Google's Legal Responsibility in Displaying Phishing Ads Through Google AdWords

Regita Amanah Huzairin[1*], Mochammad Tanzil Multazam[2],Rifqi Ridlo Phahlevy[3],Farhod Ahrorov[4]
*Correspondence author email:regitahuzairin48@gmail.com
[1,2,3]Department of Law, University of Muhammadiyah Sidoarjo, Indonesia
[4]Samarkand branch of Tashkent State University of Economics, Samarkand, Uzbekistan

Abstract. The discovery of phishing website advertisements served by the Google AdWords advertising platform, which then raises the question of whether Google AdWords has filtered the advertisements that have been submitted and will be served on its advertising services and whether Google as the provider of the Google AdWords advertising platform can be punished for phishing advertisements that appear in its advertising services. Phishing is a criminal tool that functions to steal sensitive information belonging to users and commit crimes on the Internet for the benefit of phishers who can harm victims. Provisions regarding phishing are regulated in Law No. 11 of 2008 concerning Electronic Information and Transactions. The research method used is the normative juridical method with a statutory approach. Using deductive analysis to analyze legal materials. The results of the research show that Google must be responsible for its advertising platform, namely Google AdWords for advertising phishing websites, where this has violated the rules in Law No. 11 of 2008 concerning Electronic Information and Transactions Article 28 Paragraph (1).

Keywords - Phishing Ads, Google, Google AdWords

1 Introduction

Along with the development of increasingly modern times, advertising ideas or businesses is increasingly easy to do online using existing advertising platforms including phishing website advertising.[1] One of the online advertising platforms is Google AdWords owned by Google. Advertising phishing websites through Google AdWords services is increasingly easy to find from time to time, especially phishing websites that use Google AdWords advertising services, are always displayed on the top page of google search which of course causes losses to the parties, both the original website owner (*Non Phishing*) and visitors or internet users who think that the website they are accessing is the original website they are looking for.

Phishing crimes are always growing and becoming more sophisticated criminal tools from time to time carried out by criminals to steal sensitive information belonging to users and commit crimes on the Internet for their individual interests which can then harm victims.[2] There are actually 2 popular services that can protect Internet users from visiting phishing sites such as Google Safe Browsing Services.[3] and Microsoft Smart Screen service.[4] Both services receive and provide information to clients with blacklisted URLs so that users will be protected from accessing URLs or websites that have been blacklisted. However, both

B. Sobirov et al. (eds.), *Proceedings of the 2nd International Conference on Advanced Research in Social and Economic Science (ICARSE 2023)*, Advances in Social Science, Education and Humanities Research 842,
https://doi.org/10.2991/978-2-38476-247-7_53

protection services still have shortcomings, namely reactive. What is meant by reactive is that phishing URLs found can only be blacklisted if they have appeared elsewhere and have been reported by users. For new URLs or Phishing Websites, they have not been blacklisted, so users can still access and can become victims of the phishing website.

Phishing does not only occur in Indonesia, but is also rampant in various countries. The Indonesian Internet Domain Name Manager (PANDI) explained that the number of reports about phishing in Indonesia received from April to June 2022 reached 5,579 phishing reports, this number has increased very rapidly when compared to reports submitted from January to March which only amounted to 3,180 reports. Then, it was noted that in April 2022 there were phishing reports with a total of 2,122 which were unique attacks on websites, 45 cases regarding the use of special domains, and 54 cases regarding brand names or certain organizations.

Phishing activities aim to lure Internet users into providing their personal information without the potential victim realizing it.[5] Phishing is used to obtain personal or sensitive information such as login username, login password and detailed data from credit cards by using an impersonation method so that it is considered a genuine website.[6] Then internet users will be asked to provide their personal information, and in this process the information will be sent directly to the perpetrator and data theft occurs.[7] Phishing applies social engineering and technical deceptions to steal users' personal data.[8] The most common phishing method used by perpetrators is to create fake websites that resemble legitimate websites, such as online store websites, bank websites, or even other reputable service websites. The fake website link is then spread by criminals using their own phishing website advertising, phishing emails, social media, and text messages.[9]

Phishing offenders often use websites to carry out these actions. Website is a collection of pages that are connected to each other and can be accessed easily via the internet network using a unique address that needs to be included in the search engine, namely the URL (Uniform Resource Locator).[10] Phishing that uses web URLs tends to make the web in the link look very authentic and similar to the original so that if the user is not careful when accessing the Web, the data entered on the login page can be stolen by irresponsible parties, namely the Phishing link maker.[11] Thus, Phishing is a method of online crime committed by criminals by stealing data for their individual interests which can then harm the victim.[12]

Phishing crimes have several stages and modus operandi carried out by the perpetrators of phishing crimes in the cyber world. Phishers who carry out their activities to deceive and get potential victims on online platforms with the aim of stealing their personal data, can be subject to criminal sanctions such as those in the legal arrangements for phishing offenders in the Criminal Code Article 378 which explains that parties who carry out activities with the aim of unlawfully benefiting themselves or others using false names, deception, and various kinds of lies can be subject to imprisonment and Law No.11 of 2008 concerning Electronic Information and Transactions Article 35 jo. Article 51 which explains that any person who intentionally and without rights manipulates or creates electronic documents so that they are considered as authentic data can be subject to imprisonment and fines.

