

DISTRIBUTION OF PHISHING LINKS OF MINISTRY OF EDUCATION QUOTAS ON PERSONAL INFORMATION AWARENESS

Joseph Paul John Jansz

Sekolah Tinggi Ilmu Hukum dan Politik Pelopor Bangsa

Keywords

Phishing Link,
Ministry of Education,
Culture Quota,
Information

Hoax are becoming one of the things that are increasingly found in today's digital era. The types of hoaxes circulating in the community are also very diverse, one of which is the Ministry of Education and Culture quota phishing link hoax. This hoax is targeting the personal data of students, students, and people who need internet quota during this pandemic. For this reason, in this study we want to find out how aware Uninus students are about the importance of personal data security. This study uses a qualitative approach with a descriptive method, and the data collection technique is through interviews and questionnaires. This type of research data is primary data, and the research subjects are Uninus students. The object of this research is the awareness of Uninus students towards personal information, and the informants are class A students of the Communication Studies study program. As a result, the informants admitted that they had received phishing links from the Ministry of Education and Culture quota and knew that phishing links could threaten personal data and could also cause material and non-material losses. They also know the steps to avoid becoming a victim of phishing links and how to identify phishing links circulating in the community. The informants admitted that they are very aware of the importance of personal information security.

Email : joseph.paul@gmail.com

Copyright 2021 Fox Justi : Jurnal Ilmu Hukum

1. INTRODUCTION

In today's era, which is better known as the 4.0 era, in which we must prepare ourselves for the 5.0 era. We are required to be able to recognize and master the technology that has been very far in development. What used to be factory employees had to be replaced by robot machines because technology had developed very rapidly. Previously, if you wanted to meet you, you had to meet in person, now you only need to use smartphone technology with long distance calls. As said by Zuria, FS & Totok Suyanto (2018: 565) The development of technology and information has become a part of the entire world community, especially at the time of the emergence of the internet. The internet has made a big change in people's lives, with the internet it makes it easier to get information and communicate quickly and cheaply. However,

If we can not make the best use of technology, there will be many negative sides. With the internet, it can also have a negative impact, because some information on the internet is made with the aim of provoking so that it creates conflict in society. The content of the news is usually made based on someone's thoughts alone and some of the news posted on the internet cannot be confirmed, so the news often contains false news or hoaxes and hate speech. Zuria, FS & Totok suyanto (2018: 566) for example, such as the existence of hoaxes on social media where the whole world uses social media, and only a few percent do not know social media. Maybe now the proverb "Language is sharper than a sword" is not appropriate if it becomes a reference in social life, would be more appropriate if "type your finger is sharper than a sword" why do I dare say that? Because hoaxes in the media are very dangerous, they can cause propaganda, fights, and even losses.

according to Herlina. M & Arbi Cristional Lokananta (2018:103) The term hoax describes false information, slander, or the like. At first, hoax news often afflicted groups of artists or public figures on social media who were attached to false and confusing information whose truth was not yet clear. In Indonesia, the term hoax itself has been widely used by infotainment media on celebrity or public figure

Fox Justi is licensed under a Creative Commons Attribution-NonCommercial 4.0 International



License (CC BY-NC 4.0)

information in order to increase the rating of the infotament media. In an era full of social media, the term Hoax is increasingly known as it is becoming easier to find news stories on social media and information sites. Since then the news that is still confusing the truth is often said to be hoax news. As we know now, the person who spreads hoax news is not only intended for public figures, there are many targets, there are those who want to bring down a person, agency, group, group, and others. The circulation of hoax news is easy, especially in people whose literacy levels are still very low. Usually, they easily take information for granted without finding out the truth of the information. They even share or share without considering the consequences of the information they receive. The public was finally consumed by the news in the confusion of news, provocation and mutual suspicion (Maulana Luthfi, 2017: 210). especially in people whose literacy levels are still very low. Usually, they easily take information for granted without finding out the truth of the information. They even share or share without considering the consequences of the information they receive. The public was finally consumed by the news in the confusion of news, provocation and mutual suspicion (Maulana Luthfi, 2017: 210). especially in people whose literacy levels are still very low. Usually, they easily take information for granted without finding out the truth of the information. They even share or share without considering the consequences of the information they receive. The public was finally consumed by the news in the confusion of news, provocation and mutual suspicion (Maulana Luthfi, 2017: 210).

