iscte

INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Raising Cybersecurity Awareness of Telecommunication Company Employee Through Instagram Campaign, Case Study: PT Media Telekomunikasi Mandiri

Farisah Adilia

Master's in International Management

Supervisor:
PhD, Carlos José Corredoura Serrão, Associate Professor,
ISCTE-IUL

INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Raising Cybersecurity Awareness of Telecommunication Company Employee Through Instagram Campaign, Case Study: PT Media Telekomunikasi Mandiri

Farisah Adilia

Master's in International Management

Supervisor:
PhD, Carlos José Corredoura Serrão, Associate Professor,
ISCTE-IUL

Acknowledgment

The journey to study a master's degree with a double degree coupled with working full time and going back and forth from Jakarta to Lisbon was not easy. My time and concentration are scattered, and it is very difficult to focus on one thing. However, reaching the end is an achievement for me, and I want to dedicate it to those who contributed to this process.

Allah SWT has given me strength and a way to overcome all the problems that arise on this journey.
My parents and all family who always support and pray for me.
The lecturers at ISCTE-IUL and Gadjah Mada University have always supported me, especially my advisor, Professor Carlos Serrão.
My superiors and co-workers have always supported and helped me in completing this thesis.
Friends who always comfort me and tell me everything will be okay and I can do it.
Most importantly, I thank myself for going through this journey.

Thank You.

Resumo

Este estudo concentra-se na conscientização dos funcionários sobre segurança cibernética por meio de uma campanha no Instagram. Explora a interseção entre tecnologia e comunicação, destacando o potencial de uma campanha inovadora no Instagram para mudar a conscientização sobre segurança cibernética.

A pesquisa reconhece que a conscientização em segurança cibernética vai além dos departamentos técnicos e afeta toda a organização. Na era digital, com oportunidades e ameaças em constante evolução, a segurança cibernética requer uma força de trabalho informada, indo além das barreiras de firewalls e criptografia.

O estudo investigou se campanhas no Instagram podem aumentar a conscientização dos funcionários de empresas de telecomunicações sobre os perigos da segurança cibernética. Utilizando uma abordagem qualitativa, foram distribuídos questionários aos funcionários da PT Media Telekomunikasi Mandiri, realizando duas rodadas, com uma campanha no Instagram entre elas. A campanha ocorreu na conta do Instagram da MTM durante um mês, apresentando 12 materiais em quatro temas. Os resultados indicaram um aumento na conscientização dos funcionários entre as duas rodadas.

As conclusões não se limitam à MTM; oferecem orientação para outras empresas de telecomunicações que enfrentam desafios semelhantes. Em uma era de vulnerabilidades dinâmicas e oportunidades transformadoras, este estudo destaca a sinergia entre tecnologia e envolvimento humano, definindo a essência da conscientização sobre segurança cibernética na era digital.

Palavras-chave: Conscientização, Conscientização sobre segurança cibernética, Ameaça cibernética, Campanha no Instagram, Eficácia da campanha

Abstract

This research endeavor is encapsulated within the thesis about raising cybersecurity awareness of employees through an Instagram campaign. It navigates the intersection of technology, and communication, and explores the potential of an innovative Instagram campaign to ignite a paradigm shift in the cybersecurity awareness landscape.

The foundation of this study is rooted in the recognition that cybersecurity awareness transcends technical departments, reverberating through the corridors of every facet of an organization. As the digital age ushers in a confluence of opportunities and threats, the fortification of cybersecurity extends beyond firewalls and encryption—it necessitates a vigilant and informed workforce.

This study was conducted to answer whether social network campaigns, in this case, Instagram, can increase telecommunications company employees' awareness of cyber security dangers.

This study uses a qualitative method with data obtained from distributing questionnaires to PT Media Telekomunikasi Mandiri employees. The questionnaire was carried out 2 times with an Instagram campaign in between. The campaign was carried out on the MTM company Instagram for 1 month with 12 materials from 4 topics. The results of the study show an increase in awareness from the first questionnaire to the second questionnaire. The findings are not confined to the walls of MTM, this offers a guiding light to other telecommunication companies grappling with similar challenges. In this age of dynamic vulnerabilities and transformative opportunities, this study stands as a tribute to the synergy between technological fortitude and human engagement that defines the essence of cybersecurity awareness in the digital age.

Keywords: Awareness, Cybersecurity Awareness, Cyber-threat, Instagram Campaign, Campaign Effectiveness

Table of Contents

Figure Index

1. Introduction

In today's rapidly evolving digital landscape, the ICT industry plays a pivotal role in facilitating communication and connectivity. As telecommunication companies embrace innovative technologies and digital transformation, the importance of cybersecurity becomes paramount. These companies handle vast amounts of sensitive data, including personal and financial information, making them attractive targets for cybercriminals.

One significant challenge within telecommunication companies is the need to raise cybersecurity awareness among employees. According to data, cybercriminals are very interested in people's ignorance, so literacy regarding cybersecurity awareness is essential (Furnell & Science, 2020). Employees play a critical role in maintaining a secure environment, as their actions and knowledge directly impact the organization's overall cybersecurity posture. However, according to a study conducted by IBM, human error is the main cause of 95% of cybersecurity breaches**.** These types of errors include weak passwords, clicking on suspicious emails or links, or transferring funds to a hacker because of fake email posing as a supervisor (Logan, 2022).

PT Media Telekomunikasi Mandiri, as a prominent ICT company, also feels the challenge of cybersecurity awareness among its employees. To mitigate the risks and enhance its cybersecurity culture, it is essential for PT Media Telekomunikasi Mandiri to implement effective awareness campaigns tailored to the needs and characteristics of its workforce.

This study focuses on the development and evaluation of an Instagram campaign aimed at raising cybersecurity awareness among PT Media Telekomunikasi Mandiri employees. By leveraging the popularity and reach of Instagram as a social media platform, the campaign aims to engage and educate employees on various cybersecurity topics, empowering them to make informed decisions and adopt secure practices.

By addressing the gaps in employees' cybersecurity knowledge and behavior, this campaign seeks to enhance the overall cybersecurity resilience of PT Media Telekomunikasi Mandiri. The insights gained from this study can also serve as a valuable resource for other ICT companies seeking to improve their cybersecurity awareness initiatives.

1.1 About PT Media Telkomunikasi Mandiri

PT Media Telekomunikasi Mandiri (MTM) was named an ICT company that now evolved into an ICT company which providing full ICT solution services with more emphasizing on IT Networking, software and application delivery as well as security solutions. PT Media Telekomunikasi Mandiri (MTM) established in 2008. Along with the support of their professional team, they always committed to deliver customer requirement and satisfaction. After 14 years of operation, MTM has become the top nation-wide contractor of IT Network Infrastructure Solutions to major Telco and Enterprises.

The leadership and all levels of management of PT Media Telekomunikasi Mandiri are committed to implementing an information security management system in providing Manage Service Connectivity & Security services to customers, through: Determination of information security goals by maintaining the level of confidentiality, upholding integrity, and maintaining the availability of information based on the results of risk identification & assessment, providing and managing the resources needed to implement an information security management system by increasing awareness of all employees on the importance of information security, carrying out HR development activities related to the management of Manage Service Connectivity & Security services, as well as maintaining and maintaining all facilities and devices supporting the technology services used, continuous improvement and improvement in compliance with laws and regulations relating to information security and the requirements of the ISO 27001:2013 standard. In 2022, MTM launched a new business, namely Managed Security Services. Where MTM is referred to as Managed Security Services Provider (MSSP). Services offered include SOC as a Service, Offensive Security, Defensive Security, etc.

1.2 Problem Statement

This thesis aims to increase cyber security awareness among PT Media Telekomunikasi Mandiri employees through the development and evaluation of Instagram campaigns. By utilizing Instagram's popularity and visual nature, the campaign aims to captivate and educate employees on various cybersecurity topics in an easily digestible and interactive format. Through the campaign, PT Media Telekomunikasi Mandiri seeks to raise employees' awareness levels, enhance their understanding of cybersecurity risks, and promote the adoption of secure behaviors in their daily work routines.

PT Media Telekomunikasi Mandiri, as a prominent ICT company, recognizes the importance of maintaining a robust cybersecurity posture to protect its operations and the data it handles. However, one of the critical challenges that PT Media Telekomunikasi Mandiri faces is the lack of cybersecurity awareness among its employees.