Research related to phishing has been conducted by previous researchers. However, the research is still related to the analysis of Legal Arrangements Against Cyber Crime in the Form of Phishing, and Legal Policy Against Cyber Crime in the Form of Phishing.[13], then models

of phishing attacks on Fintech service users, and ways or stages regarding the anticipation of phishing attacks.[14], as well as sources of phishing threats, how phishing works, and how to prevent phishing. So that existing legal research still focuses on general knowledge, not specifically on existing advertising service provider platforms. So it is important for researchers to conduct research on Phishing on advertising service platforms, especially those on GoogleAdswork such as advertising rules using its advertising services, accompanied by legal regulations that have been applied and related.

The focus of this research is on whether Google AdWords has filtered the advertisements that have been submitted and will be displayed on its advertising services? And whether Google as the provider of the Google AdWords advertising platform can be punished for phishing ads that appear in its advertising services?

The purpose of this research is to understand the application of ad filters by Google AdWords when serving ads and to find out about Google's role as a provider of the Google AdWords advertising platform and its legal responsibilities regarding the appearance of phishing ads in its advertising services. This research article is important to do so that people are more careful when doing activities on the internet media so that they are not trapped in crime, fraud and avoid cyber crime, especially phishing. And as a guideline for advertising platform services that still advertise phishing website links, regarding the legal consequences that can be borne.

2 Methods

The research method used in this research proposal is the normative juridical method with a statutory approach (statue approach). Using deductive analysis to analyze primary and secondary legal materials, namely:

2.1.Primer :

a. Law No. 11/2008 on Electronic Information and Transactions Article 28 Paragraph (1)
b. Law No. 11/2008 on Electronic Information and Transactions Article 32 Paragraph (2) jo. Article 48 Paragraph (2)
c. Law No. 11/2008 on Electronic Information and Transactions Article 35 jo. Article 51
d. Criminal Code Article 378 on Fraud
e. Law of the Republic of Indonesia Number 27 Year 2022 on Personal Data Protection
f. Indonesian Advertising Ethics Amendment 2020

2.2. Secondary :

a. GoogleAdswork official website
b. Lens.Org with Keyword "Phishing"
c. IDADX (Indonesia anti phishing data exchange) https://idadx.id/

3 Results And Discussion

3.1 Ad Serving Mechanism on Google AdWords

Google AdWords provides advertising services for our business, which will then be forwarded to customers or potential customers when they are searching and searching for a business topic, service, or product on the Google search engine. Whether they use desktop or mobile media, the ads served by Google AdWords will help our business get potential customers. The existence of Google AdWords as an advertising service can help increase online bookings and sales with their online advertising services that will directly direct these potential customers to our site.

Google AdWords can increase incoming phone calls from customers with advertising services that display our business phone number. And Google AdWords advertising services can help our business or site get more visitors with business ads that can tell visitors about our business or site on the map. Google AdWords as an advertising service provides convenience by giving control to its service users to set advertising budget limits, so that it will not exceed the budget that has been set. The ad pays according to results, such as clicks to your site or phone calls to your business.

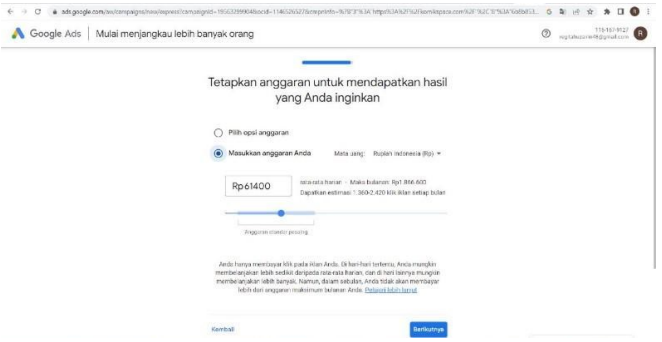


Figure 1: Setting Ad Budget Limits on Google AdWords

Users of Google AdWords advertising platform services can also make further settings regarding campaign objectives, campaign types, networks, targeting and audience segments, and setting keywords. As can be seen in Figures 2,3,4,5, and 6

