SCIENTIFIC JOURNAL OF MEANING COMMUNICATION
Vol. 12, No 2 (2024): Agustus 2024,pp.73-84

E.ISSN:2334-4606, P-ISSN:2087-2461
http://jurnal.unissula.ac.id/index.php/makna
DOI:http: /dx.doi.org/10.30659/jikm.v12i2.39208

Issue Management in Maintaining Digital Campus Reputation (Insan Cita Indonesia University Case Study in Facing Cyber Attacks in 2022)

Nike Ardina

Postgraduate Study Program in Communication Sciences/ Faculty of Social and Political Sciences/ Universitas Al Azhar Indonesia
Nikeardina1191@gmail.com

Abstract

As the first digital campus in Indonesia and carrying a brand image as a university at the forefront of digital technology, UICI faced challenges with cyber attacks in the form of hacking of UICI's social media accounts. This attack not only has the potential to lose UICI's digital assets in the form of Instagram, but also has the potential to damage its reputation. So in handling and dealing with this potential crisis, UICI must manage the circulating issues so that they do not become a crisis. This research uses a qualitative approach and case study method with data collection techniques in the form of observation and documentation studies. The research results found that in managing issues, UICI formed a crisis team and appointed one person as a spokesperson who then succeeded in turning the situation around with proper issue management. This cyber attack provides an opportunity for UICI to prove the campus' brand image with technology. From this research, it is recommended for both UICI and other institutions to implement multi-layered security for digital asset managers. As well as forming guidelines in the form of strategies and management plans for the digital assets owned.

Keywords: Digital Campus, Brand Image, Reputation, Cyber Attacks, Issue Management

Abstrak

Sebagai kampus digital pertama di Indonesia dan mengusung *brand image* sebagai perguruan tinggi terdepan dalam teknologi digital, UICI menghadapi tantangan berupa serangan siber berupa peretasan akun media sosial UICI. Serangan ini tidak hanya berpotensi meruginya aset digital UICI berupa Instagram, tetapi juga berpotensi merusak reputasinya. Maka dalam menangani dan menghadapi potensi krisis ini, UICI harus mengelola isu-isu yang beredar agar tidak menjadi krisis. Penelitian ini menggunakan pendekatan kualitatif dan metode studi kasus dengan teknik pengumpulan data berupa observasi dan studi dokumentasi. Hasil penelitian menemukan bahwa dalam mengelola isu, UICI membentuk tim krisis dan menunjuk satu orang sebagai juru bicara yang kemudian berhasil membalikkan keadaan dengan manajemen isu yang tepat. Serangan siber ini memberikan kesempatan bagi UICI untuk membuktikan brand image kampus dengan teknologi. Dari penelitian ini, direkomendasikan bagi UICI dan institusi lain untuk menerapkan keamanan berlapis bagi pengelola aset digital. Serta membentuk pedoman berupa strategi dan rencana pengelolaan aset digital yang dimiliki.

Keywords: Kampus Digital, Brand Image, Reputasi, Serangan Siber, Manajemen Isu.

SCIENTIFIC JOURNAL OF MEANING COMMUNICATION
Vol. 12, No 2 (2024): Agustus 2024,pp.73-84

E.ISSN:2334-4606, P-ISSN:2087-2461
http://jurnal.unissula.ac.id/index.php/makna
DOI:http: /dx.doi.org/10.30659/jikm.v12i2.39208

INTRODUCTION

Since its founding in January 2021, Universitas Insan Cita Indonesia (UICI) has received public attention with the image of the first digital campus in Indonesia. The image of this first digital campus received a lot of mass media coverage and public attention on social media. In the annual report of the UICI Public Communication and Content Production Division (KPPK) in 2022 or one year after its launch, there was 299 mass media coverage for one year, both tier one, second and third tier media. Previously, in the quarterly report since its launch for the period June – August 2021, there was 96 mass media coverage. Meanwhile, social media and websites managed by the UICI public relations team also received public attention with the number of followers increasing significantly on social media pages both on Instagram and Facebook. In the 2022 annual report it is also stated that the number of followers on Instagram is 17,778 and the number of followers on Facebook is 2,960. In 2022, the website itself will receive 2.67 million impressions and YouTube will have 2,059 followers or an increase of 1,289 percent.

