Online Ad-fraud in Search Engine Advertising Campaigns

Prevention, Detection and Damage Limitation

Andreas Mladenow[1], Niina Maarit Novak[2(✉)], and Christine Strauss[3]

[1] Secure Business Austria, Favoritenstr. 16, 1040 Vienna, Austria
amladenow@sba-research.org
[2] Institute of Software Technology and Interactive Systems, Vienna University of Technology, Favoritenstr. 9-11, 1040 Vienna, Austria
niina.novak@ifs.tuwien.ac.at
[3] Department of e-Business, Faculty of Business, Economics and Statistics, University of Vienna, Oskar-Morgenstern-Platz 1, 1090 Vienna, Austria
christine.strauss@univie.ac.at

Abstract. Search Engine Advertising has grown strongly in recent years and amounted to about USD 60 billion in 2014. Based on real-world data of online campaigns of 28 companies, we analyse the incident of a hacked campaign-account. We describe the occurred damage, i.e. (1) follow-up consequences of unauthorized access to the account of the advertiser, and (2) limited availability of short-term online campaigns. This contribution aims at raising awareness for the threat of hacking incidents during online marketing campaigns, and provides suggestions as well as recommendations for damage prevention, damage detection and damage limitation.

Keywords: Online advertising · Online Ad-fraud · Search engine marketing, SEM · Search engine advertising, SEA · Paid-Search · Security · Availability · Reliability · Online campaigns · Typology

1 Introduction

From the viewpoint of information economics peoples' attention is seen as a scarce commodity [1–4]. Through the use of search engine advertising (SEA), companies aim at improving their visibility among the search engine results in order to attract the attention of potential customers [5]. It is a global phenomenon that companies tend to invest more and more in sponsored search in electronic markets. It is estimated that in 2014 businesses have spent USD 60 billion in Search Engine Marketing (SEM) [6]. From an international perspective, Google was the undisputed global leader in 2014 with a market share of more than 90 % in Germany and 65 % in the US, which allowed the company to increase its revenues from advertising by 17 % compared to the prior year [6].

Quality, costs and time are major drivers on key success factors. For this reason, it is for many companies one of the main motivational reasons to perform online-campaigns [7–9]. Unlike traditional marketing campaigns, online campaigns provide

I. Khalil et al. (Eds.): ICT-EurAsia 2015 and CONFENIS 2015, LNCS 9357, pp. 109–118, 2015.
DOI: 10.1007/978-3-319-24315-3_11

the advertiser with fast information on the campaign's effectiveness. Moreover, online campaigns are highly flexible and allow a custom-tailored and targeted advertising approach. The flexibility and the time savings of online campaigns rely on fast transaction processes, based on the usage of tools such as Google *AdWords* [10] and Bing *Ads* [11] which allow to create online campaigns within a couple of minutes, and which allow to evaluate the campaigns' success within a few hours by means of predefined and built-in analysis functions [10, 11].

However, whereas these advantages seem to be quite obvious for the success of a marketing campaign, dealing with online campaigns often results in facing different kinds of problems such as trust and security issues. In this regard, advertisers and search engines representatives are confronted with the topic of ad-frauds. In the literature, this subject has mainly focussed on the so-called "click-fraud" problem [12–16], while other issues concerning ad-frauds have been neglected.

Against this background, this paper contributes in filling this research gap by providing a typology covering current types of ad-frauds as well as analysing the neglected topic of ad-frauds caused by unauthorized access to campaign accounts, so-called "hacks". What happens to hacked advertising accounts in the context of short-term online campaigns using the example of Google *AdWords*? What are the alternatives of action for campaign providers in the event of a hacker attack? Are there any prophylactic security controls to be set? Hence, this paper is structured as follows: the next section pinpoints theoretical insights of both, online ad-campaigns using the Google search engine tool *AdWords* as well as a typology of ad-fraud. Section 3 analyses scenarios based on real-world data. Section 4 provides a discussion, and the final section summarizes major findings and gives a brief outlook on future developments.

2 Online Campaigns and Ad-Fraud Using AdWords Accounts

2.1 Online Ad-Campaigns

When battling for customers' attention, businesses seek for the best ranking position – and thus visibility – in the results' list of search engine queries. In addition to the possibility of improving the organic search results through search engine optimization (SEO), which very often turns out to be highly time-consuming, search-engine advertisements (SEA) allow to address the customer in a rapid and targeted manner. The display of advertisements in search engines follows the keyword-principle, which allows buying an advertisement-position on the first page of the search engine results based on specific keywords. In the case of the big players, including Google, Yahoo and Bing, paid advertisements are grouped together in a commercial advertisement-block and are thus visually separated and highlighted from the unpaid (organic) results [cf. 10, 11].