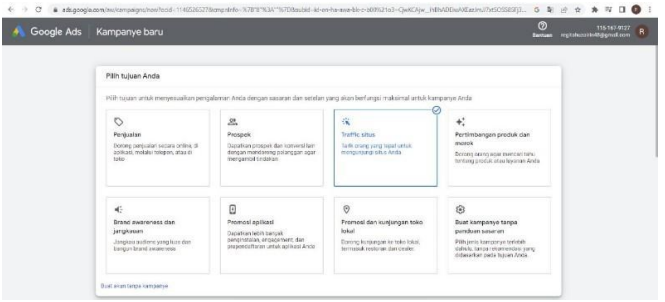


Figure 2 : Advertising Objectives on Google AdWords

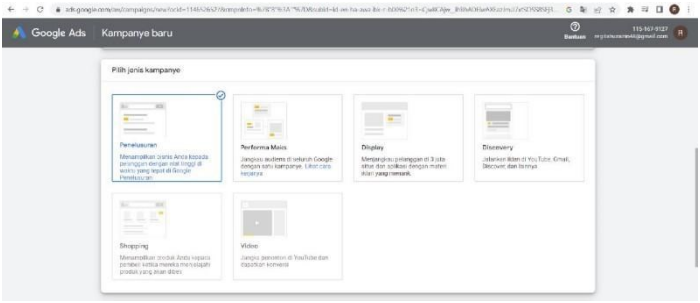


Figure 3 : Types of Advertising on Google AdWords

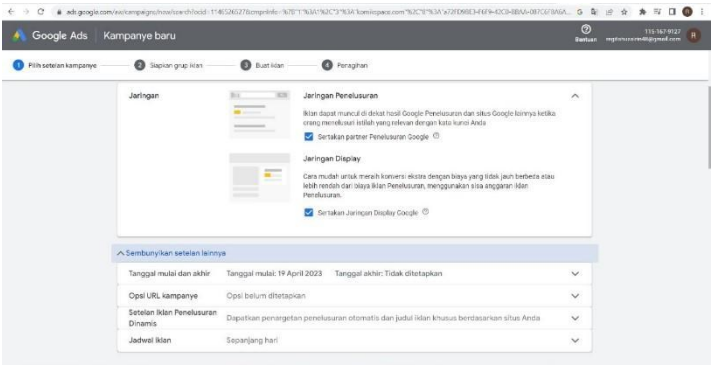


Figure 4 : Advertising network on Google AdWords

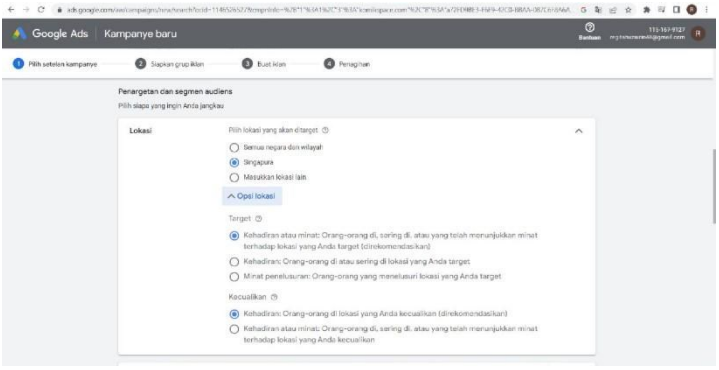


Figure 5: Targeting and Audience Segments in Google AdWords

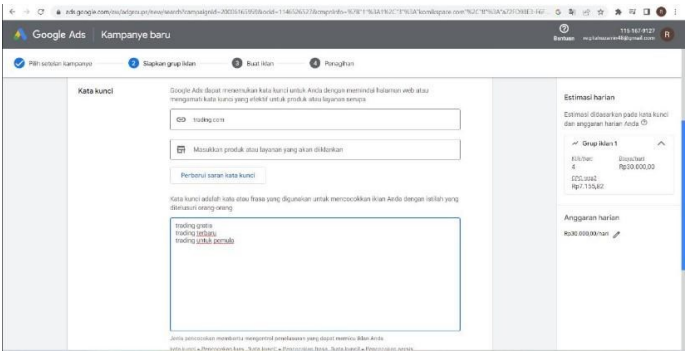


Figure 6 : Keyword Setup and Implementation on Google AdWords

Figure 7. Schematic of Ad Creation in Google AdWords

Table 1. Legal Acts and Things to Watch out for when advertising on Google AdWords

No.	Legal Actions	What to watch out for
1	Setting Ad Budget Limits on Google AdWords	Ensure that budget expenditures paid are in line with advertising objectives, advertising results, competition with other advertisers. Google must also apply electronic signatures to users of advertising services in accordance with what is regulated in the ITE Law No. 11 of 2008 Articles 11 and 12.

2	Purpose of Advertising on Google AdWords	Google must ensure that the purpose of advertising that has been set by users of advertising services is correct without any hidden intentions. Google can also cooperate with the BPP (Advertising Supervisory Agency) in monitoring
3	Types of Advertising on Google AdWords	Ensure that the type of advertisement desired by the user of advertising services is in accordance with the contents of the proposed advertising content. By reviewing the contents of the advertisement.
4	Advertising network on Google AdWords	Google shall ensure that the ad network selected by the ad service user can be served on the correct layout and schedule.
5	Audience Targeting and Segments on Google AdWords	Ensure that the country or region that is the target of the advertisement, which is submitted by the user of advertising services is appropriate. And ensure that the advertisement does not violate the advertising provisions in a country that is targeted.
6	Keyword Setup and Implementation on Google AdWords	Ensure that the selection of keywords by users of advertising services is in accordance with the content of the proposed advertising content without any manipulation as regulated in ITE Law No. 11 of 2008 Article 35. So that advertisements that appear when searching using these keywords will not trap users.
7	Create Ad Content	Google must ensure that the content of advertisements submitted by users of advertising services does not violate the provisions in Google's terms and conditions and does not violate the provisions in the Indonesian Advertising Ethics Amendment 2020.

Google AdWords as Google's advertising platform has 4 advertising policies, namely:

a. Prohibited Content: The type of content that should not be advertised on the Google AdWords advertising platform service. For example, counterfeit goods disguised as genuine goods. Dangerous products or services such as drugs, explosives, or ammunition. Facilitation of false behavior, such as manipulative software and websites or even fake documents. Inappropriate content such as discrimination, animal abuse, murder, etc.

b. Prohibited Practices: Things that are strictly prohibited by Google AdWords. For example, blaming the ad network for malware. Data usage, e.g. misuse of information, such as personal data and credit card information. Misrepresentation, e.g. making false offers, false physical address, Phishing

c. Restricted Content and Features: Content that can be served by Google AdWords but content restrictions will be applied. Such as, default ad treatment (restriction of ads for ages under 18).

Sexual content such as overnight dating, and models in sexual poses, Alcohol, Copyright, Gambling, drugs, politics.

d.Editorial and Technical: Ads or Sites that will be served in Google AdWords must comply with the quality standards that have been set.

