

# FAKE ADVERTISEMENTS AND THEIR CONSEQUENCES

## **AD Phishing: The Consequences of Fake Advertisement On Social Media**

Rediet Negash

Department of computer science, Stony Brook University

CSE 300: Technical Communications

Prof. Joseph Labriola

December 7, 2020

# FAKE ADVERTISEMENTS AND THEIR CONSEQUENCES

## Abstract

Social media platforms have become irreplaceable tools-- in allowing trending news topics, instantaneous communications, advertising campaigns, political debates, and social circles-- to connect for privileged human beings living in the 21 first century. The contents consumed on social media platforms have increasingly shaped our beliefs and preferences. With this increased reliance also comes the uneasy realization that fake information and advertisements on the internet have hushed knowledge of value to us. Since the issue of fake ads is an epidemic, software companies should address the problem immediately. Similarly, customers need to be aware, alert, and skeptical about the information they consume. Besides, it should be the users' responsibility to fact check before purchasing from websites or taking an informed decision-- as it is for tech companies to present filtered and fact-checked advertisements.

# FAKE ADVERTISEMENTS AND THEIR CONSEQUENCES

## **Defining Fake Advertisement and Introducing Its Severity**

Living in the era of technology has enabled customers to access services hosted by tech companies at the cost of watching advertisements embedded together with content. This brilliant idea incorporates both the customers' and the service providers' interest. It enables tech companies to profit from hosting other businesses' advertisements on their platforms. Similarly, the customers benefit from the services and ideally from the ads at no cost.

Although ad-supported content has made services available for free, it has brought some vulnerabilities to our table. These vulnerabilities include: websites being less manageable with advertisements, fake advertisements emerging as a plague, irrelevant with offensive messages being sent through ads, and websites tracking customers' online behavior (Guttman, 2020). Fake advertising refers to the use of false, misleading, offensive, sexual, violent, or unproven information to advertise products or phish customer's identities, behavior, and money. The epidemic of these fake advertisements has led customers' need for ad-blocking software to grow every year by 10%. It is predicted that in 2021 the number of ad-blocking software users in the US will increase to 27% (Guttman, 2020).

Others who prefer ad-supported content --which currently account for 78% of the total consumers-- are expressing their hatred for ads: though they don't want to pay for the services. They suggest advertisers be less of an obstacle and onerous-- avoiding to overuse the platform and filtering fake ads (WARC staff, 2019). 51% of these customers know-how companies need ads to make money without customers making direct payment to the services. They know advertisements are necessary trade-offs to get free or cheaper content. Nevertheless, the vulnerabilities ads bring are intolerable from their perspectives (WARC staff, 2019). Despite the

## FAKE ADVERTISEMENTS AND THEIR CONSEQUENCES

concerns, ad-content has been the number one revenue collection system that most tech companies count on.

### **Advertisements as Companies' Revenue**

As crazy as it might sound, most big companies -- such as Google, Facebook, and Twitter -- rely on advertisements for their revenue. In 2019, advertising accounted for the majority of Google's total revenue, which amounted to a total of 160.74 billion U.S. dollars. In the most recent fiscal period, advertising revenue through Google Sites made up 70.9 percent of the company's revenues (Clement, 2020). Facebook currently makes 98.5% of its money from digital advertising-- mostly from ads on Facebook and Instagram (Gunnars, 2020). The same applies to Twitter with 86.5% of its income being generated from advertisements (Clement, 2020). This clearly shows that advertisement is a big income generator which also became a big interest for scammers to phish customers. Consequently, cybercrime through fake ads has been significantly increasing every day.

### **Alarmingly Increasing Cybercrime through Fake Advertisements**

Recent studies show that fake advertisements have gained more territory over the years. According to an FTC report, Americans have lost more than \$77 million in fraud related to COVID-19 so far this year (Bizga, 2020). Additionally, impersonation scams cost UK consumers a whopping £58 million within the first six months of 2020 (Bizga, 2020). It is insane to see this much fraud being committed in just less than a year. Imagine how big of concern these types of crimes become as the whole world moves all its activities to the internet.

