

Content Analysis of Cybercrime Infographic

ZETI AZREEN AHMAD*
International Islamic University Malaysia

NUR NADIA ABD MUBIN
Universiti Pendidikan Sultan Idris

AKMAL ARZEMAN
Cardiff University, United Kingdom

ABSTRACT

Malaysia is one of the vulnerable regions of cyberattack in which cybercrimes continue to increase at alarming rate. Cyber criminals are attacking not only organisations but also individuals. Various types of cybercrimes that have resulted in significant financial losses have been reported in the media. Despite the daily coverage of cybercrime incidents, people continue to fall victims. Keeping the public informed of the potential online threats should not be taken for granted. This study argues that effective communication of cybersecurity information is essential to enhance public's resilience in dealing with cybercrimes. Infographic is a useful tool for conveying cybersecurity information. Infographic is a visual communication that is often used to communicate complex messages that include science related information. Literature on infographics often emphasizes on its key components that include; visual, content and knowledge. As a visual form of communication, it makes information appear to be appealing and easier to understand to diverse types of publics. The format could be easily shared with others through different types of social media platforms. This study examined infographics related to cybercrimes from CyberSecurity Malaysia's Facebook account. Visual content analysis has been adopted to analyse more than 20 infographics based on content, visual and knowledge. The study found the content of infographics was mainly text and graphic with instructive guidelines. However, the visual elements appear cluttered, potentially compromising the efficacy of the conveyed message.

Keywords: *Infographic, cybercrimes, scam, CyberSecurity Malaysia, cyberthreat.*

INTRODUCTION

Cybercrimes have emerged as one of the biggest threats worldwide. Crimes are occurring every second in the cyber space with criminals lurking for opportunity to deceive victims 24/7. The heavy reliance on online platforms imposes threats to all online users. The Global Risk Report 2023 continues to identify cybersecurity as a constant concern thus demands global attention (World Economic Forum, 2023). In Malaysia 70 percent of commercial crimes have fallen under the category of cybercrimes (Zahari et al., 2019) that target both organisations and individuals. Various types of cybercrimes that have resulted in significant financial losses have been reported in the media. Despite the daily coverage of cybercrime incidents, people continue to fall victims. In view of this worrying trend, it is crucial not to underestimate the importance of keeping the public informed of the potential online threats.

The publics need to be reminded of the recent tactics used by the cyber criminals. Constant information on cybercrimes empowers the public to perform the right action thus not be falling into the criminal's traps. This study asserts that effective communication of cybersecurity information is essential to enhance public's resilience in dealing with cybercrimes and suggests that infographics are valuable tool for conveying cybersecurity information.

Infographic is a visual communication that is often used to communicate complex information that include science related information such as sustainability, climate change, health related information, disease outbreak and others. Its visual approach enables communicators to simplify abstract, complex, and dense messages (Naparin & Saad 2017; Ginzburg et al., 2021) making it easier for the publics to comprehend a specific issue. As a visual form of communication, infographics capture publics' attention amidst information overload, enabling the information to stand out. Literature on infographics often emphasizes on its key components that include; visual, content and knowledge. This study affirms that a good infographic would help to enhance publics' understanding of cybercrimes and subsequently empower them to take the right action in responding to the threats. Among others, this study aims to address the content, visual elements and knowledge embedded in infographics posted in CyberSecurity Malaysia's Facebook account. A total of 23 infographics posted from January 2021 until November 2022 have been analysed using a visual content analysis.

LITERATURE REVIEW

There are various terminologies used to represent or explain cybercrime in the literature such as e-crime, internet crime, computer crime (Goni, 2022), digital organized crime (Di Nicola, 2022). However, until now there has been an absence of a universally accepted definition for cybercrime (Boraine & Doris, 2019; Robert, 2021). Donalds and Osei- Brysons (2019) described cybercrime as any illicit acts performed by either individuals or groups against computers, computer-related devices, or information technology network; including traditional crimes, targeting individuals supported by the Internet and/or technology (p.403). McGuire and Dowling (2013) have provided two-category classification of cybercrimes; cyber-dependent crime and cyber-enabled crime. The former refers to crimes that are committed by using a computer or computer network or other forms of information communication technology (ICT) such as distribution of Malware or viruses. Whereas, cyber-enabled crimes are initiated offline but amplified through the Internet or technological devices, e.g., cyber bullying, theft and many other trafficking activities. Types of cybercrimes range from launching Malware or virus attack to stealing a person's identity. Marelino (2022) provides ten types of cybercrimes that include:

- a. Spamming
- b. Phishing
- c. Piracy or theft
- d. System damage
- e. Malicious software
- f. Fraud calls and messages
- g. Dark web market
- h. Cyber stalking
- i. Theft of a person's identity
- j. Cyber extortion

Cybercriminals involved in illegal activities targeting computer users or the Internet users with the intention to make money or to do harm to the users (Ally & Gadgala, 2022). At present, cybercriminals are using multiple media platforms (Zainal Abidin et al., 2018) such as emails, instant text messaging, Facebook, TikTok, Telegram, Instagram and many others to find targets. They often impersonate as a close friend or as an employee from established organisations either appealing for donations or offering products. Lack of awareness of cybercrimes and ignorance of new cybercrime tactics can lead online media users to become victims. Thus, information about cybercrimes focusing on recent tactics employed and ways to mitigate cyber risks are essential to be communicated to the public at large. Equally important is to ensure the information about cybercrime is able to capture the public's attention and is easy to understand in the midst of information overload. This study posits infographics as a valuable tool to convey information about cybercrime thus should be given attention from the agencies responsible for managing cybercrimes.

