BIZCOMMUNITY

How online marketing is shifting through data privacy

By Craig Lebrau , issued by Lebrau Press

8 Apr 2021

Recently, most companies have shifted to online marketing owing to the convenience of this option and the opportunity to reach a larger market than they would in traditional stores. Even so, clients have also become quite intent on the privacy of their data. You can get away with delaying a customer's package, cancelling services and delivering a substandard product, but if you compromise a customer's data, you will probably lose the client.

Breach of clients' private data has unfortunately been quite common in the last decade. For instance, in 2013, more than 110 million clients of Target had their credit card information compromised. This led the retail giant's CIO and CEO to resign the following year.

To help you understand the impact of data privacy on online marketing and how best to handle it in your company, here are a few guidelines on the subject.

What is the motivation for breaching data?

While the motivation behind breaching the personal data of your clients by hackers varies, intelligence gathering has been shown to influence about 90% of the breaches. Below are the ways in which hackers use the information they will gather:

- The information can be used to sell your business secrets to competitors, start smear campaigns against your company or take down your e-commerce site.
- The hackers can use the information they have gathered to extort your company and your clients.
- Consumer data like names, social security numbers, addresses and phone numbers can be used for identity theft.
- Your data and that of your customers can be sold on the dark web to the highest bidder. This sold information gives hackers a direct pass to harm your online business and clients.

What are the consequences of a data breach to an online business?

As an online business, you are responsible for the collection, storage and transmission of your clients' private information. As such, you will be held responsible for the consequences of a breach of this data. The information below will help you

appreciate the consequences of a data breach.

1. Financial impact

Other than the primary cost you will spend fixing the data breach and preventing hackers from accessing your other data, your stock price will probably decline. According to a study, stock prices fall soon after a data breach and take about 45 days to fully recover. In addition to these, you will often deal with lawsuits and government penalties for the breach. You can get a data breach lawyer to help you minimise the financial impact of the lawsuits from the breach.

2. Consumer trust impact

Trust is essential in e-commerce. When people share their sensitive data with your business, they should be sure that your company will secure it. Data breaches will become a stumbling block in the establishment of a good relationship with your online market. It makes clients start second-guessing sharing their information with your business, meaning you can hardly sell anything online.

3. Brand reputation impact

Your brand's reputation is a valuable asset that you will spend a lot of time and money building. A single data breach will topple your brand's reputation in hours and negate your huge investment.

How can you guarantee data privacy on your e-commerce website?

Understandably, your e-commerce site is bound to be a hit among your target market if clients are sure that the privacy of their data is assured. Here are some ways of guaranteeing the privacy of the data you gather from your clients.

- If you have not done so already, shift to a first-party measurement structure. With this, you will directly ask for permission from clients to gather and use the data they share with you. This way, you avoid solutions that are incompatible with your market's expectations of privacy.
- Place your digital ads with publishers who have a first-party, consent-driven relationship with their clients.
- Hire agencies or build in-house teams that are well-versed with the regulatory requirements for collecting and using client data to avoid legal issues.
- Employ data redundancy in which your data is secured in multiple locations. Other than secure data storage, this solution allows you to update your data accurately from one location in case of a breach so that you minimise disruptions.
- Ensure your web hosting complies with the standards of PCI DSS (Payment Card Industry Data Security Standard). PCI compliance dictates the minimum approaches for securing a client's payment data, like restricting data access and maintaining a firewall.

Data breaches are currently changing how e-commerce businesses operate. With the threat of a data breach, e-commerce companies are going all out to review their security measures and protect their clients' information. The security measures also protect your business secrets and internal records from competitors. With the information you have gathered from the above tidbits, you now appreciate the impact of data breaches and can take the necessary steps to protect your online business.