Having the brand image of the first digital campus in Indonesia, UICI uses the Articial Intelligence Digital Simulator Teaching Learning System (AI DSTLS) platform as a technological innovation for education. In the campaign carried out, this technology is said to be the first in Indonesia and the fifth in the world. With this innovation, UICI ensures itself as a digital campus pioneer or advanced level of Distance Education (Online Learning/Distance Learning) which is already popular in Indonesia. Such as the Open University (UT), Cyber Asia, and other online learning education.

In the campaign carried out, UICI took three keywords, including; Innovative with developed technology, strong network or network-based because it was founded by the Islamic Student Association (KAHMI) alumni association organization which has members in various professional fields and top leaders in government, bureaucracy, politics, business and academia. Third is flexibility. Because of the technology created, UICI promises flexibility in its lecture system, so that students can study anywhere and at any time. Meanwhile, in the Strength, Weaknessess, Opportunity, Threat (SWOT) analysis test in the Public Relations sector report as of August 2021, UICI's strengths as selling points include: firstly innovative with the AI DSTLS technology innovation used, secondly ideological by integrating Islamic and Indonesian values , thirdly flexible because it creates flexibility both in the learning system (place and time, open assessment system, synchronous and asynchronous, also in the payment system which allows for a system of being paid based on ability (in installments), and fourthly network-based because it was founded by HMI alumni .

By carrying out the concept of high technology and advanced levels of online learning, UICI faced challenges in the second year with a cyber attack in the form of hacking on UICI's social media. The official Instagram account @UICIOfficial was hacked by the hacker group Tolgadarius13K on March 22 2022. UICI's social media also changed its name and several posts appeared from hackers asking the management for ransom. According to official information from the Head of the UICI Public Communications and Content Production Division, Izzaty Zhepania, the UICI Instagram account was hacked using the phishing method. Where the UICI social media manager can no longer access the UICI Instagram account and the account changes its name to the hacker's.

According to this term, phishing is an attempt to obtain information about someone's data using deceptive techniques. Quoting from the official website of the General Department

SCIENTIFIC JOURNAL OF MEANING COMMUNICATION
Vol. 12, No 2 (2024): Agustus 2024,pp.73-84

E.ISSN:2334-4606, P-ISSN:2087-2461
http://jurnal.unissula.ac.id/index.php/makna
DOI:http: /dx.doi.org/10.30659/jikm.v12i2.39208

of State Assets (DJKN Ministry of Finance, March 22, 2022), the data targeted for fraud is personal data (name, age, address), personal data (name, age, address). Account data (username and password). and financial information (credit card information, account information. The term phishing comes from the word fishing which comes from the word fishing. Phishing attempts to trick people into voluntarily providing personal information without realizing it(Irawan & Kom, 2020). Even if the information shared will be used for criminal purposes.

In the case of social media hacking, hackers usually target accounts with many followers, and at the time it was hacked, the UICI Instagram account itself had 13.4 thousand followers. A similar incident also occurred on the official Instagram account of the Ministry of Tourism and Creative Economy. (Kementerian Pariwisata dan Ekonomi Kreatif) on March 10th, 2022. Previously, in mid-March 2022 there was also an attack on the DJKN website. Hacker attacks on official accounts of organizations and companies continue to increase significantly yearly. In a 2017 report, the Indonesian Ministry of Communication and Information and the Coordinating Ministry for Politics, Law and Security stated that during 2017, as many as 1,225 hacker attacks occurred daily in Indonesia.

In the 2022 Kaspersky Security Networks report, Indonesia is at the top in the Southeast Asia region and 60th in the world as a country that is vulnerable to the threat of cyber-attacks (Antara, 26 April 2022). From this data, almost 12 million online threats were recorded targeting users in Indonesia during the first three months of 2022. In the period January to March 2022, Kaspersky has detected and blocked 11,802,558 different cyber-attack threats spread via the internet on KSN users' computers (Kaspersky Security Networks) in Indonesia, and as many as 27.6% of digital technology users in Indonesia were targeted by the threat of cyber attacks in that period. According to data from the National Cyber and Crypto Agency (BSSN) in(Astasia Utari et al., 2023)The impacts of this hacking activity include:

1. Stop business activities.
2. Potential loss of confidential customer data and important information.
3. Cyber-attacks are expensive and financially detrimental.
4. Damage to reputation.
5. Loss of business or other material loss.

