

Online Advertising and its Security and Privacy Concerns

Angelia, Davar Pishva

Ritsumeikan Asia Pacific University, Beppu City, Oita Prefecture, Japan

an09@apu.ac.jp, dpishva@apu.ac.jp

Abstract— Commercial advertising has greatly benefitted from Internet services and online advertising can even be considered as the foundation of web economy. However, despite the availability of many books on how to create, use and make profit from online advertisement; there is little in-depth study on its true nature, security and privacy concerns. Through this research, the authors were able to establish an in-depth understanding of online advertising by collecting and analyzing numerous data on online advertising, with the hope that it could serve as a basis for further study on the field. The authors have also examined the security and privacy concerns of online advertising and the various gimmicks used to victimize innocent people. On the positive side, the paper explains the attractiveness of free online advertising services and the mechanism through which website owners profit from hosting online advertisements despite the fact that neither advertisers nor users pay for the services. On the negative side, the paper shows how online advertising hosts could be victimized by some shroud users for their money making purposes by continuous clicking of online advertisements without any intention of purchase. It also cites cases in which some website owners have marketed users' private information behind the scene. The paper concludes by highlighting pros and cons of online advertising, i.e., despite its numerous advantages, such as efficiency and range, it presents many dangers to advertisers, providers, website owners, and users.

Keywords— Online Advertising, Web Economy, Internet Services, Security, Privacy

I. INTRODUCTION

The system of online advertising is quite unique. Unlike conventional forms of advertising, the system of online advertising allows its target to receive something in return in exchange for viewing the advertisement. Besides getting information from the advertisement itself, the target of online advertising is usually allowed to use the advertisement host website's service. For example, video2mp3.net, a website that offers free file conversion from YouTube video to mp3 format, has numerous advertisements displayed on its page. It even goes as far as setting a hidden advertisement that will only appear when the user clicks the "High

quality" option. Nevertheless, the users are not required to pay for the service. They are instead offered a premium service where they can get exclusive access to the website without advertisements popping up along the way.

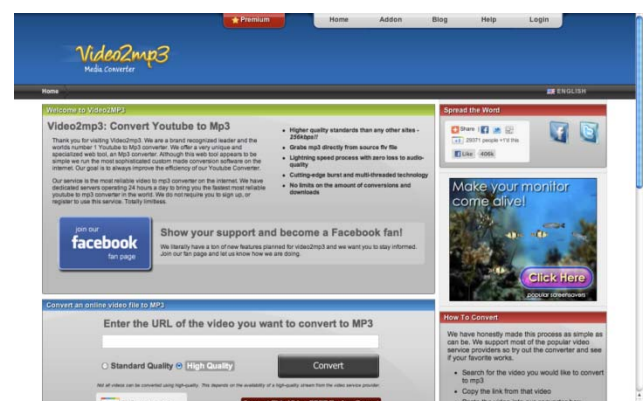


Figure 1. A view of Video2mp3.net. On the right side is one of its many advertisements.

In this way, online advertising has defined a new term of “free service”, where four parties – the advertisers, the ad network, the ad hosts, and the users - are involved within it.

A. The Nature of Online Advertising

Online advertising began like any television advertisement, where the goal was for the advertisement to be viewed by as many people as possible without caring who the advertisement was for. Many online advertisements were placed in popular websites in order to make sure the ad was viewed as much as possible.

However, with the rapid growth of online content in the last decade, advertisers became more aware that demographic information would allow more targeted approach in the advertisement. As database-mining techniques become more and more sophisticated, advertisers find more effective

strategies, e.g. contextual targeting, in order to attract the attention of more targeted audiences as opposed to the basic targeting techniques such as time, frequency, demography, etc [1].

Today, with the prevalence of Internet access and the amount of time consumers spend online, advertisers have moved away from mass marketing programs and are more focused on targeted and personalized marketing.

B. Parties Involved in Online Advertising

The first party is the advertisers. The advertisers are the “payer” in this relationship. All money comes from the advertisers and is distributed among two other parties, the ad network and ad host, who deliver the advertiser’s ads to the users. In turn, some of the users will become the advertisers’ customers and give the advertisers the profit they need to keep their economy wheel rotating. Advertisers are most vulnerable to attacks like click-fraud and usually incur the most damage monetary wise.

The second party is the ad network. The ad network’s job is to find websites—that are willing to host an advertiser’s advertisement. Advertisers pay the ad network and in return the ad network pays the host websites. The ad network measures the price of their service by counting how much the ads are viewed or accessed. The more an ad is seen or accessed, the higher the pay. The ad network is the only party who can profit from click-fraud attack.

