RAPIDSPIKE®

Preparing your Website for **Black Friday**

INCREASE SALES, IMPROVE CUSTOMER EXPERIENCE, AND AVOID DATA BREACHES DURING THE HOLIDAY SEASON.

CONTENTS: **PAGE NUMBER:**

2021 BLACK FRIDAY AND CYBER MONDAY

Black Friday and the holiday season are important events in the ecommerce calendar and can make or break a business. The 2021 holiday season is going to be unlike previous years due to the ongoing impacts of the COVID-19 pandemic. Business owners can expect a continued decrease in brick-and-mortar footfall and a massive increase in online traffic. It is essential website owners correctly prepare and monitor websites to keep their website up, serving happy customers, and most importantly secure.

KEY HOLIDAY SEASON STATISTICS

$910BN

Predicted global spend for 2021 holidays.
- Adobe Analytics

$14.3BN

Online U.S. sales for Thanksgiving and Black Friday 2020.
- Adobe Analytics

$86BN

Predicted online spend using smart phones in the 2021 holiday season.
- Adobe Analytics

$10.8BN

U.S. Cyber Monday online sales in 2020.
- Adobe Analytics

477.5M

Visits to electronics retailers during the 2020 holiday season.
- Queue IT

5.76BN

Spent on online Black Friday weekend sales in the UK in 2020.
- Statista

2000%

Spike in U.S. online sales during the final hours of Black Friday 2020.
- Klarna

30%

Of all retail sales occur from Black Friday until Christmas.
- Ecommerce News

The 2021 holiday season is expected to out-perform the previous year. Ecommerce is expected to increase dramatically due to the ongoing COVID-19 pandemic driving consumers online. Website reliability, performance, and security optimisation need to be prepared in advance of the season to increase sales, improve customer experience, and avoid data breaches.

U.S. online Thanksgiving and Black Friday sales increased from $11.9 billion in 2019 to $14.13 billion in 2020 according to Adobe Analytics. It is also predicted that online sales for Black Friday in 2021 are to reach a massive $17 billion. Although the UK is less involved with Black Friday campaigns, statistics from Statista show that £5.76 billion was spent on online Black Friday weekend sales in the UK in 2020, an increase from £3.77 billion online spent in 2019.

According to Queue IT, Technology, Fashion and Health & Beauty retailers continued to be the most popular online across the holiday season in 2020. Visits to electronics retailers reached 477.5 million during the 2020 holiday season making up 30% of all traffic during the period.

SEMRush report the most popular retailers searched with 'Black Friday' in 2020 were (by searches):

Walmart - 8,241,900
Amazon - 6,927,300
Best Buy - 5,543,600
Target - 4,413,400
Home Depot - 2,026,200
Macy's - 2,025,000
Kohl's - 1,595,680
Apple - 1,398,500
Nike - 1,344,000
Costco - 1,327,010

CASE STUDIES

Every year companies are named and shamed due to their lack of preparation for Black Friday, and the holiday season. Ill-prepared companies find themselves with website crashes, loss of sales, and reputational damage. There are however some companies who flourish in these demanding times. Throughout this white paper, we examine some of the best and worst cases, to gather key insights from their experience.

WEBSITE TRAFFIC GAINS

Understanding how much traffic you can expect on Black Friday is essential to understanding how to prepare your website for the holiday season. SimilarWeb analysed the top 100 shopping sites specifically focusing on apparel, general merchandise (marketplaces), and consumer electronics, for the timeframe of November to December 2019. This shows the biggest daily traffic gains on Black Friday 2019 in the US:

UGG	BEST BUY	HOLLISTER	KOHL'S	macy's	AMERICAN EAGLE OUTFITTERS	jcpenney
↑909%	↑600%	↑539%	↑507%	↑428%	↑412%	↑412%

Increase compared to average daily traffic in August - October 2019. Source: SimilarWeb

KEY INDUSTRIES TO WATCH

Using some of the world's largest databases we are able to understand the key industries which are most popular in the holiday season. These industries are vulnerable to reliability, performance, and security issues in this period. Additionally, RapidSpike's Client-Side Security Scanner works by scanning over 1 million websites each day and pattern-matching those websites against known malicious JavaScript code. In 2020, RapidSpike monitored the websites hacked with a web-skimmer, observing the industry, location, malicious code, and vulnerabilities of each website and compiled the results from this data.