Cyber-attacks on a business or organization can lead to several serious consequences. In terms of public relations, these attacks can erode public trust, generate negative perceptions, and potentially harm the organization's image and reputation. This damage can, in turn, indirectly affect the organization's overall stability in multiple ways..(Nova et al., 2020). The cyber-attack by hacker Tolgadarius13K on UICI's Instagram account is a challenge and threat to the brand image it has built. As a university that has declared itself a digital campus with its technological innovations, UICI must prove itself capable of facing the crimes of the digital world. In addition to recovering the Instagram account, UICI must implement an issue management strategy to uphold its reputation, maintain public trust, and address concerns before they escalate into a larger crisis with more significant consequences. Brand image is an intangible asset that significantly impacts consumer loyalty and trust in a product or the public's perception of an organization. According to Kotler (2009) brand image is a vision and belief hidden deep in consumers' minds, reflecting the associations stored in their memories (Bastian, 2014). Brand image is related to product trust and reputation. So a trusted brand must be able to fulfill the promised value. In Dani Alexander Bastian's research (2014) entitled "Analysis of the Influence of Brand Image and Brand Trust on Brand Loyalty of ADES PT Alfindo Putra Setia, it was found that based on the research results Brand Trust has a significant influence and positive towards loyalty (Bastian, 2014).

SCIENTIFIC JOURNAL OF MEANING COMMUNICATION
Vol. 12, No 2 (2024): Agustus 2024,pp.73-84

E.ISSN:2334-4606, P-ISSN:2087-2461
http://jurnal.unissula.ac.id/index.php/makna
DOI:http: /dx.doi.org/10.30659/jikm.v12i2.39208

Issues and crises are an inherent part of organizational and company operations (Saputra, 2020). Effective issue management is crucial to prevent these situations from escalating into crises that could negatively affect the organization (Nova et al., 2020). Unmanaged issues can develop into crises that might damage brand image and reputation, despite the critical role brand trust plays in maintaining customer loyalty. During the issue and crisis management process, public relations must engage in a planned, systematic, and targeted communication strategy, especially when dealing with crises caused by cyber attacks (Astasia Utari et al., 2023).

The main goal in issue management is to manage issues circulating in the public. Barry Jone & W. Howard Chase (1976) in "Corporate Public Issues and Teir Management" define issue management as a tool that can be used by companies to identify, analyze and manage various issues that emerge to the surface and react before these issues are known by the public. Wide community(Nova et al., 2020). There are many approaches that can be used in issue management, one of which is the Strategic approach (Strategic Reduction of Uncertainty Approach). The strategic approach emphasizes efforts to reduce uncertainty and complements the previous approach, namely the systems approach.

The strategic approach derives from the study of strategic decision making, organizational processes, managerial behavior, and sociopolitical behavior to develop an understanding of environmental events and organizational actions(Prayudi, 2007). Implicitly, the strategic approach emphasizes the cognitive orientation of organizational actions and individual decision-making behavior. The main concern is the individual and collective interpretation of a problem in relation to action at the organizational level. Dutton's research emphasizes a series of concepts that help identify and explore problems and ultimately lead to organizational decision making. The core of this concept is Strategic Issue Diagnosis (SID) (Journal of Management Studies, 1993: 339).

This research aims to analyze the strategies and best practices carried out by Insan Cita Indonesia University, especially the Public Communication and Content Production Division, in carrying out its strategic role in managing and managing issues when facing cyber attacks that have the potential to damage UICI's brand image and reputation as a digital campus. Research is important because it can enrich communication science studies, especially on the theme of the strategic role of PR and practical methods that can be used in managing issues so that they do not develop into crises.

RESEARCH METHODS

The approach used in this research is a descriptive qualitative approach. Where this method is used to explore, describe and understand a symptom centrally(Akhyar & Pratiwi, 2019). Meanwhile, the method used in this research is a case study with data collection techniques in the form of documentation studies and literature reviews. Primary data sources are documentation in the form of official reports in the form of minutes of meetings, press releases, official documentation from organizations, and other physical artifacts that are relevant to the research. Meanwhile, other sources of secondary data are library studies in the form of reports in the media, books and related journals. In technical data analysis, researchers used narrative descriptive methods. The data is then processed and analyzed descriptively, with the findings connected to the relevant theory.