Hoax is one of the great enemies of all society in this day and age. There are also many types, such as fake content, false news, manipulated content, to fake links or commonly called phishing links. Phishing is a person's activity that aims to obtain personal information from internet users by deceiving someone using a fake web that looks almost similar to the real web (Wibowo, MH & N. Fatimah, 2017:1) Phishing is one type of hoax that often appears on the internet. According to Wibowo and Fatimah (2017: 1), phishing is one type of cyber crime, which currently often occurs via computer networks. Usually, phishing links are spread with attractive lures, so that people are tempted to open the link and submit their personal information. One of the phishing links that often appears is the Ministry of Education and Culture Quota Assistance Link.

As we know, during the Covid-19 Pandemic, the government forbade gathering activities, including schools. And that's why the government socializes online teaching and learning activities and provides free quota subsidies to support these learning activities. Unfortunately, this phenomenon is exploited by cybercriminals to profit from users' personal information. In addition, public awareness of personal information is still very poor. Many people don't really care about this kind of threat, and think that it is a trivial thing and doesn't need to be worried (Wibowo, MH & N. Fatimah, 2017:2)

Personal Information is one of the most important things in a human's life, because the information involves very sensitive matters and should only be known by oneself. Personal information includes several things, such as full name, place and date of birth, home address, residence number, cellphone number, and so on. It is this data that should be private and protected. Otherwise, it can lead to misuse of data and can be a loss. Cases that can arise due to theft of personal information are hacking, email spamming, fraud, data manipulation, data interception, and others (Aswandi, R & Muchin, PRN, 2020:169)

Awareness of the importance of confidentiality of personal information should be the responsibility of every individual, including the intellectual generation such as students. According to Huluwati, W & Djibran, MR (2018: 73) A student is someone who enters adulthood, and at that time has responsibility for his life and development. Students can also be interpreted as people who are studying at a university. Currently, all student activities involve technological processes, such as creating bank accounts, registering for universities, lectures, and others. However, although most of their activities use technology, it is undeniable that there are still many who do not care about the security of personal data. Therefore, we are interested in examining how aware millennials, especially students, are about the importance of personal data security. Moreover, the millennial generation is the generation that will continue to live side by side with technological advances. This research is also based on the fact that cyber crimes such as spreading phishing links are increasing in number from time to time. Education and socialization are one way to reduce the possibility of cyber crimes against the millennial generation. Previous research has raised the effectiveness of personal data threat education

on social media. As a result, education using the video format showed successful results, where 89% of them admitted to being educated through the show (Pane., et al, 2021:417) Although the phenomenon of personal data threat has been raised by the previous research, the main discussion between this research and the research is very different. This study wants to find out how aware UNINUS students as millennials are against personal threats that threaten through phishing links that are widely spread on social media.

2. METHOD

This study uses a qualitative research approach. According to Gumilang, S. G (2016: 145), qualitative research is a multiple method in focus, which involves an interpretative and mandatory approach to the subject matter and also this research works naturally which seeks to understand and interpret phenomena given by people. to him. In addition, this study also uses descriptive qualitative research methods. As explained by Zaluchu, E. S (2021:256), qualitative descriptive research methods are usually presented descriptively and are relative, theoretical and use a lot of theoretical analysis. This study seeks to describe the phenomena that occur today, with a focus on research on the Impact of the Spread of Phishing Links for Quotas from the Ministry of Education and Culture on Personal Information Awareness among UNINUS Students. The source of this research uses premier data, which is data obtained from the distribution of research questionnaires shown to the research sample (Budiarto samsul 2020:16).

The subjects of this research are people who have the status and are registered as students of the Nusantara Islamic University. While the object of this research is students' awareness of personal information. Informants from this study were specific students of class A Communication Studies study program Uninus, amounting to 31 people. Data collection techniques in this study used interview techniques and questionnaires. This study also uses data analysis techniques. According to Rizali, A (2019:84) data analysis is an effort to search for data in the field, systematically organize the results found in the field, present the results of the field findings, and seek meaning or conclusions. More specifically, we use Miles and Hubberman model data analysis. According to Miles and Hubberman, (in Hardani, et al 2020:163) data analysis is divided into 3 flows, namely data reduction, data presentation, and drawing conclusions.

3. RESULTS AND DISCUSSION

In this era, we should be aware of the dangers that threaten the theft of personal data. Especially in the midst of a pandemic where the need for internet quotas is increasing, the spread of phishing links for quotas from the Ministry of Education and Culture is increasingly spreading among the community. The spread of the link targets young people who are still in school and students who need a quota to study and study.

