International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Cyber Threats through Various Digital Marketing Techniques in India

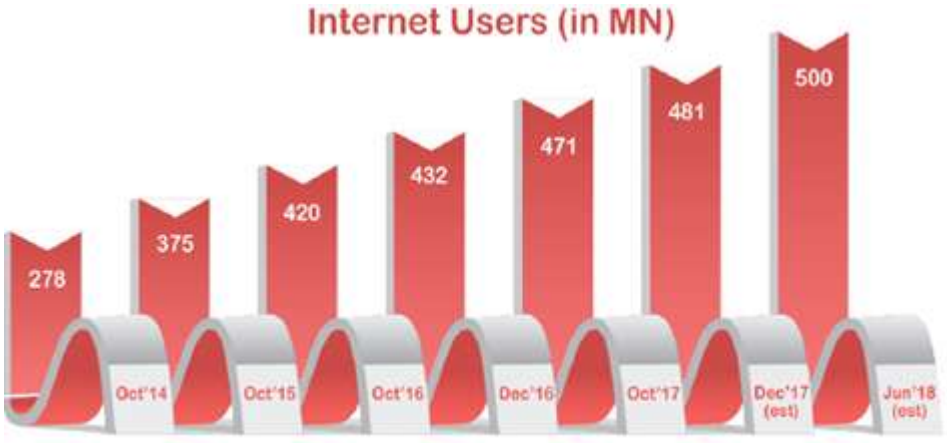
Nandan R. Naresh

Assistant Professor AIGS Bangalore

Abstract: ***The massive Indian market is changing fast. Internet access is mainstreaming among professionals and the use of mobile is intensifying. More people spend more time online in India every year, and the digital tools and sites they use play an ever-growing role in their lives. Smart marketers keep on top of the scale of change and ensure their marketing strategies and touch point's mirror where the consumer is spending their time. A cyber threat can be both unintentional and intentional, targeted or non targeted, and it can come from a variety of sources, including foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, disgruntled employees and contractors working within an organization. In this paper, we investigate and study the cyber threats through various effective ways of Digital Marketing in India.***

1. Introduction

The number of internet users in India will reach 500 million by June 2018, a report by IAMAI and Kantar IMRB says. At the end of December 2017, India had 481 million users, growing 11.34% from 2016. According to the findings of the report, urban India witnessed growth of 9.66% from December 2016 and is estimated to have around 295 million internet users as on December 2017.On the other hand, rural India witnessed growth of 14.11% from December 2016 and is estimated to have around 186 million internet users as on December 2017.Therefore millions of internet users regularly visit thousands of social website to keep linking with their friends, share their thoughts, photos, videos and discuss even about their daily-life.. Now Indian consumer is spending more time on social media and internet surfing. Thus the visibility of any product is more through digital medium than traditional marketing techniques. Digital marketing techniques include Content Marketing, Marketing Automation, AdWords, SEO, Social Media, Email Marketing and Website Design. Digital Marketing is a part of a Digital Economy. India is a fast moving nation towards digital economy and this movement has been accelerated with the recent trends.



Source: IAMAI & Kantar IMRB I-CUBE 207. All India Users Estimates. October 2017

Due to the fact that the numbers of Internet Users are increasing and the digital marketers are also using this chance to grow rapidly we can find that the Cyber Threats are also increasing at the same phase. The number of attacks carried out by hackers to steal personal information is also raised. Hacked information is being used for many other purposes. The purpose of this paper is the study the various Cyber Threats in each Digital Marketing techniques.

2. Techniques of Digital Marketing & Threats Associated

1) **Search Engine Optimisation (SEO):** Search engine optimization, or SEO, is the technique of designing a website to improve its ranking in search engines. This is a normal operational concern for websites and not inherently malicious; if a website operator wants to attract more visitors, he or she will want the search engines to steer people to the site. However a malicious person (or group) who wants others to visit a Web server that will attempt to compromise the browsers of visitors. Just like a commercial or ad-driven website, the malicious site's operator needs to get the search engine to deliver some users. This is where search engine optimization comes in to play; the malicious website is created with wording that will increase its search engine ranking. Unlike a "normal" website, however, that wants to attract people with a specific interest -- an online sports site, for example, needs readers interested in sports

-- a malicious website operator wants anyone and can change the focus to increase its visitors. Therefore when visitors start visiting the website malware installed will typically add the infected system to a botnet for long-term command and control of that asset. That computer can then be used to send spam, transmit attacks, and capture sensitive information and user credentials for financial institutions and online merchants. The use of the infected computer becomes a commodity for sale, and information stolen from the visitor(s) can be used for identity theft and financial crimes.