SCIENTIFIC JOURNAL OF MEANING COMMUNICATION
Vol. 12, No 2 (2024): Agustus 2024,pp.73-84

E.ISSN:2334-4606, P-ISSN:2087-2461
http://jurnal.unissula.ac.id/index.php/makna
DOI:http: /dx.doi.org/10.30659/jikm.v12i2.39208

RESULTS AND DISCUSSION

1. Universitas Insan Cita Indonesia (UICI)

Universitas Insan Cita Indonesia (UICI) is a digital-based higher education institution authorized by the Indonesian Ministry of Education and Culture under Number 143238/A5/HK/2020, effective December 30, 2020. This campus was established by the National Assembly of the Islamic Student Association Alumni Corps (MN KAHMI) and emphasizes higher education through the Distance Education (PJJ) model. The brand image of UICI represents an advanced evolution of PJJ, which is well-known in Indonesia. The UICI campaign includes narratives that highlight:

1. The first digital campus in Indonesia.
2. Utilizing the Artificial Intelligence Digital Simulator Teaching Learning System (AI DSTLS), making it the fifth university to implement AI in education.
3. Fully supported by the government, with its establishment announced directly by the President of the Republic of Indonesia, Joko Widodo, on January 15, 2021. This date marks the founding of UICI.
4. UICI also has the backing of the extended KAHMI family, which includes members active in government, politics, bureaucracy, business, and 3,000 HMI alumni professors.

Situation Analysis

As the pioneering digital campus in Indonesia and the fifth globally to fully utilize digital technology in its management and learning systems, UICI is committed to maintaining a cutting-edge brand image. However, in its second year of operation, the university encountered significant challenges. On Wednesday, March 23, 2022, UICI's official Instagram account (@UICIOfficial) was hacked. The hackers changed the account handle to @tolgadarius13k. According to an official release on the UICI website, Izzaty, Head of the Public Communications Division, confirmed that the hack was executed using a phishing attack.

Phishing is an attempt to obtain information about someone's data using phishing techniques(Irawan & Kom, 2020). Usually, the data targeted for phishing is personal data (name, age, address), account data (username and password), and financial data (credit card information, account)(Saputra Gulo et al., nd). The official term for phishing is phishing, which comes from the word fishing, namely fishing(Irawan & Kom, 2020). Phishing activities aim to lure people into providing personal information voluntarily without realizing it. Even though the information shared will be used for criminal purposes.

SCIENTIFIC JOURNAL OF MEANING COMMUNICATION
Vol. 12, No 2 (2024): Agustus 2024,pp.73-84

E.ISSN:2334-4606, P-ISSN:2087-2461
http://jurnal.unissula.ac.id/index.php/makna
DOI:http: /dx.doi.org/10.30659/jikm.v12i2.39208

Figure 1.1: Screenshot of the official announcement on the uici.ac.id website

This piracy incident attracted public attention, because at the same time UICI was implementing its second batch of new student admissions (PMB) and UICI's reputation as a digital campus was under threat. As a campus that declares itself to be advanced in technology, UICI must be able to show the public the brand image it is campaigning for.

Based on the chronology report document and the efforts made by the Public Communications and Content Production Division team in dealing with this crisis, the piracy incident started with a confirmation request for blue tick registration on UICI's Instagram. At that time, the official UICI account was registering or verifying the account to get a blue tick on Instagram.

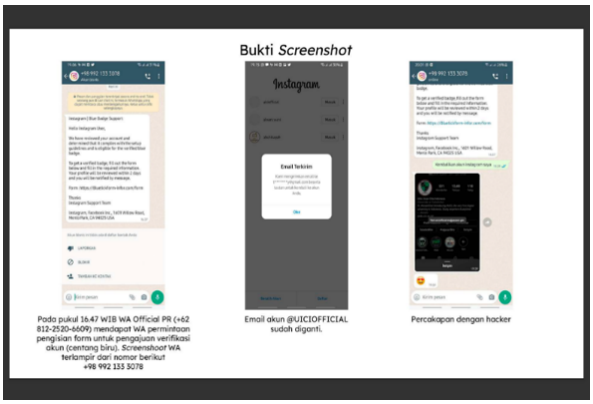


Figure 1.2. Screenshot of the chronology report on the occurrence of piracy.

