IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138
INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG
An International Open Access, Peer-reviewed, Refereed Journal

ROLE OF CYBER SECURITY IN DIGITAL MARKETING --Steps to fight cyberthreat

Dr.T.Lokeswara Rao. Assoc. Professor
Dr. N V J Rao. Professor
School of Management Studies
GIET University, Gunupur, Odisha

Diptiranjan Pati (I MBA)
Sidhanta Nayak (I MBA)
School of Management Studies
GIET University, Gunupur, Odisha

Abstract

Now-a-days Digital Marketing often focuses on reaching a customer with increasingly conversion-oriented messages across multiple channels as they move down the sales funnel. Cyber-attacks are threatening the security of the user and can steal private information like that information may his include his details or his business details and by this, it can also affect the security of his business. Cyber security is relevant to all system that supports an organization business operations and objective as well as compliance with regulation and laws. With cybersecurity, a business protects its data from hackers and secures business information online. With advanced technologies, businesses are able to secure their data with different systems.

Key words: Digital Marketing, Cyber-attacks, cybersecurity, online, technology.

Introduction

This paper discourses the essential for cyber security on digital marketing, and some of the cybercrime's effects. Cyber security is used to provide prevention against cybercrime. Aim of cyber security is to protect systems, software, networks, computers and data from attack. The term 'digital' can be described as a technology related to the limited transfer of information and which is steady in characteristics. Digital technology uses a constant transfer of consistent information technology. If a marketing task is dependent on digital medium for the execution of its marketing facilities, then that is termed as to be digital.

Digital Marketing is a command to use the information technology for achieving the marketing operations which involves generating, interactive and passing on important things to the clients along with looking after the client relations. Web based business is concerned with the purchase and sale part of the business, using the internet and uses electronic media for money proceedings.

Digital Marketing is initiative that leverages online media. It is connected devises such as mobile phones, home computers, or the Internet of Things (IoT). Common digital marketing initiatives center around distributing a brand message through search engines, social media, application, email, and websites.

Cybersecurity threats for Digital Marketers

1. Email

Yep, email. If your marketing team spends most of its time on social media, it can be easy to forget the oldest digital communication medium is still the most dangerous. Even today, the vast majority of hacks – up to 91% – start with an email.

2. **Malware**

Most people are aware of the standard computer virus. But are you also aware how modern malware has evolved? Today, there's spyware that can record your passwords and keystrokes, while ransomware encrypts a site's sensitive data and only decrypts it when a ransom is paid.

3. **WordPress**

It might seem strange to give WordPress its own entry in this list, given how many systems digital marketers use on a daily basis.

4. **Domain**

WordPress isn't the only web host with issues. Popular forms of attack, like Cross-Site Scripting (XSS), SQL injection, and DDoS have been on the rise in recent years, and all make use of domain-level faults in your security. These dangers are amplified if your website has multiple users, such as freelancers or consultants.

5. **Social media**

Modern marketers are well aware of how effective social marketing can be. But with great power comes great danger. Social media accounts are a favorite target of hackers, because they can cause exponentially more havoc – not just stealing personal information, but hijacking accounts to post offensive material until you pay them to stop.

Importance of cyber security in digital Marketing

Developing a good Digital Marketing strategy is crucial for your business growth. However, you also have to consider the security of the entire marketing campaign- from your website to emails to social media. Neglecting this aspect can cause privacy risks for both you and your customers.

Here are some typical forms of cyber-attacks that involve Digital Marketing:

- Malware infection from files downloaded or links clicked.
- Browser hijacking and redirection.
- Stealing of data and other sensitive information.
- Identity theft.
- Proliferation of fake news.
- DDoS attacks on website.
- Word Press malware.

Scope of Cyber Security in Digital Marketing

Although not as important as your domain knowledge, with the wide scope of cyber security, businesses are looking for dynamic individuals who can combine their product knowledge with a learning orientation. Every role in the cyber security profile has different demands. But there are some basic technical skills;

- **Python**.
  Python has a code readability and syntax which makes it easy to use as it needs lesser lines of codes than other programming languages like C++ and Java to complete a task. Python can be used in a variety of operating systems such as mac, windows, Linux, Unix, etc.
- **Android**.
  From research we find that 1.4 billion Android devices provided in the market. This App can help users to reach their desired services within a second.
- **IoT**.
  It enables the development and deployment of smart devices to solve real-world challenges and issues.
- **Cryptography**.
  As the foundation of modern security system, Cryptography is used to secure transactions and communications.

The National Association of software and services (NAS&S) companies has estimated that India alone will need about 1 million cyber security professionals by the end of 2020 to tackle cyber-crime dangers.

Digital Marketing Strategies

While our favourite digital marketing tricks and strategies can be applied to any industry, they're especially important for cyber security companies, which need to establish a strong sense of trust within their customers. With that in mind, here are some tips to help you better address the marketing needs of your cyber security company

- **Prioritize credibility and trust**

Credibility is, of course, important in every industry, but it's particularly important for cybersecurity companies. This is because cyber-tech customers aren't only looking for a good solution to help them expand and improve business. They're also looking for a good solution that will help them protect their business.

- **Understand your customers**

This leads us to another important point: In order to understand the security issues that affect your targeted customers' industries the most, you'll need to develop a deep understanding of your buyers.

- **Focus on teaching, not selling**

As a cybersecurity company trying to grow your customer base, you're going to want to use inbound marketing strategies that organically focus on lead generation and drive your customers to you. One of the best ways to do this is to offer your customers free value.

- **Go beyond customer expectations**

With the growing number of cybersecurity companies flooding the market, ensuring your company meets customer demands and expectations is vital. But, remember that your customers aren't the cybersecurity experts – you are.