The State of Cybercrimes in Malaysia

The Internet users in Malaysia has constantly increased over the years with 92.7 percent of the population using the Internet in 2022. Smartphones have been the most popular device to access the Internet in which 94.4 percent of users are using them (Malaysian Communication and Multimedia Commission, 2022). The Internet Users Survey 2022 that was initiated by the Malaysian Communication and Multimedia Commission (MCMC) reported that 40 percent of the Internet users in the country spend between 5 to 12 hours online daily (Malaysian Communication and Multimedia Commission, 2022). This study concurs that the Internet technology has facilitated cyber threats activities (Ahmad Arifin et al., 2019) and a long time spent online exposes users to various cyberthreats.

The Royal Malaysia Police (PDRM), reported an upward trend in cybercrimes from the year 2020 up to May 2022 with 71,833 reported cases resulting in RM5.2 billion losses (Salleh, 2022). More than half of these cases involved online scams. Scam is the most common type of cybercrime in Malaysia. The percentage of online scam has increased from 47.4 percent in the year 2020 to 68.5 percent in 2022 (Malaysian Communication and Multimedia Commission, 2022). The word scam refers to misleading business practices to con victims (Hawkswood et al., 2022).

Increased expertise in exploiting technology among scammers and lack of information on cybercrime are among reasons behind a high number of online scam incidents (Basyir & Harun, 2022). Victims usually encounter the criminals through social media platforms; Facebook, Instagram, WeChat, and WhatsApp and their social media account would be blocked once payment is successfully transferred into the criminals' account (Tharshini et al., 2021). Cybercriminals have employed increasingly sophisticated and subtle techniques including using psychological principles that made victims unconsciously make poor decisions (Kajave & Nismy, 2022). In the fourth quarter of 2022, Malaysia experienced an average of 84 million cyber-attack daily compared to 200 billion attacks per day globally (Bernama, 2023, February 22). Being one of the most vulnerable regions of cyber-attacks in Southeast Asia imposed high risks to online media users in the country thus requiring them to be more vigilant when navigating in cyberspace. Therefore, online media users in particular and public at large should be given adequate information on cybercrimes to remain resilient of cyberattacks.

CyberSecurity Malaysia

CyberSecurity Malaysia is the national cyber security specialist agency under the purview of the Ministry of Communications and Digital (KKD). In 1997 it was established as the Malaysia Computer Emergency Response Team (MyCERT), operating as a unit under Malaysian Institute of Microelectronic System (MIMOS) Berhad. In 2001, it was placed under the National ICT Security and Emergency Response Centre (NISER). NISER was spun-off from MIMOS in 2007 and registered as a not-for-profit company limited by guarantee under the Ministry of Science, Technology and Innovation (MOSTI). NISER was later rebranded to CyberSecurity Malaysia and entrusted to provide technical support for the implementation of the National Cyber Security Policy (NCSP). At present, CyberSecurity is responsible for developing and implementing the National Cyber Security Policy and Strategy, and providing a wide range of cyber security services to Malaysian organizations and individuals. Among its major services include:

- a) Malaysia Computer Emergency Response Team (MyCERT)
- b) Digital Forensics
- c) Cryptography Development
- d) Malaysian Security Evaluation Facility (MySEF)
- e) Malaysia Vulnerabilities Assessments Centre (MyVAC)
- f) CyberSecurity Industry Engagement and Collaboration (CIEC)
- g) Information Security Certification Body (ISCB)
- h) Outreach & Corporate Communication
- i) Cyber Security Professional Development
- j) CyberGuru
- k) Information Security Management & Assurance (ISMA)
- l) Government and International Engagement
- m) Strategic Study & Research

(Source: CyberSecurity Malaysia, 2022)

CyberSecurity has been proactive in creating awareness about cybercrimes to the publics through its official website and social media platforms such as Facebook, Instagram, YouTube channel and X (previously known as Twitter). It has the most followers in FB as compared to its other social media platforms. The agency has constantly updated information related to cybercrimes in their social media platforms in a form of media release, poster, announcement and infographics. Furthermore, CyberSecurity also organizes awareness programme through its Cyber Security Awareness for Everyone (CyberSAFE) to educate the public on cybercrimes and enhance cybersecurity.

Besides CyberSecurity, other organizations such as the banking sector has been active in promoting cybercrime awareness. Bank Negara Malaysia (BNM), together with Association of Banks in Malaysia (ABM) namely Association of Development Finance Institutions of Malaysia (ADFIRM), and Association of Islamic Banking and Financial Institutions Malaysia (AIBIM) have launched a campaign called the National Scam Awareness Campaign (NSAC). This campaign sought to keep the public safe through its reminder logo of three-second rule which is "Stop, Think and Block" with their tagline of "*Ingat 3 Saat OK*" and #JanganKenaScam (Bernama, 2022, October 30).

META Malaysia also launched #TakNakScam awareness campaign to educate the public to be more vigilant online through its tagline, “spot, check and report”. This campaign is centred on five types of online scams; illegal loans, electronic commerce, jobs’ offer, money muling, and investment (Mageswari, 2022, August 8).

