Title – Marketers Beware: Security Risks of CRMs
WC - 575

Marketers Beware: Security Risks of CRMs

So maybe this is a bit of reach from our usual blog content. But while it may seem unrelated to what Diana Alexia Creations does, it actually relates to content writing and marketing more than any of us wish it did.

According to Salesforce, the definition of Customer Relationship Management—better known as CRM—is software intended to streamline the management of company interactions from communications, documents, invoices, and more.

In fact, CRMs are used by most businesses out there, not just marketing teams. Businesses that are large corporations, small businesses, entrepreneurs, and anyone who works with clients use CRM software. CRMs can be the lifeline of a business managing its finances, projects, and client relationships.

CRMs are a project management tool that manages everything related to your clients and finances. So, one hack can really ruin your day.

What Can a CRM Do For Your Business?

CRMs help streamline internal processes, like organizing projects and preparing relevant invoices that would take multiple tracking systems to keep organized. Many companies and businesses use CRM systems to automate their workflow and organize their projects and finances. However, although CRM systems bring ease to the workplace, they pose potential security risks to company information.

Prevent Security Issues

Companies should research their software options before investing in any CRM software. The reason why is quite simple: security threats can place all internal information at risk.

Companies must have employees dedicated to addressing CRM issues, including security. And they should limit the number of hands allowed to change data. This is why many companies choose to have a database administrator or limit access to project managers only. Unfortunately, all it takes one mistake or inadvertent change to settings to put the whole company's internal system at risk or in the hands of hackers.

Let's Practice Safety First

There are a few steps that marketers can take to prevent security issues. The Pipeline suggests creating limits to access levels on a need-to-know basis. If only a handful of employees need access to a project, keep it at just that. The more access points to a project, the more risk are taken. Moreover, the software must be up to date to minimize security vulnerabilities. Whichever

Title – Marketers Beware: Security Risks of CRMs
WC - 575
CRM software is invested in would constantly work in revisiting and updating security measures to keep client information safe from hackers.

Lastly, companies that have invested in CRMs should secure their physical servers. These are usually located in a physical office space and should have limited access and be placed behind closed doors. Additionally, disabling the router's SSID broadcast, and locking down the SSID in general, will enforce safety from hackers. Finally, IT teams should enable firewalls and other software updates that would otherwise be vulnerable to hackers.

Breathe…It Takes Time, But You Can Manage

Businesses that use CRM systems must acknowledge the tradeoff between the software's convenience and potential security threats. If they place measures to prevent security threats, they should be able to use the software effectively and safely.

Diana Alexia Creations loves to share what they know. Learning about different CRM software and what can be done to ensure safety was hard for us, too. But we figured it out and are confident you can, too.

On another note, if you are looking for help with your content writing, Diana Alexia Creations is here to help. Check out our services, or contact us today. Let's work together!

WC: 312