CyberSecurity and Digital Forensics e-ISSN: 2615-8442
Vol. 5, No. 2, November 2022, p.77-82

CRIME ACTIONS IN THE DIGITAL WORLD IN THE FORM OF PHISING

I Kadek Odie Kharisma Putra[1], I Made Adi Darmawan[2], I Putu Gede Juliana[3], Indriyani[4]

[1,2,3,4] ITB STIKOM Bali

Email: [1]odiekharisma@gmail.com, [2]adidarmawan2705@gmail.com, [3]gedejuliana234@gmail.com, [4]indry.joice@gmail.com

Abstract

The development of information technology, especially internet communication, has brought major changes nationally, economically and culturally. The development of information technology has in turn changed social order and behavior, especially in the last decade the use of information technology has grown rapidly. On the one hand, information can provide benefits, simplify and speed up access to the information we need in every way, and can change economic models and business models. However, many negative impacts arise and cannot be avoided because the internet has become part of everyone's daily activities in accessing various kinds of information and also helping or lightening everyone's work.

Keywords*: Cyber Crime, Digital World*

1. PRELIMINARY

Information technology is capable of changing economic, cultural, political and legal realities. As the development of information technology is able to have a positive impact on many people, this has also led to the emergence of new crimes called new cybercrimes through the internet network. Where there are several people who take advantage of security holes in information technology on the internet network as a means to commit crimes, hereinafter known as cybercrime.

*Cybercrime*is a very worrying phenomenon, considering that carding, hacking, fraud, terrorism, and the dissemination of disturbing information are part of the activities of cybercrime actors.(Gulo, Ardi Saputra; Sahuri, Lasmadi; Khabib, Nawawi;, 2021).

Cybercrimes are cases of violations involving computers or communication devices as targets and commission instruments or related to the prevalence of computers.

Cybercrime or cybercrime will cost nearly 6 trillion dollars per year by 2021 according to the 2020 cybersecurity effort report. For illegal activities, cybercriminals use any network computing device as the primary means of communicating with the victim device, so attackers gain financial, publicity and other benefits by exploiting vulnerabilities in systems.

Cybercrime is improving every day, evaluating cybercrime attacks and providing protective measures with manual methods using existing business and investigative approaches often fail to control cybercrime attacks. Common forms of cybercrime are carding, hacking, phishing, terrorism. Dissemination of disturbing information is part of criminal activity in cyberspace. Lawsuits in cyberspace must have something to do with why someone commits cybercrime. Because you need to know that when cyber crimes are committed, other parties will certainly be harmed. Cybercrime is not only known as hacking or hacking, it is also known as cracking or cracking, and it should be noted that there are similarities and differences between hacking and cracking. One of the crimes committed by this cracker is phishing. Because this crime aims to exploit oneself. Phishing is a form of activity in which a person is threatened or caught with the concept of fishing for that person(Marliani, Miftahuddin Siagian;, 2017).

*Phishing*is a type of cyber fraud that aims to steal the victim's account. Of course, most cyber crimes usually start with phishing, so Internet users must always be on the lookout. Phishing also usually targets online banking users, because the use of user data and passwords does not rule out the possibility of being transferred to other online users. When users enter their user credentials and passwords into the login form, which is a fake login form, cybercriminals can find out in the form of phishing. Phishing is usually done through social media connected to the internet, such as via email or SMS and websites. Users' minimal knowledge of the information technology tools being used is what drives phishing. Phishing can occur across multiple platforms, including social media, websites, as well as applications. Currently, many people use the WhatsApp application as an application for exchanging messages, and Instagram as an application that allows users to take photos and videos and share them to be shown to many people. This is also used by irresponsible people and use it for crime. On WhatsApp, crooks try to send messages to certain numbers. This message may contain information that this number has been selected as a lottery winner, and when the user clicks on the link, they are asked to confirm via the link. The user will be taken to a malicious website that has been modified by the perpetrator. and Instagram as an

