Digital marketing is the use of internet, search engines, social networking websites, and other platforms for reaching consumers of a product or service. If we compare digital marketing with conventional marketing, experts believe it to be a much more effective way of studying consumer behaviors and planning marketing activities accordingly. Every marketer faces different challenges and threats such as attracting traffic from social media sites or improving search engine rankings. However, all digital marketers face cybersecurity threats that can cause serious damages to the brand in the form of loss of customer data, reputational damage, and financial losses.

## Common Cybersecurity Threats in Digital Marketing

To understand how we can overcome cybersecurity threats, let us first have a look at some common cybersecurity threats in digital marketing.

* Browser hijacking and redirection
* Theft of data and customer confidential information
* Malware infection resulting from opening links or downloading files
* Identity theft
* Spreading fake news
* Website attacks in the form of Distributed Denial of Service (DDoS)

In addition to these threats, there are numerous other cyberattacks that many digital marketers are not aware of. Therefore, it is important for all organizations to adopt a cybersecurity strategy that focuses on digital marketing aspects and provides strong security against malware, protects your client’s information, and safeguards your website.

## How to Overcome Cybersecurity Threats in Digital Marketing

Let’s look at various aspects of digital marketing, the threats they face, and how digital marketers can overcome those threats.

**Social Networking Websites**

Social media has changed the way people think and make decisions. When it comes to social media marketing, the main risk and concern associated with it is identity theft, which can lead hackers to steal personal information of the user as well as their contacts.

To overcome this threat, the following solutions can help:

* Social media users should make their privacy settings as strict as possible.
* Social networking websites should implement robust password authentication strategy such as two-factor authentication for its users.
* Administrator should track user activity on the social network.

**Ecommerce**

To help the business grow and stay in the competition, digital marketers now use cutting-edge technology such as machine learning, which improves site-search analytics to provide data on user activity and helps improve conversion rates. However, Ecommerce websites face serious cybersecurity threats as they need to secure customer’s personal data, payment card information, [transaction](http://www.cardzgroup.com/BankCards.html) details, and buying behaviors.

To avoid security threats, ecommerce websites should take the following measures:

* Set up Secure Sockets Layer (SSL) protocol and two-step verification for users before authenticating a transaction.
* Provide secure payment methods to customers.

**Email Marketing**

Email is one of the oldest, yet useful digital marketing tool. However, its success has also led cyber attackers to launch phishing attacks by sending malware emails from hacked workplace email accounts or sending marketing emails to lure customers into clicking malware links. If a website gets hacked, the host may blacklist and block it. This can have an impact on the email marketing strategy of the firm.

Just like customers, your digital marketing staff is also prone to phishing attacks, since they are the ones who frequently deal with client data. Hackers also sometimes act as customers to get sensitive information from digital marketers.

To overcome this problem, it is important to:

* Avoid opening and responding to emails that are from an unknown sender.
* Verify the reliability of the ISP and servers.
* Encrypt emails to reduce the risk of phishing attempts.
* Include email security as a part of regular network security audits.
* Create outbound filters to prevent emails that have hidden viruses.

**Content Management Systems**

Content Management Systems (CMS) like WordPress have made content marketing easier for digital marketers. However, it is one of the easiest targets of cyber attackers. To launch website attacks, hackers use vulnerabilities in the platform itself or its plugins. Content Management Systems are vulnerable to different attacks including:

* Distributed Denial of Service (DDoS) attacks – this involves attacking your website with massive traffic to bring your website and server to a halt.
* Cross-site Scripting (XSS) – hackers inject malicious code into the website to steal your server data.
* SQL Injection – these are attempts to have access to the website’s database.

To overcome attacks on your CMS, it is important to:

* Always keep CMS account up to date, as it provides latest security patches to address known vulnerabilities on time.
* Update the plugins and addons to get maximum security.
* Use strong passwords and activate multi-factor authentication.
* Purchase a digital certificate to encrypt the website with SSL.
* Install a Web Application Firewall on the website to safeguard it from dangerous content.

**Customer Relationship Management Software**

CRM software is a basic component of digital marketing as it stores information collected from customers and clients. It is used for analyzing acquired data and designing marketing plan for the company for better customer services and engagement. If hackers get access to your CRM system, they can get all customer-related sensitive information and use it for malicious purposes. This can result in the company losing money as well as brand reputation.

Only using complex passwords for securing CRM is not enough. It is important to take other measures such as:

* Restricting access to the CRM software to only concerned and trustworthy employees to avoid insider threats.
* Using a tracking tool to keep a track of all account logins.
* Not allowing Bring-Your-Own-Device (BYOD) policy and only allowing employees to use devices issued by the company to avoid potential data breaches.

**Conclusion**

From management to employees, cybersecurity is the responsibility of everyone and not only of the IT department alone. Digital marketers need to understand and cater to related security risks and devise marketing strategies accordingly. Every digital marketing plan must be developed while keeping in mind all aspects of cyber threats to the business in order to effectively market the brand to potential customers.