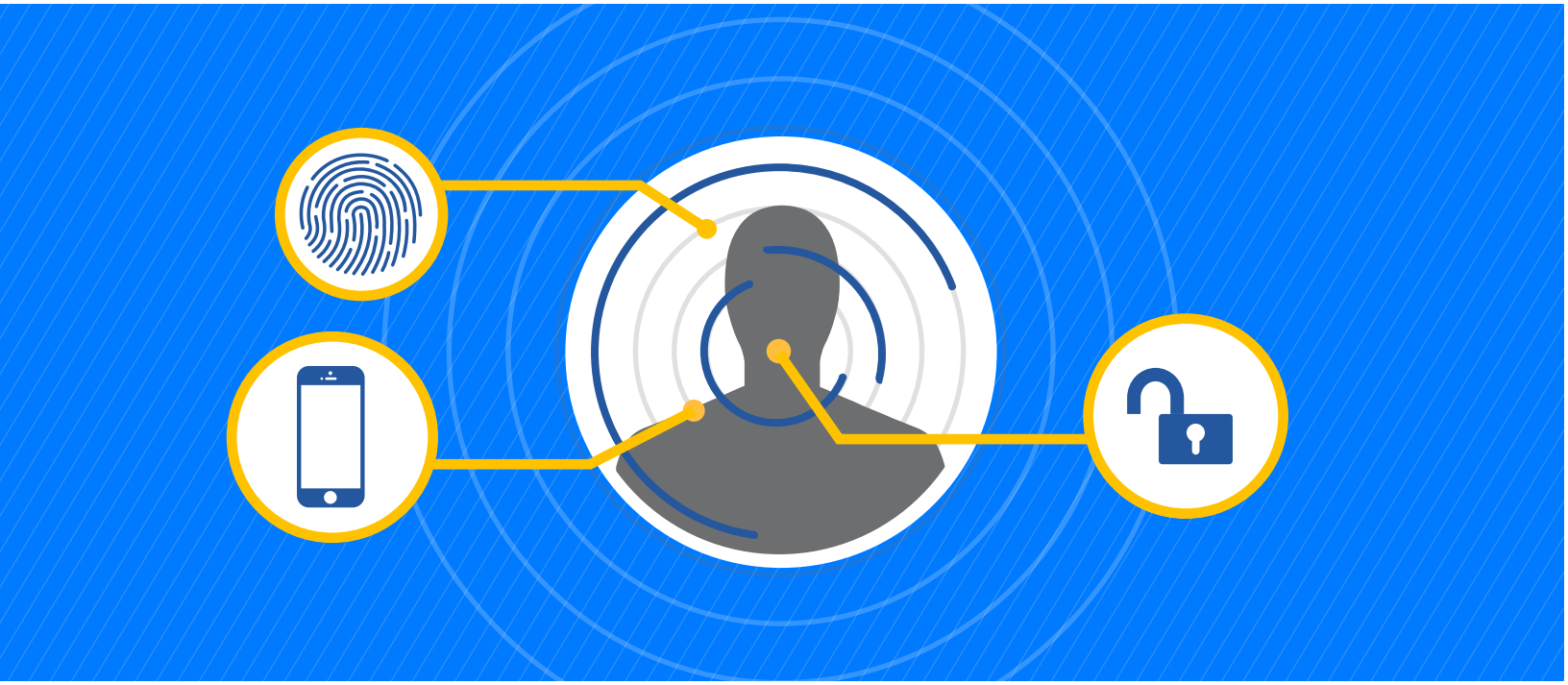
PERFORMANCE MARKETING FRAUD:

How to Detect and Prevent



has offers by TUNE

PERFORMANCE MARKETING FRAUD:

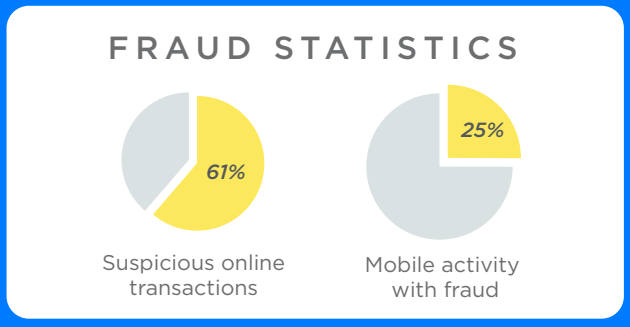
How to Detect and Prevent

Performance marketing can help drive sales without risking a lot of capital upfront, as businesses only pay for advertisements that successfully achieve a goal, such as prospects visiting a landing page or downloading a file. Unfortunately, there's a great deal of fraud in the industry, and that can turn business owners away from the performance model. Since entering the performance marketing arena in 2009, HasOffers by Tune has seen every type of fraud imaginable, so we think it's important for you to be aware of the scams out there and take action to protect yourself.

Introduction

Performance marketing fraud is a widespread problem. According to Ben Edelman of Harvard Business School, up to 10 percent of affiliate links are fraudulent, and problems such as cookie-stuffing, use of spyware, and improper trademark bidding are rampant throughout the industry.[1]

Performance marketing fraud wastes advertising dollars. A 2013 survey suggested that fraud was one of the largest problems facing the performance marketing industry, and that fraudulent practices were likely to cost the industry at least $10 billion in wasted revenue. Of further concern is the fact that the survey found 61 percent of online transactions to be suspicious and 25 percent of mobile activity also may have involved fraud.[2] This year, marketers worldwide expect fraud to cost them about $6.3 billion.