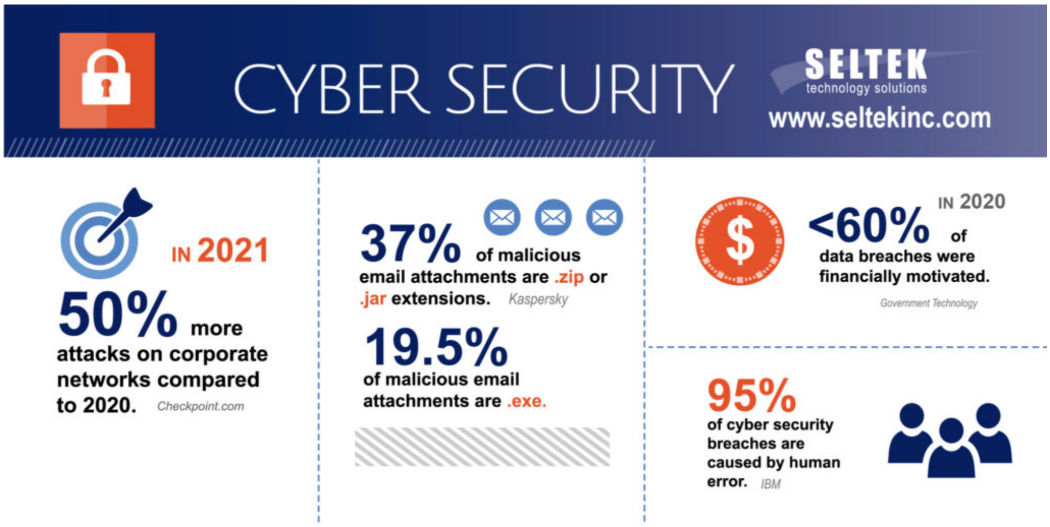

CYBER SECURITY
SELTEK
technology solutions
www.seltekinc.com
IN 2021
50% more
attacks on corporate networks compared to 2020.
Checkpoint.com
37% of malicious
email attachments are .zip or .jar extensions.
Kaspersky
19.5%
of malicious email attachments are .exe.
IN 2020
<60% of
data breaches were financially motivated.
Government Technology
95%
of cyber security breaches are caused by human error.
IBM

Figure 1-1. Top 3 Concerns About Cybersecurity (Logan, 2022)

Cyber-attacks are on the rise each year. 2021 saw 50% more attacks per week on corporate networks compared to 2020 (Logan, 2022)**.** The employees of PT Media Telekomunikasi Mandiri play a crucial role in the organization's overall security posture. Their level of awareness, understanding, and adherence to cybersecurity best practices directly impacts the company's resilience against cyber threats. However, studies have shown that many employees lack the necessary knowledge and skills to identify and respond effectively to cybersecurity risks. This knowledge gap makes them vulnerable to social engineering attacks, phishing attempts, and other malicious activities that can compromise the company's sensitive data and disrupt its operations.

The existing approaches to cybersecurity awareness within PT Media Telekomunikasi Mandiri have not fully addressed the specific needs and challenges faced by its employees. Traditional training methods, such as classroom sessions and email campaigns, have limitations in engaging and sustaining employees' interest in cybersecurity topics. Additionally, the remote work environment and the prevalence of mobile devices pose additional challenges to delivering effective cybersecurity awareness programs.

Therefore, there is an urgent need to design and implement a comprehensive cybersecurity awareness campaign targeting PT Media Telekomunikasi Mandiri employees and addressing their unique knowledge gaps and behavioral challenges. Such a campaign should leverage innovative and engaging strategies to effectively communicate cybersecurity concepts, promote best practices, and empower employees to become active participants in safeguarding the company's digital assets.

By tackling this problem head-on, this research aims to contribute to the overall improvement of PT Media Telekomunikasi Mandiri's cybersecurity posture, reducing the risk of data breaches, and fostering a security-conscious organizational culture. Furthermore, the findings and insights from this study can serve as a valuable reference for other telecommunication companies facing similar cybersecurity awareness challenges, helping them develop effective strategies tailored to their specific organizational contexts. By utilizing Instagram as a platform for cybersecurity awareness campaigns and analyzing engagement metrics, feedback, and data on employee's knowledge and behavior changes, the study will evaluate the impact of the Instagram campaign in effectively raising cybersecurity awareness among PT Media Telekomunikasi Mandiri employees.

1.3 Research Question

Therefore, the research question on this study is:

Is it possible to increase cybersecurity awareness using Instagram social network campaigns?

With this research question, it is expected that this study will provide more information along the way such as gain a comprehensive understanding of the current state of cybersecurity awareness among PT Media Telekomunikasi Mandiri employees, the effectiveness of an Instagram campaign in raising cybersecurity awareness, the key factors influencing employees' knowledge and behaviors, and the impact of the campaign on their cybersecurity practices. The answers to these research questions will contribute to the development of evidence-based recommendations for enhancing cybersecurity awareness initiatives within PT Media Telekomunikasi Mandiri and potentially other ICT companies facing similar challenges.

1.4 Scope and Limitations

This thesis focuses on raising cybersecurity awareness among PT Media Telekomunikasi Mandiri employees through an Instagram campaign. The study specifically targets the employees of PT Media Telekomunikasi Mandiri and aims to evaluate the campaign's effectiveness in improving their cybersecurity knowledge and behaviors.

The scope of this study encompasses the following:

1. PT Media Telekomunikasi Mandiri: The research is limited to PT Media Telekomunikasi Mandiri as the case study organization. The findings and recommendations are tailored to the specific needs, challenges, and organizational context of PT Media Telekomunikasi Mandiri. The campaign design, implementation, and evaluation are conducted within the parameters set by the organization's resources, policies, and guidelines.
2. Instagram as the Campaign Platform: The study focuses on utilizing the Instagram social network as the primary platform for the cybersecurity awareness campaign. The design and development of the campaign leverage the visual and interactive features of Instagram to effectively engage employees. Other social media platforms or communication channels are beyond the scope of this study.
3. Cybersecurity Awareness: The research specifically targets cybersecurity awareness, which includes knowledge, understanding, and behaviors related to cybersecurity best practices. The campaign aims to enhance employees' awareness of common cyber threats, secure online practices, data protection, and incident reporting. However, it does not cover technical aspects of cybersecurity, such as network security configurations or vulnerability management.
4. Time Constraints: The campaign implementation and evaluation occur within a specific time frame due to the practical limitations of the study. The long-term sustainability and impact of the campaign beyond the research period are not within the scope of this study.

[This page is intentionally left blank]

2. Literature review

This section will discuss the literature review of the topics discussed in this study, the precise understanding and previous studies that have the same discussion as this study.

2.1 Cybersecurity Awareness and Previous Studies

Studies that covered cybersecurity awareness in the educational community and among students have been carried out in many countries, including Indonesia such as (Chasanah & Candiwan, 2020) and (Chandarman & Niekerk, 2017). Meanwhile, in this thesis, the study was conducted on employees of a company because it was deemed important for an organization to develop and increase employee awareness of the importance of cyber threats and cyber security. Awareness is the starting point for all employees of an organization in pursuing or understanding knowledge about information technology security. With security awareness, an employee can focus his attention on one or a number of problems or threats that may occur. (Kader, 2021) did a similar study with a descriptive survey in which data has been collected from prospective teachers at Aligarh Muslim University. The questionnaires distributed have topics such as password strength, virus attacks, cybercrime, and misuse of social networks. In Indonesia specifically, (Islami, Bunga, & Candiwan, 2016) did qualitative research by interviewing bank employee to measure their level of awareness of cybersecurity. Similar to (Alrobaian, Alsahrani, & Almaleh, 2023) which assesses the level of awareness of cybersecurity, users' activities, and user responses to cybersecurity issues in the Technical and Vocational Training Corporation (TVTC) in Saudi Arabia.

2.2 Cybersecurity

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes (CISCO, 2017).

Indonesia as a developing country, is trying to develop the country's economy by increasing investment in the ICT sector. Data from the Ministry of Finance of the Republic of Indonesia shows an increase of approximately 18.24% or equivalent to USD 219 million in the realization of Central Government ICT Expenditure in the period Fiscal Year 2009-2010 (BPPT, 2011).

In line with the increase in technology in the digital era, cyber threats are also increasingly widespread with increasingly diverse types. According to cyber security firm Kaspersky, Indonesia has seen more than 11 million cyber-attacks in the first quarter of 2022. Kaspersky discovered and prevented a total of 11,802,558 different cyber threats between January and March 2022. The amount marked a 22% increase over the previous year when it was 9,639,740. However, only 32 percent had a security system installed on their devices prior to the possible attack (Mordor Intelligence, 2022).

Cyber threat itself is defined as any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat source to successfully exploit a particular information system vulnerability (NIST SP 1800-15B).

Convention of Cybercrime has been split into several sections or called by typology of cybercrime (International Telecommunication Union (ITU), 2019) such as:

1. Offenses against the confidentiality, integrity and availability of computer data and systems
2. Computer-related offences
3. Content-related offenses
4. Offenses related to infringements of copyright and related rights.
5. Ancillary liability

The number of related policies and regulations on ICT security are still very limited to protect the rapid growth of the ICT sector in Indonesia. Compared with another countries, Indonesia lagged behind in ICT security policy and regulation, such as Malaysia that has already had Computer Crime Act (1997), digital signature act (1997), telemedicine act (1997), communication and multimedia act (1998), payment system act (2003), personal data act (2010), etc., even other countries like Slovenia have PDP act (2004) and E-commerce & E-signature act (2004) while Estonia has Estonia-Digital Signature Act (2000) and Electronic Communication Act (2004) (Lubis & Maulana, 2010).

According to research made by "Positive Technologies", a survey by Cloudflare that involved more than 4,000 cybersecurity managers in Australia, China, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, Singapore, South Korea, Taiwan, Thailand, and Vietnam showed that 78% of those interviewed had experienced at least one cybersecurity incident in the previous 12 months. Of these, 80% reported 4 or more incidents, and 50%, 10 or more. Around 63% put the financial impact of cyber incidents on their organizations in the previous 12 months at a minimum of $1 million, with 14% saying their losses had exceeded $3 million (Positive Technologies, 2023).

The cyber security threat is being well identify and the effort to increasingly attach value to developing national cybersecurity programs and investing in the implementation of these preventions and mitigations, one of the foundations to prevent cyber incidents by providing enough and proper cyber security awareness campaign which can reach all multi elements society on national level.