Therefore, this study seeks to determine the impact of spreading the Ministry of Education and Culture's quota on information awareness of Nusantara Islamic University students. From the data we managed to collect, we selected 2 informants whose answers were representative of all informants who had been interviewed and filled out the questionnaire. We disguised the informant's name as initials for mutual convenience.

First, we asked about the distribution of the Ministry of Education and Culture's quota phishing link to informants. And the answers from informants A and B stated that they had "never received" a phishing link for the Ministry of Education and Culture quota from the WhatsApp social media group and personal chat from their friends. From this statement, it can be seen that the spread of the Ministry of Education and Culture quota link is very wide on public social media and many are affected by the hoax. This is in line with Juditha (2018:32) that social media is the place where the most hoaxes are spread. Second, we asked about the experience of the informants after receiving the Kemendikbud Quota phishing link.

According to the answer put forward by Informant A:

"Warning, first perception of fraud"

According to the answer put forward by Informant B:

Fox Justi is licensed under a Creative Commons Attribution-NonCommercial 4.0 International

"At first it became a big question mark, right, is this true or not?" I kept thinking "just try it, it's just for real" but here and there you know that it's a fake website, so it's more like "okay this one is fake, it means I can't fill it out because it's dangerous"

From the statement of informant A above, it can be said that the informant has suspicions about the link he received. He even knew that the link was a fraudulent link that could compromise his personal information. In contrast to informant B, who initially did not know what danger lurked him. And he only realized when he knew that the web was a fake web over time. The thing experienced by informant B is very often the case with people who are not aware of the characteristics of the fake web with the real one. This is a gap as well as an opportunity for internet criminals, namely taking advantage of the innocence of internet users. This is in line with Rachmawati (2014: Third, we asked whether or not the informant knew about phishing links that could steal personal data. They both said in unison "Yes, I know". After that, we asked about the informants' knowledge of the dangers of targeting phishing links that were spread. This aims to find out how aware the informants are of the security of personal data.

The answer put forward by Informant A:

"Threats related to personal matters such as finances, identity, and matters on behalf of the individual concerned"

From the answers above, it can be seen that the informants are aware of the importance of personal information security. The informants also know that the threats that can arise from being exposed to a phishing link hoax are very detrimental, such as financial problems, identity, and misuse of data by irresponsible parties. This is in line with Rachmawati (2014:211) that internet criminals commonly called phishers usually threaten personal data, such as account passwords and credit card numbers. These negative impacts can arise not only now, but also in the future. To find out more about the awareness of Nusantara Islam University students towards the security of personal information, we asked about the steps so that no more victims were exposed to the hoax link.

Answer from Informant A:

"Seeking out related information for comparison. Do not immediately follow without knowledge "

Answer from Informant B:

"Knowledge of ICT is important, so there's nothing wrong if we study it, so we know if this one will have this impact, that one will have that impact, basically knowledge is important"

From the two answers above, we can see that the steps to avoid becoming a victim of phishing links are not to go along with it and immediately trust the information we receive. We must be more aware of the spread of the Ministry of Education and Culture's quota phishing links and must know the knowledge, especially knowledge of Information communication technology which will be very useful as a provision in this day and age. According to Rachmawati (2014: 216) there are several steps to avoid the trap of phishing links, including typing personal data on secure websites, being aware of unsolicited emails, paying attention to URL addresses, and installing anti-virus as well as security patches on personal computers. We also asked how we could identify the phishing link of the Ministry of Education and Culture quota according to the opinion of the informant, and the informant's answer was

Answer from Informant A:

"Thinking critically and skeptically"

From the informant's answer, he argues that in order not to become a victim of phishing links, think critically and be vigilant. Usually, phishing web links have a domain that is very similar to the original web. However, we can tell the difference by looking at the web as a whole. Where, fake websites usually have a very bad layout and user interface. In addition, the web domain can be very different, where if the original web from the ministry usually uses .Go.id as the official web domain, while phishing web links use the .co.id domain as the domain. The domain is a free domain that is usually used for personal needs and non-profit organizations. From this, we can conclude that we must be careful with the websites we enter, because fake websites have been designed in such a way as to trick users into entering into phishing methods. It will be very dangerous if users are not careful in accessing the internet and fall into a phishing trap (Irawan, 2020: 46).