## FAKE ADVERTISEMENTS AND THEIR CONSEQUENCES

“I was scrolling through Instagram when the fake ad showed up,” says a victim of a scammer who lost money recently on Halloween after ordering from a fake website following a fake ad on Instagram. “I checked the reviews on Instagram; it seems to have a legitimate site. I did not doubt that it was a real website until my money got stolen” (Negash, 2020), says the victim with deep sorrow. It indicates how these ads have been camouflaged with real ads that lead to a scammed site that phishes customers. The severity of the situation is revealed more through this pandemic as criminals are actively using the global crisis to commit fraud and identity theft. These types of crimes are becoming alarming problems that require attention from individuals, government officials, and tech companies to protect customers from predators.

### **Other Negative Consequences of Advertisements**

In addition to being exposed to scammers, customers are tired of the distraction fake advertisements bring while they are doing work. Some users complain that ads are wasting their time by diverting their attention from their purpose when visiting websites. The complaint has escalated-- claiming that ads are draining the generation's ability to focus and complete tasks. Although the ability to focus might seem a personal attribute, ad intrusions are certainly contributing to the overall linger in the human race-- causing less productivity through time wasted in scrolling: thus, subscribing to less development of a country.

Research conducted on an in situ field study witnesses that most customers are getting distracted by advertisements-- affecting their productivity at work. The research was conducted on 32 information workers in their workplace to test if the use of ad-blockers can increase focus and productivity: preventing non-work-related distractions. Participants worked for five days in a baseline condition. Then, they worked another five days on ad-blocked machines. The result

## FAKE ADVERTISEMENTS AND THEIR CONSEQUENCES

assessed that participants' focus and productivity were significantly higher with an ad-blocker than without it. People who benefited the most from the ad-blocking software were those who were easily distracted by social media (Mark et .al, 2017, p. 933).

In addition to distractions, advertisements could have violent, fake, or sexual content that has the potential to spoil the younger generation. Parents are scared of what their kids are watching on the internet-- as there are many distractions-- with ads popping up everywhere. Furthermore, young children do not understand the concept of a sales pitch. Hence, they tend to easily believe what they are told-- making them victims of scammers through fake advertisements. Studies conducted by pediatrics show that most children do not understand the difference between a program designed to entertain and a commercial designed to sell (Paediatrics 2003). It also works against the parent's desire-- hindering them from easily controlling their children to not consume unnecessary content introduced by ads. For instance, if parents are trying hard to protect their children from pornographic sites, it becomes challenging for them to monitor their kids: as the new generation is learning sin through the sexual ads on the internet. Young kids will continue to be targeted for scams by fake ads unless ad-blockers are used.

One of the other most devastating consequences of fake advertisements is intentionally disseminating misleading information through social networks. The national bureau of economic research --at the Massachusetts Institute of technology-- has conducted a study on the role of advertising on social networks in spreading false news stories about childhood vaccines. They created a Facebook group of anti-vaccine advocates with fake stories. The result showed that "the 'anti-vaccine' Facebook groups spread false stories beyond the groups serving as an echo chamber " (Chiou & Tucker, 2018, p. 3). It created so many "like" posts from other users as the

## FAKE ADVERTISEMENTS AND THEIR CONSEQUENCES

fake stories got shared on their friends' social network-- swiftly propagating fake news (Chiou & Tucker, 2018). A small fraction of authors account for a large majority of posts, which reinforces the concern on social media's potential to allow an individual to reach a wide audience and share information without editorial. This rapid circulation of fake news can potentially harm consumers: it simply puts a whole community's opinion on vaccination at the risk of individuals who distribute false information-- making it a pressing public concern.

### **Combating Fake Advertisements and Potential Solutions**

#### **Responses of Tech Companies Towards Fake Advertisements**

Most victims --who are customers of companies like Facebook-- blame tech companies for being a platform of cybercrimes. They wonder if the companies care for their customers enough to protect them from fake ads. The impressions the companies create and their trustworthiness gets challenged as these cybercrimes soar. If users got an advertisement on Instagram that stole their identity or money, they tend to easily condemn Instagram for ushering the fake ad to their feed or story. The crime has happened to me once; blaming Instagram was my immediate reaction. Therefore, these big tech companies should care about the credibility of the advertisement they transmit on their platforms.

