UNDERSTANDING ONLINE TRAFFIC FRAUD

Based on document published by IAB US' Traffic of Good Intent Task Force;
Adapted for Australia by the IAB Australia Brand Safety Council, July, 2014.

SUMMARY

Advertisers expect that all online content is viewed by human audiences - real consumers who have the potential to buy a product or service. That is not always the case. The interactive advertising industry is plagued by an increasing level of illegal activity,known as traffic fraud,which is used by criminals to exploit the system and get paid for fake,non-human traffic. Traffic fraud is a serious problem. Addressing the issue together as an industry is essential to preserving the integrity of the online ecosystem and for maintaining trust from marketers. Read on to learn about the criminal practice of generating fraudulent traffic and what you can do about it.

WHAT IS ONLINE TRAFFIC FRAUD?

The potential for digital advertising fraud exists anywhere that media spending is significant and performance metrics are ambiguous or incomplete. Nefarious groups have found ways to profit by infiltrating legitimate systems and generating false ad views,ad clicks,and site visits using robotic programs. Robotic traffic,commonly known as “bots”, is driven by code,not humans,so it has no ability to generate real conversions or purchases. Bots are smart enough to mimic human behavior,making them difficult to detect. The activity generated by these bots muddles the engagement metrics driven by real,human traffic,which dilutes the value of legitimate publisher inventory. In addition,advertisers end up paying a material portion of their campaign dollars to fraudsters who deliver specious ad impressions that are never seen by humans.

WHY YOU SHOULD CARE

Allowing “bad actors” to profit from traffic fraud affects the entire online advertising industry. In addition to diluting inventory value and diverting payment from legitimate businesses to fraudulent ones,traffic fraud also impacts the integrity of digital media.

Six negative impacts of traffic fraud:

1. Brands waste money on ad campaigns that include a material portion of fraudulent impressions.
2. Fraud complicates campaign performance analysis when human and non-human activity for ads and site visits are both included in reports.
3. Brands lose confidence in digital media.
4. The supply of inventory is inflated artificially,reducing the value of legitimate publishers.
5. Failing to root out traffic fraud funds criminal activity and supports organized crime.
6. Fraud undermines industry self-regulation efforts,invites negative press about the industry,and potentially intervention by government regulators.

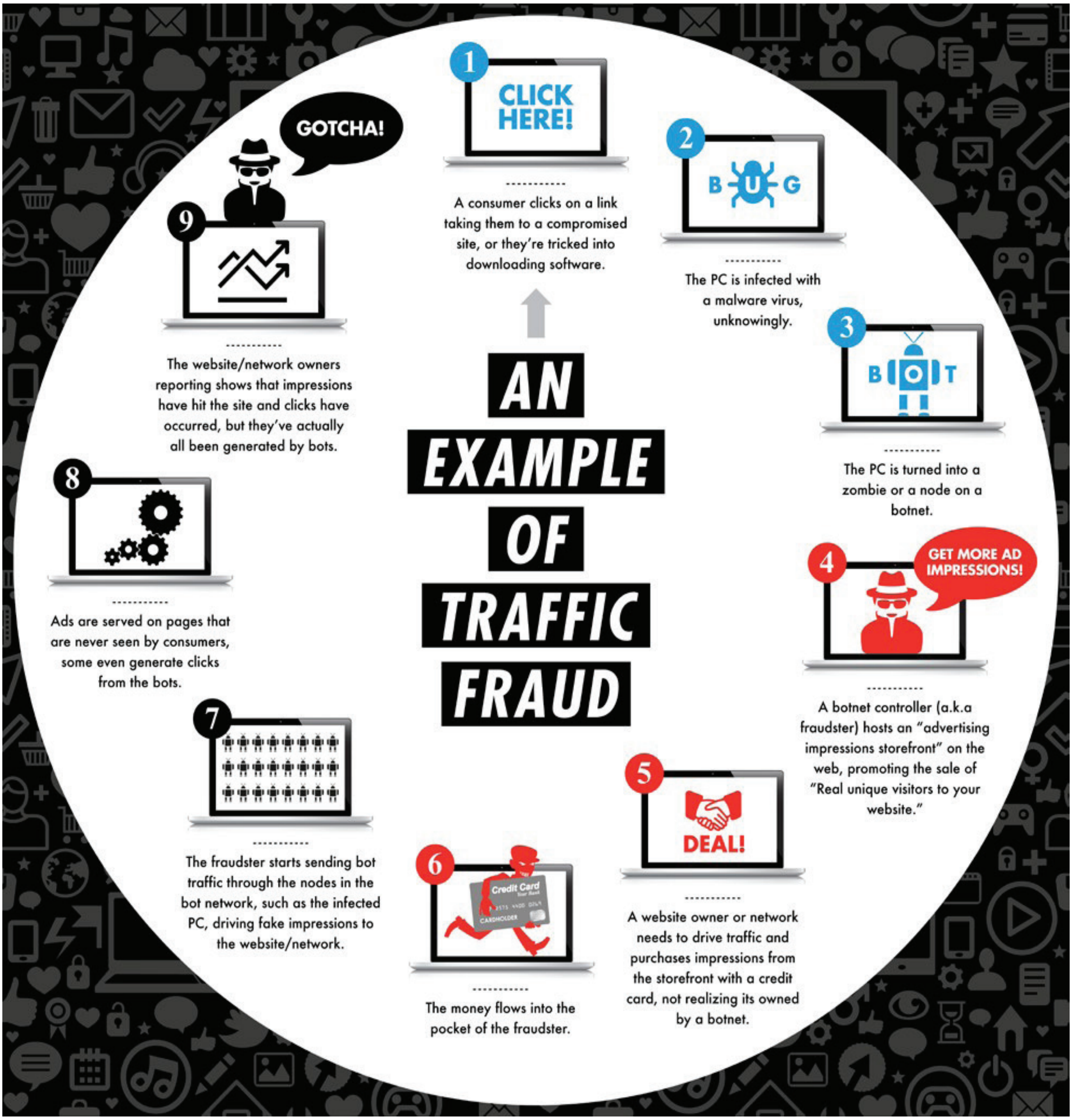
WHO ARE THE BAD ACTORS?