The third party is the ad hosts. The ad hosts are websites that host the advertisements received from ad networks or directly from advertisers. Websites like blogs or social networking websites (e.g. Facebook) cannot directly charge their users or visitors money for fear of losing them. By hosting ads, they can get profit without worrying about charging their users while keeping their focus on maintaining the website.

The last party is the users themselves. The users are the target of online advertising, and more often the most vulnerable party among the four. While they can enjoy web surfing without paying, thanks to the unique system of online advertising, they are potential victims of online advertising malpractices. Yet, at the same time, they can also be involved in

online advertising fraud without realizing it. This aspect shall be explained further below.

Unlike common perception, the issues revolving around online advertising do not concern only the users, but also the other parties. Some parties may incur even more damage more than the users. Below are the two most common issues of online advertising.

II. TRACKING & THE INFORMATION MARKET

Online advertisement use cookies, a technique mainly used to identify users, as a means to deliver targeted advertising by tracking a user’s movements in the website. The cookies used for this purpose are called tracking cookies. An ad network company like Google uses cookies to deliver ads that are relevant to the user’s interests, control the number of times the user sees a given ad, and “measure the effectiveness of ad campaigns” [Google Policies & Principles, 2012].

The problem with tracking cookies is that when the user visits multiple websites with the same ad provider, the same cookies from the ad provider will be used. This means that the ad provider will be able to track the user’s activity in numerous sites just by compiling the information via tracking the cookies without the user’s knowledge. The result of this action means the loss of anonymity to the users, which is a blatant breach of information security as well as privacy. Although the ad network are obliged to comply with privacy act and use the information only for marketing strategy, users cannot be sure if it is not used for other purposes. Their suspicion is not off the mark.

Unknown to most people, personal information are traded freely without the consent of the owners. Practically speaking, it is a blatant breach of privacy to make money from the unregulated trade of personal information. Yet at the same time, personal information, especially the ones that are related to interest and habit, are an essential component for delivering online advertising, which is the lifeline of many websites.

It is only recently that people and governments started to pay attention to this previously unscrutinized golden goose. The Wall Street Journal’s investigation in 2010 revealed an array of cookies and surveillance technologies, with real time

function and deactivation resistance, are being used to monitor the users' personal information. The investigation also found out that online tracking is not a small business. The top 50 websites kept close tabs on their users by installing, on the average, 64 different pieces of surveillance technology [1].

The personal information trade has grown into a thriving micro-economy where the information is traded in stock-market-like exchanges. If the government started protecting people's right to online privacy, this economy will most likely regress. The businessmen involved believe that "the appropriate approach to addressing consumer online privacy issues is through industry self-regulation and education" [2].

The base of this problem lies on the difficulty of differentiating "tracking" and "harm." Every person has a different standard of privacy. What businessmen think is all right to use might differ from what consumers think is all right to share. The businessmen also argue that the consumers profit on tracking more than losing. However, ultimately it is up to the users to decide if advertising is worth the risk of anyone being able to acquire the users' personal information.

III. THE USE OF PERSONAL INFORMATION IN ONLINE ADVERTISING

Another privacy problem is the use of personal information without consent on social networking websites. A famous example comes from Facebook's "Social ads." The program was introduced in 2007, and has been known for using the names and "likes" of Facebook users to boost promotions. The system of the ad is integrated with Facebook's "like" and "news feeds" feature. Whenever a user 'likes' something, it will appear on his/her friends' news feeds and "recommended pages" [3].

A serious problem may arise especially when minors are involved. Some parents, whose children used Facebook, claimed that the move was unauthorized by them and view it as a privacy breach. A man named Nastro sued Facebook by claiming that "Facebook, Inc. has regularly and repeatedly used the names and/or likenesses of the plaintiff (Nastro) and the members of the Class for the commercial purpose of marketing, advertising,

selling and soliciting the purchase of goods and services"[3]. Even though the items were already concealed on the news feed, the child's name and photos kept appearing on the ads of the items they had liked.

These privacy problems are problematic for both users and the advertising side. Privacy is a thin ice to walk on and one wrong move can trigger the users to complain, mistrust, sue, and even seek a portion of the revenues for themselves.