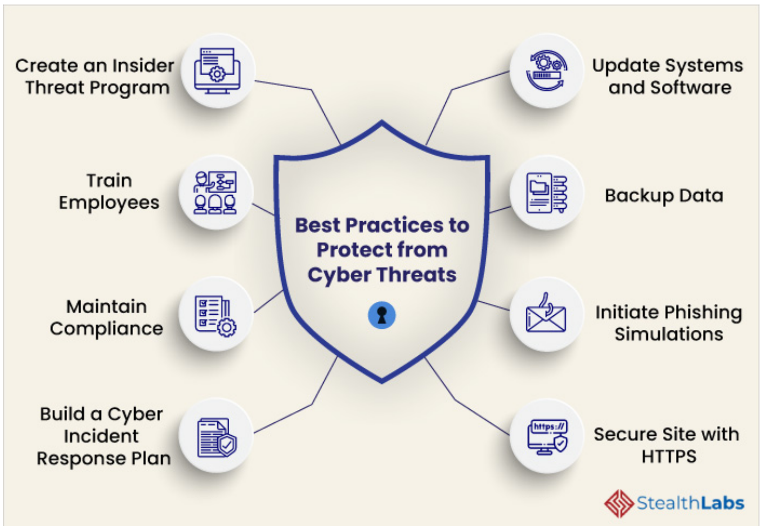

Create an Insider Threat Program
Train Employees
Maintain Compliance
Build a Cyber Incident Response Plan
Best Practices to Protect from Cyber Threats
Update Systems and Software
Backup Data
Initiate Phishing Simulations
Secure Site with HTTPS
https://
StealthLabs

Figure 2-1. Sources of Cybersecurity Threat (StealthLabs, 2020)

To prevent these threats, organizations must refine their cybersecurity program. An effective cybersecurity program can help organizations disrupt attacks as they occur, reduce recovery time, and contain future threats (StealthLabs, 2020).

Therefore, this research could be one way for a company to increase employee awareness of the dangers of cyber threats.

2.2 Cybersecurity on Social Network

Cybercrime is a violation committed using a technical device such as a computer, smartphone, and internet (P. Warren; M. Streeter, 2013). With the popularity of the Internet, criminals also see the opportunity to commit crimes using the ICTs or by targeting the ICTs. According to the 2017 Internet Crime Report, the Internet Crime Complaint Centre (IC3) under the Federal Bureau of Investigation received 301,580 complaints with an estimated loss of USD 1.418 billion in 2017 (Internet Crime Complaint Centre, 2018). Southeast Asia region is also benefiting from the advancement of the digital world. The advancement of the digital world promotes economic growth in Southeast Asia. Digital trade (e-commerce) and online transportation contribute to the growth of the Southeast Asian digital economy (Yuniar, R.W, 2017). According to economists, Southeast Asia's total trade is expected to reach 102 billion US dollars by 2025. Cyberspace itself is accessible to approximately 132 million Indonesians and 67 million Filipinos (ASEAN-

UP,2019).

By viewing the characteristics of the social media, it can be understood that it has a great power to disseminate a message to the mass audience in a faster way than conventional mass media. It is a tool that can spread words, pictures, and videos all over the world, in a global scope. It carries and sends the message to the people who have access on it (Anggreni, 2017).

Wood & Smith (2005: 40-41) stated that there are five features of online communication: packet-switching, multimedia, interactivity, synchronicity, and hyper textuality. As a tool of communication, Instagram has an important role in disseminating the message. Just like any other communication tool, Instagram can also be explored in terms of the communication process based on its elements (Anggreni, 2017). When it was first appearing in October 2010, Instagram was mostly used for personal issues. The recent change has happened where it is used for business, promotion, and gaining revenue for institutions and companies. The use of Instagram by various groups, individuals, companies, and even governments, has invited many irresponsible individuals to start carrying out cyber-attacks with various kinds of attacks and creativity. While this may seem obvious, most small firms overestimate or underestimate the importance of their data (Paulsen, 2016).

Reuters Institute (2020) analyzed a sample of 225 pieces of misinformation rated false or misleading by fact-checkers and published in English between January and the end of March 2020. In terms of responses, social media platforms have responded to a majority of the social media posts rated false by fact-checkers by removing them or attaching various warnings. There is significant variation from company to company, however.

Initially, cyber security was described by a highly specialized technical approach that should be left to professionals (Georgiadou, Mouzakitis, Bounas, & Asko, 2020). However, in today’s world of ever-increasing hazards and threats, cyber security is crucial for all users and suppliers of systems and data, from the smallest individual to the greatest enterprise and most powerful state (Ghernaouti & Wanner, 2018). In fact, several businesses overlook cybersecurity threats and respond only after a breach has occurred (I. C. Eian, L. K. Yong, M. Y. X. Li, Y. H. Qi & F. Z, 2020). This increases the likelihood of cybercrime being successful.

2.3 Instagram Campaign

Instagram first started in 2010 by cofounders Kevin Systrom and Mike Krieger, and it is now owned by Meta Platforms Inc. Instagram has at least 1.318 billion users around the world in January 2023 (Datareportal, 2023) and Indonesia is listed as the country with the 4th most Instagram users in the world with approximately 104 million users (NapoleonCat, 2022).

Instagram is one of the largest internet platforms used by Indonesian people. This can also be seen from the many stars/influencers who were born and famous on the platform and also Instagram is enabling the success of SMBs by allowing them to reach a broader range of customers within their own cities, throughout Indonesia and abroad. 76% of Instagrammers have purchased from a brand after discovering them on Instagram, either locally or internationally (Ipsos, 2018).

Therefore, Instagram is considered worthy of being a platform to raise awareness for any topic. Central to this subsection is the acknowledgment of the campaign's role in shaping the essence of cybersecurity awareness. It's a nod towards the symbiotic relationship—the campaign serves as a catalyst to elevate awareness, while the essence of awareness infuses depth and resonance into the campaign's messages.

Instagram's visual-centric nature, as expounded by Brown and Squire (2018), provides a unique opportunity to communicate complex ideas succinctly (Brown & Bessant, 2004).

The amalgamation of images, videos, and concise captions facilitates cognitive resonance, enhancing comprehension and retention. This aligns with the study's approach of using visuals to distill intricate cybersecurity concepts into easily digestible content.

In an increasingly visual-oriented digital landscape, the visual advantage of platforms like Instagram has become a pivotal force in communication strategies. This subsection navigates the terrain where the visual prowess of Instagram synergizes with the campaign's objectives. Carrying out a campaign on Instagram in this research is primarily to increase awareness of the dangers of Cybersecurity for MTM employees, but this can also be a way to increase awareness of the dangers of cyber threats on Instagram itself. Material posted on Instagram can not only be seen by employees but can also be seen publicly by other users. This is possible because of the Instagram algorithm and hashtags which can make this post visible in the explore menu of other users. According to the basic idea behind Instagram and the two main functions of hashtags, Instagram users employ hashtags to mark their photos and gather attention from other users. On social media, the use of hashtags can increase the audience beyond one’s own followers due to their high searchability (Zhan & Yu, 2020).

[This page is intentionally left blank]

3 Methodology

This chapter will discuss how the research study will be carried out. This chapter will discuss how this research will be conducted. The process is carried out from the start of creating the right research flow to getting good research results.

3.2 Research Design

Research design is a blueprint of a scientific study. It includes research methodologies, tools, and techniques to conduct the research. It helps to identify and address the problem that may rise during the process of research and analysis (Emeritus, 2023).

In this study, the research design consist of a long to-do list. Since the research is performed in a company, permission is the first obstacle to overcome.

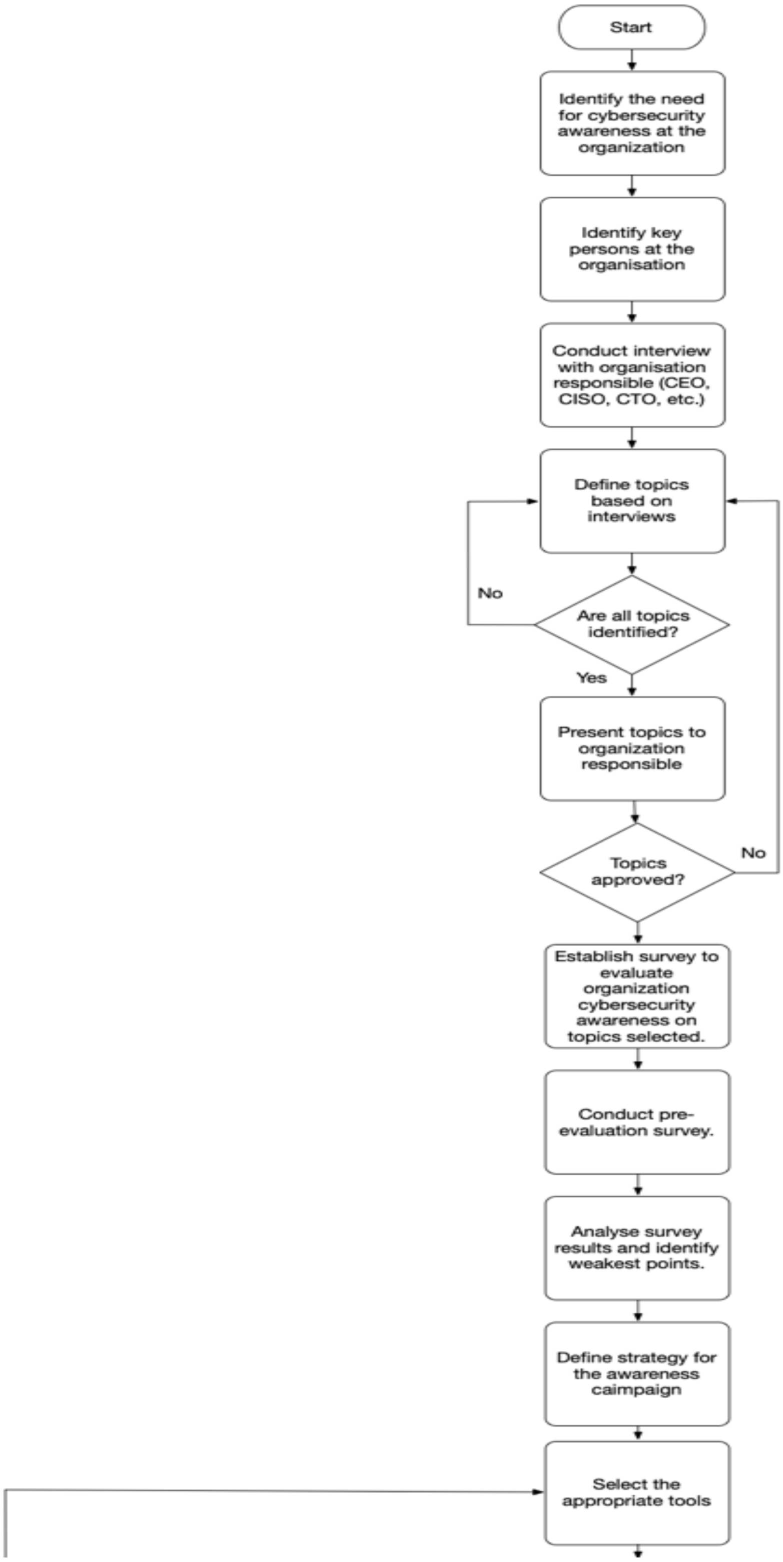
In this research conducted at PT Media Telekomunikasi Mandiri (MTM), a letter requesting permission was issued by ISCTE and then given to HR at the company. After the head of the HR division agrees, then a meeting process with stakeholders in the company is carried out and then the process runs according to the process plan that has been made.