Since the beginnings of text-based advertisement in search engines, advertisers aim to create specific advertisements matching query results, hoping to create a highly effective advertising tool. In contrast to traditional advertising (where costs incur when

placing an advertisement) in SEA one does not pay for impressions, but for clicks made. This is referred to as cost per click (CPC) or pay per click (PPC) [7, 9].

Paying for SEA is performance-based advertising [8]. Thus, the advertiser has to pay only for the click, and – as a consequence – only if a user visits the advertised website. Impressions are free of charge. This concept seems to be highly effective as auction-based text advertisements are by far the largest source of income for search engines, and there are still no signs indicating that this will change in the foreseeable future [8].

In the case of Google the *AdWords* tool supports the development of effective SEA-campaigns. When it comes to SEA, the positioning of an advertisement-candidate related to a specific search term is based on the willingness of the advertiser to pay a certain amount, previously specified by the advertiser. The entire set of advertiser candidates takes part in an auction for the entered search term of the Internet user. The order of display, or the positioning of advertisements is (for example in the case of Google) determined through an "advertisement-ranking procedure", a weighted second price auction. This ranking-position is further determined by the maximum amount for the homepage visit set by the advertiser and by Google's advertisement quality score (QS), an indicator which is highly influenced by the performance of the advertiser.

Typical advantages of online campaigns include factors such as elimination of geographic barriers, cost-efficiency, target group precision, measurability of the response, and personalization [8]. But what are the challenges and limitations of online marketing campaigns for companies? Experts agree that the integration of search engine marketing and more traditional forms of marketing is one of the biggest challenges [17]. Multi-channel marketing often require coordinated action in terms of content and time. In this regard, the design and creation of online marketing campaigns require specific competences and different strategic and operational approaches compared to conventional marketing. In their effort to reach potential consumers, advertisers are facing several risks. Besides the possibility to have advertisements blocked by the consumer, e.g. through software-based AdBlocker applications, online-advertising accounts may be the target of unauthorized usage through hacking activities leading to considerable loss of money and/or reputation. In the case of a hacker attack advertisers are confronted with problems of loss of integrity and reputation, lack of face-to-face communication, violation of privacy-issues, lack of trust and security. Moreover, advertisers and clients depend on the availability and reliability of the provided online tools.

2.2 Types of Ad-Fraud

Two types of ad-fraud in the context of online campaigns are to be distinguished, i.e. hacking and click-fraud. A third type of ad-fraud are so-called customer-misleading ads, which is beyond the scope of this paper due to the fact, that it is not directly targeting a certain advertiser. Furthermore, we refer to the most widely used search engine, i.e. Google (cf. Fig. 1).

Hence, Fig. 1 locates the two types of online ad-fraud in the case of *AdWords* within the pattern of interaction of four involved parties: the advertiser, the consumers,