application that allows users to take photos and videos and share them to be shown to many people. This is also used by irresponsible people and use it for crime. On WhatsApp, crooks try to send messages to certain numbers. This message may contain information that this number has been selected as a lottery winner, and when the user clicks on the link, they are asked to confirm via the link. The user will be taken to a malicious website that has been modified by the perpetrator. and Instagram as an application that allows users to take photos and videos and share them to be shown to many people. This is also used by irresponsible people and use it for crime. On WhatsApp, crooks try to send messages to certain numbers. This message may contain information that this number has been selected as a lottery winner, and when the user clicks on the link, they are asked to confirm via the link. The user will be taken to a malicious website that has been modified by the perpetrator. crooks try to send messages to certain numbers. This message may contain information that this number has been selected as a lottery winner, and when the user clicks on the link, they are asked to confirm via the link. The user will be taken to a malicious website that has been modified by the perpetrator. crooks try to send messages to certain numbers. This message may contain information that this number has been selected as a lottery winner, and when the user clicks on the link, they are asked to confirm via the link. The user will be taken to a malicious website that has been modified by the perpetrator.

Similar to the Instagram application, these criminal acts can be carried out through direct messages and comments on posts. For example, in Direct Messages, a user receives a message from another user containing tempting information that the user has a chance to win a prize, and a link will be included where the user is sent to a malicious website run by an irresponsible person. Another way is by commenting on posts where one user will post a photo or video that contains information about an incident that is of interest to other users. So, other users will be curious about the complete information from the post so that other users will send a link where the user ensures that we will get complete information from the posts that have been made. So, other users will try to send a link and convince other users to click on the link because the link contains complete information about what is explained in the post. Even though the link may contain a virus or the user will be taken to a dangerous site that can threaten the security of the user accessing it. other users will try to send a link and convince other users to click on the link because the link contains complete information about what is explained in the post. Even though the link may contain a virus or the user will be taken to a dangerous site that can threaten the security of the user accessing it. other users will try to send a link and convince other users to click on the link because the link contains complete information about what is explained in the post. Even though the link may contain a virus or the user will be taken to a dangerous site that can threaten the security of the user accessing it.

Crime can happen anywhere, even in cyberspace. So users must always be vigilant when using the internet because there are still many people who do not have sufficient knowledge to access the internet and irresponsible elements try to take advantage of these people. Ignorance of users about things on the internet that makes users fall victim to cybercrime. Therefore, when exchanging messages with strangers or obtaining information sent by others, users must always be vigilant and ensure that users can verify the accuracy of the information provided.

2. LITERATURE REVIEW

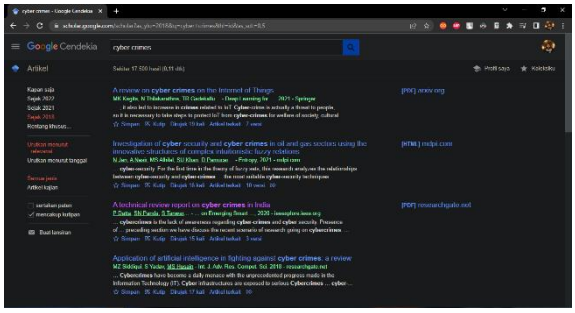
The literature review used in this article is the theory that underlies the article. In addition, literature review is also carried out through national and international research journals. When writing this article, the author first tries to connect several journals to connect with this article. Journals referred to by the authors are:

Journal of Ardi Saputra Gulo, Sahuri Lasmadi, Kabib Nawawi, Faculty of Law, Jambi University with the title:*CyberCrime*in the Form of Phishing under the Information and Electronic Transactions Act. This journal covers cyber crimes such as phishing under the Information and Electronic Transactions Act. The results of this journal are legal arrangements for cyber crime in the form of phishing based on the Information and Electronic Transactions Law subject to Article 35 in conjunction with Article 51 Paragraph (1) and Article 28 Paragraph (1) in conjunction with Article 45A Paragraph (1). , the legal policy against cybercrime in the form of phishing based on the Information and Electronic Transactions Law amends the law on ITE by formulating the concept of phishing and changing the contents of Article 35.