Another significant institution responsible to combat cybercrimes is the Royal Malaysian Police (PDRM) that has formed the Scam Response Centre under the Commercial Crime Investigation Department (CCID) in responding to an increased number of phone scam cases in the country. Recently, the National Scam Response Centre (NSRC) has been launched to combat scam related crimes. The NSRC is a collaborative effort of several agencies namely the National Anti-Financial Crime Centre (NFCC), the Royal Malaysian Police (PDRM), Bank Negara Malaysia (BNM), Malaysian Communication and Multimedia Commission (MCMC) and other financial and telecommunication institutions (National Anti-Financial Crime Centre (NFCC), 2021).

Infographics

Communication is not merely a process of transmitting information, its purpose is to inform, to persuade and to motivate people to take action. Information is the key to empowering people to make informed decisions and subsequently accomplish their intended goal. However, the communication process is not always straightforward. Oftentimes, the target audience neither pays attention to the message nor understands it clearly as intended. Therefore, communicating complex information imposes a great challenge to organisations including governments. In the midst of containing the spread of COVID-19, for instance, health authorities and governments have used various means of communication to provide information on what the public need to do to save lives. In an attempt to communicate COVID-19 effectively, the World Health Organisation (WHO) has developed innovative ways of communicating the disease scientific information to ensure that information shared is understandable and beneficial for every community (WHO, 2022, May 25). Infographics have been one of the main formats used to communicate about COVID-19.

Murray et al. (2017) defined infographic as a tool to convey knowledge using data visualisation and images to supplement text that facilitate understanding. Infographic is also known as information visualization (InfoVis) or data visualization that can be easily shared through various social media platforms (Sirichareon & Siricharoen, 2017). Recent literature has found that infographic have been useful and perceived favourably in conveying scientific information about COVID-19 (Lee et al., 2022), environmental issues (Ginzburg et al., 2021), climate change (Azizah et al., 2021) and help readers understand news content (Sjafiie et al., 2018). Besides, infographics were also found to be helpful in teaching and learning for difficult subjects for students (Naparin & Saad, 2017). This study argues that complex information is not limited to health, disease and environmental issues but also applies to cybersecurity, where infographics would be useful. Sheikh et al. (2015) proposed six main categories of infographics that include statistic, timeline, process, geographical, research and activity based that could be either static (fixed visuals), moving (may include voice or audio and more engaging for audience) or interactive (dynamic; that requires readers’ involvement such as clicking to view the next slide) (Suleiman, 2023).

Basco (2020) affirmed that infographic consists of three main elements; content (e.g., facts, statistics, text and references), visuals (e.g., colour, graphics, signs or symbols) and knowledge is the conclusion to the message from the content and visual elements. Scholars

posit that through its attractive and persuasive design, infographics are capable of disseminating information, increase awareness and influence a community about a specific issue (German, Ramilo & Gonzalez, 2020; Ginzburg et al., 2021). It is worth highlighting that accuracy is the key for a good infographic. There are several components that the infographic creators should consider that include the structure, accuracy, reliability, depth, and functionality before adding the aesthetic element (Siricharoen & Siricharoen, 2015). Nevertheless, not all infographics are effective or of good quality. A study on public transportation infographics found a lack of design principles applied to infographics thus unable to capture audience's interest or to engage them (Shahbazi et al., 2021). Davidson (2014, cited in Azizah et al., 2021, p.2) described a good infographic to have relevant details in a single visual, emphasizing simplicity, clarity, precision, and the ability to convey complex information efficiently by combining visuals and text for self-explanatory and attractive presentation.

This study examines the infographics to communicate about cybercrimes in CyberSecurity Malaysia's Facebook with a focus on visual, content and knowledge. These are among widely accepted criteria for evaluating the quality of infographics found in the literature (Jahan et al., 2021; Arum, 2017; Siricharoen & Siricharoen, 2017, 2015). Usefulness refers to content that is easy to understand, has clear purpose and shows information from a reliable source. Legibility is where text and font used is easy to read and should not hinder the viewer's readability. Design is the graphics used should reflect purpose with the appropriate size, colour and contrast. Finally, aesthetics is the design's pleasing qualities that includes factors like composition and organization of the elements.

METHODOLOGY

The study is conducted using visual content analysis, a process fundamental to the derivation of meaningful descriptors for image and video data. Within the domain of infographic creation, the incorporation of visualization is important to constitute an integral facet of the very ideas, concepts, and linguistic expressions that collectively convey a message. As Sjaifiie et al. (2018) explained in their work, visualization goes beyond making things look nice; it's a vital piece that significantly improves how effective the infographics are at communicating. Such an understanding emphasizes that visualization is an integral constituent, contributing significantly to the overall effectiveness of message delivery.

In this study, complex data found in infographics related to online scams is identified, enabling researchers to recognize patterns, trends, and anomalies more easily. The data collection process involved the following steps; (1) Sample selection: Create specific inclusion and exclusion criteria, such as the timeframe for infographic creation, source (e.g., social media platforms), and the content related to online scams, (2) Data source: Identify the data source(s) where the infographics can be found. For this study, the primary data source is the CyberSecurity Malaysia Facebook account, (3) Data collection tool: Develop a data collection tool or instrument for systematically recording information from each infographic. This tool could be a data coding sheet with fields for relevant variables, categories, and subcategories, (4) Data coding: Define the coding scheme based on the predetermined categories and subcategories as described in the methodology, (5) Data collection: Collect data from the identified infographics according to the coding scheme. Ensure rigorous documentation of each infographic's source, date, and any other relevant contextual information, (6) Data analysis: Prepare the data for analysis, which involve content analysis as per the research questions. Through the methodical execution of these data collection steps, this study

establishes a robust foundation for the thorough analysis and interpretation of the selected infographics, fostering a deeper understanding of the subject matter and its implications.