TECHNOLOGY

Black Friday and Cyber Monday are notoriously technology-based events. According to Queue IT Electronics retailers attracted the highest website visitors in the 2020 holiday season reaching 477.5 million with a 30% share of all traffic during the season. Adobe Analytics predicts the most sought-after technology products in the 2021 holiday season will include Airpods, Smart Mugs, Instapots, Air Fryers, Smart Waterbottles, Drones, Record Players and Samsung & LG TV's.

Technology sites were the number one most hacked websites in 2020 making up 15.4% of all hacked websites. Within the technology sector, websites included both hardware sites and software sites. The two technology streams made up 50% of the affected websites in this industry.

There are several reasons why technology sites are targeted so heavily by hackers, especially in the holiday season. Firstly, hackers attack technology sites for bragging rights, looking for a potential reward. If technology websites or services are down in the holiday period, these sites are losing a significant revenue stream. Additionally, it could be expected that as technology products are often expensive, customers purchasing the products are likely to have excess income. This means cybercriminals can sell their data for an excess. Finally, technology sites had some of the poorest cybersecurity out of the industry sectors monitored.

GARMIN™

Case Study - Garmin SA

On September 12th 2019, it was reported that Garmin South Africa (SA) disclosed malicious activity was found on their shopping site portal. The attack affected customers shopping on shop.garmin.co.za (operated by Garmin South Africa). A Garmin spokesperson confirmed that their site portal, operated by a third-party, was compromised by a card skimming script which affected 6,700 South African customers.

FASHION

Fashion retailers have always been a key player in Black Friday and the holiday season. In 2019, the category with the highest amount of sales on Black Friday was clothing and accessories. Fashion websites received over 194.2 million website visitors in the 2020 holiday season. Typically, Fashion websites have suffered with website performance on Black Friday. Fashion website issues mainly involve downtime however customers also suffer with key journeys. In 2018, Hollister was down for multiple hours on Black Friday and many people took to Twitter to voice their frustrations, this led to the brand putting on an extended sale to make up for the website performance issues. Unfortunately, the brand also suffered with website issues in 2019.

The fashion sector made up 14.0% of all hacked websites in 2020. The most hacked websites were located in the US, France, and the UK. An ever-increasing number of popular brands are falling victim to attacks. The holiday season is a prime-period for cybercrimes in particular to the fashion sector. The popularity with Gen X and Millennials is an attractive consumer group for cybercriminals to target. Phishing and social media campaigns to target this consumer group. According to the FTC, in Q1 2020 and Q2 2020, 28% of reports of frauds that started on social media were categorised as online shopping fraud where the goods were ordered but not received.

Cybercriminals use a spray and pray technique to target lower-budget ecommerce sites. For larger brands, many attacks are planned months in advance of going live, to try to blend in with website third-parties to avoid detection from website administrators.

Case Study - Khaadi

Pakistani fashion brand - Khaadi has over 5.4 million social followers, ranks in the Alexa Top 50,000, and has approximately 1.5 million monthly site visitors. RapidSpike reached out to the company twice across two weeks without any response, one month later and the skimmer was still active on the site. Other fashion companies who have suffered Magecart attacks include Macy's, Sweaty Betty, Fila UK, Sixth June, and Princess Polly.

COSMETICS

According to Queue IT, website traffic to health and beauty websites had over 400.7 million visitors (25%) in the 2020 holiday season. This increase trend continues from a rise in sales by 464% on Black Friday 2019 compared to 2018.