Facebook and Google have recently been trying to address the issues regarding fake ads-- though it hasn't solved the problem. Google has been suspending spamming accounts with real-time search. However, even though Google doesn't display tweets from usages that have a spammer signature, it does display tweets from non-suspected users: even when these are retweets coming from spammers. They should come up with a mechanism to retroactively detect retweets of spam, and label some Twitter users as enablers of spam. As the tech proliferates, the

## FAKE ADVERTISEMENTS AND THEIR CONSEQUENCES

scammers' technique gets more profound; thus Google should work on developing a better algorithm. (Mustafaraj & Metaxas, 2017, p. 238).

On the other hand, Facebook has been hiring individuals to fact-check before advertisements get posted since 2015. However, some of the employees were detected with conservative bias; the company decided to replace people with algorithms. One important feature that has rolled out recently is the labeling of news posts as “Disputed” via fact-checking third-party providers-- such as Snopes or PolitiFact. In addition to labeling posts, Facebook warns users with an alert box before they try to share a disputed story-- although they are still allowed to share it (Mustafaraj & Metaxas, 2017, p. 239). Nevertheless, all these efforts --to battle scammers through fake ads-- has not been enough. The issue still escalates as the internet continues to become the world's virtual meeting room.

### **Tech Company’s Role in Combating Fake Advertisements**

Tech companies have undeniable roles in combating cybercrimes committed through fake ads. They have a huge responsibility for mitigating the frauds committed every day. One might be critical enough to hold the companies accountable for not protecting their customers from scams. It is true that if the tech companies dare not to care about their customers enough and invest in heavily filtering fake advertisements on their platforms, they would lose their credibility and reputation from their customers-- casting a bad impression on themselves. Given the fact that ads are the company's major source of income, customers' choice of not clicking on the ad because of skepticism can lead to bankruptcy for the company. Hence, the companies should consider this and invest more than they are doing right now to alleviate the problem.



## FAKE ADVERTISEMENTS AND THEIR CONSEQUENCES

Especially when it comes to health issues, consumers benefit when firms and policymakers take direct action to prevent the spread of fake news articles. This is because consumers find health information extremely difficult to evaluate and to determine validity. As the childhood vaccine study from MIT shows, banning fake news sites and filtering advertisements plays a significant role in reducing the issue. For example, after Facebook's ban on advertising by fake news sites, the sharing of fake news articles on Facebook fell by 75% compared to Twitter (Chiou & Tucker, 2018, p.23).

The article --from the MIT study conducted on childhood vaccines-- suggests another potential mechanism for counteracting fake news: creating Facebook pages of real news and using this advertising to disseminate accurate information. Positive advertising can counteract the effects of negative advertising (Chiou & Tucker, 2018, p.23).

### **Customer's Responsibility in Combating Fake Advertisements**

In addition to tech companies banning fake sites and filtering fake advertisements, customers should also take a role in combating the issue regarding fake ads. All users should see the damage that fake ads bring to society. It has the potential to spread false information and influence society's behaviors and decisions. Therefore, the customers should also consider this and be watchful of the sources they use for getting information, and the sites for making transactions. Using credible sites, refuting to expose personal information right away, being watchful, and not believing some "too good to be true" deals play a big role.

Furthermore, customers take some part of the responsibility in fighting back the cyber crimes in collaboration with the solutions that tech companies provide. Most of the social media platforms have the option of reporting a spammer or a potential cyber-criminal. This would help

## FAKE ADVERTISEMENTS AND THEIR CONSEQUENCES

in alleviating the problem to some extent. In general, not being ignorant about the situation and protecting oneself from that attack is very important along with the measures that the companies should take.

Most customers might not be aware of how the crimes that attack them work. However, just like other social media stories that get shared, if experts share their tips on how the community can protect themselves from scams, it will save many people. It could be hard to teach customers, but to some extent, I believe that there is room to easily educate with the help of technology experts and the government.

### **Other Potential Solutions**

There were other solutions provided by the guardians' authors --Nguyen Vo and Kyumin Lee-- from Worcester Polytechnic Institute. The solution provided was to collect and analyze online users called 'guardians'-- who correct misinformation and fake news in online discussions by referring to fact-checking URLs. They also proposed a novel fact-checking URL recommendation model to encourage the guardians to engage more in fact-checking activities. The authors have found that the guardians usually took less than one day to reply to claims in online conversations, and took another day to spread verified information to hundreds of millions of followers. However, "the proposed recommendation model by the research conducted outperformed four state-of-the-art models by 11%~33%" witnessing that this model will be a solution to alleviate the spread of fake advertisements (Lee & Vo, 2018, p. 275).