The process begins by gathering information about the situation and the need for awareness about cyber security in the company. Information was obtained by interviewing the Director of Operations and Chief Information Security Officer at Media Telekomunikasi Mandiri. From the results of the interview, the topics that will be discussed in this research are concluded. This topic is then submitted to the relevant stakeholders to obtain approval whether this topic is appropriate or not. If the topic is appropriate, a set of questions for the questionnaire will be created which will be distributed to employees in the company. The questionnaire was carried out using Google Docs and then distributed to all employees to complete.

At the same time as creating a set of questions for the questionnaire, content was also created for the campaign to be carried out on Instagram. After discussing with the marketing department as the department that handles social media, content had to be created because they did not yet have material regarding the topic to be discussed. The content material created is then submitted to the marketing department to be processed into content suitable for uploading to the company's Instagram.

After the first questionnaire has been distributed, the campaign begins on Instagram for a predetermined period. Then a second questionnaire was distributed, only to participants who had completed the first questionnaire. After the period for filling out the second questionnaire is complete, a report on the results of the two questionnaires is drawn and then the report is processed. With that, this study was completed.

The entire process has been summarized in the flowchart below:


Start
Identify the need for cybersecurity awareness at the organization
Identify key persons at the organisation
Conduct interview with organisation responsible (CEO, CISO, CTO, etc.)
Define topics based on interviews
No
Are all topics identified?
Yes
Present topics to organization responsible
Topics approved?
No
Establish survey to evaluate organization cybersecurity awareness on topics selected.
Conduct pre-evaluation survey.
Analyse survey results and identify weakest points.
Define strategy for the awareness caimpaign
Select the appropriate tools

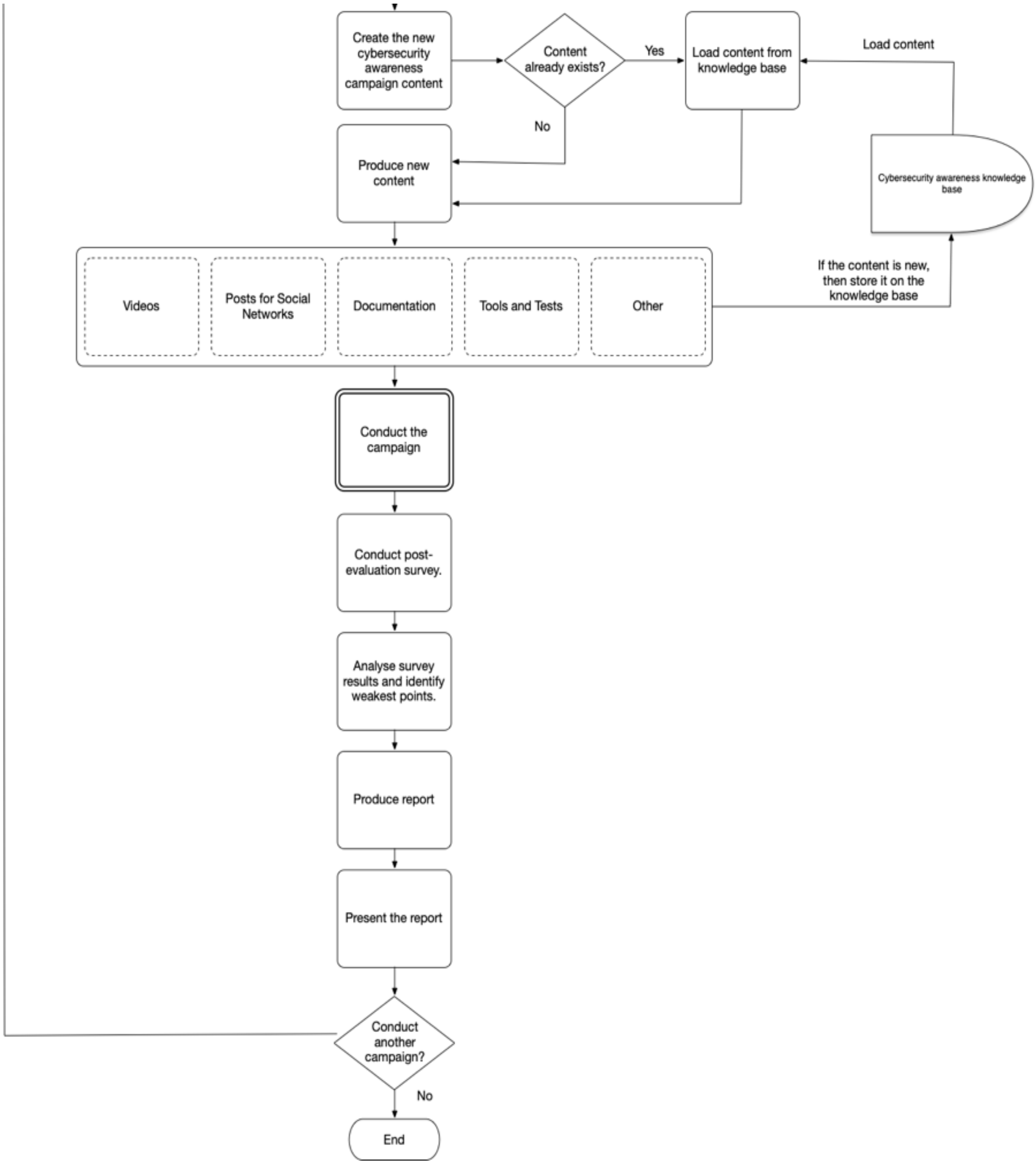

Create the new cybersecurity awareness campaign content
Content already exists?
Yes
Load content from knowledge base
Load content
No
Produce new content
Cybersecurity awareness knowledge base
Videos
Posts for Social Networks
Documentation
Tools and Tests
Other
If the content is new, then store it on the knowledge base
Conduct the campaign
Conduct post-evaluation survey.
Analyse survey results and identify weakest points.
Produce report
Present the report
Conduct another campaign?
No
End

Figure 3-1. Flowchart Research Design

3.3 Information collection

Before starting a research plan, there are several steps that must be taken as planning. The process must start by knowing the problems and gaps that exist internally at PT Media Telekomunikasi Mandiri. For this reason, interviews were conducted with stakeholders who could be the IT director, security team and others. In this research, interviews were conducted with the Director of Operations and Chief Information Security Officer (CISO). In the results of the interview, it was discovered that there was a large lack among PT Media Telekomunikasi Mandiri employees regarding Cybersecurity Awareness. It is said that regarding day-to-day operations in the office, there are many things that employees should be aware of but are ignored because of their insensitivity to the dangers of cyber-attacks.

In this regard, both the Director of Operations and the Chief Information Security Officer (CISO) mentioned the matters that were of most concern to them. The first is the habits of the employees themselves. Using free WiFi in public places using office property is the main priority. This is considered dangerous because there are many confidential assets that may compromise the organization's security if they fall into the hands of other people. Hence, it is agreed that the first topic to be discussed in this study is about habits. The next thing that is also a concern for both is Phishing. It is said that several employees have become victims of phishing. Some of them are even top-level management who should be more aware of cybersecurity threats. Followed by concerns about employee password management and also malware which has also occurred several times in the office environment.

3.4 Data Collection Instruments

Within research, data collection instruments form the threads that weave insights into the fabric of understanding.

In this study, there will be 2 reports produced from the distribution of questionnaires and data analytic of Instagram. To get accurate results regarding the effectiveness of the Instagram campaign in raising security awareness, the questionnaire will be conducted twice. The first questionnaire is intended to measure the level of employee awareness of cybersecurity. The second is intended to see whether the Instagram campaign being carried out is effective in raising the level of alertness itself. The Instagram campaign will be carried out for 1 month with a total of 12 posts in feeds. The length of time of this research will also be a factor that will influence the results.

3.5 Survey Questionnaire

Embedded within this data collection arsenal is the survey questionnaire—a carefully curated set of questions that traverse the dimensions of cybersecurity awareness. It resonates with the understanding that each question is a strategic gateway into employees' knowledge, behaviors, and perceptions.

The questionnaire consists of 5 sections with:

- Section 1: Participant demography,
- Section 2: Employee's habit,
- Section 3: password security,
- Section 4: Phishing attacks and,
- Section 5: Malware.

