational initiatives. An informant highlighted the unit’s extensive public education efforts: “It is commonplace. We often serve as resource persons for various community groups… The point is to educate the public about IT-related crimes, which are increasingly prevalent in Indonesia.” These educational programs reflect the unit’s recognition of the importance of digital literacy in preventing phishing crimes.

The findings indicate several significant challenges in implementing communication and collaboration competencies. First, regulatory barriers to coordinating with international digital platforms, as explained by the informant, are often due to differences in national regulations, which impede data request processes. Second, limitations in the standardization of communication protocols across institutions complicate information-sharing processes. Third, there is a need for a more integrated communication platform to facilitate multi-stakeholder coordination.

3. Digital Content Creation

The analysis of digital content creation at Ditreskrimsus Polda DIY, based on the DigComp 2.2 framework (Vuorikari et al., 2022), focuses on three aspects: creating and editing digital content, integrating information while respecting copyright and licensing, and providing clear instructions for computer systems.

In the context of creating and editing digital content, Ditreskrimsus Polda DIY has implemented standardized forensic documentation procedures. As explained by the informant, the unit uses standard equipment in the digital forensic laboratory to document evidence, including detailed and step-by-step photographic capture. This capability is supported by various digital forensic tools, such as Celebrate, Ankom, and XRW, which extract and analyze data and verify the authenticity of stored data copies.

Regarding the second aspect, the ability to integrate information, the unit has developed a standardized documentation system through the Lab Information Management Forensic System (LIMFS). As described by the informant, the unit uses standardized reporting formats aligned with Indonesian National Police SOPs, covering an executive summary, technical details, forensic analysis, and conclusions. LIMFS enables structured integration and management of information while maintaining confidentiality and access control.

To provide instructions that computer systems can understand, personnel must have an in-depth understanding of forensic tools and analysis. The informant emphasized that the effectiveness of tool usage depends on personnel's ability to explore and understand device architecture. This highlights the importance of continuously updating knowledge to keep pace with technological developments.

Despite these efforts, the implementation of digital content creation continues to face several significant challenges. First, there is a limited number of personnel with competence in using advanced forensic tools. Second, the documentation and information integration process across units requires further standardization. Third, there is a need for improved capability in utilizing the latest forensic technologies. Fourth, constraints remain in developing analytical systems capable of keeping pace with evolving crime modus operandi.

4. Safety

The safety aspect in the DigComp 2.2 framework (Vuorikari et al., 2022) includes three core dimensions: protection of devices and data, protection of physical and psychological well-being, and awareness of the environmental impact of digital technology. In the context of Ditreskrimsus Polda DIY, the implementation of safety measures demonstrates layered security protocols in handling phishing cases.

In the dimension of device and data protection, Ditreskrimsus Polda DIY has established a comprehensive security system. The unit uses a local server for data storage, with access restricted to specific devices. An informant explained that the “original copy” of the data is stored on the server until a court decision has the force of law, with strict logging of every access. Security is reinforced through multi-factor authentication and periodic password updates every two weeks. The system is also equipped with a backup mechanism through a network-attached storage (NAS) that is isolated from internet access, providing an additional security layer for sensitive data.

Regarding the protection of physical and psychological health, the unit recognizes the impact of heavy workloads on personnel. As the informant stated, handling major cases often creates significant mental pressure. To address this, the unit applies a work rotation policy and provides sufficient rest periods. Stress management training programs are also conducted regularly to help personnel cope with work-related pressure. In the dimension of environmental impact awareness, the unit has developed data management policies that consider efficient use of digital resources. The informant explained that the unit limits the number of digital forensic requests to 75 cases per month, taking into account storage capacity and resource efficiency. This policy reflects efforts to balance operational needs with infrastructure limitations.

However, implementing the safety aspect still faces several significant challenges. The rapid growth of data volume requires increased capacity in security infrastructure. High workload levels continue to be a concern for personnel's mental health. Meanwhile, the need for a more efficient data management system is becoming increasingly urgent as case complexity increases.

5. Problem Solving

The analysis of the problem-solving aspect in Ditreskrimsus Polda DIY, based on the DigComp 2.2 framework (Vuorikari et al., 2022), highlights three key competencies: identifying technical needs and problems, using digital tools for innovation, and keeping up with technological developments. These competencies are essential for addressing increasingly complex phishing cases.

The unit's ability to identify needs and technical problems is reflected in its systematic approach to case analysis. An informant explained that each case has unique characteristics despite involving similar modus operandi. This approach is strengthened by detailed digital forensic examinations, in which the informant also emphasized the importance of analyzing the victim's device to understand the mechanism of account compromise and to identify the presence of malware or malicious links.

In terms of using digital tools for innovation, Ditreskrimsus Polda DIY has adopted various modern forensic tools. However, the informant emphasized that tools are merely instruments whose effectiveness depends heavily on the user's exploratory skills and deep technical understanding. The unit has even developed a chipset-based approach to overcome limitations in device databases within existing forensic tools.