So that phishing website advertising has violated the advertising policy in Google AdWords in the category of Prohibited Content and Prohibited Practices, but the consequences given by Google to Phishing actors are very light. Because, the consequences that will be given by Google to perpetrators who violate Google AdWords policies are in the form of 3 reprimands and the toughest consequence is only account suspension without warning. So, of course there are still many phishing behaviors that carry out their activities if the consequences are very light. Because, if it's just an account suspension, the perpetrators can easily create a new account and then register it again with Google AdWords.

In contrast to the rules regarding Phishing in the provisions of Law No.11 of 2008 concerning Electronic Information and Transactions Article 35 jo. Article 51 which explains that any person who intentionally and without the right to manipulate or create electronic documents so that they are considered as authentic data can be subject to a maximum imprisonment of 12 years and a fine of Rp.12 Billion. So it can be considered that the consequences of Google AdWords are not commensurate and equivalent to the rules that apply in Indonesia.

Before serving ads, Google AdWords applies several filter mechanisms to advertisements that have been submitted by its service users to ensure that these ads comply with and are in accordance with the advertising policies in Google AdWords. Some of the filters applied by Google AdWords are:

a.Automated Filters: Google AdWords implements an automated system to determine incoming ads, then displays ads that have been confirmed to comply with Google AdWords rules using machine learning technology.

b. Manual Review: Google AdWords' manual ad review team will ensure that ads are displayed in accordance with Google AdWords policies.

c.Advertiser Policies: Google AdWords strictly adheres to the advertising standards that have been set by a regulatory body. Ads submitted by users of its services will not be displayed if they violate the rules of Google AdWords.

d.User Feedback: Google AdWords uses feedback from its users to identify and eliminate offensive or unwanted ads.

e. Content ad filters: Google AdWords implements a content ad filter to analyze the content on the web page where the ad will be served. If there is content that is considered to violate Google AdWords policies and is considered a suspicious web page, Google AdWords will not display ads from that web page.

f. Keyword ad filters: Google AdWords applies a keyword ad filter to check whether the keywords used in the ad are appropriate and comply with the policies of Google AdWords. So, if the existing keywords are deemed inappropriate and are considered to violate the policies in the provisions of Google AdWords, then the ad will not be displayed by Google.

g. Image ad filters: Google AdWords will apply an image ad filter to analyze the content of the images used in the web pages to be advertised to ensure that the content is appropriate for display and is in accordance with what has been regulated in Google AdWords policies.

h. Destination ad filter: Google AdWords will apply a destination ad filter to review the purpose of the ad page so that the website to be advertised complies with the terms and does not violate Google AdWords policies, such as phishing or malware websites.

i. Advertiser account historical ad filters: Google AdWords will monitor and use the advertiser's account history information to determine the trustworthiness of the advertiser's account and how compliant the advertiser is with Google AdWords policies. Thus, if the advertiser's account is found to have a history of violating Google AdWords policies, then most of their ads will be rejected or approved by Google AdWords but with restrictions applied.

By implementing these filter mechanisms, Google AdWords ensures that the ads to be served are in accordance with the rules and advertising policies in Google AdWords.[15] But even though it has applied the Filter Mechanism to incoming advertisements and wants to be served, in fact there are still phishing website ads that escape the Google AdWords filter mechanism, so that Phishers manage to advertise their website, escape the advertising filter, and can be served by Google AdWords, It is caused by:

a. Acts of Forgery: Criminals create phishing websites by creating domains that look very similar to the real website, which makes it difficult for the Google AdWords system to tell the difference between the real website and the fake, manipulative or phishing website. They add different words or letters between their URLs that look similar to the URLs on the real website.
b. Technology Development: Phishing websites use new and more sophisticated techniques from time to time, so phishing websites that deceive users and steal their personal data are difficult to detect.
c. Review Error: Errors in determining ads that violate policies or not by automatic filters and manual reviews from Google AdWords, so that some phishing or policy-violating ads are considered as ads that do not violate policies.
d. New Fraud Tactics: Cybercriminals are getting smarter at circumventing Google's automated filters and manual reviews of Google AdWords using new and innovative tactics.
e. Creating a website that looks exactly the same as the original website: For example, a landing page, login page or registration page, using images, logos and designs similar to the original website with the aim of deceiving potential victims to enter their personal information.
f. Using certain advertising services: Phishers usually use advertising services, where advertising policies are not too strict so that phishing ads can appear on Google AdWords.
g. Using focused ad campaigns: Usually, phishers use ad campaigns that only focus on a few keywords. Thus, the perpetrators can ensure that the ads are displayed to users who are interested in the topic based on the keywords that have been set by the phishers.

h. Using different ad networks: The use of different ad networks is used by phishers to avoid detection of ad policies by Google AdWords. such as ad context and ad banners. Thus, it is certain that phishing ads will not be detected by Google AdWords' ad filters.

i. Evading ad filters: Phishers apply their techniques to circumvent Google AdWords' ad filters. Phishers will replace phrases or words that are usually used in ad filters. Also, the perpetrators also trick Google AdWords ad filters using videos or images instead of text with the aim that the perpetrator's phishing website is difficult to detect by Google AdWords.

There are several techniques used by phishing criminals in manipulating website addresses (URLs) so that users who are not careful will be deceived.[16] Namely:

1.Using IP Address

Phishers will include the IP Address in the hostname section of the website URL address to steal sensitive and personal information belonging to someone who accesses and enters their information on the Website. An example of a site address used by phishers using an IP Address is "http://118.75.1.680/fake.html"

2.URLs that are too long

Phishers usually use long URLs to hide suspicious parts in the address bar of their phishing sites. URLs that have a number of characters between 54 and 75 characters are categorized as suspicious websites, if more than 75 characters then it is already in the phishing category, because the normal number of website URLs is less than 54 characters. An example of a phishing website address that uses a long URL is "http://onlinecodeadv.com.dx/1c/dex/lo00e9e979e4308d400cgv20a613z1o/?cmd=_home& dispatch=b74f8dc1e7c2e8dd4105e8@website.phising.html.