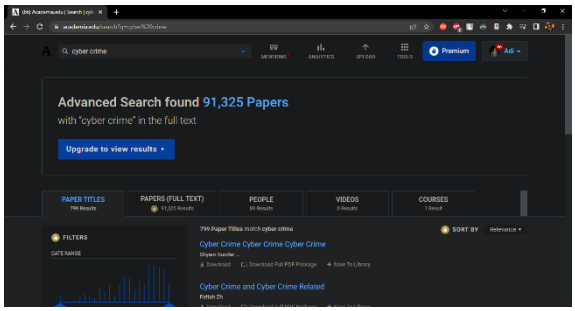
3. RESEARCH METHODS

Given these problems, this paper examines the development of cybercrime in the form of phishing using a systematic review method. In this discussion, a systematic review is carried out by first selecting and determining a list of journals related to cyber crime. Starting from looking for journals that discuss the digital world, technological developments, and continuing to cyber crime or cybercrime, in the end the author gets a journal that discusses digital world crimes in the form of phishing.

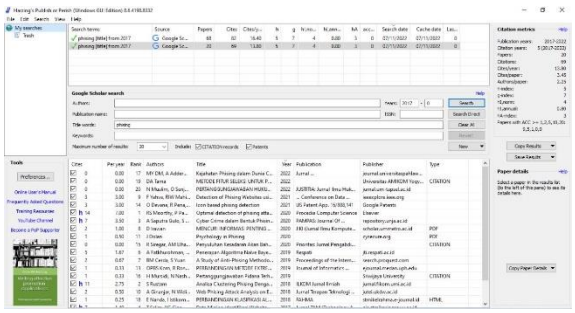
The following are some screenshots when searching for several journals for the needs of writing this scientific work:



Picture1Journal search on Google Schoolar



Picture2Journal Search in Academia



Picture3Journal search via Publish or Perish

4. RESULTS AND DISCUSSION

Cyber crimes with phishing methods are often found on social media platforms. Social media is the main target for hackers to carry out their actions because social media has many users and is very free without any filter. Lack of education on the use of social media makes it easier for hackers to commit fraud. Social media with the most phishing incidents are WhatsApp and Facebook. Facebook social media is often used to steal data from users. Hackers take advantage of Facebook views to create fake duplicate views.

When a user accidentally enters a fake page and registers or logs in, the hacker will immediately get privacy data from the user.

Apart from social media, websites are also one of the targets of hackers for phishing. By utilizing advertisements and fake icons on websites that users can click on, users will be directed to a link that has been configured by hackers to steal data. Very many cases like this, especially among students. The fraud that has occurred is the acceptance of free quotas organized by the Ministry of Education and Culture. This is used by hackers to create fake links containing information on receiving free quotas. Currently, cyber crimes using phishing methods are regulated in the Information and Electronic Transactions Act (UU ITE). With this law in place, when someone is identified as committing phishing, then the person will be subject to a punishment in accordance with what is stated in the law. Victims can report this crime to the appropriate authorities for investigation.

Based on the results that have been analyzed, phishing crimes can be carried out from various examples of attacks such as through various types of social media and websites, if users are not careful in using social media and visit websites that have been modified by perpetrators, it is very easy for perpetrators to retrieve user privacy data. . From the several cases described, phishing acts often occur on social media platforms such as WhatsApp and Facebook where many actors carry out their actions on behalf of official agencies and as if they are acting from official employees of these agencies where if they are not aware that the targeted user is following the wishes of the perpetrator. to make the action successful.

Table1Fraud Proof Screen Notes

No.	Application	Date/Time	Shape
1.	WhatsApp	27-09-2022/13:42:00 WITA	*Chat*and Links
2.	SMS	29-11-2021/02:33:00 WITA	*Chat*and Links
3.	WhatsApp	07-11-2022/17:10:00 WITA	*Chat*and Fig

The results of the research conducted are based on searching data about genuine fraud that occurs on social media platforms. The deception that occurs consists of receiving messages from hackers under the guise of offering benefits to the recipient of the message. Here is the real proof of receiving fake messages from hackers.

