DIGITAL MARKETING SECURITY

Roy Dovaston explains the importance of maintaining a secure digital campaign

Recently, digital marketing has become an invaluable platform for businesses to cost effectively reach an extended audience base; particularly as social media has become an integral part of public life. However, a sufficient digital marketing campaign requires considerable investment in both time and effort. More specifically, to ensure seamless success throughout an online campaign, market research must be conducted, content developed, online ads created and a budget devised.

While these expenditures often gain significant rewards for aspirational businesses, targeting an enhanced pool of potential clientele through the ease of the internet, only converts to profit if the security of the campaign is efficiently maintained. This may otherwise prove to be a somewhat pointless activity, with any benefit being lost to the pitfalls and perils of online marketing platforms. It appears that developing a good strategy is crucial for success within digital marketing, as web security involves distinct risks for you and your customers – as privacy may easily be sacrificed. This is particularly evident when considering the vulnerability of online ads, which are increasingly susceptible to click fraud – the disingenuous clicking of your ads to deplete your daily advertising budget.

To proactively prevent such an event and fully comprehend the importance of web security, you must understand exactly who your website must be secured against – namely hackers. Hackers are highly skilled individuals capable of harvesting your data with ease – no matter the size or credentials of your business.

HACKERS' DELIGHT

These culprits typically seek three things when exploiting online platforms: personal information, financial information and login details. Meanwhile, it is worthwhile noting that the intelligence and adaptability of these individuals is ever increasing. The immediacy in establishing improved web security has never been more prominent. With regards to click fraud for example; fraudulent clicks now originate from a multitude of sources – from manual click farms to automatic click bots.

The importance in creating and sustaining a secure digital campaign similarly becomes all the more apparent when considering the vast popularity that use the web, social media and technology; as it has been suggested that cutting-edge tech is set to define 2018. These ongoing developments, when paired with the diverse skill base of rising hackers, require businesses to consider their marketing strategies more closely.

Business owners may see this to be somewhat daunting, particularly when considering the rapidly advancing diversity of cyber attacks. To further emphasise the importance of web security and click fraud prevention within digital marketing campaigns, here are some specific online security threats and methods of avoiding these hurdles.

One way in which your website's security may be sacrificed, is maladvertising; whereby hackers install malware in ads which appear on trusted websites, largely in the hope that customers will click on them and innocently download or install malware on a computer containing critical information. Worryingly, there are numerous types of malware that can endanger your system; with viruses plaguing your network, corrupting data and system files. Similarly, as an unfortunate consequence of tech developments, hackers can corrupt your server by installing malicious software; infecting the computers of your clients, who may click on ads hosted by your own website or links included within your newsletters. If this happens, your customers will be significantly less inclined to return and utilise your services.

Fortunately, it is not difficult nor necessarily expensive to protect against these issues. You should only need to remain educated and knowledgeable with regards to how your systems may become infected, including knowledge of sufficient methods to avoid these risky circumstances. If you feel particularly daunted by this prospect and believe that remaining up to date with current prevention software and threats is beyond your realm of understanding, it may prove invaluable to seek the advice of industry experts. As a result, you will be able to educate staff on the dangers of clicking untrustworthy ads or links, preventing a large majority of cyber attacks. Should you opt for a simple fix, however, your first line of defence should begin with acquiring the best firewall and anti-virus software available. Similarly, installing an anti-virus browser plug-in or extension can help you decide whether it is safe to click or not.

Pay-per-click ads are known for attracting this malware, however this comes in addition to alternate forms of persistent hacking – such as click fraud. This may prove particularly difficult to identify, as there are several methods of click fraud; predominantly, automated and manual. Automated click fraud uses software – frequently coined 'click bots' – to repeatedly click on your ads, while manual click fraud is committed by actual people, often employed in 'click farms'. Adding to this difficulty, there are several, very different, common sources of click fraud. These include your competitors, site owners

> IT HAS BEEN REPORTED THAT MORE THAN HALF OF ALL WEB TRAFFIC IS NON-HUMAN

(publishers or their employees can click on their own website ads, and therefore make their own site more attractive for ad placement) and customers; who may unknowingly contribute to click fraud when they regularly click through on paid search ads to regularly access your site, as opposed to using a search or bookmark.

While you may use your own analysis to identify and prevent instances of click fraud, liaising with Google and filling out time-consuming online forms, it may be worth considering the use of third-party specialists of such fraudulence.

This form of digital threat is becoming rife within the realm of online ads, as non-human traffic – such as click bots – continue to be a persistent concern, hindering the success of digital campaigns. It has been reported that more than half of all web traffic is non-human, developed with the sole purpose of diminishing the accomplishments of your marketing campaigns; therefore, avoiding the often-overlooked issue of click fraud no longer serves an organisation's needs. With the evolution of malware and its couriers, this fraudulent non-human traffic comes in several alternative formats. For example, scrapers record links and other information from every page on a site. Unfortunately, the automated nature of online advertising, which in many cases is what makes this the most beneficial form of marketing, makes online advertising the perfect hunting ground for these bots.

Additionally, impersonators are pieces of software capable of capturing and recreating user credentials; opening the floodgates to a potential influx of spy bots, click bots or fraudulent browsers. Advertising that gets little human attention may be repeatedly crawled by these impersonators, designed to create false traffic counts and clicks. Acting as a form of pay-per-click fraud, these lead many business owners

to believe their campaigns are much more successful than they actually are – wasting critical time and energy as a result.

CREATING CHAOS

Social media is an increasingly popular tool for business owners wishing to remain up to date with regards to the design of their advertising campaigns. Unfortunately, the use of social media, however simple, does not prevent against similar web security threats. Unfortunately, just as customers are increasingly familiar with and show a preference for the use of major social media sites – so are hackers. Unexpectedly, it also appears that in many cases these hackers do not want access to private information – yet solely aim to create chaos for you or your customers. In such instances, social media appears to be the perfect hot bed for this activity – allowing hackers to make changes to your profile, add offensive photos or false statements and subsequently quickly diminishing the success of your marketing strategy. Additionally, fraudsters may be more inclined to target ads presented across social media platforms, for this may be seen to be the most fiercely competitive advertising channel. To prevent against this, the use of click-fraud prevention software may again be of benefit – particularly as sponsored ads are being promoted more frequently across social media channels. In addition, simplistic techniques often prove to be incredibly valuable. For example, strong passwords changed regularly, are very useful. Strong passwords have at least 12 characters, including lower-case and capital letters, numbers and symbols. For clear purposes, it is similarly recommended that personal information is not to be included within these passwords.

Fundamentally, the answer as to why web security is so important rests with the basic goal of your business. This includes the ability to earn money form this venture and expand as a dedicated organisation. All aspects of your daily operations, therefore, need to be carefully considered, including your web security. While relying on the internet as an invaluable source it's a predictable and warranted path for most businesses, benefits will only be seen if necessary measures are implemented. Unsecure websites and ads lead to compromise not only for you as an owner or manager, but also your clientele – preventing return and upping costs as remarketing strategies subsequently need to be devised, where this may easily be avoided

DIGITAL MARKETING REQUIRES CONSIDERABLE INVESTMENT IN BOTH TIME AND EFFORT

Roy Dovaston is the owner of pay-per-click agency and anti-click fraud specialist Click Guardian. Having been managing Google Ads since the inception of Google AdWords, in 2014 Roy realised a major issue was going undetected in the form of excessive clicks on his client's ads. Click Guardian was born from this insight and now actively protects thousands of AdWords advertisers in the fight against click fraud.

Hackers can corrupt your server by installing malicious software

Picture credit: Getty