A total of 23 infographics that were shared on the CyberSecurity Facebook account during the period from January 2021 to November 2022 were analysed. The selected infographic was categorised based on date of post, title, type of the infographic, source, language and message. The selected infographics specifically contained information related to online scams and did not encompass other types of posts, such as notices and news. It is important to note that these infographics were shared by the CyberSecurity Malaysia Facebook account and were not exclusively created by CyberSecurity.

The analysis of these infographics was conducted through a combined approach of deductive and inductive coding, in line with the methodological framework proposed by Elo and Kyngas (2008). The deductive coding phase initiated the analysis process, wherein the structure of the analysis was operationalized based on the three major elements typically found in infographics; visuals, content, and knowledge as outlined by Siricharoen and Siricharoen (2015). In this study, the methodology involved the development of a coding scheme designed to categorize and assess the infographics based on three primary categories, each encompassing specific subcategories. The coding scheme used in this study included the following categories:

Table 1: Major elements in infographics (Adapted from Siricharoen & Siricharoen, 2015)

Primary Category	Subcategory	Description
Visual	Usefulness (V1)	The infographic's visual elements contributed to its practicality and effectiveness in conveying information.
	Legibility (V2)	The text and graphics within the infographic could be read and understood.
	Design (V3)	The overall layout and arrangement of visual components within the infographic.
	Aesthetics (V4)	The aesthetic appeal of the infographic, including its visual attractiveness and appeal.
Content	Text (C1)	The textual information presented within the infographic, assessing its clarity, conciseness, and relevance.
	Graphic (C2)	The graphical elements, such as images, charts, or icons, and assessed their contribution to conveying information.
Knowledge	Reminder (K1)	The infographics that aimed to serve as reminders of specific cybersecurity-related information.
	Awareness (K2)	The infographics designed to raise awareness about cybersecurity issues.
	Guideline (K3)	The infographics that provided guidelines or recommendations for safe online practices.
	Identification (K4)	The infographics that aimed to help users identify potential online security threats or scams.
	Instruction (K5)	The infographics that provided step-by-step instructions for specific actions or responses related to cybersecurity.

These categories and subcategories formed the foundation for coding and analyzing the infographics, allowing for a systematic and comprehensive assessment of their visual, content, and knowledge-related aspects. These elements served as predefined categories, guiding the initial organization of the data. Subsequently, during the inductive coding phase, a detailed examination of the content within each infographic was carried out, leading to the identification of subcategories within the broader predefined categories.

This dual approach to coding aimed to provide a structured yet flexible method for analyzing the infographics, allowing for the exploration of both the predetermined elements and emerging patterns within the data. The combination of deductive and inductive coding facilitated a comprehensive analysis of the infographics, enabling a deeper understanding of the information related to online scams as presented in the sample.

FINDINGS

In the findings of this study, the analysis revealed a diverse array of infographics in terms of format and content. Among the 23 infographics examined, it was observed that 15 were static infographics and five were animated infographics. These infographics were attributed to various sources, with nine originating from CyberSecurity, nine from Wethinkdigital, two from Ministry of Domestic Trade and Costs of Living (KPDHEP), one from the Ministry of Communication and Multimedia (now known as Ministry of Communication and Digital) and one from the Royal Police (PDRM). A linguistic variation was noted as well, with 12 infographics presented in Malay language and 11 in English.

Table 2: Type of infographics from the CyberSecurity Malaysia FB from January 2021 until November 2022

No	Date of post	Title	Type of infographic	Infographic Data Source	Language	Type of Scam
1	18 January 2021	There is always someone out there trying to pick or break in your lock	Static	CyberSecurity	English	Computer Scam
2	20 June 2021	Privacy: Act now, turn on your privacy settings	Static	CyberSecurity	English	Computer Scam
3	17 July 2021	#TakNakScam	Animated	Wethinkdigital	Malay	Scam
4	19 July 2021	#TakNakScam 3 langkah	Static	Wethinkdigital	Malay	Scam
5	19 July 2021	membanteras scam #TakNakScam 3 steps to combat	Static*	Wethinkdigital	English	Scam
6	21 July 2021	#TakNakScam 3 langkah	Static	Wethinkdigital	Malay	Scam
7	21 July 2021	membanteras scam #TakNakScam 3 steps to combat scam	Static*	Wethinkdigital	English	Scam
8	27 July 2021	Cybersafe Ketirisan Data	Static	CyberSecurity	Malay	Data Scam
9	27 July 2021	Cybersafe Data leakage	Static*	CyberSecurity	English	Data Scam
10	24 September 2021	SCAM	Static	CyberSecurity	English	Scam
11	9 October 2021	Lindungi privasi peribadi anda	Static	CyberSecurity	Malay	Data Scam
12	25 October 2021	Beware of phishing attacks	Static	CyberSecurity	English	Data scam (Phishing)
13	19 November 2021	Online banking transition	Static	CyberSecurity	English	Online banking Scam