Section 1:	Directorate
Demography	Age
	Gender
	How long have you been working in Telecommunication Company?
	In your opinion, how well you know about cyber threats?
	Have you ever been a victim of a cyber-attack?
	If yes, what kind of cyber-attacks?
	Do you follow @mtm.id on Instagram?

In this section, only participants who said yes to the last question would be able to continue to the next section. If they said no to the question, which they don't follow @mtm.idn Instagram, they will be headed to the end of the survey. This is because they can't see nor participate in the campaign that going on @mtm.idn Instagram.

Section 2:	I've never been suspicious of e-mails from anywhere.
Employee Habits	I often forget so I write my password in a visible place.
	I look for the application I need from the internet then download it without being concerned with the source.
	When I see free WiFi, I always use it.

In this section, participants will be asked to answer the questions on the scale 1 to 5. With 1: Strongly Agree and 5: Strongly Disagree. After filling all the answers, participant will be directed to the next section.

Section 3:	I know what Two-Factor Authentication (2FA) is and I use it.
Password Security	I never use password based on my personal information.
	I changed my password regularly.
	I use different password for every account I have.

In this section, participants will be asked to answer the questions on the scale 1 to 5. With 1: Strongly Disagree and 5: Strongly Agree. After filling all the answers, participant will be directed to the next section.

Section 4:	Phishing attack is a danger to my computer.
Phishing Attack	Phishing attack pose a threat to me.
	I feel phishing attack would invade my privacy.
	I feel like phishing attack could steal my personal information from my computer without my knowledge.

In this section, participants will be asked to answer the questions on the scale 1 to 5. With 1: Strongly Disagree and 5: Strongly Agree. After filling all the answers, participant will be directed to the next section.

Section 4:	I never clicked on a suspicious link or downloaded a file from an untrusted source.
Malware	I regularly back up important data to protect it from loss due to malware or other cyber threats.
	I avoid using public Wi-Fi networks to reduce the risk of malware infection.
	I regularly update my anti-virus software to protect against malware.

In this section, participants will be asked to answer the questions on the scale 1 to 5. With 1: Strongly Disagree and 5: Strongly Agree. After filling all the answers, participant will be directed to the end of the questionnaire.

3.6 Instagram Campaign Design

Content created to be uploaded to Instagram is based on topics that have been created. For this study, there are 4 topics that will be discussed. With the aim of proving this research model, with a limited time frame, 3 pieces of content were created for each topic to be uploaded. Thus, the number of uploads in this campaign is 12 pieces of content. After curating from many sources, the following is the content of the Instagram content that will be uploaded to Instagram @mtm.idn.

Topic 1: Habits

1. **How to protect your information:**

Use strong password, Avoid public devices, Don't overshare, Disable geolocation data, Don't click on suspicious links, Use two-factor authentication.

2. **Most Data Breaches Come from Insiders**

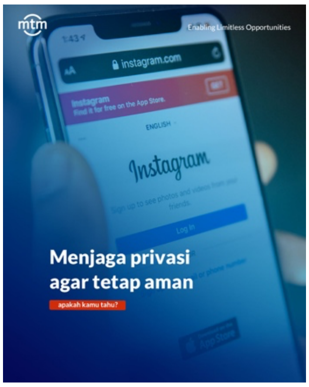
The information security leaders surveyed implicated their organizations' own employees in 50 percent of data breaches. Other causes included "external actors" (e.g. cybercriminals via malware) at 28 percent, and "software failures" at 27 percent.

*Source: Data security firm Code42**.**

3. **Public Wi-Fi: lots of risks?**

Public Wi-Fi security risks: Malware distribution, Wi-Fi snooping and sniffing, Man-in-the-middle attacks, Unencrypted networks

How to stay safe on public Wi-Fi: Avoid accessing sensitive information, Use a VPN, Use a privacy screen, Turn off file sharing, Use two-factor authentication, Remember to log out. Use antivirus software.


mtm
Enabling Limitless Opportunities
Menjaga privasi agar tetap aman
apakah kamu tahu?

mtm
Enabling Limitless Opportunities
Kebocoran Data Pribadi
Berawal dari Orang Dalam?

mtm
Enabling Limitless Opportunities
Wi-Fi Publik Banyak Resiko?
Apakah benar?

Topic 2: Password Security

1. **Create your safe password!**

- Create passwords that are at least 12 characters long, with a mix of uppercase and lowercase letters, numbers, and symbols.

- Don’t use personal info, Examples: Your nickname or initials, Important birthdays or years
- Don’t use common words & patterns, Examples: "password”, "abcd” , "1234”, "qwerty" or "qazwsx”

2. **Be Prepared if someone gets your password**

   - Add a recovery email address

   - Add a recovery phone number

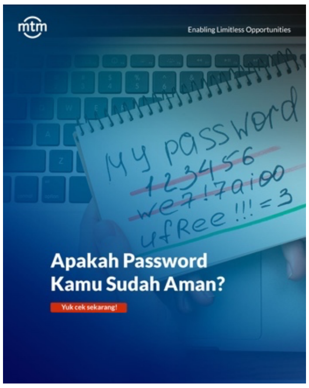
Recovery info can be used to help you:

- Find out if someone else is using your account
- Take back your account if someone else knows your password
- Get into your account if you forget your password or can’t sign in for another reason

3. **What is Two-factor Authentication?**

Two-factor authentication is designed to make sure that you're the only person who can access your account. Two-factor authentication is an extra layer of security, designed to make sure that you're the only one who can access your account—even if someone else knows your password.

The most popular forms of 2FA that you can use to secure your accounts today: SMS (Short message service), OTP (One Time Passwords), and FIDO U2F (FIDO Universal 2nd Factor).


mtm
Enabling Limitless Opportunities
My password
123456
we7!7ai00
ufRee!!!=3
Apakah Password Kamu Sudah Aman?
Yuk cek sekarang!

mtm
Enabling Limitless Opportunities
Password Anda Tersebar?
Apa yang harus kita lakukan?

mtm
Enabling Limitless Opportunities
2FA
******
Apakah Anda Sudah Menggunakan “2FA”?
Apa itu 2FA?

Topic 3: Phising Attacks

1. **What is Phising attacks?**

Phishing attacks are scams that often use social engineering bait or lure content. Legitimate-looking communication, usually email, that links to a phishing site is one of the most common methods used in phishing attacks.

Ex. Invoice phishing, Payment/delivery scam, Downloads

2. **What Is Vishing?**

Vishing—or voice phishing—is the use of fraudulent phone calls to trick people into giving money or revealing personal information. It's a new name for an old problem—telephone scams.

Watch out for:

- Offers from companies you do not do business with and/or have not heard of.
- An announcement that you have won a prize in a contest you did not enter.
- Promises of unrealistic returns for your money.
- Pressure to make immediate decisions to give the caller what they want, which may include Money and Financial account information.

3. **Types of Phising:**

1. Email phishing

Most phishing attacks are sent by email. The crook will register a fake domain that mimics a genuine organisation and sends thousands of generic requests.

The fake domain often involves character substitution, like using ‘r’ and ‘n’ next to each other to create ‘rn’ instead of ‘m’

2. Spear phishing, describes malicious emails sent to a specific person. Criminals who do this will already have some or all of the following information about the victim:

- Their name.
- Place of employment.
- Job title.
- Email address; and
- Specific information about their job role.

3. Whaling attacks are even more targeted, taking aim at senior executives.

4. Smishing and Vishing, SMS Phising and Voice Phising, telephones replace emails as the method of communication.

mtm
Enabling Limitless Opportunities
Phising Attacks
jenis-jenis serangan phising
yang harus kalian ketahui

mtm
Enabling Limitless Opportunities
Vishing Attacks
Apa yang harus kita waspadai?
apakah kamu tahu?

Topic 4: Malware

1. **What is Malware?**

Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems.

Malware can be about making money off you, sabotaging your ability to get work done, making a political statement, or just bragging rights.

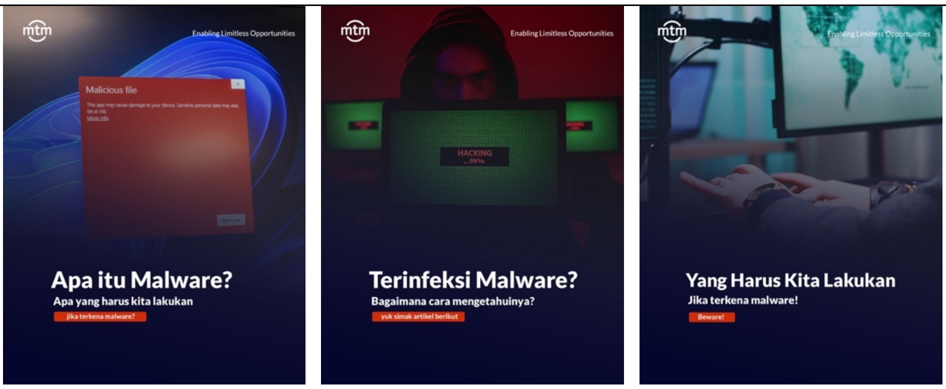
Although malware cannot damage the physical hardware of systems or network equipment, it can steal, encrypt, or delete your data, alter or hijack core computer functions, and spy on your computer activity without your knowledge or permission.

2. How can I tell if I have a malware infection?

- Your computer slows down.
- Your screen is inundated with annoying ads.
- Your system crashes.
- Your antivirus product stops working and you cannot turn it back on
- You lose access to your files or your entire computer.