Finally, we also asked how aware the informants were after knowing the importance of personal data security, as well as the impact and how to prevent it. They argue:

The answer put forward by Informant A:

“Very conscious”

the informant admitted that he was very aware of the importance of personal data security, supported by knowledge of the impacts that would be caused and how to prevent them. This is a very good thing for the younger generation who are very aware of the security of personal data and are provisions for living in this technological era. This must continue to be improved and educated to the public, considering that fake web sites are now increasingly similar and make victims unaware that they have become victims and are harmed (Irawan, 2020:44)

4. CONCLUSION

With the development of increasingly rapid and sophisticated technology, it makes it easier for someone to do something, not to mention committing crimes such as theft of personal data through the lure of free quota phishing links. Based on the data we have taken from the two informants, we can conclude that personal data information is very easy to steal with current technological developments. And also this phishing link spreads to students very easily through social media, from several informants they admit that they have received the phishing link, this proves that there are still a lot of distributions of this phishing link. Personal data information is very important, because if other people take personal information data, our own security can be threatened.

5. REFERENCE

1. Aswandi, R., Muchin, PRN, & Sultan, M. (2020). Protection of Data and Personal Information Through the Indonesian Data Protection System (Idps). *Legislative Journal*, 3(2), 169-170.
2. Budiarto, S. (2020). Marketing Strategy Using Mark Plus & Co Approach at Kandatel Jakarta. *Journal of Electrical and Aviation Industry*, 3(1). 16-17.
3. Fatimatus, zuria. S., & Totok Suyanto. (2018). A study of the intellectual skills of UNESA students in recognizing hoax news on social media. *Moral and Citizenship Studies*, 6(2), 565-567.
4. Gumilang, GS (2016). Qualitative research methods in the field of guidance and counseling. *Counseling Focus Journal*, 2(2). 145-146.
5. Hardani, HA, Ustiawaty, J., Istiqomah, RR, Fardani, RA, Sykmana, DJ, & Auliya, NH (2020). *Book of Qualitative & Quantitative Research Methods*. Yogyakarta: CV. Group Science Library.
6. Herlina, M., & Lokananta, AC (2018). The impact of hoax information on social media on the level of conflict and attitudes in adolescents. *Promedia (public relations and communication media)*, 4(2), 103-104.
7. Hulukati, W., & Djibran, MR (2018). Analysis of Student Development Tasks at the Faculty of Education, State University of Gorontalo. *Bikothetics (Guidance and Counseling: Theory and Practice)*, 2(1), 73-74.
8. Maulana, L. (2017). The Holy Book and Hoaxes: The Qur'an's View in Responding to Fake News. *Insights: Scientific Journal of Religion and Socio-Cultural*, 2(2), 210-211.
9. Pane, CGG (2021). EDUCATION TO STUDENTS OF SMA NEGERI 1 MIMIKA TO OVERCOME ONLINE MEDIA THREATS IN PERSONAL DATA. *CONSTELATION: Convergence of Information Technology and Systems*, 1(2), 417-418.
10. Rijali, A. (2019). Qualitative data analysis. *Alhadharah: Journal of Da'wah Science*, 17(33), 84-85.
11. Valentina, E., & Sari, WP (2019). Study of Verbal and Non Verbal Communication Game Mobile Legends: Bang Bang. *Connections*, 2(2), 301-302.
12. Wibowo, MH, & Fatimah, N. (2017). PHISHING THREATS TO SOCIAL MEDIA USERS IN CYBER CRIME. *JOEICT (Journal of Education and Information Communication Technology)*, 1(1), 1-2.
13. Zaluchu, SE (2021). Research Methods in Religious Scientific Journal Manuscripts. *Journal of*

- Life News Theology, 3(2), 256-257.
14. Juditha, Christian (2018) Hoax Communication Interaction in Social Media and Anticipation of Hoax Communication Interactivity in Social Media and Anticipation, Pekommnas Journal, 17(1), 31-44
 15. Rachmawati, D. (2014). Phishing As A Form Of Threat In The Cyber World. Journal of SAINTIKOM Vol, 13(3), 211-216.
 16. Irawan, D. (2020). STEAL IMPORTANT INFORMATION BY TAKING OVER FACEBOOK ACCOUNTS WITH PHISING METHODS. JIKI (Journal of Computer Science & Informatics), 1(1). 45-46.