2) **Search Engine Marketing:** Search engine marketing (SEM) is a form of Internet marketing that involves the promotion of websites by increasing their visibility in search engine results pages (SERPs) primarily through paid advertising. Here the malicious websites pay to search engines for them to be ranked in the first page of the search results. Thus when visitors start using the websites, the personal information are being hacked by the malicious groups either by asking various questions or by sending Spam contents.
3) **Email Marketing:** Email is one of the most valuable channels for marketers to communicate with consumers. Sixty-one percent of consumers prefer to receive offers from brands over email and marketers have responded by optimizing and personalizing email content to deliver the best experiences possible. It sounds like a perfect relationship. But while email may be the best way for brands to reach consumers, it's also one of the most common threat vectors for cybercriminals looking to steal sensitive information, such as passwords and credit card data. Recently email attacks have become so sophisticated, that it's hard for brands to fight back. Around 97% percent, people globally cannot identify an advanced phishing email. To make it worst most people open their emails in mobile devices which make it harder to spot a phish.
   - **SPAM:** Spam's are classified as unsolicited emails sent in bulk. Even if spams do not have the threat like a virus-infected attachment, junk email can quickly overwhelm a user making it challenging and impossible for owners to view legitimate messages. In some cases, spam may contain phishing links which trick users into giving confidential information to cyber criminals, or malware sites that download malicious software onto the user's computer.
   - **SPOOFING:** Spoofing can be defined as the forgery of an e-mail so that the message that appears to have come from a person or brand other than the actual source from the cyber criminals. Spoofing takes place in many ways. One of the most common ways is by concealing the actual sender's name and the origin of the email; sometimes the source may be masked from the recipient.
   - **PHISHING:** Phishing can be defined as a kind of spam that is intended to trick email recipients into giving sensitive information or credentials for malicious reasons; this information is then misused. Phishing attacks try to utilize social engineering to steal a particular consumers' personal and financial data Phishing perpetrators operate by hiding under phony identities and names that are stolen from corporate banks, online businesses, and credit-card companies.
4) **Content Marketing:** This is type of marketing that involves the creation and sharing of online material (such as videos, blogs, and social media posts) that does not explicitly promote a brand but is intended to stimulate interest in its products or services. Many businesses use a Content Management System (CMS) such as WordPress to support content marketing. This allows marketers to easily upload, edit, and feature new content like blog posts. However, as the most popular CMS, hackers are very familiar with how WordPress functions. If they hack the site they can use it to distribute malware to users.
5) **Social Media Marketing:** Social media is a great way to share information. Social media is based on the fact that we trust messages on social media platforms more than we do elsewhere, especially if they are messages that are forwarded to us by a friend. Social Media Marketing or SMM is an offshoot of your SEM efforts. It involves driving traffic to sites or business through social sites like Facebook, Instagram, Twitter, Pinterest, Google+, Linkedin, etc. Here good contents are shared and liked. Cyber Threats are more prone through SMM technique of Digital Marketing, the way it works is that a person is targeted with a social media message with a link to the malware. Once that link is opened, the hacker gains access to that person's computer or device and all that person's contacts. They can then send the original message on again – this time from a friend. It's not just the malware that is dangerous; it's the fact that it can be sent on to so many people. As the only thing in the malicious social post itself is a link, then it's something that can be used on any social media platform that contains external links – which is pretty much all of them. While only 30% of people will open a spear phishing email, 66% of people will open a spear phishing link if it's recommended through social media
6) **Mobile Marketing:** Here the website, apps and content is being customized for mobile devices. The mobile users are growing day by day and it is the most effective way of marketing. There has been a dramatic increase in the number of mobile malware with complexity and sophistication. Both Google Play and Apple App Store have found hundreds of malicious and privacy concerns apps and pulled them out. There are tons of free apps available with vulnerabilities and malicious code that have access to personally identifiable information data that is used for advertisement and marketing purposes, and device sensors like camera, microphone etc. These malicious apps can monitor and track activity, steal sensitive data and photos from mobile devices, make unauthorized calls, SMS etc.

3. Conclusion

In the era of mobile applications and various multimedia functions, are enabling the Indian customers within the reach of sellers. Therefore marketers try to find customers here and choose this as their favoured channel. But as a society that runs largely on technology, we are also as a result dependent on it. And just as technology brings ever greater benefits, it also brings ever greater threats: by the very nature of the opportunities it presents it becomes a focal

point for cybercrime, industrial espionage, and cyber attacks. We think that the advancement of new technology in general and social websites in particular will bring new security risks that may present opportunities for malicious actors, key loggers, Trojan horses, phishing, spies, viruses and attackers. In this paper, we briefly described the cyber threats each customer would face through various digital marketing techniques that are existing. Information security professionals, Government officials and other intelligence agencies must develop new tools that prevent and adapt to the future potential risks and threats.

References

[1] "Number of Indian internet users will reach 500 million by June 2018, IAMAI says" Times of India Feb 20 2018
[2] Abdullah Al Hasib, "Threats of Online Social Networks", IJCSNS, Vol. 9, No 11, November 2009.
[3] https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf
[4] https://medium.com/@oliversild/positive-and-negative-impact-of-security-to-your-seo-ranking
[5] Wajeb Gharibi and Maha Shaabi "CYBER THREATS IN SOCIAL NETWORKING WEBSITES" (IJDPS) Vol.3, No.1, January 2012
[6] https://www.relevance.com/overcoming-cyber-security-challenges-in-digital-marketing/