3. What Happens If I Opened an Attachment from a Phishing Email or Clicked on a Spam Link?

- Disconnect from your wireless network. Turn off Wi-Fi or cellular data capabilities if you're on a mobile device or disconnect from Wi-Fi if you're using a laptop or desktop.
- Backup your files.
- Scan your computer for malware or viruses.
- Change your passwords immediately.


mtm
Enabling Limitless Opportunities
Malicious file
This app may cause damage to your device. Sensitive personal data may also be at risk.
More info
Apa itu Malware?
Apa yang harus kita lakukan
jika terkena malware?
mtm
Enabling Limitless Opportunities
HACKING
...99%
Terinfeksi Malware?
Bagaimana cara mengetahuinya?
yuk simak artikel berikut
mtm
Enabling Limitless Opportunities
Yang Harus Kita Lakukan
Jika terkena malware!
Beware!

Before the content plan was fixed, the contents are then taken to the Marketing team at MTM for them to curate and adjust. Content uploaded to Instagram @mtm.idn will be translated into Indonesian to make it easier to reach Instagram followers in the Indonesian market. If the content has been approved by MTM and the translation is appropriate, then the marketing team will create a visual design and then the content will be uploaded to Instagram periodically.

3.7 Sample selection

The study's findings are based on a sample of PT Media Telekomunikasi Mandiri employees, which may not represent the entire employee population. The sample size and characteristics are determined based on practical constraints and the organization's cooperation.

PT Media Telekomunikasi Mandiri employees currently number 254 people with details of 177 men and 39 women with vulnerable age of workers is 20-60 years. Following the provisions of Dworkin (2012) points out that in qualitative research of the "grounded theory" type, having 25 to 30 participants is a minimum to reach saturation. Therefore, the minimum number of participants in this study is 25 people.

[This page is intentionally left blank]

4 Results and Discussion

In this chapter, the results of the research that has been carried out will be discussed. The research was conducted for approximately 3 months at the Mandiri Telecommunication Media company. The results of the research process and methodology discussed in the previous chapter will be seen here.

This study aims to know if a simple Instagram campaign can be effective in increasing cybersecurity awareness. The campaign was held for one month on MTM Instagram, @mtm.idn with the total of 12 post that concludes 4 topics.

In this research, data collection was carried out by distributing questionnaires to MTM employees. To facilitate the data collection method, Google forms were used as a tool for data collection. The data displayed below was obtained from 2 sources, the first is from survey results from Google Forms and the second is from Instagram analytics as a result of the campaign carried out.

4.1 Data Result Survey

In this section, the data displayed is the result of a survey filled in on Google Forms. The data displayed is divided into 5 sections as displayed on Google Forms to participants. The results of the first and second surveys will be displayed side by side with the aim of making it easier to compare survey results before the campaign and after the campaign.

Starting from the demographic results of the participants in the form of age, directorate (part of work), length of time working at a telecommunications company, how well the participant understands cyber threats, known types of cyber-attacks, whether the participant has ever experienced a cyber-attack and what type of cyber-attack they have experienced. by participants. This is to find out more about the experience and knowledge of the participants, who are employees of PT Media Telekomunikasi Mandiri, regarding cyber threats and attacks.

4.1.1 Participant Demography

a)

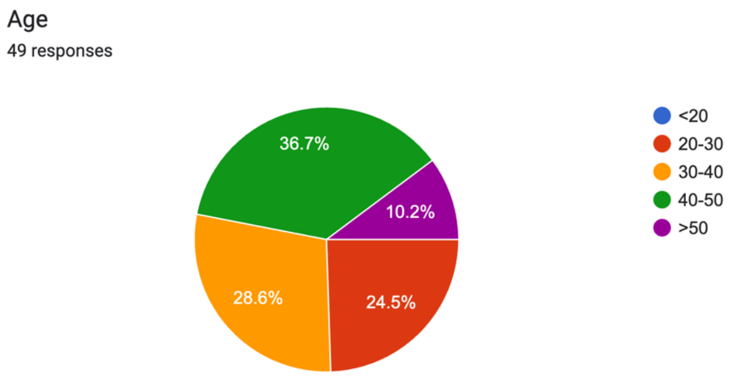


Figure 4-1. Age of Participant

The age distribution of Telecommunication Media employees who have Instagram is between 20 years old and over 50 years old, with details of 20 to 30 years old vulnerable in 24.5 percent, 30 to 40 years old 28.6 percent, 40 to 50 years old 36.7 percent and over 50 years 10.2 percent.

b)

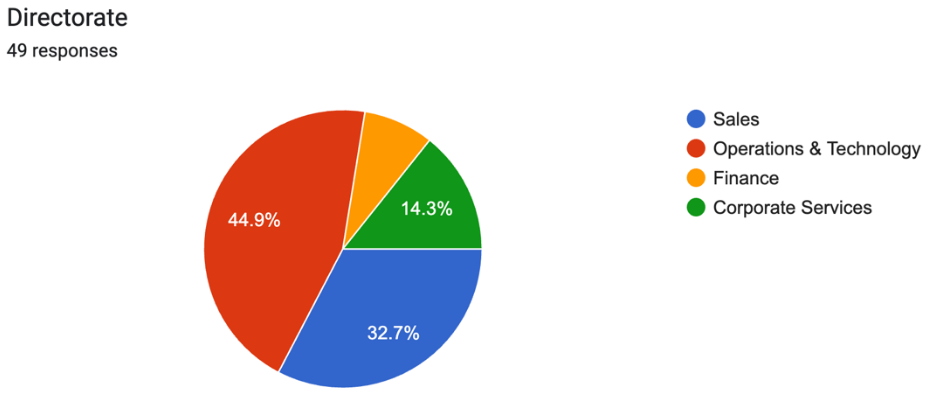


Figure 4-2. Directorate Participant

From the first questionnaire, 49 results were obtained with varying distribution from 4 directorates at PT Media Telekomunikasi Mandiri. The largest number of participants came from the Operations and Technology section, which is the largest number of employees in MTM in that section. This was followed by participants from the sales department, then corporate service and the smallest number from the finance department.

c)

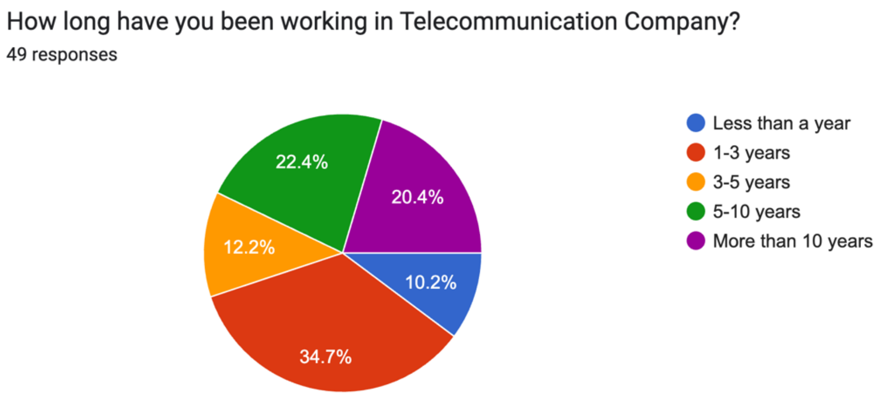


Figure 4-3. Telecommunication Company Experience

Most of the participants who took part in the survey had worked in the telecommunications sector for 1 to 3 years, although most of them were aged 30-40 years. Employees with more than 10 years of experience account for 20.4 percent. This number can be said to be quite large, and it is hoped that the number of employees who are aware of the dangers of cybersecurity will be high in the survey.

d)

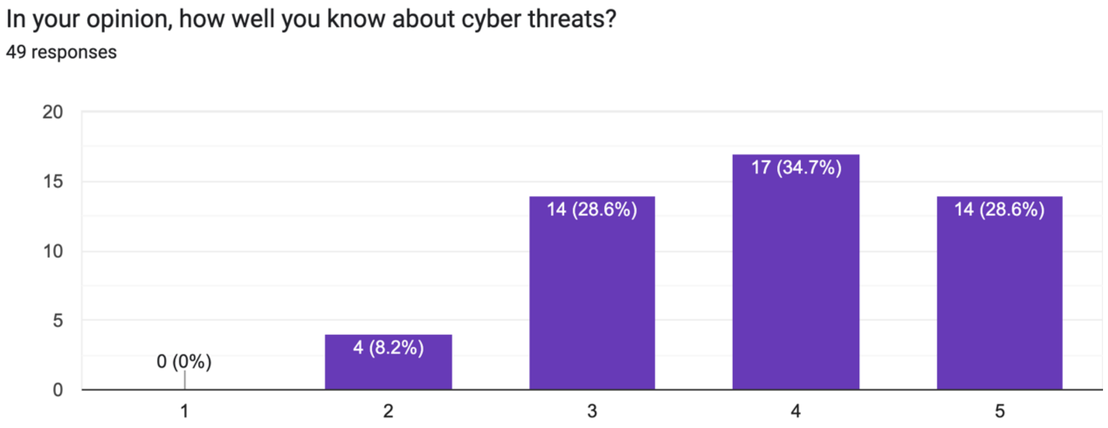


Figure 4-4. Cybersecurity Knowledge

28.6 percent of participants stated that they were very aware of cyber threats. 34.7 percent chose a score of 4 which means they understand, and 28.6 percent is at number 3 indicating they understand quite well. Participants who felt they did not understand were in 8.2 percent and no one chose that they did not understand cyber threats at all.

e.