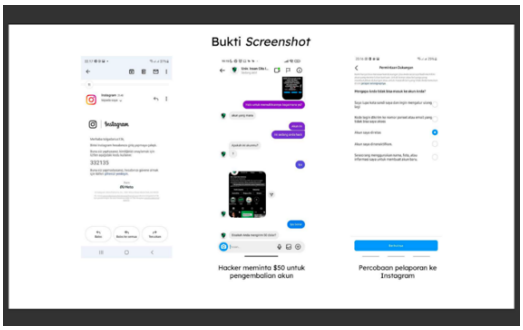


Figure 1.3. Screenshot of the blackmail attempt by the hacker and the attempt to report it to Instagram

SCIENTIFIC JOURNAL OF MEANING COMMUNICATION
Vol. 12, No 2 (2024): Agustus 2024,pp.73-84

E.ISSN:2334-4606, P-ISSN:2087-2461
http://jurnal.unissula.ac.id/index.php/makna
DOI:http: /dx.doi.org/10.30659/jikm.v12i2.39208

Besides carrying out piracy, this hacker group also carried out extortion by asking for $50 to return the account. With the threat of the account being deleted or using the account for different activities. Efforts to communicate with the hacker were also made, as well as reporting efforts to Instagram as the platform provider so that ownership of the account could be returned.

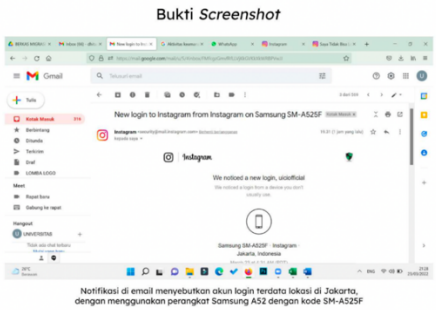


Figure 1.4. Screenshot of the hacker's location

2. Crisis Management

Based on documentation studies and crisis management reports, several steps can be taken, including:

1. **Form a crisis management team**

   UICI's official social media is managed by the Public Communications and Content Production Division (KPPK), where the social media admin is handled by four people, namely:

   - Izzaty Zephaniah (Division Head)
   - Nike Ardina (Head of Public Relations Sub Division)
   - Dhita Virgian (Head of Human Resources Division)
   - Muhammad Alwani (Social Media Management)

   Phishing was carried out on the cellphone number held by Alwani in the form of a text message to confirm the blue tick. Because social media is the responsibility of the KPPK division, the crisis handling team only involves social media admins. The aim of this strategy is to localize and prevent panic in handling.

   The division of tasks in the crisis handling team includes:

1) Izzaty as coordinator and spokesperson to University leaders and public leaders.
2) Nike develops narratives and communication strategies to the public and coordinates with the IT team in saving accounts.
3) Dhita, who has expertise in the field of information technology, is tasked with carrying out various account rescue efforts.
4) Alwani is tasked with coordinating with the IT team and communicating with hackers.

2. **Prepare reports and narratives for the public**

   The second step in handling the crisis, the team then held a joint meeting with the IT team. The results of the report are recommendations for strategies and mitigation efforts that can be carried out.

SCIENTIFIC JOURNAL OF MEANING COMMUNICATION
Vol. 12, No 2 (2024): Agustus 2024,pp.73-84

E.ISSN:2334-4606, P-ISSN:2087-2461
http://jurnal.unissula.ac.id/index.php/makna
DOI:http: /dx.doi.org/10.30659/jikm.v12i2.39208