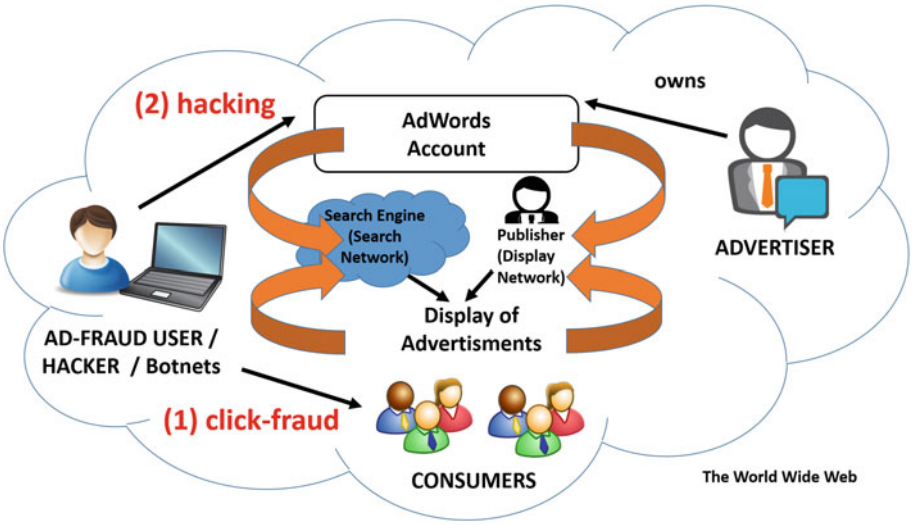

Fig. 1. Click-fraud and hacking

the publisher, and the hacker. The advertiser holds a Google *AdWords* account. Consumers surf on websites or use the search engine to perform search queries. Advertisements are displayed either via the search engine network or via website or blog of a publisher from the display network. Ad-fraud in such a context may include one or both of the two following activities: (1) hacking and/or (2) click-fraud. Hacking refers to a direct attack on an advertiser's *AdWords* account aiming at taking over control on that account. Click-fraud in contrast, involves taking on the role of a consumer either directly (personally) or indirectly (software-supported). In the case of click-fraud the goal of the attacker is an increase of the advertisers' costs by artificially increasing the number of clicks per ad. Click-fraud is a method frequently used by both, publishers and competing businesses, with the intention to significantly damage and downgrade a competitors ranking-position or/and improving one's own search engine ranking-position.

3 Ad-Fraud by Hacking Online-Campaign Accounts

Whereas click-frauds are difficult to be detected and revealed by the advertiser, hacking very often implies the difficulty for the advertiser to regain access to his/her own account, third party control through account blocking and limited or no access to the online campaigns. This may result in disrupting short-term online-campaigns, which might have been carefully orchestrated with other marketing activities e.g. in multi-channel campaigns, or which were launched with the intention to promote a specific time-dependent event.

Against this background, we analyse an ad-fraud scenario, which is based on real-world data selected from a set of a total of 28 online campaigns that were performed between 2013 and 2015 from the Google online marketing challenge [18] each

during a three-week period. In the following selected companies and their usage of SEA will be described in detail, based on their necessity for marketing campaigns with short-term availability. During these campaigns, one account was hacked. Hence, we describe this event of campaign account hacking and the perceived difficulty to regain access [19–21] for the remaining campaign time in Subsect. 3.2. The selected cases had to be anonymised to protect the involved parties. The selected examples shall give an insight into the importance of time-critical availability of campaign-tools during certain time-windows due to either event-driven necessities (*Case3* and *Case4*) or multi-channel ad-strategies (*Case1* and *Case2*).

3.1 Four Exemplary Cases for Short-Term Online Campaign

Case1 is a family-owned brand of fur products based in Vienna, Austria, originally established in 1948 in Prague. The company's core business is the manufacturing of fur-based products, including coats, jackets, blankets, pillows, accessories and custom-tailored products. The company positions its own brand as a high quality brand and expert for fur products. Although the company possesses a license for trading its products online, the company's online presence and penetration could be described as modest mainly depending on the company's website created in 2008, a Facebook-fan page, Pinterest and Instagram accounts in addition to an email newsletter and a cooperation with the online shop platform *case1partner.com*. As *case1.com* relies heavily on the local customer base in its three main cities (Vienna, Budapest and Bratislava), the client database generated by using *case1partner's* online presence offers the company the possibility to acquire global customers.

Case2 was originally founded in August 2010 in order to satisfy the local demand for limited, exclusive and edition-specific sneakers in Vienna. Since April 2012 the business runs as well an online-shop. Besides sneakers the company sells a small selection of T-shirts, shoelaces and shoe-cleaning kits. In addition, customers have the possibility to sell and trade their private and limited editions of sneakers that are no longer commercially available for sale via the online-shop. This feature represents a marketing tool for case2.at and generates traffic for the online-shop. The company's website, customer-management and social media presence (including Facebook, Google+, Twitter, Tumblr, Instagram and Pinterest) is maintained by the company itself. Currently the larger amount of sales is done over-the-counter, highlighting the company's necessity for an online-marketing campaign with the goal of increasing online sales. Both case1.com and the *Case2* operate in a small but highly competitive niche segment of the fashion industry. In these niche segments companies rely strongly on local customer bases and word-of-mouth. A company such as *Case1*, having a long tradition of operating in the fur segment of the fashion industry, undergoes by definition some seasonality. *AdWords* campaigns are thus especially used to promote after-season products, as well as to announce sales and new season or product lines. Furthermore, they allow for targeting not only German-speaking customers but also customers e.g. from Czech Republic, Hungary, Slovakia and Russia. *Case2* utilizes *AdWords* campaigns to target specific consumer-groups and to promote their online

shop as well as special sales and products, which allows the company to differentiate itself from big players of the industry segment (e.g., Zalando, Foot Locker, etc.).