Overall, there has been an increase in the number of attacks on this industry year on year. Cosmetic websites made up 5.1% of hacked websites in 2020. Some attacks observed were highly advanced with a dedicated customised skimmer for the website as well as multiple layers of encoding to disguise the skimmer. The majority of hacked cosmetics sites were based in the US (31.6%), followed by France, (15.8%), and India (10.5%).

Perricone MD

Case Study - Perricone MD

In 2020, RapidSpike discovered two hacking groups attempting to steal credit card information on the European ecommerce websites for the science-backed skincare brand Perricone MD (affecting perriconemd.co.uk, perriconemd.it and perriconemd.de). The hacking groups were able to insert malicious code directly into the websites, most likely due to a vulnerability in the Magento platform.

The first hack dated back to November 2018, meaning it had been present on the websites for over a year. The second hacking group gained access to the websites in November 2019, likely through the same vulnerability. They registered the domain perriconemd.me.uk to help avoid detection and only load the skimmer on the checkout page.

HOMEWARE AND GARDENING

Homeware and Gardening is a leading industry in the holiday season, and it is likely to continue to be popular in 2021. During the start of the pandemic, there was a large increase in consumers purchasing homeware and gardening supplies. Contentsquare reports transactions on furniture and DIY websites in the UK and US were up +52.3% at the beginning of the pandemic compared to the previous week, contributing to a +101.4% increase in home purchases since the start of the pandemic. In the 2020 holiday season, Homeware and hardware websites attracted 58.8 million online visitors.

Homeware and Gardening websites made up 11.2% of hacked websites. 35.7% of sites featured in the sector were from the US, 22.6% were from the UK, followed by Germany and Spain making up 7.1% each. Previous high-profile homeware site attacks include OXO, Mypillow & Amerisleep, and Greenworks.

Robert Dyas

Case Study - Robert Dyas

UK hardware site Robert Dyas suffered a web-skimming attack lasting over three weeks from 7th-30th March 2020. The attack left customers vulnerable to payment data theft by an unauthorised third party. According to Robert Dyas, this data breach affected approximately 20,000 customers.

HOLIDAY SEASON MAGECART ATTACKS

In 2019, there was an increase in companies impacted by Magecart attacks compared to the previous year. In 2021, companies are now more aware of web-skimming attacks, however, it is almost impossible for companies to keep up with web-skimming techniques, and to properly monitor their website to protect against attacks alone. In 2018, RapidSpike launched Magecart Attack Detection to monitor for data breaches. The monitor consists of Client-Side Security Scanner, Synthetic Attack Detection, and Real User Attack Detection, giving data control back to companies. High-profile attacks in 2018 and 2019 prompted updates to the General Data Protection Regulation (GDPR) in 2018, and the California Consumer Privacy Act (CCPA) in 2020, meaning companies now need to take precautions to protect customers' data or face fines.

The holiday season is a particularly dangerous time for companies to fall victim to Magecart attacks. Websites are being changed regularly, adding third-party plugins such as advertisers, live chat and customer service tools. Although these tools can be useful for customer experience, they can also be dangerous for website security. Misconfigurations or out of date software can lead to website vulnerabilities. These vulnerabilities can be taken advantage of by cybercriminal groups including Magecart. Magecart have more of an incentive this time of year to go the extra mile to go undetected. More customers on a website means more stolen payment data for them. Cybercriminals will often set up attacks just before the holiday season so malicious code doesn't stand out to administrators. We are proud to support thousands of ecommerce websites with website reliability, performance and security in Black Friday and holiday season.

HIGH-PROFILE HOLIDAY SEASON REPORTED ATTACKS

Sixth June

7 days before removal.

RapidSpike Security Researcher informed the French fashion brand about the skimmer on their website on October 23rd. The skimming code was finally removed on October 30th. The brand has approx. 70,000 monthly site visitors.

macy's

1 week before detection.