Figure 2.5. Screenshot of the first step taken

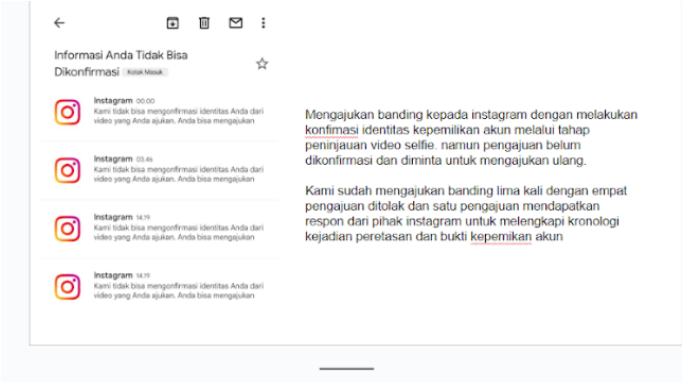


Figure 2.6. Screenshot of an attempt to appeal to Instagram regarding account ownership

In the communication strategy, the team then prepares a written report to the leadership and an explanation to the public in the form of a release. The release is then distributed to affiliated media networks. The team then recommended efforts to localize the issue by taking advantage of the same situation of attacks on state institutions, such as the Ministry of Tourism and Creative Economy which was attacked a week earlier.

Figure 2.7. Screenshot of the official release about the hacker attack

Narratives used in this release include:

SCIENTIFIC JOURNAL OF MEANING COMMUNICATION
Vol. 12, No 2 (2024): Agustus 2024,pp.73-84

E.ISSN:2334-4606, P-ISSN:2087-2461
http://jurnal.unissula.ac.id/index.php/makna
DOI:http: /dx.doi.org/10.30659/jikm.v12i2.39208

1) Apart from informing that UICI's official media account was hit by a hacker attack, it also built a narrative that it was not only UICI's account that was attacked.
2) UICI is not responsible for information during an attack that occurs.
3) Information and explanations about hacker attacks in the form of phishing and cases that often occur.
4) Building a narrative that when an account is attacked, it means the account has a large capital value.
5) Appointing a spokesperson is up to the Division Head only. This is done so that the issue does not become big.

3. Handling efforts with the IT team

Because cyber attacks are closely related to crime in the digital world, the crisis team then invited a joint team consisting of:

a) Head of the Informatics Study Program and lecturer in Informatics
b) IT Support and technology development

Several steps are taken, including:

1)Using various account reclaim efforts from various features
2)Carrying out counterattack efforts against hackers
3)Make efforts to trace the source of the attack

Meanwhile, options for steps that can be taken or recommended as a result of discussions with the IT team include:

1)Try to apply for a reclaim according to Instagram procedures up to 1 x 24 hours
2)Option to pay the ransom request of US$ 50 via Binance Wallet with full supervision of the Instagram account recovery procedure on UICI's part.
3)Create a new Instagram account with tighter security, including strengthening the security of all UICI digital assets, such as websites and other social media.

4. Take advantage of reputation-building opportunities

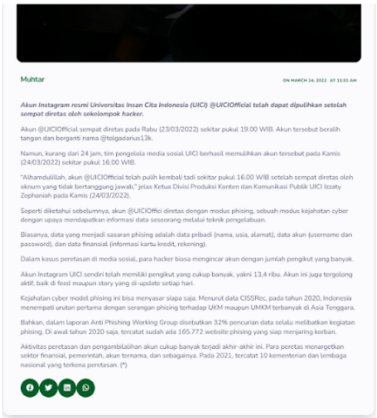
In the development of crisis theory, it is believed that a crisis has the potential to be a turning point for an organization. Where there are opportunities that, if managed well and exploited intelligently and creatively, can provide benefits to the organization. In Chinese, crisis means wei-ji which can mean two things, namely "danger" or "opportunity"(Nova et al., 2020). This opportunity was also utilized by the UICI crisis management team. Efforts to reclaim the account and deception or counterattack from the joint IT team were successful, so that the UICI Instagram account was successfully reclaimed in less than twenty-four hours.

The team then took advantage of this momentum by building a narrative that benefited UICI. In the form of building a positive reputation.

Figure 2.7. UICI official release screenshot

SCIENTIFIC JOURNAL OF MEANING COMMUNICATION
Vol. 12, No 2 (2024): Agustus 2024,pp.73-84

E.ISSN:2334-4606, P-ISSN:2087-2461
http://jurnal.unissula.ac.id/index.php/makna
DOI:http: /dx.doi.org/10.30659/jikm.v12i2.39208



Muhtar

Akun Instagram resmi Universitas Insan Cita Indonesia (UICI) @UICIOfficial telah dapat dipulihkan setelah sempat diretas oleh sekelompok hacker.