14	4 April 2022	Perkhidmatan Jabatan Siasatan Jenayah Komersil	Static	Jabatan Siasatan Jenayah Komersil – JSJK PDRM	Malay and Chinese	Scam
15	26 May 2022	Kenal pasti tanda-tanda penipuan malware	Animated	Maybank	Malay	Malware Scam
16	13 July 2022	Awas scam SMSSpy	Static	CyberSecurity	Malay	Data Scam (SMSSpy)
17	8 August 2022	Modus operandi vishing kad kredit	Static	Kementerian Perdagangan Dalam Negeri dan Hal Ehwal Pengguna KPDHEP	Malay	Data Scam (Vishing)
18	10 August 2022	Awas taktik pancing data! Phishing, Vishing, Smishing	Static	Kementerian Perdagangan Dalam Negeri dan Hal Ehwal Pengguna KPDHEP	Malay	Data Scam (Phishing, Vishing, Smishing)
19	10 August 2022	Kenalpasti. Semak. Lapor	Animated	Wethinkdigital	English	Scam
20	14 August 2022	Waspada panggilan palsu menggunakan nama K-KOMM	Static	Kementerian Komunikasi dan Multimedia	Malay	Phone Scam
21	17 August 2022	Amaran Scam!	Static	CyberSecurity	Malay	Scam
22	1 September 2022	Loan Scam	Animated	Wethinkdigital	English	Loan Scam
23	15 September 2022	Sell responsibly online	Animated	Wethinkdigital	English	E-commerce Scam

Categorically, the infographics were thematically diverse, with seven of them being centered on the broader topic of scams in general. Another six infographics pertained to data scams, two focused on computer scams, while the remaining infographics were each dedicated to specific scam types, including phone scams, online banking scams, loan scams, malware scams, and e-commerce scams.




Table 3: Major elements in infographics analysis from CyberSecurity Malaysia Facebook

No	Infographic	Visual (V)	Content (C)	Knowledge (K)
1		1,2,3,4	1,2	2,5

2		2	1,2	1,5
3		2	1,2	3
4		2,3	1,2	3
5		2,3	1,2	3
6		2,3	1,2	3
7		2,3	1,2	3

8		1,2,3,4	1,2	3,5
9		1,2,3,4	1,2	3,5
10		2	1,2	2
11		2	1,2	1
12		2	1,2	2,5
13		2	1,2	5

14		1,2,3,4	1,2	5
15		1,2,3,4	1,2	3,4,5
16		1,2,3,4	1,2	2,4,5
17		1,3,4	1,2	4, 5
18		1	1	1,2,4,5
19		4	1,2	2
20		1,3	1,2	1,5

21		1,3,4	1	2
22		2,4	1,2	3
23		2,4	1,2	3

Visual

In the coding process, the visual category, which encompassed four distinct subcategories, played a pivotal role in this analysis. Within this framework, it was observed that 10 infographics received coding in the subcategory of Usefulness (V1). This indicated that these infographics excelled in incorporating visual elements that significantly contributed to their practicality and overall effectiveness in conveying information. Among the coded subcategories, Legibility (V2) emerged as the most frequently coded, with 18 infographics falling under this classification. This observation underscores the paramount importance of legibility in infographic design. This prevalence of V2 coding emphasizes the significance of ensuring that information within an infographic is presented in a clear and accessible manner, as this directly impacts the effectiveness of the communication. Moreover, the substantial number of infographics coded under V2 suggests that legibility should be a primary concern in infographic creation, particularly when the goal is to convey information effectively to a diverse audience. While Design (V3) and Aesthetics (V4) were also integral subcategories in the visual coding scheme, they received coding for 13 and 11 infographics, respectively.

The predominance of Legibility (V2) coding among the analyzed infographics highlights the critical role that clear and comprehensible text and graphics play in effective information communication. The emphasis on V2 reflects the acknowledgment that an infographic's primary purpose is to convey information efficiently. While other subcategories, such as Design (V3) and Aesthetics (V4), contribute to the visual appeal of an infographic, it is the legibility and clarity of content, represented by V2, that form the foundation for a successful infographic. In terms of aesthetics, it was noted that 11 of the infographics demonstrated a thoughtful application of visual hierarchy in their design, thereby enhancing the overall visual appeal and readability. However, a notable counterpoint was observed in

the case of 12 infographics, where the design elements appeared cluttered, potentially compromising the efficacy of the conveyed message.

Content

In the analysis of the infographics, the content category, it was observed that the majority of the infographics incorporated a combination of text and graphic elements, aligning with the multimedia nature of infographics. It was instrumental in evaluating the textual and graphical elements within each infographic, with subcategories Text (C1) and Graphic (C2) serving as key criteria for assessment. There were 23 infographics coded under C1, indicating a significant emphasis on the textual information presented within the infographics. These infographics excelled in terms of the clarity, conciseness, and relevance of the textual content. In the context of conveying information, C1 is of utmost importance as it signifies the quality of the written content within an infographic. Similarly, the subcategory Graphic (C2) received coding for 21 infographics, underlining the critical role of graphical elements such as images, charts, or icons in conveying information. The high incidence of coding in both C1 and C2 underscores their collective significance in infographic design. Infographics that excelled in these categories were able to balance the textual and graphical elements effectively, resulting in a harmonious blend of information communication. Nevertheless, one infographic was notable for its exclusive use of text, with different segments differentiated through proximity and colour, offering a unique approach to information presentation. Regarding the knowledge shared within the infographics, the study unveiled a predominantly instructive and guideline-oriented approach. Many infographics sought to educate viewers about various scam types, providing definitions, raising awareness, and offering reminders. The infographics featured practical guidelines aimed at guiding individuals on how to avoid falling victim to scams.