Picture4Evidence of Fraud Cases on WhatsApp (Chat and Link)

Picture5Evidence of Fraud Cases in SMS (Chat and Link)

Picture6Evidence of Fraud Cases on WhatsApp (Chat and Pictures)

The perpetrators of phishing carry out their actions by using links or icons with pictures to facilitate their actions so that users believe that the things given by the perpetrators are official. From this, the perpetrator has gained the user's trust so that the perpetrator can continue his action to obtain privacy data and fulfill wishes that can harm the user. With the explanation above, the author recommends that users always be careful in the digital world and not visit carelessly, especially using social media and websites, it is hoped that users will always ensure that if there is context or something that is fake or distorted, it can be checked for officialness through official media from the context. and can report to the authorities so that the relevant article can be imposed.

5. CONCLUSIONS AND RECOMMENDATIONS

Cybercrimes are cases of violations involving computers or communication devices as targets and commission instruments or related to the prevalence of computers. The forms of this crime are so diverse that hackers can choose the method they want to use to carry out crimes in cyberspace.

*Phishing*is a type of cyber fraud that aims to steal the victim's account. Phishing acts often occur on social media, especially on the WhatsApp and Facebook applications. One of the cases of phishing crimes that have occurred is the case of receiving free quotas organized by the Ministry of Education and Culture.

All cybercrime acts are regulated in the Electronic Information and Transaction Law (UU ITE). With this law in place, when a person is identified as committing phishing or other cybercrime, that person will be subject to a penalty according to what is stated in the law.

Acts of cyber crime can target various groups, ranging from the community, organizations, governments, and others. Therefore, as a user who frequently surfs in cyberspace, you should always be careful and not easily believe everything that exists in cyberspace. In addition, users must also learn every new thing that is in cyberspace in order to prevent being affected by criminal acts.

BIBLIOGRAPHY

CASCAVILLA, G., TAMBURRI, D. A., & VAN DEN HEUVEL, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers and Security, 105, 102258. https://doi.org/10.1016/j.cose.2021.102258.

AL-KHATER, W. A., AL-MAADEED, S., AHMED, A. A., SADIQ, A. S., & KHAN, M. K. (2020). Comprehensive review of cybercrime detection techniques. IEEE Access, 8, 137293–137311. https://doi.org/10.1109/ACCESS.2020.3011259

CH, R., GADEKALLU, T. R., ABIDI, M. H., & AL-AHMARI, A. (2020). Computational system to classify Cyber Crime offenses using machine learning. Sustainability (Switzerland), 12(10). https://doi.org/10.3390/SU12104087

FAHLEVI, M., SAPARUDIN, M., MAEMUNAH, S., IRMA, D., & EKHSAN, M. (2019). Cybercrime Business Digital in Indonesia. E3S Web of Conferences, 125(201 9), 1–5. https://doi.org/10.1051/e3sconf/201912521001

KOTO, I. (2021). IJRS: International Journal Reglement & Society Cyber Crime According to… Cyber Crime According to the ITE Law. August, 103–110. http://jurnal.bundamediagrup.co.id/index.php/ijrs

PARANDE, S. (2021). and Engineering Trends. Engineering, 6(1), 2020–2022.

SADIQ, A., ANWAR, M., BUTT, R. A., MASUD, F., SHAHZAD, M. K., NASEEM, S., & YOUNAS, M. (2021). A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. Human Behavior and Emerging Technologies, 3(5), 854–864. https://doi.org/10.1002/hbe2.301

RUSTAM, S. (2018). Analisa Clustering Phising Dengan K-Means Dalam Meningkatkan Keamanan Komputer. ILKOM Jurnal Ilmiah, 10(2), 175–181. https://doi.org/10.33096/ilkom.v10i2.309.175-181.

HAYATI, M., & FATA, D. (2021). Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit Melalui Teknik Phising. Djtechno Jurnal Teknologi Informasi, 2(1), 21–28. https://doi.org/10.46576/djtechno.v2i1.1252.