Akun @UICIOfficial sempat diretas pada Rabu (23/03/2022) sekitar pukul 19.00 WIB. Akun tersebut beralih tangan dan berganti nama @telgadarius13k.

Namun, kurang dari 24 jam, tim pengelola media sosial UICI berhasil memulihkan akun tersebut pada Kamis (24/03/2022) sekitar pukul 16.00 WIB.

"Alhamdulillah, akun @UICIOfficial telah pulih kembali tadi sekitar pukul 16.00 WIB setelah sempat diretas oleh oknum yang tidak bertanggung jawab," jelas Ketua Divisi Produksi Konten dan Komunikasi Publik UICI Izzaty Zephaniah pada Kamis (24/03/2022).

Seperti diketahui sebelumnya, akun @UICIOffici diretas dengan modus phising, sebuah modus kejahatan cyber dengan upaya mendapatkan informasi data seseorang melalui teknik pengelabuan.

Biasanya, data yang menjadi sasaran phising adalah data pribadi (nama, usia, alamat), data akun (username dan password), dan data finansial (informasi kartu kredit, rekening).

Dalam kasus peretasan di media sosial, para hacker biasa mengincar akun dengan jumlah pengikut yang banyak.

Akun Instagram UICI sendiri telah memiliki pengikut yang cukup banyak, yakni 13,4 ribu. Akun ini juga tergolong aktif, baik di feed maupun story yang di-update setiap hari.

Kejahatan cyber model phising ini bisa menyasar siapa saja. Menurut data CISSRec, pada tahun 2020, Indonesia menempati urutan pertama dengan serangan phising terhadap UKM maupun UMKM terbanyak di Asia Tenggara.

Bahkan, dalam laporan Anti Phishing Working Group disebutkan 32% pencurian data selaku melibatkan kegiatan phising. Di awal tahun 2020 saja, tercatat sudah ada 165.772 website phising yang siap menjering korban.

Aktivitas peretasan dan pengambilalihan akun cukup banyak terjadi akhir-akhir ini. Para peretas menargetkan sektor finansial, pemerintah, akun ternama, dan sebagainya. Pada 2021, tercatat 10 kementerian dan lembaga nasional yang terkena peretasan. (*)

Figure 2.8. UICI official release screenshot

The narrative that was built was to show that UICI was able to save the official UICI account in less than 24 hours. The emphasis on the words "less than 24 hours shows that in terms of expertise in handling IT, UICI is better than other institutions at the same time. Where when state institutions and several other accounts face cyber attacks in the form of taking over accounts, they can be restored in more than 24 hours. The Kemenparekraf account itself can be retrieved after three days after being hit by a cyber attack.

3. The Strategic Role of Public Relations in Building and Maintaining the Organization's Intangible Assets

In modern organizations, PR plays an important role in maintaining intangible assets that are very valuable for the organization. Intangable assets are often overlooked in strategy and planning because of their intangible - physical nature. Due to their intangible nature, many organizations neglect the governance and management of these assets. Several examples of organizations or companies that were destroyed because they did not have standards, planning or strategies for managing them. Even though these intangible assets are also equally important for the organization. According to Irma (2013), in today's era of knowledge and technology, intangible assets play a very important role in achieving competitive advantage ((Irma Anggraeni, 2013).

For PR itself, the intangable assets that are its main task and function to manage include: digital assets consisting of websites and various communication channels such as official social media platforms, brand image and reputation. This asset also has a value that can be calculated. In the case of a cyber attack on UICI, hackers not only have the potential to destroy one social media asset, but also UICI's brand image and reputation as a university that emphasizes technology as a built brand image.

From this research it was found that in the case of managing UICI's digital assets, UICI does not yet have a strategy or plan including mitigation in managing these intangible assets. However, in dealing with cyber attacks in the form of hacking social media using the phishing method, UICI has a team that acts quickly and effectively so that it can be controlled quickly. Apart from that, the sharpness of the crisis handling team in building a strong narrative made this issue an opportunity for UICI to prove the promise of its brand image as a digital campus.