3.URLs that have the "@" symbol

The use of the "@" symbol is included in the phishing category. This is because the use of the "@" symbol included by the phisher in the website URL can direct the browser to ignore everything that precedes the "@" symbol.

4.Adding affixes to the beginning or end of a sentence (Prefix and Suffix)

What is meant by this affix word is for example a dash in the website URL. This is because the use of affixes is very rare in genuine (non-phishing) URLs. Meanwhile, the perpetrators of Phishing prefers to add a word at the beginning or end such as a "-" sign to the website domain. So that users who see the domain or URL feel that the web page they are accessing is a genuine website. An example of a URL or domain name that uses this affix is "http://www.Payment-confirmation.com/.

1.Unreasonable URL

If a domain name or website page identity is found that does not match the one in the WHOIS site database "http://who.is/" then the website can be categorized as a phishing website.

2.Redirect Page

This redirect page feature is usually used by phishers to hide the actual destination link by requesting users to provide sensitive or personal information to suspicious websites.

3.Using Pop-up Window

The use of a pop-up window feature that appears on the original website is unnatural. So if a website uses a pop-up window feature with the aim of getting users to submit their identity. Then the website is categorized as a phishing website

4.Turn off Right Click Function

Phishers are adept at using JavaScript. The perpetrator will use JavaScript to turn off the right-click function on the monitor, so that users who are accessing the website will not be able to see

and save the source code of the website page being accessed. Thus, if this right-click function is turned off, the website can be categorized as a phishing website.

The following phishing website links have escaped Google AdWords' ad policy filters and have been served on its advertising platform:

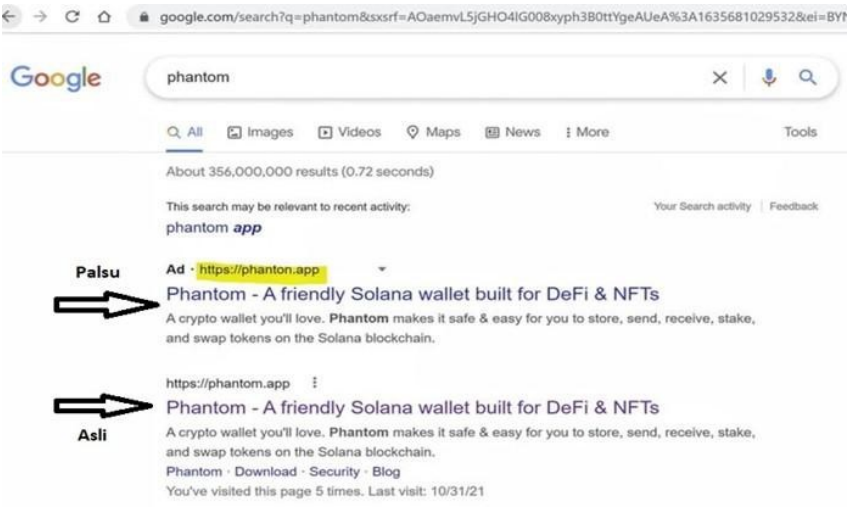


Figure 8 : Phishing website link by Google AdWords and Phantom Original Website Link[17]

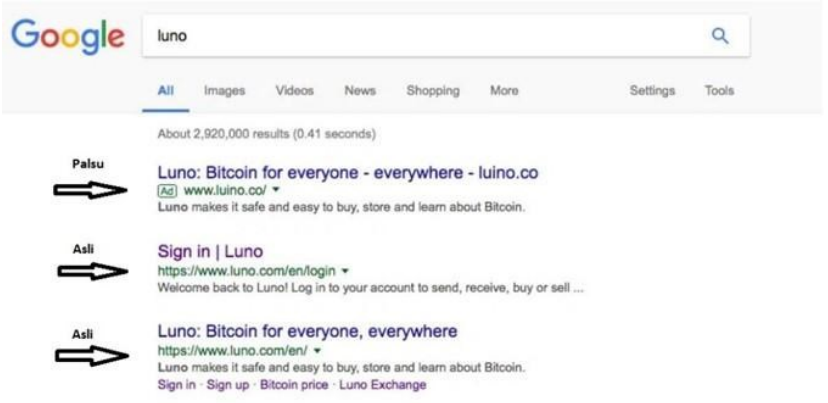


Figure 9: Phishing website link by Google AdWords and the original Luno website link[18]

In addition to creating a site that looks similar to the original website, phishing also deceives and misleads others so that users experience losses because their personal information

is known by the phisher and can be used for bad things. Therefore, the act of phishing can also be subject to Article 32 paragraph (2) jo. Article 48 paragraph (2) of the Electronic Information and Transaction Law which explains that any person who intentionally and without the right to transfer and transfer someone's Electronic Information to another person's Electronic System, can be sentenced to imprisonment for a maximum of 9 years or a maximum fine of Rp.3 billion.