EFENDY, Z., PUTRA, I. E., & SAPUTRA, R. (2019). Asset Rental Information System and Web-Based Facilities At Andalas University. Jurnal Terapan Teknologi Informasi, 2(2), 135–146. https://doi.org/10.21460/jutei.2018.22.103

GULO, A. S., LASMADI, S., & NAWAWI, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. PAMPAS: Journal of Criminal Law, 1(2), 68–81. https://doi.org/10.22437/pampas.v1i2.9574

Informatika Universitas Buddhi Dharma Jl Imam Bonjol No, T., & Ilir Tangerang Banten, K. (2017). Data Mining Identifikasi Website Phising Menggunakan Algoritma C4.5 Tomy Salim 1) Yo Ceng Giap 2). Technology Acceptance Model, 8, 130–135.

MISHRA, A., & FANCY. (2021). Efficient Detection of Phising Hyperlinks using Machine Learning. International Journal on Cybernetics & Informatics, 10(2), 23–33. https://doi.org/10.5121/ijci.2021.100204.

MARLIANI, SIAGIAN, M. (2017). Jurnal Pendidikan dan Konseling. Al-Irsyad, 105(2), 79. https://core.ac.uk/download/pdf/322599509.pdf.

IRAWAN, D. (2020). Mencuri Informasi Penting Dengan Mengambil Alih Akun Facebook Dengan Metode Phising. JIKI (Jurnal Llmu Komputer & Lnformatika), 1(1), 43–46. https://doi.org/10.24127/jiki.v1i1.671.

MOORTHY, R. S., & PABITHA, P. (2020). Optimal Detection of Phising Attack using SCA based K-NN. Procedia Computer Science, 171(2019), 1716–1725. https://doi.org/10.1016/j.procs.2020.04.184.

RAMADHAN, A., ALHAFIDH, M. A., & FIRMANSYAH, M. D. (2022). Penyebaran Link Phising Kuota Kemendikbud Terhadap Kesadaran Informasi Pribadi Di Kalangan Mahasiswa UNINUS. Kampret Journal, 1(1), 11–15. https://doi.org/10.35335/kampret.v1i1.9.

MUSLIM, N., SENJAYA, O., HUKUM, F., & KARAWANG, U. S. (2022). Pertanggungjawaban Hukum Platform Media Sosial Terhadap Korban Phising Melalui Mass Tagging. 9(2), 955–963.

ALMSEIDIN, M., ABU ZURAIQ, A. M., AL-KASASSBEH, M., & ALNIDAMI, N. (2019). Phishing detection based on machine learning and feature selection methods. International Journal of Interactive Mobile Technologies, 13(12), 71–183. https://doi.org/10.3991/ijim.v13i12.11411

CHARAN, A. N. S., CHEN, Y. H., & CHEN, J. L. (2022). Phishing Websites Detection using Machine Learning with URL Analysis. Proceedings - 2022 IEEE World Conference on Applied Intelligence and Computing, AIC 2022, 808–812. https://doi.org/10.1109/AIC55036.2022.9848895

ALABDAN, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future Internet, 12(10), 1–39. https://doi.org/10.3390/fi12100168

RACHMAWATI, D. (2014). Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber. Jurnal Ilmiah Saintikom, Universitas Sumatera Utara, Medan, 1978–6603, 209–216

DOLAN, J. (2020). Psychology in Phishing Jonathan Dolan IASP 470 System Security Capstone March 17

LATIFAHI, F. N., MAWARDI, I., & WARDHANA, B. (2022). Ancaman Pencurian Data (Phishing) Di Tengah Trend Pengguna Fintech Pada Pandemic Covid-19. Islamic Banking and Finance Journal, 6(1), 73–85. https://doi.org/10.21070/perisai.v6i1.

WAHYUDI, D., NISWAR, M., (2022). Website Phising Detection Application Using Support Vector Machine (Svm). Journal of Information, 5(2). https://media.neliti.com/media/publications/432156-none-2b0098ce.pdf