# FAKE ADVERTISEMENTS AND THEIR CONSEQUENCES

## **Conclusion**

Although advertisements have enabled tech services to be accessed for free while making a profit for themselves, they have also caused significant damages. The injuries range from distracting customers during working hours, spreading fake advertisements to major cybercrimes, identity thefts, and compromised privacy. Although some customers who were aware of the situation chose to subscribe to ad-blockers, others still aren't willing to pay for ad blockers. The statistics show that the number of customers purchasing ad-blockers are increasing every year, but so will cybercrime get much more sophisticated; we need to start combating the problem starting from now.

It should be our responsibility to fact check before purchasing from websites or taking an informed decision. The situation is going to continue being aggravated shortly. Consequently, all hands including companies and customers should work together to solve the problem. Hence, the tech companies would need to find a way to mitigate the issue arising from hosting ads on their platforms --either by filtering fake ads, or making the ads less annoying and destructive-- while allowing blocking the ads when necessary to build their credibility among customers.

# FAKE ADVERTISEMENTS AND THEIR CONSEQUENCES

## References

- Bizga, A. (2020). More than 12 Data Points are Publicly Available on 60% of Internet Users. Retrieved November 30, 2020, from <https://securityboulevard.com/2020/09/more-than-12-data-points-are-publicly-available-on-60-of-internet-users/>
- Chiou, L. & Tucker, C. (2018). Fake News and Advertising on Social Media: A study of the Anti-Vaccination Movement. *National Bureau of Economic Research 1050 Massachusetts Avenue Cambridge, MA 02138*. Retrieved November 30, 2020, from <http://www.nber.org/papers/w25223>
- Clement, J. (2020). Google: Ad revenue 2001-2018. *Statista*. Retrieved November 30, 2020, from <https://www.statista.com/statistics/266249/advertising-revenue-of-google/>
- Clement, J. (2020). Twitter: Annual segment revenues 2019. *Statista*, Retrieved November 30, 2020, from <https://www.statista.com/statistics/274566/twitters-annual-revenue-by-channel/>
- Gunnars, K. (2020). How Does Facebook Make Money? The Unbiased Truth. *Stock Analysis*. Retrieved November 30, 2020, from <https://stockanalysis.com/how-facebook-makes-money/>
- Guttmann, A. (2020). Ad blocker usage in U.S. *Statista, Advertising and Marketing*. Retrieved November 30, 2020, from <https://www.statista.com/statistics/804008/ad-blocking-reach-usage-us/>
- Impact of media use on children and youth. (2003). *Paediatrics & child health*, 8(5), 301–317. Retrieved November 30, 2020, from <https://doi.org/10.1093/pch/8.5.301>
- Lee, K. & Vo, N. (2018). The Rise of Guardians: Fact-checking URL Recommendation to

## FAKE ADVERTISEMENTS AND THEIR CONSEQUENCES

Combat Fake News. *Computer Science Department, Worcester Polytechnic Institute Worcester, Massachusetts 01609*. Retrieved November 30, 2020, from <https://doi.org/10.1145/3209978.3210037>

Mark, G., Iqbal, S., & Czerwinski, M. (2017). How Blocking Distractions Affects Workplace Focus and Productivity. *Microsoft Research, One Microsoft Way*. 978-1-4503-5190-4/17/09. Retrieved November 30, 2020, from <https://dl-acm-org.proxy.library.stonybrook.edu/doi/pdf/10.1145/3123024.3124558>

Mustafaraj, E., & Metaxas, P. (2017). The Fake News Spreading Plague: Was it Preventable? *In Proceedings of ACM Web Science Conference, Troy, NY, USA, (WebSci'17), 5 pages*. Retrieved November 30, 2020, from <https://doi.org/10.1145/3091478.3091523>

Negash, R. (2020). *AD Phishing: The Consequences of Fake Advertisement On Social Media*. Unpublished Paper, Stony Brook University of New York.

WARC staff, M. (2019). Consumers reluctantly prefer ad-supported content. *WARC News*. Retrieved November 30, 2020, from <https://www.warc.com/newsandopinion/news/consumers-reluctantly-prefer-ad-supported-content/43053>