IV. THREATS AND ATTACKS FROM OUTSIDE

A. To Advertisers: Click Fraud and PTR Websites

Online advertisement is well known for its "charge only when prospective customer views" system. However, in 2006, Bloomberg BusinessWeek brought to light an important issue for the advertisers: the click fraud [4]. Click fraud is a scam where a malicious party uses a network of human clickers and/or software to deceive the system for monetary gain, resulting in the inflation of advertisement bills of the advertisers. This scam is mostly happening in Google and Yahoo, the two search engine giants as well as two of the biggest ad providers.

Normally, ads are displayed on actual ad provider web pages or next to search results, where the ad contents are similar to the web page and search contents. However, the ads can also be recycled and displayed to millions of other websites from the well-known CNN to dummy websites such as insurance1472.com and insurance060.com. Even if it is "recycled," the advertisers are still charged when the ad is clicked. Click-fraud exploits this weakness to squeeze money from the advertisers.

Click fraud can be done either manually or automatically. In the manual way, the scammers hire a group of people under the pretence of a job called paid-to-read (PTR). They use their main website to recruit the clickers and then set other dummy websites to contain the advertisements. They will then direct the clickers to the dummy websites and ask them to click on the ads. For each click, the scammers will get a certain amount of money from the Ad Providers, and then use a portion of the money to pay the clickers, who are paid per click. This is a loss to the advertisers because the clickers click without paying attention

to the advertisement and never become their customer.

Another scheme is to use a program called “clickbot”. Clickbot is said to be more efficient than its human counterpart because it can automatically click in a time interval of several minutes to avoid detection. It is more difficult to detect them, but one way to detect is to look for a pattern [5]. It is rare for a human to perform a click habitually at the exact same time interval, so if a log finds a user that clicks exactly every hour three times a week, it is certainly a bot.

With the emergence of the click fraud, the confidence of online advertising is waning. Big ad providers such as Google and Yahoo claim that they have a way to screen the clicks and bill the advertisers accordingly. They refuse to disclose the mechanism of the screening because they are afraid of a malicious party learning something from it. However, the percentage of false clicks may be as high as 15%. If ad providers like Google and Yahoo really could do the screening effectively, the figure should not be that high. This raises a question whether or not the ad providers are really into eliminating click fraud. After all they also gain from the fraud and therefore, have an incentive to be an accomplice.

B. To Users: Malvertisements & Improper Advertisements

According to William Salusky, malicious advertising, or malvertising, is a criminal method that is “focused on the installation of unwanted or outright malicious software through the use of Internet advertising media networks, exchanges and other user supplied content publishing services common to the Social Networking space (Salusky, 2007).” He also mentioned that the most popular form of malvertising is actually “a result of the client rendering Adobe Flash SWF files that contains maliciously coded Flash ActionScript” (Salusky, 2007). In other words, flash based advertisements are more likely to be a malvertisement.

The modus operandi of the malvertising is to steal personal information, transforming end-user system into botnets [6] and/or extracting the user’s virtual wallet [7]. In the case of money extraction, the most common scheme is the act of sending the

users fake notices about a malware that doesn’t exist and forcing them to buy bogus security software. This is especially effective when the malvertisement is placed on a trusted website.

Besides malvertisements, there are also some inappropriate ways of advertising done by the advertiser and/or website owners, in their attempts to make Internet users to view or click the ads and raise their earnings from online advertising. The attempts vary; from placing it in strategic places to forcing and tricking the users to see or click it. Although it does nothing more than annoying the users, there is the possibility for the ads to be a malvertisement.

A good example of improper online ads placements in a website can be seen in Video2mp3.net, a website that offers a free service of converting YouTube videos to mp3 format. Those placements are:

1) **An advertisement link hidden in a button:** an ad that loads when the user clicks on a button.

2) **Misleading ads:** this ad has misleading appearance, such as false “download” sign, that will prompt the user to click it. The ads had an “advertisement” label on it to indicate that it is an ad, but it is hard to spot it.



Figure 2. An example of misleading ad taken from Video2mp3.net.

3) **Waiting time advertisement:** this advertisement forced the user to wait and see an ad before they can advance to destination page.

Besides causing the users to feel annoyance and discomfort, they also also consume time because users need to close the ad or wait until they can advance. This is why some websites offer the users the option to donate or pay to get rid of the ads.

C. To Website Owners: Being Forced to Host Malvertisements Through Hacking and Other Means

Malvertising is most effective when it is placed on a well-known and trusted websites. Malvertising

can thereby get access to millions of people using the website. Sites hit by a series of recent strikes include the New York Times and Horoscope.com, each of which receives millions of visitors every day.

Graham Cluley, a consultant with online security firm Sophos states: "Hackers are making more and more use of ad networks to distribute their attacks to users visiting legitimate well-known sites."