Case3 is a website reporting on all games of the Austrian amateur soccer-league and is available free of charge. More than 100 private editors ("fans") cover the various national leagues. The company has four employees only who maintain the website and perform online marketing. This highlights that the website is fully dependent on the work of private individuals, or fans to report the latest news. The website has its own self-administered content management system, which delivers the latest information to readers (e.g., game reports, photos, previews, headlines, etc.). Particular attention should be paid to the so called "live ticker" covering even the smallest soccer-league-games in real time. The live ticker is also available as a mobile-app to keep readers 24/7 up-to-date. Since 2009 when *Case3* was founded, the number of users had continuously increased and large social media communities around the topic of the amateur-soccer-league with multiple thousands of participants had been formed. Besides the information-portal the company also operates a web-shop, selling soccer related sport products. As *Case3* is a website which heavily relies on advertising to finance itself, a high website traffic is crucial for its success. Thus targeted *AdWords* campaigns generating website-traffic through website promotion and its special features such as the live ticker, are of paramount importance. Furthermore, due to the fact that *AdWords* campaigns can be used to promote time- and date-specific events during a short time-window (e.g., final game of a sports tournament) emphasizes the importance of perpetual availability of this marketing tool.

Case4, is a famous and exquisite party and bar location offering a relaxed and beach-like atmosphere. At *Case4* one can enjoy delicious Israeli dishes together with various cocktails or drinks. The owners cooperate with an advertising agency to promote the location using various media channels. For restaurants no longer it is just about quality of food, beverages and services but also about location and about image and reputation. Diversification is an important strategy in a saturated market. One way to do so is to organize special events such as in the case of *Case4*, which organises special viewing parties, e.g. for the finals of the Eurovision Song Contest. These kind of events, which are planned on a short-term basis, are best promoted through short time advertisements. Based on the fact that individuals use online search engines in order to find out what is happening in town tonight and where to go, *AdWords* campaigns are the self-evident choice. Another argument strongly suggesting the use of *AdWords* campaigns is the fact that these events are weather-dependent open-air events.Thus, the chosen media channel needs to be very flexible in order to stop or change the advertisement in case the event has to be cancelled, substituted or postponed.

3.2 Hacking a Campaign-Account

In one of the described cases the campaign-account had been subject to unauthorized access, i.e. hacking. Due to the fact that the verification process of new advertisements and keywords normally takes some time the hacked account was not in use during a period of about 12 h. During this time window the account has been hacked and a new

advertisement in Russian language and Cyrillic writing was implemented and approved by Google. The fast approval by Google was the result of setting the newly created advertisement budget as: 'Budget delivery method set to accelerated: show ads as quickly as possible', which in turn may accelerate the approval procedure of Google. The campaign created produced stunning numbers in less than 18 h: 1,646,824 impressions and 6,190 clicks, generating costs of 207.66$. Achieving these amazing performance index figures in such a short period of time reveals professional skills and malicious intentions as drivers of such an activity.

After reporting the attack to Google, the *AdWords* account was deactivated and all *AdWords* campaigns were put on hold. Since the investigation process lasted longer than the remaining campaign-window (i.e., two weeks) the campaigns could not be restarted until Google finished the investigation process and had re-credited the amount lost due to the attack. Creating a new account to run another short-term campaign would have involved considerable amount of additional time, effort and expenses. To put it in a nutshell: the attack resulted in the loss of potential sales revenues as the *AdWords* campaigns had to be suspended.

In addition to the experience gained by the advertisers, a desk research revealed that *AdWords* seems to be an attractive target for hacking activities as many entries on web pages, in blogs and IT journals can be found on the internet. It is to be assumed that security mechanisms have not provided sufficient protection for the advertisers of the hacked campaign-accounts.

4 Prevention, Detection and Damage Limitation

Since its launch in the year 2000 Google *AdWords* [22] developed into Google's main source of revenue but became at the same time a target for online ad-fraud. From various incident reports and forum entries can be concluded that in most cases the Gmail-account address and password were used for unauthorized access to the campaign-account. In the case of Google *AdWords* most hacks follow a simple but effectual pattern involving (i) brute-force login, (ii) phishing carried out via email spoofing and very similar looking phishing websites asking the user to sign-in, as well as (iii) spy- and malware tools in order to acquire the user's account details [23]. Once the fraudsters have gained access to a campaign-account they typically duplicate campaigns, add a vast variety of keywords aimed to generate high amounts of clicks and redirect the target URL to some African airfare company [24], a Spanish online shop or some Russian website advertising bracelets [25].These practices cause fraudulent charges on users' credit cards quite often in the amount of several thousand US-Dollars caused by a single fraud-campaign over a time frame of less than 24 h. Furthermore, for people and businesses depending on Google *AdWords* to generate traffic for example to their online shops for direct sale purposes, considerable amounts of money are also lost in terms of revenue, reputation and benefits from historical account performance [26].