That means that while offering them the solution they're looking for, you should also educate them about newer, better solutions that they themselves might not have thought about before.

Cyber-secure countries in the world

Continuing on from the last two years the safest country is Denmark with a score of 3.56. It was placed in the top three 10 times out of possible 15, scoring particularly well in categories such as,-

- 1% of users attacked by ransom ware Trojans (0.02%).
- 1% of attack by Crypto miners (0.11%).
- 10% users' attacks by mobile ransom ware Trojans and mobile banking Trojans.

Tajikistan is the least cyber secure country in the world followed by Bangladesh and China. Tajikistan was the worst scoring country for the % of users attacked by banking Malware (4.7%).

- % of computer facing at least one local Malware attack (41.16%).
- % of attacks by crypto miners (5.7%).

It also scores poorly for % of user attack by ransom ware Trojan (1.35%).

- It also has some positive or better scoring country for several countries include.
- % of user attacked via web sources (0.03%).
- % of telnet attack by originating country (0.01%).
- %of share of country of country target by Malicious mailing (0.01%).
- Zero users were attacked by mobile ransoms were Trojans and SSH- based attack originated from Tajikistan.

The cyber risks and threats

- Cyber security is relevant to all system that supports an organization business operations and objective as well as compliance with regulation and laws. An organization implements cyber security control across the entity to protect the integrity confidentiality and availability of information assets.
- Cyber-attacks are committed for a variety of reasons includes financial fraud, information leaked, personal data leaked and organization secret leak.

The Common Type of Cyber Security risk

i. Denial of service Attack
ii. Malware- Worm, Trojans, Virus, Spy Ware
iii. Man in the Middle attack
iv. Drive By downloads
v. Password Attack

Specific attacks impacted countries in Covid- 19

- According to the report from Word Health Organization (WHO) that cyber criminals take advantage of the Covid- 19 Pandemic.
- The Cyber Security changes in period of pandemic.
- According to the quarry reports release by Kaspersky. There were a few areas that saw a rise in Q2 tying in with the beginning of the pandemic. The most significant of these were % of attacks by crypto miners' % of mobiles infected with Malware and % of using attacked by mobile banking Trojans.

Last five years Cyber Crime Cases in India

- India recorded 50,035 cases of cyber-crime in 2020 with 11.8% surge in such offences over the previous year as 578 incidents of "fake news on social media" were also reported official data showed on September 15.
- The rate of cyber-crime (incidents per lakh population) also increased from 3.7% in 2020 in the country according to the NCRB (National Crime Record Bureau) data.

- In 2019 'The country recorded 44,735 cases of cyber-crime. While the figures stood at 27,248 in 2018.
- The year saw 4,047 cases of online banking Fraud, 1093 OTP Fraud and 1,194 credit/debit card Fraud while 2,160 cases related to ATM were reported in 2020, the NCRB figured showed.
- There were also 578 cases of fake news on social media 972 related to cyber stalking bullying of woman and children 149 incidents of fake profile and 98 of data theft.
- Interns of motive the maximum 60.2% cyber-crimes lodged in 2020 were done for fraud (30,142 out 50,035 cases). The NCRB which function under ministry of home affairs stated.
- Among the state, the maximum 11,097 cyber-crime cases were reported in Uttar Pradesh followed by Karnataka (10,741), Maharashtra (5,496), Telangana (5,024), and Assam (3,530).

  However, crime rate related to cyber-crime is highest in Karnataka 16.2% followed by Telangana 13.4%, Assam 10.7%, and Uttar Pradesh 4.8%, and Maharashtra 4.4%.

  National capital Delhi recorded 168 such cases during the year with a crime rate 0.8%, according to NCRB, which is responsible for collection and analyzing crime data as define by the Indian Penal Court and special and local Laws in the country.

Government Action against Cyber-Crime

The Government has established **Indian Cyber Crime Coordination Centre (I4C)** to provide a framework and eco-system for LEAs to deal with the cyber-crimes in a comprehensive and coordinated manner.

Government arises 9 types of policy against cyber-crime like;

- CERT – In.
- Cyber- Surakshit Bharat.
- National Critical Information Infrastructure Protection Centre.
- Appointment of chief Information Security Officers.
- Website Audit.
- Crises Management Plan.
- Training and Mock Drills.
- Malware Protection.
- Personal Data Protection Bill.

Steps to fight cyberthreat

Markets and companies should take the serious measures are steps for avoiding the cyber threats, few steps are discussed below.

Step-1: Companies must keep offline backup of data

Step-2: Enhance staff awareness about ransomware

Step-3: Strong spam filter that continually adapts needed

Step-4: Network must be configured to block.exe files

Step-5: Restrict use of privileged access to the network.

The above discussed steps are help to avoid the cyberthreats, so digital markets and companies better to follow the above steps.

Conclusion

Digital Marketing is initiative that leverages online media. It is connected devices such as mobile phones, home computers, or the Internet of Things. Neglecting this aspect can cause privacy risks for both you and your customers. Cyber-attacks are committed for a variety of reasons includes financial fraud, information leaked, personal data leaked and organization secret leak. The Government has taken serious action and established Indian Cyber Crime Coordination Centre (14C) to provide the cyber security. Digital markets and companies need to take the serious measures are steps for avoiding the cyber threats.

References:

1. Bala M., Verma D. "A Critical review of Digital Marketing," www.ijmrs.us,
2. Elizabeth S. B, "Digital Marketing", February 2011, webservices.itcs.umich.edu/.
3. K. K. R. Choo, "The cyber threat landscape: Challenges and future research directions," Comput. Secur., 2011, doi: 10.1016/j.cose.2011.08.004.
4. M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," Comput. Secur., 2015, doi: 10.1016/j.cose.2014.11.007.

www. cybercrime.gov.in