Regarding keeping up with technological developments, the unit faces significant challenges, as the pace of technological advancement often outpaces the team's capacity to update tools and competencies. The informant acknowledged that the pace of team research and adaptation remains slower than the rapid evolution of technologies used in cybercrime.

The implementation of problem-solving in the unit faces several significant constraints. First, only 3 of 37 staff members are certified in digital forensics. Second, there is a gap between the speed of technological advancement and the team's ability to update tools and skills. Third, case complexity continues to increase, requiring more advanced analytical approaches.

Based on an analysis using the DigComp 2.2 framework, this study identifies three major patterns in the digital competence of Ditreskrimsus Polda DIY personnel in handling phishing cases. First, there is a gap between standard procedures and actual implementation, as only 3 of 37 personnel hold digital forensics certification, due to the high cost of certification and limited budget allocation. Second, the unit relies heavily on tools such as Cellebrite, Magnet Axiom, and Oxygen, yet still encounters challenges when dealing with new technologies that these tools cannot accommodate. Third, there is a trade-off between the need for rapid case handling and compliance with digital security protocols, limiting case requests to 75 per month to maintain the quality of case processing. These findings demonstrate that the five competence areas in DigComp 2.2 provide a clear understanding of the strengths, weaknesses, and development needs of personnel's digital competence in the context of phishing investigations.

Several unexpected findings also emerged, including the high awareness among personnel of the importance of fundamental digital forensics knowledge beyond tool-based proficiency. There is also an initiative to develop chipset-based analytical methods to overcome tool limitations. Implementing personnel rotation systems helps reduce psychological strain

associated with case handling. Additionally, the development of special coordination channels with relevant institutions accelerates the processing of urgent cases. These findings offer new perspectives on how the unit adapts to resource limitations and the growing complexity of cases. The study also highlights the importance of a holistic approach to digital competence development, encompassing technical skills, operational capabilities, and personnel well-being.

The findings regarding the digital competence of Ditreskrimsus Polda DIY personnel in handling phishing cases hold important theoretical and practical implications. Theoretically, this study reinforces the relevance of the DigComp 2.2 framework (Vuorikari et al., 2022), which encompasses information and data literacy, communication, content creation, safety, and problem-solving, in the context of cyber law enforcement. However, the study also asserts that cybercrime investigations require expanding this framework to include digital forensics and evidence management, which are not explicitly covered. These findings also confirm Martin's (2005) digital literacy theory on the importance of awareness, attitude, and digital capability, emphasizing that the competence of law enforcement personnel is not solely dependent on tool usage but also on a fundamental understanding of technological architecture and functionality. Scientifically, this study contributes to understanding the implementation of the digital competence framework in Indonesia's cyber law enforcement context, identifying gaps between theoretical constructs and practical field needs, and highlighting the importance of balancing technical competence with foundational knowledge in cybercrime handling.

From a practical standpoint, the study offers several recommendations to strengthen law enforcement's capacity to address phishing. First, training programs must expand beyond tool-based forensics and include a deeper understanding of fundamental technologies. Second, establishing minimum digital competence standards for cybercrime personnel is essential to ensure the quality of case handling and the validity of digital evidence in court. Third, personnel's psychological well-being must be addressed through stress management and more structured task rotation. Fourth, improvements to digital forensic infrastructure are urgently needed to address storage capacity limitations that limit the number of cases processed each month. Additionally, coordination mechanisms with digital platforms and related institutions must be strengthened, including international cooperation to address challenges related to cross-border data access. These recommendations offer an empirical basis for developing policies and capacity-building programs to enhance law enforcement readiness in addressing the growing complexity of cybercrime.

Conclusions

This study demonstrates that the digital competence of Ditreskrimsus Polda DIY personnel in handling phishing cases continues to face several challenges, particularly due to a gap between required competencies and the number of certified personnel: only 3 out of 37 members hold digital forensics certification. This condition affects the unit's capacity, limiting case handling to 75 requests per month. Although the unit has a relatively comprehensive set of operational procedures, its implementation is hindered by infrastructure limitations, a high reliance on forensic tools, and suboptimal development of adaptive analytical methodologies. The study also highlights a trade-off between the speed of case resolution and adherence to chain-of-custody protocols to maintain the integrity of digital evidence.

Several limitations of the study should be noted, including its focus on a single institution, limited access to detailed technical information, and a relatively short observation period. Based on these findings, human resource capacity building becomes a priority, including increasing the number of certified personnel, developing training programs that balance technical skills with foundational understanding, and strengthening internal knowledge management. In terms of infrastructure and coordination, improvements are needed in forensic data storage capacity, the development of more adaptive analytical systems, and the enhancement of cross-agency collaboration. Future research comparing digital competence across regional police departments (Polda) or evaluating competence development models is also necessary to enrich strategies for improving law enforcement capabilities in addressing increasingly complex cybercrime.

Acknowledgements

The author would like to express his deepest gratitude to Beasiswa Komdigi for providing comprehensive financial support for this research and publication.