The bad actors in digital advertising traffic fraud are organized criminals preying on legitimate businesses. Successful traffic fraud requires a concerted effort to generate “results” that fool the buyers.

These are not university students just trying to make some cash or rebel-techies from Silicon Valley. The bad actors are organized criminals,usually operating outside of countries with tighter regulations such as the United States and Australia,and are often funded by larger criminal organizations. The bad actors are not just gaming the system, they are engaging in organized criminal activity.

EXAMPLE OF TRAFFIC FRAUD

The following illustrates how easy it can be to become a victim of traffic fraud.



1. A consumer clicks on a link taking them to a compromised site, or they're tricked into downloading software.

2. The PC is infected with a malware virus, unknowingly.

3. The PC is turned into a zombie or a node on a botnet.

4. A botnet controller (a.k.a fraudster) hosts an "advertising impressions storefront" on the web, promoting the sale of "Real unique visitors to your website."

5. A website owner or network needs to drive traffic and purchases impressions from the storefront with a credit card, not realizing its owned by a botnet.

6. The money flows into the pocket of the fraudster.

7. The fraudster starts sending bot traffic through the nodes in the bot network, such as the infected PC, driving fake impressions to the website/network.

8. Ads are served on pages that are never seen by consumers, some even generate clicks from the bots.

9. The website/network owners reporting shows that impressions have hit the site and clicks have occurred, but they've actually all been generated by bots.

HOW YOU CAN REDUCE RISK

Reduce your risk of exposure to traffic fraud and help the industry fight the bad actors by being more proactive in your operations:

Educate yourself about traffic fraud, the risks that it poses to your business,and identify activities that can help you mitigate them.

Craft policies and procedures to eliminate low-level fraud,such as comparing impression volumes to audience sizes reported by third-party measurement services.

Set clear objectives for your media campaigns that focus on the measurement of real ROI,which is difficult for fraudsters to falsify. Measurements such as click- through rate,completion rate,or last-touch attribution can easily be faked or gamed.

Practice safe sourcing. Only trust business partners who have earned trust. Implement technology to detect and prevent fraud. Filter traffic through vendors who specialize in fraud detection.

Get involved with IAB's fraud initiatives and its Brand Safety Council (see below).

DEFINITIONS

Online Traffic Fraud: Visits to publishers' site(s) which occur without the knowledge of a user,or driven by non-human actors; Can be initiated by a person's online actions,or fully controlled by a bot that has infected a personal computer.

Fraudster: A person,company or organization that knowingly engages in the perpetration of online traffic fraud.

Bots or Robots: Any non-human or automated user-agents that produce HTTP web traffic.

Botnet: A network of robots consisting of PCs that have been infected with malicious software that turns them into slave computers managed by a botnet controller.

Bot Node: A single infected PC within a botnet.

Non-Human Traffic: Online advertising traffic that is artificially generated from machine-initiated or other non-human activity.

Hidden Ad Impressions: Ad impressions that are not observable because they are hidden behind other ads or content,displayed in tiny iFrames or served in other ways that prevent them from being seen by consumers.

Laundered Ad Impressions: Ad impressions where the original traffic source or other delivery characteristics are obfuscated,altered or misrepresented by the seller.

Learn more at http://www.iabaustralia.com.au/