What can be done to prevent an attack? Choosing strong passwords is the most obvious and effective measure. Choosing a complex and long password involving not only letters but also numbers and special characters as well as changing the password

on a regular basis increases security and protects the account owner from simple attacks. Checking for spyware and using browsers with phishing filters [27], especially when signing into a Google-account from an unsecured Wireless Fidelity(WIFI) connection are highly recommended. Moreover, for businesses it is advised to have a contingency advertising-plan to be able to counter possible revenue drops caused by fraudulent campaigns [28].

How to detect an attack? Checking ones' account several times per day is not only a good practice to improve the performance and the cost-benefit ratio of the campaign itself. At the same time frequent checks protect from possible money and reputation losses caused by an attack. Best practice involves close monitoring and analysing the performance of each individual *AdWords* campaign several times per day.

How to behave during an attack? What happens after an attack? If the advertiser is able to access his/her own account the immediate activity is to change the password. This action will lock-out hackers. Ongoing campaigns shall be suspended or deleted. If access to the advertisers account is denied, the hacker may have changed the password, preventing the account owner from regaining access to his/her own account [29]. In such cases the account owner needs to contact the Google *AdWords* Support either per email or via the live help desk and report the incident. Google typically reimburses the fraud-victim for the money lost during the attack, following a thorough investigation. Moreover, it should be mentioned that Google *AdWords* has an inherent fraud-detection mechanism disabling the account [30] once a possible fraud is detected based on unusual activity, preventing both the display of campaigns created by hackers and further money loss of the user [30].

Based on our analysis of online campaigns of 28 companies in the following we suggest several methods, focusing on authentication, notification and budget limitation, aimed to increase the security of online campaigns and to protect users from ad-fraud.

Authentication. Unauthorized access to online advertising accounts could be impeded by use of encryption (adoption of best practice for security from online banking), digital signatures or a mandatory two-step verification process for each login-process (e.g., including username, password and for example a code sent to the user by email or SMS).

Notification. Push messages, SMS or E-Mail notifications for defined activities which are sent automatically and with the intention to inform advertisers about signification changes and performance details of their online campaigns could help to detect fraudulent activities in a timely manner and could thus prevent losses.

Budget limitation. Pre-setting a fixed daily maximum budget per campaign or a total maximum budget for the whole account prevents from considerable financial losses.

5 Conclusion and Outlook

Paid search marketing through Google *AdWords* exists now for more than 15 years and has been established as an essential and indispensable advertising channel. In every industry and every sector local, regional and global advertisements are placed in search

engines, the majority of advertisements are placed in Google. *AdWords* has become a widespread and widely accepted tool characterized by high reliability and flexibility. The analysis provides a typology of occurring ad-frauds and points to potential flaws in account handling that might be used for hacker attacks. When it comes to the integration of online marketing activities temporarily blocked accounts can cause financial losses. Ultimately, the understanding of search engine developments dependent on the dominant search-engine market providers represents a challenge for companies.

In the future the risk of ad-fraud seems to remain a major challenge for advertising companies, search engines and ad campaigners. Whereas ad-centers from Google, Yahoo and Microsoft have developed large data mining systems to score traffic quality, some types of ad-fraud are still to be resolved. More research needs to be addressed to all types of occurring ad-fraud. In the context of online marketing campaigns this includes not only click-fraud, but also problems such as hacking ad-campaign accounts.