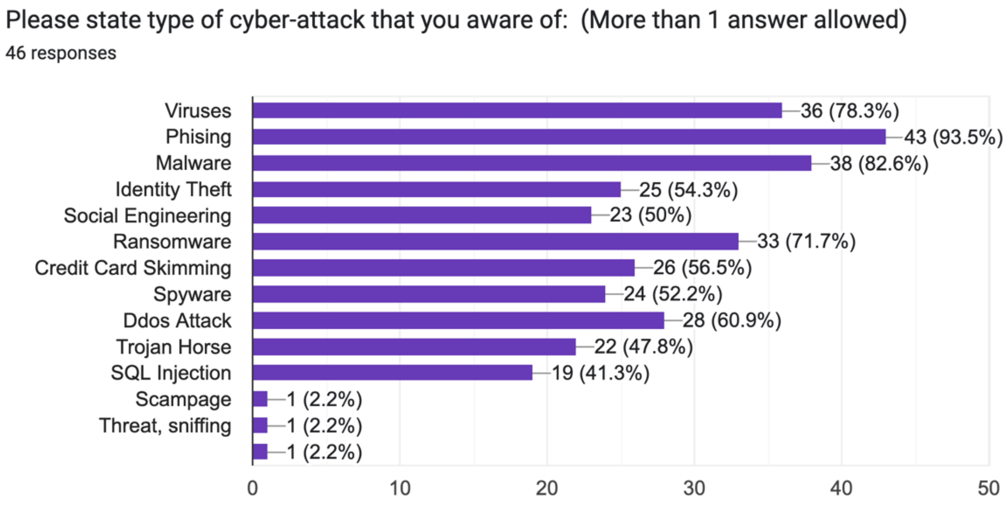


Figure 4-5. Cyber-attack Knowledge

From the choices about cyber-attacks given, almost one hundred percent, to be precise 93.5 percent of participants knew about phishing attacks, making the survey materials and campaign content presented very suitable to their knowledge. The next highest numbers is Malware with 82.6 percent, Viruses with 78.3 percent and Ransomware with 71.7 percent. Participants also added 2 new types of cyber threats, namely Scampage and Sniffing showing that there are participants who know more about cyber threats.

f.

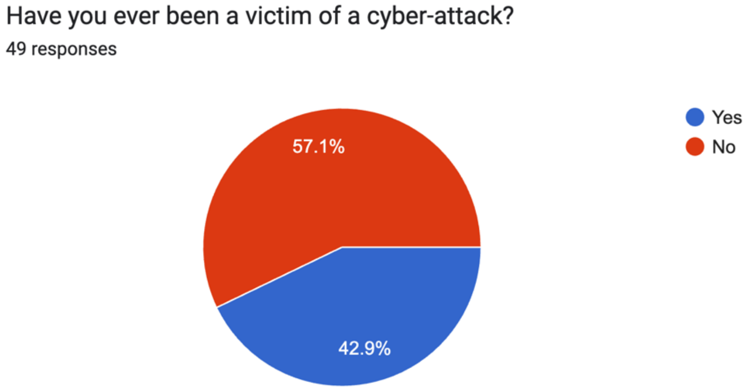


Figure 4-6. Cyber-attack Victim

Almost half of the participants had experienced a cyber-attack, 42.9 percent. Compared to the figure stating that they understand cyber threats, namely 63.3 percent, however, some of the participants in this number have been exposed to cyber-attacks. This shows that awareness of cyber security remains low. So, socialization about the dangers of cyber-attacks and awareness of cybersecurity needs to be carried out in the company.

g.

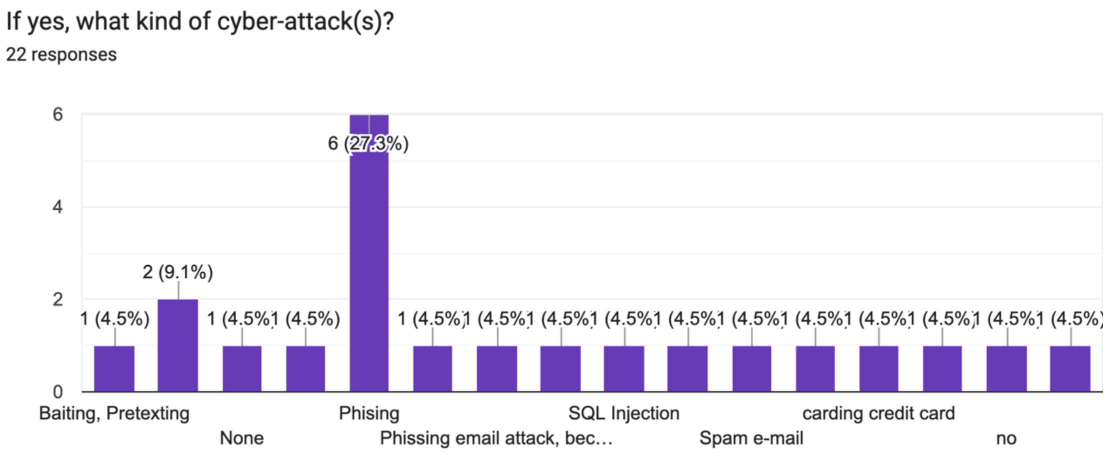


Figure 4-7. Cyber-attack Victim Experience

Out of the 42.9 percent of participants who admitted to having been exposed to a cyber-attack, 27.3 percent stated that the attack they were exposed to was phishing. Again, this is inversely proportional to the cyber-attacks they are most aware of, namely phishing attacks. It is hoped that this is because they have been exposed to it and are now more aware of the attack.

4.1.2 Habits

Pre-Campaign Survey:

Questions	1 (Strongly Agree)	2	3	4	5 (Strongly Disagree)
I've never been suspicious of any e-mails	10.2%	6.1%	16.3%	28.6%	38.8%
I often forgot, so I write my password in a visible place	12.2%	16.3%	8.2%	18.4%	44.9%
I look for the application I need from the internet then download it without being concerned with the source	4.1%	14.3%	10.2%	22.4%	49%
Whenever I see free WiFi, I always use it	0%	6.1%	22.4%	30.6%	40.8%
Average percentage	6,6%	10,7%	14,3%	25%	43.4%

After Campaign Survey:

Questions	1 (Strongly Agree)	2	3	4	5 (Strongly Disagree)
I've never been suspicious of any e-mails	12%	12%	16%	8%	52%
I often forgot, so I write my password in a visible place	8%	8%	12%	16%	56%
I look for the application I need from the internet then download it without being concerned with the source	12%	8%	12%	20%	48%
Whenever I see free WiFi, I always use it	8%	4%	16%	24%	48%
Average percentage	10%	8%	14%	17%	51%

In the first section which discusses habits, the average percentage of participants who understand bad habits the most increases by 7.6 percent. In the survey before the Instagram campaign, the number of points 5 (most aware) was at 43.4 percent and in the survey after the campaign, the percentage increased to 51 percent. This increase is not significant but considering that this campaign only lasted for 1 month, this increase could be called quite good.

4.1.3 Password Security

Pre-Campaign

Questions	1 (Strongly Disagree)	2	3	4	5 (Strongly Agree)
I know what Two-Factor Authentication (2FA) is and I use it	12.2%	6.1%	16.3%	22.4%	42.9%
I never use password based on my personal information	14.3%	6.1%	20.4%	24.5%	34.7%
I changed my password regularly	10.2%	12.2%	34.7%	18.4%	24.5%
I use different password for every account I have	10.2%	16.3%	24.5%	32.7%	16.3%
Average percentage	11,7%	10,2%	24%	24,5%	29,6%

After Campaign

Questions	1 (Strongly Disagree)	2	3	4	5 (Strongly Agree)
I know what Two-Factor Authentication (2FA) is and I use it	8%	4%	12%	12%	64%
I never use password based on my personal information	12%	8%	16%	12%	52%
I changed my password regularly	16%	12%	20%	24%	28%
I use different password for every account I have	16%	24%	4%	16%	40%
Average percentage	13%	12%	10,5%	16%	46%

In the section about password security, the average number of participants who claimed to really understand password security was 29.6 percent before the Instagram campaign. After the campaign, this percentage rose to 46 percent. This increase can be called quite significant and is a good value considering the campaign was only carried out for 1 month. But unfortunately, the value of people who are completely unaware (choose the value 1) increases from 11.7 percent to 13 percent.

4.1.4 Phishing Attack

Pre-Campaign

Questions	1 (Strongly Disagree)	2	3	4	5 (Strongly Agree)
Phising attack pose a threat to me	4.1%	2%	24.5%	36.7%	32.7%
Phising attack is a danger to my computer	2%	2%	6.1%	36.7%	53.1%
I feel phising attack would invade my privacy	4.1%	2%	6.1%	38.8%	49%
I feel like phising attack could steal my personal information from my computer without my knowledge	2%	2%	12.2%	32.7%	51%
Average percentage	3%	2%	12,2%	36,2%	46.45%

After campaign

Questions	1 (Strongly Disagree)	2	3	4	5 (Strongly Agree)
Phising attack pose a threat to me	4%	4%	4%	28%	60%
Phising attack is a danger to my computer	4%	0%	16%	20%	60%
I feel phising attack would invade my privacy	4%	0%	12%	16%	68%
I feel like phising attack could steal my personal information from my computer without my knowledge	4%	0%	8%	20%	68%
Average percentage	4%	1%	10%	21%	64%

Phishing attacks are the type of cyber-attack that participants are most familiar with. As expected, the average number of participants who claimed to be very aware of phishing attacks was very high, namely 46,45 percent for the first survey. For the second survey after the Instagram campaign, the percentage value increased to 64 percent. This value can be called very good compared to the percentage values for other topics. Participants who admitted that they did not feel that phishing attacks were a threat still existed, but their value is very small.