3.2 Google's liability for advertising phishing websites on the Google AdWords platform

As an advertising platform owned by Google, of course the appearance of phishing websites on the top page of Google AdWords causes anxiety for users. Because these phishing ads can trick users into entering their personal data and credit information without the user knowing and realizing it so that the personal data that has been obtained by the phisher can be misused for bad things. Of course, this can harm users and violate the law. Personal data has been specifically regulated in the Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection. It can be seen in article 4 of Law No. 27 of 2022 that personal data has 2 categories, namely specific and general personal data. Namely:
a. Specific personal data: health data and information, biometrics, genetic data, criminal records, child data, personal financial data
b. General personal data: full name, gender, nationality, religion, marital status, Personal Data that combined identifies a person.

Personal data that is most often stolen in phishing crimes is personal financial data (specific personal data), and general personal data. Article 65 paragraph (1), (2), (3) of Law No. 27 of 2022 also explains the prohibition of using personal data, namely:
1.Any person who obtains Personal Data that does not belong to him/her in order to benefit himself/herself and cause harm to the Personal Data Subject. May be subject to imprisonment of up to 5 years and a fine of up to Rp. 5M.
2.Any person who discloses Personal Data that does not belong to him/her. May be subject to imprisonment of up to 4 years and a fine of up to Rp. 4M.
3.Any person who uses Personal Data that does not belong to him/her. Can be subject to imprisonment for a maximum of 5 years and a fine of Rp. 5M

Google AdWords also implements a policy on the verification process of document requirements for the identity of advertisers who want to use Google's advertising platform, Google AdWords. Advertiser verification itself is a Google program that will combine advertiser identity verification and business operations in just one process. In this program, there are steps that must be followed and must be carried out by advertisers if they want to use the Google AdWords advertising platform. Advertisers will be required to submit and enter information about their business and identity. In the document verification process policy, it is explained that:
1. For an organization that wants to advertise on Google AdWords, it must prepare and send one of the required registration documents. Documents that can be sent by the organization include:
a. Deed of Establishment
b. Company registration certificate
c. Company deed
d. DUNS number
e. Business license

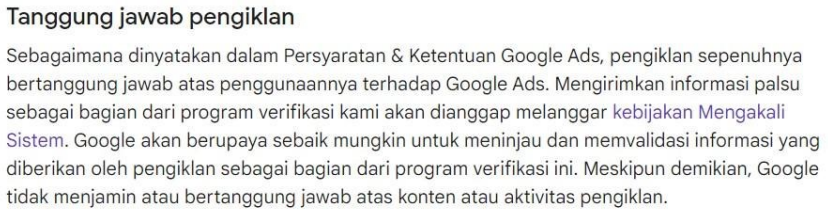
f. Tax registration letter

2. For individuals or official representatives, they must prepare and send a photo identification issued by the Indonesian government. Documents that can be sent by individuals or authorized representatives include:
a. Passport
b. Driver's License
c. National identity card
d. Residence permit

Although the policy on the verification process of document requirements has been regulated by Google AdWords, it turns out that in reality the process is not needed and is not implemented. Parties who want to advertise on the Google AdWords advertising platform can register their sites or advertisements without sending the documents required for the verification process. Therefore, the policy regarding the verification process when registering ads is not implemented by Google AdWords.

The rapid development of technology has made many parties interested in advertising their business on online advertising platforms, especially Google's Google AdWords. The perpetrators of phishing website links also began to participate in advertising their websites through advertising platforms, to trap their victims. As a result, it is often found that phishing website ads appear when users are searching through *search engines*.[19] So that the display of phishing website advertisements on Google's Google AdWords service, has violated the rules in Law No. 11 of 2008 concerning Electronic Information and Transactions Article 28 Paragraph (1), namely Every person who intentionally spreads false news (Hoax) and misleading which results in the loss of users or consumers in Electronic Transactions. May be subject to imprisonment for a maximum of 6 years and a maximum fine of Rp 1M.

There is a unilateral statement from Google through a policy on the Google AdWords advertising platform that seems hands off if there are ads that pass the filter and are successfully served by their platform, where the ad contains threatening content such as phishing, malware, various other crimes and harms users who are not careful when accessing the website they find on Google AdWords ads. The statement from Google AdWords can be seen in Figure 9.


Tanggung jawab pengiklan

Sebagaimana dinyatakan dalam Persyaratan & Ketentuan Google Ads, pengiklan sepenuhnya bertanggung jawab atas penggunaannya terhadap Google Ads. Mengirimkan informasi palsu sebagai bagian dari program verifikasi kami akan dianggap melanggar kebijakan Mengakali Sistem. Google akan berupaya sebaik mungkin untuk meninjau dan memvalidasi informasi yang diberikan oleh pengiklan sebagai bagian dari program verifikasi ini. Meskipun demikian, Google tidak menjamin atau bertanggung jawab atas konten atau aktivitas pengiklan.

Figure 10. Google AdWords' statement of abdication of responsibility.[20]

The Indonesian Advertising Ethics 2020 Amendment created by the Indonesian Advertising Council, regulates in detail the advertising code of ethics in Indonesia that must be obeyed and must not be violated.[21] Advertising provisions in Online Media, namely:

Ad Serving:

a. the media where an advertisement is aired, must be responsible for the entire material or content of the advertisement aired through the ad-serving platform used, whether its own, or belonging to other parties through an ad network.
b. Advertisements that have been aired by the ad network mechanism must display the party's identity.
c. All types of advertisements must be approved by the media where they are aired.
d. Available advertisements must have the same material content as the destination site.

Organizers of digital media advertising platforms, must properly ensure that all ads served are free from any threats, such as phishing, viruses, spyware, bugs, malware, or scripts that can harm internet users.

Retrieval of visitor data through cookies must be informed to visitors who are doing access. If the retrieval of cookies is related to personal data, it must obtain consent from the visitor first, if the visitor refuses. Then the taking of cookies should not be done.