References

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber [Challenges of Evidence in Cybercrime Cases]. *Judge: Jurnal Hukum, 5*(02), 55–63.

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security, 68*, 160–196.

Anti-Phishing Working Group (APWG). (2023). *Phishing Activity Trends Report, 4th Quarter 2022*. APWG. https://apwg.org/

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2024). Laporan survei penetrasi & profil pengguna internet Indonesia 2024 [2024 Survey Report on Internet Penetration and User Profiles in Indonesia]. https://apjii.or.id/survei2024/

Carretero, S., Vuorikari, R., & Punie, Y. (2017). *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*. Publications Office of the European Union.

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors, and technical approaches. *Expert Systems with Applications*, *106*, 1–20.

Cybersecurity Ventures. (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. PR Newswire. https://www.prnewswire.com/news-releases/cybercrime-to-cost-the-world-10-5-trillion-annually-by-2025--301172786.html

Denzin, N. K., & Lincoln, Y. S. (2009). *Handbook of Qualitative Research.* Pustaka Pelajar.

Ekayani, L., Djanggih, H., & Suong, M. A. A. (2023). Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan [Legal Protection for Bank Customers Against Personal Data Theft (Phishing) Crimes in the Banking Sector]. *Journal of Lex Philosophy (JLP), 4*(1), 22–40.

Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. *Journal of Educational Multimedia and Hypermedia, 13*(1), 93–106.

European Parliament. (2024). *The role of Artificial Intelligence in the European Union's economic and regulatory framework*. European Parliamentary Research Service (EPRS). https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf

Gilster, P. (1997). *Digital literacy*. Wiley Computer Publishing.

Guillén-Gámez, F. D., & Mayorga-Fernández, M. J. (2020). Quantitative-comparative research on digital competence in students, graduates and professors of faculty education: An analysis with ANOVA. *Education and Information Technologies, 25*(5), 4157–4174.

Harianjogja.com. (2023). *Kriminalitas di DIY menurun, ini 4 kasus yang menonjol sepanjang 2023* [Crime Rates in the Special Region of Yogyakarta Decline, Here Are Four Prominent Cases Throughout 2023]. Jogjapolitan. https://jogjapolitan.harianjogja.com/read/2023/12/28/512/1159668 /krimina litas-di-diy-menurun-ini-4-kasus-yang-menonjol-sepanjang-2023

Indonesia Anti-Phishing Data Exchange. (2023). *Laporan Aktivitas Phishing Q1 2023* [Q1 2023 Phishing Activity Report]. IDADX. https://idadx.id/laporan-aktivitas-phishing-q1-2023.pdf

Martin, A. (2005). DigEuLit – a European framework for digital literacy: A progress report. *JeLit, Journal of eLiteracy, 2*(2), 130–136.

Prakoso, A. (2022). Tantangan Forensik Digital dalam Penegakan Hukum Kejahatan Siber [Digital Forensics Challenges in Cybercrime Law Enforcement]. *Jurnal Hukum dan Peradilan,11*(1), 41–60.

Pratiwi, F. I., Hennida, C., Soesilowati, S., Berliantin, N., Ekasari, D. Y., Dewi, C. S., & Intan, A. A. (2024). Cybersecurity Challenges in Indonesia: Threat and Responses Analysis. *Perspectives on Global Development and Technology, 22*(3–4), 239–264. https://doi.org/10.1163/15691497-12341660

Purwandari, M. D. (2024). *Analisis Peran Polda Daerah Istimewa Yogyakarta dalam Pengungkapan Kasus Phishing* [Analysis of the Role of the Yogyakarta Regional Police in Uncovering Phishing Cases]. Skripsi. Fakultas Bisnis dan Ekonomika, Universitas Islam Indonesia, Yogyakarta. https://dspace.uii.ac.id/handle/123456789/49553

Sitompul, F., Manik, A. P. P., Sinaga, C. D., Purba, A. T., & Satria, A. (2024). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Hukum Indonesia [Information Technology Crime (Cybercrime) and Its Countermeasures Under Indonesian Law]. *Jaksa: Jurnal Kajian Ilmu Hukum Dan Politik, 2*(2), 222–228.

Stake, R. E. (1995). *The art of case study research*. SAGE Publications, Inc.

Sugiyono. (2016). *Metode Penelitian Adminitrasi Dilengkapi dengan Metode R & D* [Administrative Research Methods Accompanied by the R&D Method]. Alpabeta.

Van Deursen, A. J., & Van Dijk, J. A. (2014). *Digital skills: Unlocking the information society*. Springer.

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens*. Publications Office of the European Union.

Yin, R. K. (2018). *Case study research and applications: Design and methods (6th ed.)*. SAGE Publications.

Yurita, I., Ramadhan, M. K., & Candra, M. (2023). Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cybercrime (studi kasus phising sebagai ancaman keamanan digital) [The Influence of Technological Advancement on the Development of Cybercrime (A Case Study of Phishing as a Digital Security Threat)]. *Jurnal Hukum Legalita, 5*(2), 143–155.