Fraud not only wastes money, but can harm the performance marketing industry's reputation. Consumers may begin to be desensitized to or become suspicious of advertisements that require them to click on links or input their email address in order to download a file. Protecting yourself against fraud can ensure that you don't waste time and money.

Types of Fraud

Fraudsters make extensive use of technology to try to scam consumers and make extra money for themselves that they don't have any legitimate claim to. There are six main practices that you should be aware of so you can protect yourself.

01. Click Fraud

Click fraud occurs when a publisher tries to increase his or her income on cost-per-click advertisements by generating clicks from people who don't plan to look at the advertisement. This practice hurts consumers as well as marketers as fake clicks drive up the cost-per-click of advertisements and make it more difficult for publishers to afford sponsored links and other advertisements.

This scheme can be played out in several ways:

- The advertiser hires people from foreign countries to click on links over and over without looking at them.
- The advertiser has associates click on the same link over and over.
- The advertiser uses spyware or bots to generate clicks on links.

If you are considering signing up with a publisher, check where links will be posted to make sure you are not exposing yourself to click fraud.[3] (This will be covered in more depth in the section on prevention.)

02. Using Spyware/Adware

Some fraudsters use spyware or adware to generate income without actually requiring people to click on their links. These types of programs can harm your computer as well as invade your privacy.

Spyware and adware programs are similar to computer viruses in that users accidentally download and install them while surfing the web or reading an email. Once installed, the programs track users' web activity, then simulate that activity to make it appear that the user is clicking on an affiliate's link. Thus, the affiliate gets income without getting real clicks on their links. These malicious programs can also slow down a user's computer performance or cause advertisements to pop up on the screen whenever he or she uses a web browser.

03 Spam Tactics

Spam, or the unsolicited sending of advertisements and marketing materials through email, is a serious problem and has been for several years. Back in 2008, 66 percent of people were considering switching social networks because of the prevalence of spam, and this problem continues to plague consumers today.[4]

Spam may seem harmless—after all, you can delete unwanted emails—but in many cases, it extends beyond just advertising. Some spam messages contain links to phishing sites or sites that are designed to fool users into sharing passwords, bank account numbers, and other personal information. Some of the links in spam messages may also be infected with viruses or malware. When users click on these links, they infect their computers and may open themselves up to identity theft or other serious problems. Spam occurs on social networks as well as in email; spammers post advertisements or links on social media sites, and in some cases clicking on those links can open the door for fraudsters to steal the user's account credentials and post fraudulent information on their social media sites.

04 Typo Fraud

All consumers should be aware that when they mistype a legitimate site's domain name, they may be redirected to a site owned by a fraudster. For example, typing “tiwitter.com” instead of “twitter.com” might lead to a spam site. This type of fraud is becoming more and more common in performance marketing.

Publishers who engage in typo fraud spend a relatively small amount of money in order to gain a ton of illegitimate site visits and links. They register common typos as domain names so that consumers are redirected to their sites when they make a mistake while trying to access the real site. If the spam sites are signed up for an affiliate marketing program, the fraudster gets money every time someone accidentally accesses one of the sites.

05 Identity Theft/Card Theft

Identity theft is a serious concern, especially if you shop online at all; about 15 million people a year fall victim to it.[5] When it comes to performance marketing, identity theft is problematic because fraudsters can steal your debit or credit card along with your identifying credentials and use them to purchase products from affiliate links.

06 Traffic Diverting

Fraudsters will use any means possible to divert traffic from legitimate sites to their own sites. For example, they might install malware on a legitimate merchant's site so that consumers are automatically redirected to their site instead of staying on the site they meant to visit.

Ways to Detect Fraud

It's very difficult to detect fraud without utilizing a software solution because most fraudulent activity requires the use of sophisticated technology. For example, HasOffers offers a customizable tool that allows you to scan affiliate profiles for potential fraud.

Other ways to protect yourself from fraud include:

- Using security tokens to authenticate publishers and links.
- Creating a white list of IP addresses that referrals must come from.
- Track referral links to ensure traffic is coming from legitimate sources.

Fraud Prevention Tips

In order to prevent performance marketing fraud, there are a few things you can do. You should always check any affiliate you're considering doing business with to make sure they have an active website. When looking at the website, make sure the content matches the product being sold; for example, don't sign up with an affiliate that has a blank website or a website devoted to a totally different type of product than the one you are trying to sell. The website should be SEO optimized but should not use black hat techniques such as repeating keywords over and over without offering quality content.

Conclusion

Performance marketing fraud is expensive and problematic, but you don't have to become a victim! Be aware of the various types of fraud out there, check websites thoroughly before signing up for affiliate links, and use available software solutions to help detect fraud before it becomes a problem. In doing this, you can save yourself time, money, and headaches when managing your performance marketing program.

References

1. http://adexchanger.com/data-driven-thinking/5-performance-marketing-frauds/

2. http://www.cmo.com/articles/2014/6/9/ad_fraud_digital.html

3. https://www.hitslink.com/whitepapers/clickfraud.pdf

4. https://www.cloudmark.com/en/press/nationwide-survey-shows-the-prevalence-of-spam-on-social-networking-sites-threatening-growth-and-membership-retention

5. http://www.avangate.com/avangate-resources/article/affiliate-fraud.htm

6. http://www.identitytheft.info/victims.aspx

7. http://www.tune.com/blog/4-ways-to-detect-fraudulent-activity-in-your-network/