Electronic mail advertisements must include:
a. Get approval from the email owner first before sending the ad.
b. Provide the reason why the advertising platform is sending the advertisement to the recipient of the advertising message.
c. Provide easy-to-understand and very clear instructions to recipients of advertising messages on how to stop receiving advertising messages from the same party, by providing the convenience of an opt-out feature mechanism that is very visible and easy to access at any time by the user or recipient of the message.
d. Complete identity of the sender of the advertisement.
e. Guarantee the rights and personal confidentiality of the recipient of the advertising message.

Social media advertising:
a. For products intended for adults only, it is mandatory to prevent access to advertisements for users under the age of 21.
b. Not using personal social media to broadcast commercial advertisements, unless there is a prior mention of the commercial advertisement element.

The statement of release of responsibility from Google AdWords that advertises phishing websites has violated the Indonesian Advertising Code of Ethics in the category of online media advertising services which can be seen in number 1 point a, and in number 2. The Indonesian Advertising Council can impose sanctions on Google AdWords for violating the Terms of advertising in Online Media, in accordance with those listed in the Indonesian Advertising Ethics. Namely in the form of:
a. Warning, up to two times
b. Terminate or issue sanction recommendations to the relevant institutions and inform all interested parties.
c. The submission of sanctions is carried out in writing, by stating the type of violation and the reference used.For advertising phishing website links carried out by Google AdWords which is an advertising platform owned by Google. So, Google can also be subject to administrative sanctions.

Indonesia has the authority to prosecute a criminal act both inside and outside the State of Indonesia as long as the event is considered an act that harms the security and interests of the State. So that even though Google AdWords is an advertising platform owned by Google which

is based outside Indonesia, Users who feel harmed by Phishing advertisements served by Google's advertising platform, namely Google AdWords, can file a lawsuit against the party concerned. The filing of this lawsuit has been regulated in Law No. 27 of 2022 concerning Personal Data Article 12 Paragraph (1) which explains that the Personal Data Subject has the right to sue and obtain compensation for violations of the processing of Personal Data about him in accordance with the provisions of laws and regulations. Then Article 1365 of the Civil Code which contains that any unlawful act, where the act causes harm to another person or user, then the party who has caused harm to the user for his mistake is obliged to replace the existing losses.

Provisions regarding the filing of a lawsuit by an aggrieved user are also regulated in Law No. 11 of 2008 concerning Electronic Information and Transactions Article 38 paragraphs (1) and (2) which explain that:

1.Any person may file a lawsuit against a party that organizes an Electronic System or uses Information Technology that causes harm to users.

2.The public can also file a representative lawsuit against a party or platform that organizes an Electronic System or uses Information Technology that can cause harm to the public, in accordance with applicable regulations.

In addition to settling a lawsuit, the parties can also settle it in arbitration, or through other alternative dispute resolution institutions in accordance with the provisions of the Laws and Regulations. To reduce the number of victims affected by phishing websites, users can also work together by reporting website links that they find. There are several platforms available as a complaint of this phishing action, for example by reporting the link to email helpdesk@pandi.id. Which is a complaint platform owned by the Indonesia Anti-Phishing Data Exchange (IDADX) and the Indonesian Internet Domain Name Manager (PANDI). Users who find a phishing website link can also report it through the Anti-Phishing Working Group's (APWG) international complaint platform, by reporting the link to reportphishing@apwg.org.

4 Summary

Google has implemented filter mechanisms on the Google AdWords advertising platform, the filter is used to ensure that the ads that will be displayed on its platform are in accordance with the rules and advertising policies in Google AdWords. But even though it has applied the Filter Mechanism to incoming advertisements in an effort to prevent advertisements that violate the rules, in fact there are still phishing website ads that escape. Because no system is perfect, including Google AdWords' ad filter mechanism, which causes phishing ads to escape. So Google needs to conduct continuous assessments and monitoring of its filter mechanism to improve its ability to find ads that violate the law. To protect users' privacy from crimes or security hazards associated with phishing ads, Google can collaborate with law enforcement to reduce the number of phishing ads displayed.

Google must be responsible for its advertising platform, Google AdWords, which advertises phishing websites. Google has violated the rules in Law No. 11 of 2008 concerning Electronic Information and Transactions Article 28 Paragraph (1), and has violated the Indonesian Pariwara Ethics Amendment 2020 made by the Indonesian Advertising Council regarding the Terms of advertising in Online Media, namely that the media where an advertisement is displayed, namely Google AdWords, must be responsible for the overall material or content of

advertisements displayed through the advertising service platform used and properly ensure that all advertisements displayed are free from all threats, such as phishing, viruses, spyware, bugs, malware, or scripts that can harm internet users. For the act of advertising phishing websites, Google must also be held civilly responsible, as regulated in the provisions of Article 1365 of the Civil Code which explains that unlawful acts, which cause harm to users, then the party who has caused harm to users for their mistakes is obliged to replace existing losses. Users who feel harmed can file a lawsuit as stipulated in Law No. 11 of 2008 concerning Electronic Information and Transactions Article 38 paragraphs (1) and (2) concerning filing a lawsuit against the party organizing the Electronic System that causes harm to users and filing a lawsuit on a representative basis to the platform that organizes the Electronic System that can cause harm to the public. Suggestions for future research, conduct an assessment of the reasons or factors that cause the government to never impose criminal or civil sanctions on Google as the provider of the Google AdWords advertising platform that advertises phishing websites, even though the applicable regulations in Indonesia are clear and valid until now.