Knowledge

In the analysis of the Knowledge category, the subcategories Reminder (K1) and Identification (K4) were found to be the least coded, with 4 and 4 infographics respectively. The lower number of infographics coded in these categories may suggest a relatively lower emphasis on these aspects, it is important to note that they remain crucial in cybersecurity education and awareness. On the other hand, the subcategory Instruction (K5) emerged as the most frequently coded, with 12 infographics falling under this classification. This signifies that a significant portion of the analysed infographics provided step-by-step instructions for specific actions or responses related to cybersecurity. The subcategories Awareness (K2) and Guideline (K3) occupied a middle ground, with 7 and 10 infographics respectively. The distribution of coding across the Knowledge subcategories emphasizes the diverse and multi-faceted nature of cybersecurity communication. While Instruction (K5) infographics play a pivotal role in providing users with actionable solutions, it is essential not to overlook the significance of Reminder (K1) and Identification (K4) infographics, as they serve as critical building blocks in reinforcing cybersecurity knowledge and vigilance. Overall, a balanced combination of these subcategories ensures a comprehensive and effective approach to cybersecurity education, raising awareness, providing guidelines, and offering clear instructions for secure online practices.

Drawing upon the insights of scholars, particularly Harold et al. (2020), the findings highlighted the significance of simplicity in infographics' visual design. Notably, the visual elements used in the infographics predominantly featured text, designed with an emphasis

on legibility, considering the context of screen-based consumption. Recognizable fonts were employed to facilitate easy readability, with some text adopting reverse type to underscore the core message. Moreover, all infographics incorporated graphic elements that complemented the textual content, employing illustrations and symbols to enhance message clarity.

Notably, there were infographics urging the public to remember three critical steps as part of the #TakNakScam campaign. However, the level of detail provided in these infographics was found to be lacking, potentially leading to viewer confusion. Conversely, one infographic sourced from Maybank stood out as a well-executed example. It effectively depicted a scam scenario, employed relatable graphics, and offered valuable guidelines for viewers to identify scams and take appropriate action. A graphic animated infographic video with a duration of 1 minute and 50 seconds proved highly informative, educating viewers about the intricacies of malware scams, often associated with e-banking.

The research also provided insight into how frequently infographics are shared on the CyberSecurity Facebook page. The results indicated that these infographics were not as frequent as might be expected, with a total of 14 posted in 2021 and 9 in 2022. These infographics predominantly focused on data scams and served as reminders of the three steps introduced in the #TakNakScam campaign. These findings collectively contribute to a more comprehensive understanding of the visual and content aspects of the infographics analysed in the study.

The findings shed light on the primary audience demographic of Facebook, which largely consists of older adults and various organizations. These insights lead to several pertinent conclusions regarding the efficacy of infographics. It is evident that visual content is more impactful when presented in an animated format, harnessing the potential of visual, audio, and duration elements to captivate viewers and enhance their comprehension of critical issues through the judicious use of visuals and graphic representation. Additionally, the content within each infographic is largely tailored to its specific objectives, which, in many instances, involve reinforcing the three key steps introduced within the #TakNakScam campaign. The educational aspect of these infographics predominantly takes the form of providing guidelines and instructions on how to respond effectively to potential scams. These collective findings contribute to a comprehensive understanding of the dynamics at play in the presentation of cybersecurity-related information via infographics on the Facebook platform, thereby serving as a foundation for the subsequent analysis and discussions in this study.

CONCLUSION

In conclusion, this study offers valuable insights into the role of infographics in raising awareness about cybersecurity issues, particularly in the context of an increasingly digital world. The findings underscore the potential of infographics as a potent tool for disseminating crucial cybersecurity information among the public. However, it is imperative that the design and content of these infographics are tailored to the specific needs and characteristics of their target audience.

The lack of awareness emerges as a key contributor to the escalating prevalence of scam cases in Malaysia. Thus, the most effective strategy for curbing these incidents lies in augmenting public awareness and knowledge surrounding scams. An effective approach to achieving this awareness, as demonstrated by this study, is through the development of

informative infographics. These infographics should not only serve as instruments for creating awareness but should also guide viewers step-by-step on how to identify scams and protect themselves from falling prey to fraudulent activities. For maximum effectiveness, it is recommended that infographics solicit feedback and opinions from the public, incorporating this valuable input into their design and content. This iterative process will ensure that the infographics resonate with their intended audience, fostering enhanced comprehension and greater engagement in the realm of cybersecurity awareness. In essence, the study underscores the potential of infographics as a conduit for promoting cybersecurity vigilance among the public, especially among younger demographics who are more susceptible to online scams. The combination of targeted, informative infographics and an engaged public willing to provide feedback represents a promising avenue for combating the scourge of online scams in Malaysia. It is through these collective efforts that a safer digital landscape can be forged, protecting individuals from the perils of cyber threats and scams.

In conclusion, the analysis of these infographics underscores the intricate interplay of visual and content elements and their direct influence on the effectiveness of information communication. It reiterates the importance of striking a balance in cybersecurity education by providing clear, actionable guidance while also reinforcing vigilance and awareness. Overall, these findings reinforce the role of infographics as invaluable tools in promoting cybersecurity and enhancing understanding and preparedness in the digital realm.