References

1. Goldhaber, M.H.: The attention economy and the net. First Monday **2**(4), 66–78 (1997)
2. Mladenow, A., Fröschl, K.A.: Kooperative Forschung. Lang, Frankfurt am Main (2011)
3. Mladenow, A., Bauer, C., Strauss, C.: Social crowd integration in new product development: crowdsourcing communities nourish the open innovation paradigm. Global J. Flex. Syst. Manage. **15**(1), 77–86 (2014)
4. Mladenow, A., Kryvinska, N., Strauss, C.: Towards cloud-centric service environments. J. Serv. Sci. Res. **4**(2), 213–234 (2012)
5. Ghose, A., Yang, S.: An empirical analysis of search engine advertising: Sponsored search in electronic markets. Manage. Sci. **55**(10), 1605–1622 (2009)
6. Statista. http://de.statista.com/statistik/daten/studie/75188/umfrage/werbeumsatz-von-google-seit-2001/. Accessed 22 May 2015
7. Goldfarb, A., Tucker, C.: Search engine advertising: channel substitution when pricing ads to context. Manage. Sci. **57**(3), 458–470 (2011)
8. Langville, A.N., Meyer, C.D.: Google's PageRank and beyond: the science of search engine rankings. Princeton University Press, Princeton (2011)
9. Xiang, Z., Pan, B.: Travel queries on cities in the United States: implications for search engine marketing for tourist destinations. Tour. Manage. **32**(1), 88–97 (2011)
10. AdWords. https://www.google.at/adwords/. Accessed 22 May 2015
11. Bing Ads. https://secure.bingads.microsoft.com/. Accessed 22 May 2015
12. Kitts, B., et al.: Click fraud detection: adversarial pattern recognition over 5 years at microsoft. In: Abou-Nasr, M., Lessmann, S., Stahlbock, R., Weiss, G.M. (eds.) Real World Data Mining Applications, vol. 17, pp. 181–201. Springer, Heidelberg (2015)
13. Immorlica, N., Jain, K., Mahdian, M., Talwar, K.: Click fraud resistant methods for learning click-through rates. In: Deng, X., Ye, Y. (eds.) WINE 2005. LNCS, vol. 3828, pp. 34–45. Springer, Heidelberg (2005)
14. Wilbur, K.C., Zhu, Y.: Click fraud. Mark. Sci. **28**(2), 293–308 (2009)
15. Haddadi, H.: Fighting online click-fraud using bluff ads. ACM SIGCOMM Comput. Commun. Rev. **40**(2), 21–25 (2010)

16. Liu, B., Nath, S., Govindan, R., Liu, J.: DECAF: detecting and characterizing ad fraud in mobile apps. In: Proceedings of NSDI (2014)
17. Statista. http://www.statista.com/statistics/248059/biggest-challenages-in-search-marketing-worldwide/. Accessed 22 May 2015
18. GOMC. https://www.google.com/onlinechallenge/. Accessed 22 May 2015
19. Strauss C.: Informatik-Sicherheitsmanagement: eine Herausforderung für die Unternehmensführung, Vieweg+Teubner Verlag (1991)
20. Strauss, C., Stummer, C.: Multiobjective decision support in IT-risk management. Int. J. Inf. Technol. Decis. Making **1**(2), 251–268 (2002)
21. Kiesling E., Ekelhart A., Grill B., Stummer C., Strauss C.: Multi-objective evolutionary optimization of computation-intensive simulations: the case of security control selection. In: Proceedings of the 11th Metaheuristics International Conference (MIC 2015), forthcoming (2015)
22. GOOGLE Company – Our history in depth. http://www.google.com/about/company/history/#2000. Accessed 22 May 2015
23. LEFTY G BALOGH – Digital Marketing Testing Ground. http://www.leftygbalogh.com/2011/story-hacked-google-adwords-account/. Accessed 22 May 2015
24. MOZ – Blogs: AdWords Hackers – What a Nightmare. https://moz.com/ugc/adwords-hackers-what-a-nightmare/. Accessed 22 May 2015
25. GOOGLE – Official AdWords Community. https://www.de.adwords-community.com/t5/Grundlagen/Hilfe-Mein-Account-wurde-gehackt/td-p/44399/. Accessed 22 May 2015
26. ABEST WEB. http://www.abestweb.com/forums/showthread.php?113490-Google-AdA Words-account-hijacked/. Accessed 22 May 2015
27. GOOGLE – Official Blog – Insights from Googlers into our products, and technology. http://googleblog.blogspot.co.at/2008/04/how-to-avoid-getting-hooked.html/. Accessed 22 May 2015
28. GOOGLE Product Forums. https://productforums.google.com/forum/#!topic/gmail/A0wZmlrC0f8/. Accessed 22 May 2015
29. PPCDISCUSSIONS. http://www.ppcdiscussions.com/2008/09/my-personal-adwords-account-hacked.html/. Accessed 22 May 2015
30. SEARCH ENGINE Roundtable: Google AdWords Account Hacked: False Ads & False Charges. https://www.seroundtable.com/archives/017946.html/. Accessed 22 May (2015)