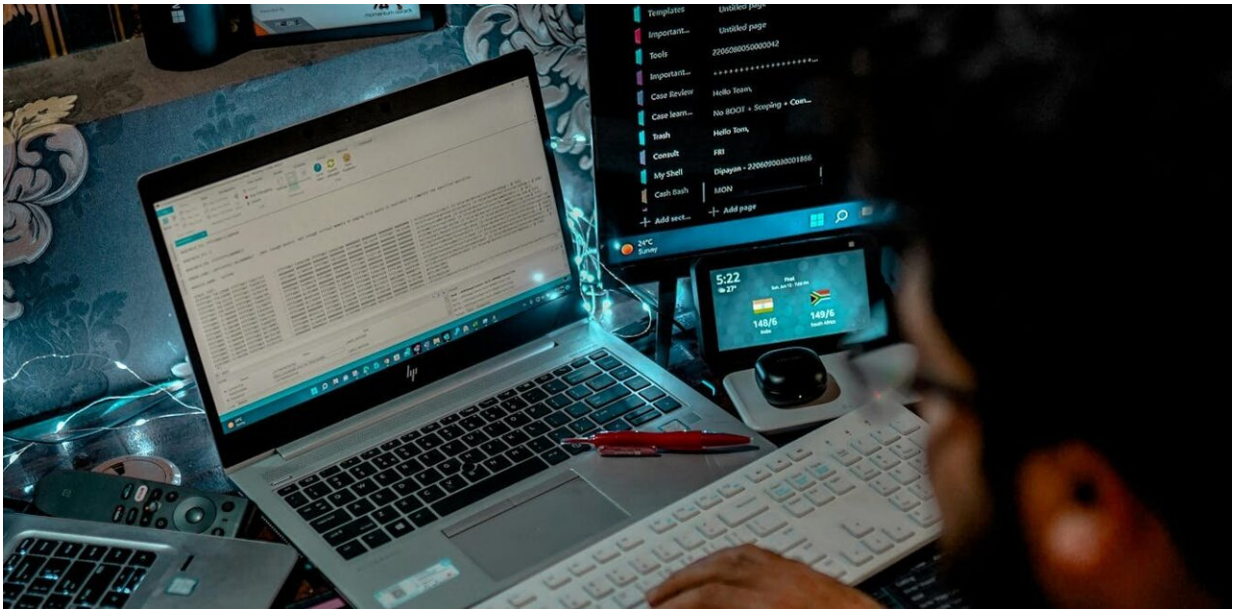
What are 'click frauds'—and how can we stop them?

August 30 2024, by Monica Whitty



Credit: Syed Qaarif Andrabi/Pexel

In the world of the internet, clicks are currency. The more people click on a website, social media post or an advertisement, the more that content generates revenue.

But cybercriminals can exploit this rapidly growing market for clicks through what are known as "click frauds." And everyone, from everyday internet users to large organizations that use the web to share content or

sell their products, is vulnerable.

But what exactly are "click frauds"? And what can be done to prevent them?

What is click fraud?

Click fraud occurs when someone creates a network of bots or sets up "farms" of human workers to generate clicks online. It can take many forms.

Fraudsters often use automated bots or click farms to generate fraudulent clicks on ads or likes on their own websites. They create websites and invite businesses to advertise on their site at a cost. If advertisers are paying per click, then the fraudster will earn money for their business (which is often a fake business) and divert traffic to their site.

Alternatively, a genuine business might create their own advertisements and place them on various websites. Cybercriminals might bombard these advertisements with clicks, which will be very costly for genuine businesses when they are paying per click.

The motivation here may be that the criminal has their own genuine business, and they are hoping the advertising cost will be so expensive it will put their competitor out of business.

A third method is that a criminal may create a fake website they hope users will click on.

This is because the site has a malicious link that will download malware onto a user's computer, or because they hope to scam the user in another way (for example, by paying upfront fees for a service or items that do

not exist).

By increasing traffic to their website, the website moves up in online search rankings. This impacts the general user who believes that because the site is high up in the order, it is a genuine and popular business they should trust.

Higher clicks can lead to higher trust

The psychological theory of planned behavior provides some explanation for why people might trust a site that has numerous clicks and likes compared to a site that has few.

According to the theory, human behavior is guided by three main factors: attitudes, subjective norms and perceived behavioral control.

Let's consider each of these with respect to click fraud:

- Attitudes: people often associate higher numbers of clicks, likes and traffic with credibility and trustworthiness. This is based on the belief that if many others engage with a site, it must be valuable, reputable or of high quality.
- Subjective norms: subjective norms involve the perceived social pressure to perform or not perform a behavior. If people see their peers, or society in general, trusting and using sites with many clicks and likes, they may feel pressured to trust these sites as well. This social influence can reinforce the behavior of valuing and trusting high-traffic sites.
- Perceived behavioral control: high traffic, clicks and likes can serve as indicators a site is reliable, reducing the perceived risk and effort required to evaluate it. When people perceive it is easier to trust a site with many popularity indicators, they are more likely to trust that site.

How can you prevent click fraud?

Ad fraud software is one method to prevent harm from click fraud.

Businesses can use specialized ad fraud detection and prevention tools, such as ClickCease, Fraudlogix or DoubleVerify. These tools can analyze click patterns, detect anomalies and block suspicious activity.

Businesses can also use IP blacklists to identify and block known fraudulent IP addresses. An IP—or "internet protocol"—address is a unique identifying number for any device connected to the internet.

Businesses can also employ geo-targeting to limit ad exposure to specific regions or locations, reducing the risk of fraudulent clicks from irrelevant or high-risk areas.

The general internet user can also be a part of the solution. We need to change our online shopping and trust behaviors. Some of the following checks will help users determine if a website or business is genuine:

- verify the source. Is it credible and well-known?
- hover over the URL. Is it a known web address? It may mimic one, so a close inspection is needed. For example, the legitimate website www.google.com might be www.go0gle.com
- become more aware of click fraud. Knowing it is prolific and that you are most likely to encounter it in your everyday life will help you learn to spot it and avoid it.
- use antivirus and anti-malware software protection to help protect you, identify malicious websites, and keep your software up to date. You cannot solely rely on this software to protect you, but it is an important part of the solution.

Commons license. Read the original article.

Provided by The Conversation