BIODATA

Zeti Azreen Ahmad is an Associate Professor at the Department of Communication, AbdulHamid AbuSulayman Kulliyah of Islamic Revealed Knowledge and Human Sciences (AHAS KIRKHS), International Islamic University Malaysia (IIUM). She received her doctoral degree in public relations from Stirling University, Scotland. Her research has been published in various scholarly journals and book chapters. At present, she is an editorial board member of the Journal of Communication and Education and a section editor for IIUM journal of Human Sciences. Her research interests are centred on crisis communication, public relations, new media, and corporate social responsibility. Email: azreen@iium.edu.my

Nur Nadia Abd Mubin completed her PhD in Mass Communication at the Faculty of Mass Communication and Media Studies, Universiti Teknologi Mara. She received her Master's Degree in Visual Communication at the Faculty of Art and Design, Universiti Teknologi Mara. Dr. Nur Nadia initiated her academic career as a part-time lecturer at International Islamic University Malaysia, Gombak campus, in 2009, where she served for one and a half years. In 2016, she re-entered the academic realm as an academic trainee at the same institution, dedicating an additional two years to her role. Subsequently, join Universiti Pendidikan Sultan Idris in the Social Communication Program within the Fakulti Bahasa dan Komunikasi. She specializes in visual communication and new media studies. Email: nur_nadia@fbk.upsi.edu.my

Akmal Binti Arzeman is a recent master graduate from Cardiff University, specialising in Digital Media and Society. Her research has been published in the Human Communication Journal on the topic 'The Usage of Pink Public Transportation among Women Users'. She is currently working as a Business Protege at a telecommunication company. Her research interests are on media and communication, digital media, and digital surveillance. Email: akmalarzeman98@gmail.com

REFERENCES

- Ally, A., & Gadgala, N. (2022). Addressing cyber scam as a threat to cyber security in India. *International Journal of Law Management & Humanities*, 5(3), 376-390.
- Ahmad Arifin, N. A., Mokhtar, U. A., Hood, Z., Tiun, S., & Jambari, D. I. (2019). Parental awareness on cyber threats using social media. *Jurnal Komunikasi: Malaysian Journal of Communication*, 35(2), 485-498. <https://doi.org/10.17576/JKMJC-2019-3502-29>
- Arum, N. S. (2017). Infographic not just a beautiful visualisation. *Academia*.
[https://www.academia.edu/31903865/Infographic Not Just a Beautiful Visualisation](https://www.academia.edu/31903865/Infographic_Not_Just_a_Beautiful_Visualisation)
- Azizah, D. N., Rustaman, N. Y., & Rusyati, L. (2021). Enhancing students' communication skill by creating infographics using Genially in learning climate change. *Journal of Physics: Conference Series*, 1806(1), 1-6. <https://doi.org/10.1088/1742-6596/1806/1/012129>
- Basco, R. (2020). Effectiveness of science infographics in improving academic performance among sixth grade pupils of one laboratory school in the Philippines. *Research in Pedagogy*, 10(2), 313-323. <https://doi.org/10.5937/istrped2002313b>
- Basyir, M. (2022, September 26). Online scam cases increasing in Malaysia. *New Straits Times*.
<https://www.nst.com.my/news/nation/2022/09/834531/online-scam-cases-increasing-malaysia>
- Bernama. (2022, October 30). Banking industry launches national scam awareness campaign. *Free Malaysia Today*.
<https://www.freemalaysiatoday.com/category/nation/2022/10/30/banking-industry-launches-national-scam-awareness-campaign/>
- Bernama. (2023, February 22). Fortinet: Malaysia recorded 84 million cyber attacks daily in fourth quarter last year. *New Straits Times*.
<https://www.nst.com.my/news/nation/2023/02/882387/fortinet-malaysia-recorded-84-million-cyber-attacks-daily-fourth-quarter>
- Borainea, A., & Doris, N. L. (2019). The fight against cybercrime in Cameroon. *International Journal of Computer (IJC)*, 35(1), 87-100.
<https://ijcjournal.org/index.php/InternationalJournalOfComputer/article/view/1469>
- CyberSecurity Malaysia. (2022). Corporate profile.
https://www.cybersecurity.my/en/about_us/corporate_overview/main/detail/2065/index.html
- Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trend in Organized Crime*. <https://doi.org/10.1007/s12117-022-09457-y>
- Donalds, C., & Osei-Bryson, K. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, 92, 403-418.
- Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, 62(1), 107-115.
- German, J., Ramilo, D., & Gonzalez, P. (2020). Effectiveness of infographics in enhancing integrated management system (IMS) policy awareness of undergraduate students. Paper presented at 2020 IEEE 7th International Conference on Industrial Engineering and Applications (ICIEA), Bangkok, Thailand, pp. 548-552. <https://doi.org/gk4r78>
- Ginzburg, S. L., Martinez, P. B., Reisner, E., Chappell, S., Brugge, D., & Kurtz-Rossi, S. (2021). An evaluation of an environmental health infographic in community settings. *INQUIRY: The Journal of Health Care Organization, Provision, and Financing*, 58, 1-10.
<https://doi.org/10.1177/00469580211059290>

