How Poor Cybersecurity Practices Can Destroy Businesses

NexxyTech March 27, 2018 0

How Poor Cybersecurity Practices Can Destroy Businesses

In a modern world that is constantly changing to catch up to new internet technology, cybersecurity for businesses becomes more and more relevant and important. This is so much so that poor cybersecurity practices can mean the end of a thriving business.

Everything from a simple weak password to not encrypting and salting hashes within a site database can cause serious damage to both the business's finances as well as their reputation. That's why it is so important that all businesses, even those without a large online presence, must stay safe online.

There are countless examples of major companies who have fallen victim to online hackers and devastating leaks of information. We will be looking at some examples of these, alongside best practices for business cybersecurity.

Keeping Passwords Secure & Encrypted

The first piece of cybersecurity advice for businesses is an obvious one. Make sure passwords are strong, secure, and fully encrypted.

Strong Passwords are:

- At least 12-characters long so they are less likely to be guessed.
- Made using a mixture of lowercase, uppercase, numbers, and symbols to protect against brute force attacks.
- Not actual words which can be found in the dictionary – this also stops brute force dictionary attacks.
- Not obvious substitutions for regular characters e.g. any kind l33tsp3@k

If you have a business website which holds people's accounts details, it's a good idea to ensure they are at least encouraged to follow the guidelines above. Many online compromises could be avoided if everyone followed best practices for passwords.

Keeping Passwords Secured & Encrypted

While most website content management systems will automatically encrypt passwords when new users sign up, there are a number of useful add-ons and tools out there to help.Encrypting passwords means that instead of a user's password being saved in the database as:

Unencrypted Password: ThIsIsMyPaSsWoRd1994

It should look like:

Encrypted Password:
2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

This is considered a basic way to store passwords so every business should be ensuring their passwords are encrypted and secure in order to avoid losing important customer information like credit card details.

Even Equifax did not fully follow these guidelines and ended up suffering a security breach, losing them millions of dollars in a contract with the IRS.

Using DDOS Protection

DDOS stands for Distributed Denial-of-Service and it's an attack carried out by thousands of different computers on a single website. Each computer keeps requesting a webpage over and over again which, through time, overloads the server and brings the website offline.This is one way in which an online company, often of an e-commerce nature, can lose thousands, sometimes millions, of dollars by not being able to serve potential customers. This is why many large corporations hire legal teams from firms like Goodwin, in order to prosecute those behind such devastating attacks.

One such example of a serious DDOS attack occurred to the Electroneum cryptocurrency site which was supposed to allow investors to buy some of their digital currency. The site was targeted by a DDOS attack which stopped investors from getting in on the shiny new cryptocurrency – perhaps, costing them hundreds of thousands of dollars in investments.

What DDOS Protection is there for Businesses?

There are a multitude of different tools and services out there which help protect against DDOS attacks. If you are a company which primarily specialises in e-commerce or provides their services online, it may be worth paying the much smaller price of a DDOS protection service rather than risking an attack.Two of the most common DDOS protection services out there are Cloudflare and Nginx which prevent any one IP address from requesting a page too often. Many

large businesses which have suffered DDOS attacks in the past now use such services to ensure they do not suffer the same fate again.

Keeping All Software Up-To-Date

Regular software updates are simple actions for businesses to take, though many neglect to do so. This makes life easier for hackers and those who are looking for easy cybercrime targets.Much like Windows or Mac OS systems, it's imperative that business owners keep all of their software up-to-date. Many of these updates are improvements to security protocols so that the latest malicious viruses and known hacking exploits can no longer be taken advantage of. It only takes one click in many instances to keep your website, plugins, and add-ons where they should be, so it is worth doing.

It's also often possible to set website CMS's and plugins to auto-update as soon as they can, something which can potentially save a business money.

Put Good Cybersecurity Practices in Place Today

I hope that this basic look over some poor cybersecurity practices, and the steps we have suggested to improve those practices, can help businesses out there ensure that they are protected against malicious attacks and breaches.Staying safe online as a business is generally very straightforward, it's just about making sure the core tenets of good cybersecurity practice are followed consistently.