It does not matter if the malvertisers do not know precisely which website will end up displaying their ads. As long as they get their victims, it is fine. The hackers may even use the "normal" way to hack, such as posing to be someone wanting to buy advertising space. E.g. in 2009, readers of the New York Times were subject to a malvertising attack by hackers posing as a legitimate company seeking to buy advertising space.

V. TACKLING THE PROBLEM

Various attempts have been made to address the problem. Means of prevention and solution include the following:

A. Detection

Sometimes the victim does not realize that he/she is being attacked. This is especially true with advertisers, who have to pay attention to their online ads to realize the problem. For example, Martin Fleischmann, the owner of MostChoice.com, only realized that he was a victim of click-fraud when he used a specially designed software to analyse his online ads [8].

B. Technological Approach

The most common approach for all parties is to rely on software technologies, like firewall, plug-ins, etc.

C. Filing Lawsuits

Although done by many, filing lawsuit is more like damage control instead of problem solving. The target is often unknown, so a lawsuit cannot be filed.

D. Join Alliance

Max Weinstein, executive director of StopBadware mentions that online advertising problem is "about managing the problem effectively." Since malvertisment only appears occasionally at a particular site and is therefore hard

to detect, the most logical conclusion is to share information on the latest types of attacks and fraud as well as best practices for defeating attackers. Proposed joint efforts include alliance between Google, Facebook, Twitter and other large Web firms with the StopBadware project [9].

VI. CONCLUSION

Although proper use of online advertising is vital to web economy as it enables each party profit from the system: the advertisers get customers, the ad networks get money, the hosts get profit without the need to charge their service, and the users get free service, its misuse and abuse could cause huge damages, especially to users and advertisers. Often times, parties like clickers do not even realize that they are committing malicious acts.

Furthermore, though the use of tracking cookies makes it easier for both users and advertisement deliverers to maximize the effectiveness of the advertising, the users' personal information that get collected in the process, can expose them to the danger of identity and privacy lose.

Finally, the presence of malicious groups likes hackers, is another source of threat to the online advertising stakeholders and their systems. Due to its complex nature, there is no single and easy counter measure except pattern matching, preventive actions, and damage control.

REFERENCES

- [1] Schwartz, M. J. (2011, March 31). *Schwartz On Security: Online Privacy Battles Advertising Profits*. Retrieved June 7, 2012, from Information Week: <http://www.informationweek.com/news/security/privacy/229400615>
- [2] Gabi Boaca (2000, May 4). *Basic tricks to do (banner) campaign optimization*. Retrieved June 12, 2012, from slideshare.net: <http://www.slideshare.net/gboaca/new-targeting-techniques>
- [3] Brown, J. (2011, May 5). *Facebook sued for using children's' pictures in ads*. Retrieved June 12, 2012, from examiner.com: <http://www.examiner.com/article/facebook-sued-for-using-children-s-pictures-ads>
- [4] Grow, B., Elgin, B., & Herbst, M. (2006, October 1). *Click Fraud*. Retrieved June 9, 2012, from Bloomberg Businessweek Magazine: <http://www.businessweek.com/stories/2006-10-01/click-fraud>
- [5] *Detecting Click Fraud - Pay per Click Click*. (n.d.). Retrieved June 9, 2012, from Expert Data Miner: <http://www.expertdataminer.com/eng/tutorial/click-fraud-detection.html>
- [6] Raywood, D. (2012, February 13). *Malvertising increases by 240 per cent as networks detected*. Retrieved July 23, 2012, from SC Magazine: <http://www.scmagazineuk.com/malvertising-increases-by-240-per-cent-as-networks-detected/article/227435/>
- [7] Ferguson, R. (2013, April 1). *Malvertising, who's responsible?* Retrieved July 23, 2013, from CounterMeasures - Security, Privacy & Trust >> A Trend Micro Blog: <http://countermeasures.trendmicro.eu/malvertising-whos-responsible/>

- [8] Grow, B., Elgin, B., & Herbst, M. (2006, October 1). *Click Fraud*. Retrieved June 9, 2012, from Bloomberg Businessweek Magazine: <http://www.businessweek.com/stories/2006-10-01/click-fraud>
- [9] Lemos, R. (2012, June 15). *Google, Facebook, Twitter Join Alliance to Block Malvertising Web Fraud*. Retrieved August 11, 2012, from eWeek.com: <http://www.eweek.com/c/a/Security/Google-Facebook-Twitter-Join-Alliance-to-Block-Malvertising-Web-Fraud-381192/>