- Goni, O. (2022). Cyber crime and its classification. *International Journal of Electronics Engineering and Applications*, 10(1), 1-17.
- Harold, J., Lorenzoni, I., Shipley, T., & Coventry, K. (2020). Communication of IPCC visuals: IPCC authors' views and assessments of visual complexity. *Climatic Change*, 158(2), 255–270.
- Hawkswood, J., Carter, E., & Brown, K. (2022). *National Trading Standards (NTS) Scams Team 'Coercion and control in financial abuse; learning from domestic abuse'*. National Trading Standard: Scam Team.
https://www.friendsagainstscams.org.uk/shopimages/FINAL_Coercion_and_control_repor.pdf
- Jahan, S., Al-Saigul, A. M., & Alharbi, A. M. (2021). Assessment of health education infographics in Saudi Arabia. *Health Education Journal*, 80(1), 3–15.
<https://doi.org/10.1177/0017896920949600>
- Kajave, A., & Nismy, S. A. H. (2022). How cyber criminal use social engineering to target organizations. *ArXiv (Cornell University)*. <https://doi.org/10.48550/arXiv.2212.12309>
- Mageswari, M. (2022, August 8). Staying one step ahead of scammers. *The Star*.
<https://www.thestar.com.my/metro/metro-news/2022/08/08/staying-one-step-ahead-of-scammers>
- Lee, S., Pandya, R., Hussan, J., Lau, R., Chambers, E., Geng, A., Jin, B., Zhou, O., Wu, T., Barr, L., & Junop, M. (2022). Perceptions of using infographics for scientific communication on social media for COVID-19 topics: A survey study. *Journal of Visual Communication*, 45(2), 39-47. <https://doi.org/10.1080/17453054.2021.2020625>
- Malaysian Communication and Multimedia Commission. (2022). Internet users survey 2022.
- Marelino, A. (2022). Understanding the types of cyber crime and its prevention. *Mathematical Statistician and Engineering Applications*, 71(1), 108–112. <https://doi.org/k6wm>
- Murray, I. R., Murray, A. D., Wordie, S. J., Oliver, C. W., Simpson, A. H. R. W., & Haddad, F. S. (2017). What surgeons need to know about infographics. *The Bone & Joint Journal*, 99-B(12), 1557–1558. <https://doi.org/10.1302/0301-620X.99B12.BJJ-2017-1301>
- Naparin, H., & Saad, A. B. (2017). Infographics in education: Review on infographics design. *The International Journal of Multimedia & Its Applications*, 9(4/5/6), 15–24.
<https://doi.org/10.5121/ijma.2017.9602>
- National Anti-Financial Crime Centre (NFCC). (2021). Mengenai NSRC.
<https://nfcc.jpm.gov.my/index.php/en/soalan/mengenainsrc>
- Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences*, 2(2), 379–398. <https://doi.org/10.3390/forensicsci2020028>
- Robert, E. (2021). Attempting a definition of cyber crime. *SSRN Electronic Journal*.
<https://doi.org/10.2139/ssrn.3830589>
- Salleh, M. B. (2022, August 5). PDRM: Over RM5.2 billion lost to scams in two years. *The Edge Malaysia*. <https://theedgemaalaysia.com/article/pdrm-over-rm52-billion-lost-scams-two-years>
- Shahbazi, M., Zainuddin, N. M. Mohd., Yusoff, R., Ten, D. W. H., & Wan Hassan, W. A. (2021). Design principle for public transportation infographic. *International Journal of Innovative Computing*, 11(1), 45–52. <https://doi.org/10.11113/ijic.v11n1.293>
- Sheikh, J. A., Tariq, I., Butt, M. A., Tariq, A., & Shahid, M. (2015). Infographics: A new era of information visualization. *International Conference on Engineering and Emerging Technologies*.

- Siricharoen, W. V., & Siricharoen, N. (2015). *How Infographic should be evaluated?* Paper presented at the 7th International Conference on Information Technology (pp. 558-564). <https://doi.org/10.15849/icit.2015.0100>
- Siricharoen, W. V., & Siricharoen, N. (2017). Infographic utility in accelerating better health communication. *Mobile Networks and Applications*, 23(1), 57–67. <https://doi.org/10.1007/s11036-017-0900-3>
- Sjafiie, S. S. L., Hastjarjo, S., Muktiyo, W., & Pawito. (2018). Graphic visualization in printed media: How does the use of technology influence journalism culture. *Jurnal Komunikasi: Malaysian Journal of Communication*, 34(4), 373–385. <https://doi.org/10.17576/JKMJC-2018-3404-22>
- Suleiman, O. H. (2023). Using infographics as communicative tools during Covid-19 pandemic in Egypt: An analytical study. *Journal of Design Sciences and Applied Arts*, 4(1), 46–59. <https://doi.org/10.21608/jdsaa.2022.144463.1197>
- Tharshini, N. K., Hassan, Z., & Mas'ud, F. H. (2021). Cybercrime threat landscape amid the movement control order in Malaysia. *International Journal of Business and Society*, 22(3), 1589–1601. <https://doi.org/10.33736/ijbs.4323.2021>
- World Economic Forum. (2023). The global risk report 2023: 18th edition. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
- World Health Organization. (25, May 2022). Launch of the WHO compilation of innovative concepts to communicate science during the COVID-19 pandemic. <https://www.who.int/news/item/25-05-2022-launch-of-the-who-scicom-compilation>
- Zahari, A. I., Bilu, R., & Said, J. (2019). The role of familiarity, trust and awareness towards online fraud. *Journal of Research and Opinion*, 6(9), 2470–2480. <https://researchopinion.in/index.php/jro/article/view/23>
- Zainal Abidin, N., Kamaluddin, M., Shaari, A., Din, N., & Ramasamy, S. (2018). Pengetahuan dan amalan perlindungan pengguna Facebook wanita terhadap penipuan cinta di Malaysia. *Jurnal Komunikasi: Malaysian Journal of Communication*, 34(4), 113-133. <https://doi.org/10.17576/JKMJC-2018-3404-07>