4.1.5 Malware

Pre-Campaign

Questions	1 (Strongly Disagree)	2	3	4	5 (Strongly Agree)
I never clicked on a suspicious link or downloaded a file from an untrusted source	2%	6.1%	18.4%	20.4%	53.1%
I regularly back up important data to protect it from loss due to malware or other cyber threats	0%	14.2%	30.6%	28.6%	26.5%
I avoid using public Wi-Fi networks to reduce the risk of malware infection	0%	8.2%	20.4%	30.6%	40.8%

I regularly update my anti-virus software to protect against malware	6.1%	10.2%	26.5%	20.4%	36.7%
Average percentage	2%	9,7%	24%	25%	39,3%

After campaign

Questions	1 (Strongly Disagree)	2	3	4	5 (Strongly Agree)
I never clicked on a suspicious link or downloaded a file from an untrusted source	4%	0%	16%	20%	60%
I regularly back up important data to protect it from loss due to malware or other cyber threats	4%	8%	12%	36%	40%
I avoid using public Wi-Fi networks to reduce the risk of malware infection	4%	0%	12%	28%	56%
I regularly update my anti-virus software to protect against malware	4%	12%	0%	32%	52%
Average percentage	4%	5%	10%	29%	52%

In surveys about malware, participants who chose number 5 (most aware) were at an average percentage of 39.3 percent before the campaign. After the campaign on Instagram, the figure rose to 52 percent. Half of the participants admitted to being aware of the dangers of malware. This percentage is also considered quite good and there is potential to increase if awareness campaigns continue to be carried out.

4.2 Data Result Instagram

After the campaign which lasted for 1 month was completed, data was pulled from the Meta platform which includes Instagram and Facebook. All posts posted on Instagram @mtm.idn are reflected on the Telekomunikasi Mandiri media Facebook account as well. Hence, data pulled from Meta automatically displays analytical data which is also generated from Facebook. In this section, all data pulled from Meta analytics will be presented to see the effectiveness of campaigns carried out on Instagram @mtm.idn. Scaling up and down, the type of post and material that has the highest, lowest engagement and posting time can also influence traffic for an account on the

Instagram platform.

Account username	Publish time	Permalink	Date	Impressions	Reach	Shares	Likes
mtm.idn	06/07/2023 05:06	https://www.instagram.com/p/CtMFoHWxfT1/	Lifetime	195	139	0	20
mtm. idn	06/09/2023 04:06	https://www.instagram.com/p/CtRJM-dNCur/	Lifetime	224	166	0	20
mtm.idn	06/14/2023 05:06	https://www.instagram.com/p/CteKC4ZvSYT/	Lifetime	247	189	2	24
mtm.idn	06/15/2023 04:06	https://www.instagram.com/p/CtgjC1uri7y/	Lifetime	130	102	0	10
mtm.idn	06/16/2023 04:06	https://www.instagram.com/p/CtjH2bdtkFK/	Lifetime	163	128	0	17
mtm.idn	06/17/2023 05:06	https://www.instagram.com/p/CtlzgZ7vU_k/	Lifetime	176	129	1	13
mtm.idn	07/02/2023 04:07	https://www.instagram.com/p/CuMYQliOk1h/	Lifetime	160	135	2	19
mtm.idn	07/03/2023 04:07	https://www.instagram.com/p/CuO_TQnNGGC/	Lifetime	172	141	5	14
mtm.idn	07/06/2023 01:07	https://www.instagram.com/p/CuWTJZIPoi6/	Lifetime	124	102	2	12
mtm.idn	07/08/2023 01:07	https://www.instagram.com/p/CubcuTANowG/	Lifetime	118	101	0	14
mtm.idn	07/10/2023 00:07	https://www.instagram.com/p/CugfdQfPoVJ/	Lifetime	123	104	0	11

Table 1 Instagram Analytic Report

The table above shows data pulled from Meta (Instagram) analytics for 12 pieces of content posted on MTM Instagram during the campaign. The data displayed is the posting time in the form of date and time, number of likes, number of reaches, number of impressions and number of shares. It can be seen that the highest number of impressions and reach were on the date 14 June 2023 with content about the dangers of public WiFi with as many impressions as 247 and reach as many as 189. Meanwhile, the smallest number of reaches and impressions were on the date ... with content about malware infections with as many reaches as 101 and as many impressions as 118. If viewed digitally, the URL can be clicked so that the Instagram page containing the content can be directed to.

[This page is intentionally left blank]

5. Conclusion

This study assessed the impact of a cybersecurity awareness campaign at PT Media Telekomunikasi Mandiri (MTM) on employee awareness of cyber threats. Key findings include an appreciable increase in awareness post-campaign, despite time and content limitations.

After going through all the processes that have been designed and then carried out, data is obtained from various platforms and finally, a conclusion can be reached. From the results of the first survey (before the campaign) conducted, the average of participants who claimed to have a sufficient understanding of cyber threats (choosing scores 4 and 5) was above 50%. This figure shows that the awareness of MTM employees can be considered sufficient. The increase in the results of the first survey (pre-campaign) and the second survey (after the campaign) shows an increase in participants' awareness. It's not a significant increase. However, considering that this campaign was carried out over a short period and the amount of content and discussion was limited, the increase was still appreciated and calculated. Recommendations that can be given are for PT Media Telekomunikasi Mandiri to continue carrying out activities to increase employee awareness in various forms. Continuing to spread awareness through the Instagram platform can be recommended. However, it would be better if the activities carried out could include more participants so that awareness of the dangers of cyber threats could spread. This is very important considering that the number of participants is only 20% of the employee population and with the alert level value still at an average of 70%, it seems that this is not enough to be a company's shield in fighting cyber threats.

In answer to this research question “Is it possible to increase cybersecurity awareness with Instagram campaign?” it can be concluded that yes, Instagram campaigns can be a way to increase awareness of the threat of cybercrime.

5.1 Future Research and Limitations

This study does have certain limitations. Firstly, the research time constraints restricted the campaign’s implementation to just one month. It's worth noting that a longer campaign duration could potentially yield greater cybersecurity awareness with the inclusion of more educational material. Furthermore, we hope this study can serve as a model for similar initiatives in other companies or organizations. We encourage further research in this area with the objective of fostering widespread cybersecurity awareness, not only in Indonesia but also in various countries globally. Expanding research in this field is crucial to addressing the evolving challenges of cybersecurity awareness.

Bibliographical References

Alrobaian, S., Alsahrani, S., & Almaleh, A. (2023). Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation. *Big Data Cogn. Comput.*

Anggreni, L. S. (2017). Social Media and Globalization: The Importance of Instagram for Communicating World-Class University. *borderless communities & nations with borders: 981*.

BPPT, P. T. (2011). Seri TIKOMETER Indikator Teknologi Informasi Dan Komunikasi Edisi 2011,.

Brown, S., & Bessant, J. (2004). Mass customization: The key to customer value?

Chandarman, R., & Niekerk, B. v. (2017). AJIC Issue 20, 2017 133Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. *The African Journal of Information and Communication*.

Chasanah, B. R., & Candiwan. (2020). Analysis of College Students' Cybersecurity Awareness In Indonesia.

CISCO. (2017, august 18). *What Is Cybersecurity?* Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Datareportal. (2023). *INSTAGRAM USERS, STATS, DATA & TRENDS*. Retrieved from https://datareportal.com/essential-instagram-stats#:~:text=How%20many%20Instagram%20users%20are,the%20world%20in%20January%202023

Dworkin, S. L. (2012). Sample Size Policy for Qualitative Studies Using In-Depth Interviews.Arch Sex Behav 41. 1319–1320.

Emeritus. (2023). *5 Types of Research Design – Elements, Needs and Characteristics*. Retrieved from https://emeritus.org/in/learn/types-of-research-design/

Furnell, S., & Science, C. (2020). Home working and cyber security – an outbreak of unpreparedness? *Fraud Secur. Bull., vol. 2020, no. 8*, 6-12.

Georgiadou, A., Mouzakitis, S., Bounas, K., & Asko. (2020). Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, 1-12.

Ghernaouti, S., & Wanner, B. (2018). Research and Education as Key Success Factors for Developing a Cybersecurity Culture. *Journal of Computer Information Systems*, 539-552.

International Telecommunication Union (ITU). (2019). Understanding Cybercrime: A guide for Developing Countries.

Ipsos. (2018). *Instagram's Impact on Indonesian Businesses*. Retrieved from https://www.ipsos.com/en-id/instagrams-impact-indonesian-businesses

Islami, D. C., Bunga, K., & Candiwan. (2016). Awareness Information Security Employees X Bank in Bandung Indonesia. *INKOM, Vol. 10*.

Kader, N. A. (2021). CYBER SECURITY AWARENESS-A NECESSITY FOR MORE PRODUCTIVE DIGITAL EXPERIENCE.

Logan, P. (2022, May 2). *Cyber Security Stats*. Retrieved from https://www.seltekinc.com/cyber-security-stats/

Lubis, M., & Maulana, F. (2010). Information and Electronic Transaction Law Effectiveness (UU-ITE) in Indonesia.

Mordor Intelligence. (2022). *INDONESIA CYBERSECURITY MARKET SIZE & SHARE ANALYSIS - GROWTH TRENDS & FORECASTS (2023 - 2028)*. Retrieved from https://www.mordorintelligence.com/industry-reports/indonesia-cybersecurity-market#:~:text=According%20to%20%20cyber%20security%20%20firm,year%20in%20it%20was%209%2C639%2C740

NapoleonCat. (2022). *Instagram users in Indonesia*. Retrieved from https://napoleoncat.com/stats/instagram-users-in-indonesia/2022/01/

Paulsen, C. (2016). Cybersecuring small businesses. 92-97.

Positive Technologies. (2023, September). *Cybersecurity threatscape of Asia: 2022–2023*. Retrieved from https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/

StealthLabs. (2020, December). *Cyber Security Threats and Attacks: All You Need to Know*. Retrieved from https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/

Zhan, M., & Yu, Q. (2020). Effectively organizing hashtags on Instagram: A study of library-related captions.