How to Prevent Black Friday Cyber Threats

www.privatetunnel.com/home/blackfriday/

Black Friday is one of the biggest shopping days of the year, especially for e-commerce businesses. According to *Fortune*, online shoppers spent $4.45 billion between Thanksgiving and Black Friday in 2015. This means that a large number of visitors will visit your website at the same time looking for great deals.

A huge influx of traffic can cause trouble for your website. Your website might crash or be vulnerable to cyber threats. Use these tips to prevent Black Friday Cyber Threats so your business can just enjoy a healthy influx in sales.

Website Crash

Depending on how you configure your website and what kind of server you use, a high volume of customer traffic could cause your website to crash. This would be a major problem for visitors who want to place an order on Black Friday, but can't because your website is down. If a traffic spike is the reason your website crashed, you should contact your hosting company to get more bandwidth. To prevent this in advance, plan to up your hosting package for Black Friday, so every customer who wants to buy something from your e-commerce store can.

A website crash may stem from brute force attacks from a hacker or possibly a competitor. This involves using spam bots and viruses to crash your website through what is called a brute force attack. This can allow the perpetrator to infiltrate the backend of your website to steal data and destroy internal IT infrastructure. Brute force attacks are one of the reasons your business should invest in cyber security programs and keep your website up to date.

Data Breach

Customers place a lot of trust in your company to protect their personal information when they place an order on your website. Some cybercriminals may use Black Friday as an opportunity to steal your company's confidential data because they suspect you'll be very busy handling sales and working with customers.

A data breach can make customers feel betrayed, which can hurt your company's reputation. Consider what happened when the Target Corporation faced a data breach. It cost the company $39 million in a legal settlement with banks and adversely impacted 40 million customers. While it's true that the Target Corporation did not shut its doors because of the data breach, a smaller company would have been forced to close.

Take all necessary steps to prevent data breach this Black Friday. Make a secure copy of current customer and company information stored somewhere that's not accessible from your website. Remove outdated information and increase your cyber security plan. Ensure that your business continuity plan is up to date and well-tested.

Interference from Hackers

Hackers know that Black Friday is a great day to launch a cyber threat against your business. After all, many businesses take extended days off around the holidays and your office might be empty, leaving your company and its data extremely vulnerable. Some hackers have been known to take advantage of this trend and make changes to your website. This might include changing prices, creating fake orders, and manipulating website data. Make sure patches are up-to-date and consider using a VPN.

Black Friday cyber threats can be overwhelming. Fortunately, many of these are preventable with the right security measures. Contact us today to discuss how we can help you prepare your IT assets this holiday season.