E.ISSN:2334-4606, P-ISSN:2087-2461
http://jurnal.unissula.ac.id/index.php/makna
DOI:http: /dx.doi.org/10.30659/jikm.v12i2.39208

Regarding the admin's negligence in experiencing phishing, this is also a note for the social media management team. That cybercrime is very diverse. Being careful and cross checking information and requests on social media is very important. Managers must also ensure that the devices used to manage social media also need to use multiple layers of security. In the situation analysis carried out by the IT team, it was also found that when attempting to log in to a new device, the management team was found to have not used the two-stage authentication method. So the new devices used by hackers are not known in advance.

CONCLUSION

From the results of this research, it was found that issue management must be carried out strategically, planned and careful in utilizing circulating issues. So it can provide an opportunity for the organization to turn things around. Where issues that previously had the potential to become a crisis and be detrimental to the organization, actually become an opportunity for the organization to demonstrate its existence and prove the promise of the organization's brand image and reputation.

As the first digital campus in Indonesia and carrying a university brand image that prioritizes technology, this cyber attack on UICI accounts is not only detrimental to the loss of digital assets in the form of social media. But it also attacks the brand image and reputation of UICI itself. So in facing this attack, UICI must be able to prove itself to be more capable of facing attacks than other institutions. In this case, it was found that UICI was successful in dealing with cyber attacks and was also able to exploit the issue with the narrative "UICI was able to deal with cyber attacks and restored the account less than 24 hours after the attack occurred."

In the case of cyber attacks in the world of social media, it is found that the threat of similar attacks is getting bigger. There are various methods for hacking, one of which is phishing. This phishing method is difficult to identify because of the hacker's skill in convincing managers of the information offered. So social media managers must create guidelines and standards for layered security, one of which is two stages of authentication (two way authentication).

REFERENCES

Akhyar, DM, & Pratiwi, AS (2019). Social Media and Crisis Communication: Lessons from the Telecommunications Industry in Indonesia. ULTIMACOMM Journal of Communication Sciences, 11(1), 35–52. http://ejournals.umn.ac.id/index.php/FIKOMhttp://ejournals.umn.ac.id/index.php/FIKOM/about

Astasia Utari, S., Ardia, V., Fitria, D., Muhammadiyah Jakarta, U., Ahmad Dahlan, JK, Ciputat Tim, K., & South Tangerang, K. (2023). How an Organization Should Implement Risk Communication in Response to Cyber Attack in Indonesia. Journal on Education, 05(04), 14314–14328.

Bastian, DA (2014). Analysis of the Influence of Brand Image and Brand Trust on Brand Loyalty of ADES PT. Ades Alfindo Putra Faithful. In Petra Marketing Management Journal (Vol. 2, Issue 1).

Irawan, D., & Kom, S. (2020). STEALING IMPORTANT INFORMATION BY TAKING OVER FACEBOOK ACCOUNT WITH PHISING METHOD. In Journal of Computer Science & Informatics (Vol. 1, Issue 1).

Irma Anggraeni, A. (2013). THE MANAGEMENT OF INTANGIBLE ASSETS IN THE ORGANIZATION.

E.ISSN:2334-4606, P-ISSN:2087-2461
http://jurnal.unissula.ac.id/index.php/makna
DOI:http: /dx.doi.org/10.30659/jikm.v12i2.39208

Nova, F., Nuriman, DA, & Akbar, M. (2020). Crisis Public Relations (M. Wahyu, Ed.). PT. Indonesian Communications Captain.

Prayudi. (2007). Management of Future Issues and Challenges: A Public Relations Approach. Journal of Communication Studies, 4(1), 25–39. https://doi.org/https://doi.org/10.24002/jik.v4i1.229

Saputra Gulo, A., Lasmadi, S., & Nawawi, K. (nd). Cyber Crime in the Form of Phishing Based on the Information and Electronic Transactions Law. PAMPAS: Journal Of Criminal, 1, 2020.

Saputra, R. (2020). Application of Situational Communication Crisis Theory for Da'wah Organizations in Facing Crisis Situations. JOURNAL OF SYMBOLICS: Research and Learning in Communication Study, 6(2), 190–201. https://doi.org/10.31289/symbollika.v6i2.4172