Acknowledgments

Thank you to both parents, and my brother who always prayed and provided material and moral support to me so that this research could run smoothly. Also, thank you to my friends, namely the Law 8 A1 class who have encouraged me during this research.

Reference

[1]L. J. Trautman, M. Hussein, E. U. Opara, and S. Rahman, "Posted: No Phishing," *Ssrn Electron. J.*, 2020, Doi: 10.2139/Ssrn.3549992.
[2]O. P. Barus, "Comparison of Extreme Learning Machine and Backpropagation Methods for Classifying Phishing Websites," *Informatics Engineering Research And Technology*, Vol . 1 No.1, Jul. 2019.
[3]"Google Safe Browsing Api.", [Online]. Available: Http://Code.Google.Com/Apis/Safebrowsing/.
[4]"Microsoft Smart Screen.", [Online]. Available: Http://Windows.Microsoft.Com/En-Us/Windows-Vista/Smartscreen-Filter-Frequently-Asked-Questions.
[5]R. Yustitiana, "Implementation of Legal Arrangements for the Crime of 'Fraud Phishing' Electronic Transactions as Part of Law Enforcement Efforts in Indonesia Linked to the Theory of Legal Effectiveness." Jul. 31, 2021.
[6]F. Kwarto and M. Angsito, "The Effect of Cyber Crime on Cyber Security Compliance in the Financial Sector," *J. Akunt. Business*, Vol. 11, No. 2, Nov. 2018, Doi: 10.30813/Jab.V11i2.1382.
[7]M. Hayati and D. Fata, "Analysis of Information Security of Social Media Users Using Setoolkit Through Phishing Techniques," *Djtechno J. Technol. Inf.*, Vol. 2, No. 1, Pp. 21-28, Jul. 2021, Doi: 10.46576/Djtechno.V2i1.1252.
[8]Z. Efendy, I. E. Putra, And R. Saputra, "Asset Rental Information System And Web-Based Facilities At Andalas University," *J. Terap. Technol. Inf.*, Vol. 2, No. 2, Pp. 135-146, Feb. 2019, Doi: 10.21460/Jutei.2018.22.103.
[9]H. Hasanah, "Utilization of Digital Marketing Using Website and Social Media to Improve Product Marketing," *Packaged J. Pengabdi. Kpd. Masy.*, Vol. 4, No. 2, Oct. 2020, Doi: 10.32486/Jd.V4i2.469.
[10]N. Karmila, "Accountability and Transparency of Public Sector Performance, Including Accountability for Service Quality and Easily Accessible Public Service Information," Dec. 2018, Doi: 10.31227/Osf.Io/Utmbg.
[11]V. F. Putra Y, "Modus Operandi of Phishing Crime According to Uu Ite," *Jurist-Diction*, Vol. 4, No. 6, P. 2525, Nov. 2021, Doi: 10.20473/Jd.V4i6.31857.

[12]A. C. Banjarnahor and P. Priyana, "Juridical Analysis of Cybercrime Against the Handling of Kredivo Phishing Cases," *Hermeneutika J. Law Science*, Vol. 6, No. 1, Feb. 2022, Doi: 10.33603/Hermeneutika.V6i1.6754.
[13]A. S. Gulo, S. Lasmadi, and K. Nawawi, "Cyber Crime in the Form of Phishing Based on the Electronic Information and Transaction Law," *Pampas J. Crim. Law*, Vol. 1, No. 2, Pp. 68-81, Apr. 2021, Doi: 10.22437/Pampas.V1i2.9574.
[14]F. Nur Latifah, I. Mawardi, And B. Wardhana, "Threat Of Data Theft (Phishing) Amid Trends In Fintech Users During The Covid-19 Pandemic (Study Phishing In Indonesia)," *Shield of Islam. Bank. Finance J.*, Vol. 6, No. 1, Pp. 74-86, Apr. 2022, Doi: 10.21070/Perisai.V6i1.1598.
[15]K. Khatimah and E. Erlina, "Islamic Law Review on Online Buying and Selling of Goods that Do Not Match the Advertisement (Case Study of Ars Shop Samata Gowa)," *Iqtishaduna J. Ilm. Mhs. Huk. Econ. Sharia*, Vol. 2, No. 2, P. 64, Aug. 2020, Doi: 10.24252/Iqtishaduna.V2i2.16426.
[16]A. Mishra and Fancy, "Efficient Detection Of Phishing Hyperlinks Using Machine Learning," *Int. J. Cybern. Inform.*, Vol. 10, No. 2, Pp. 23-33, May 2021, Doi: 10.5121/Ijci.2021.100204.
[17]O. Sandy, "Phishing Website Ads Similar to Phantom Websites", [Online]. Available: Https://Cyberthreat.Id/Read/12845/Hackers-Using-Google-Ads-Targeting-Crypto-Wallet-Users-Phantom-and-Metamask
[18]T. Luno, "Phishing Website Ads Similar to Luno Website", [Online]. Available: Https://Discover.Luno.Com/Id/Waspada-Pipuan-Phishing-Di-Iklan-Google/
[19]E. Saputri, "Information Search Strategy through Search Engine (Google)," *J. Adab.*, Vol. 23, No. 2, P. 232, Aug. 2021, Doi: 10.22373/Adabiya.V23i2.10137.
[20]G. Ads, "Advertiser Responsibility", [Online]. Available: Https://Support.Google.Com/Adspolicy/Answer/9703665#900
[21]D. P. Indonesia, "Indonesian Advertising Ethics Amendment 2020." Indonesian Advertising Council, 2020.