Infected just before the holiday period, the breach occurred from October 7th-15th, 2019. An unauthorised third-party added malicious code to two pages on macys.com, including the checkout page and the wallet page.

Smith&Wesson

6 days before skimmer removal.

Willem De Groot discovered a skimmer on the website on November 27th, just in time for Black Friday. The script loaded a non-malicious or malicious script depending on whether the customer was their target customer.

Sweaty Betty

9 days before detection.

Compromised with a payment skimmer, customers who shopped on the website between November 19th to November 27th may have had their payment details stolen. This attack did not affect customers paying by Apple Pay or PayPal.

Rooster Teeth

Detection same day.

Discovered on December 2nd, the attack redirected shoppers to a fake payment form upon checkout which would send their payment details to an external server. Once filled in, customers would be redirected to the genuine checkout form.

MISSOMA

Infected for approx. 3 months.

Third-party malicious software targeted the payments page of the Missoma website and inserted skimming code. The code was active across the holiday season, only being removed on December 16th.

OPTIMISATION - AVAILABILITY

Making sure the website is up and running is a key priority for technical teams, especially over the holiday period, when website visitors are likely to be much higher. Making changes in advance of the holiday season can create a much more enjoyable shopping season for both companies and customers.

PREVENTATIVE MEASURES

In preparation for the period, technical changes need to be made to ensure the site runs smoothly with high traffic increases. Website owners should estimate traffic increase, undertake load testing or stress testing, scale up infrastructure, and create a status page.

Estimate Traffic Increase

To find out how much more traffic a website is estimated to receive over the holiday period, companies first need to understand how much traffic is normal for their website. Google Analytics or RapidSpike Real User Monitoring can give a good idea of how much traffic your website receives, as well as the normal duration spent on different pages. These are important statistics to know for both availability and performance.

If a website has not taken part in Black Friday/Holiday sales before, and therefore has no data for this, estimates can be made by looking at similar brands or average statistics. Ometria reported the number of on-site visits from Black Friday to Cyber Monday in recent years was 150% higher than in an average 4-day period on sites, however, some websites have seen up to a 909% increase in traffic (ugg.com in 2019, according to SimilarWeb).

> The number of on-site visits from Black Friday to Cyber Monday in recent years was **150% higher** than in an average 4-day period.

Other factors to consider include marketing efforts, if a website is actively taking part in marketing themselves for the holiday period, they are likely to create demand, and therefore traffic increases. Similarly, some websites will have paid advertisements around the holiday period, again which will likely increase website visitors, all of these things should be considered when working out traffic increases.

Stress Testing

Of all the types of performance testing, on Black Friday, understanding how much stress your system can handle is paramount. Stress testing overloads a system to figure out the numerical breaking point. It is important that websites stress test before the holiday period to be prepared for a similar situation with real website visitors/requests.

In a stress test, the system is pushed beyond its intended capacity, which then shows which aspects of a website will start to fail. Companies can then analyse this data to figure out where the bottlenecks are, helping to gauge what your system can handle. Stress testing tests different components on the website to understand their limits. Aspects to monitor in a stress test include: third parties, bandwidth, Server & Database Usage, performance degradation & breaking point.

Before executing tests, all development teams should be informed about the testing schedule and backup systems should be created.

Scale up Infrastructure

In preparation for the holiday season and in particular Black Friday, websites should ensure they can scale up their infrastructure to meet the increase in traffic. It is important to ensure your hosting solution can be scaled up and down over the period. This means you can accommodate higher traffic to your website, and then decrease hosting and save on associated costs when the traffic decreases. Scaling infrastructure can include adding more machines, or for cloud-based solutions using auto-scaling and load balancing. Thinking about ways to mitigate load would also be useful - utilising visitor queuing mechanisms can help you control traffic flow and implementing serverless and caching technologies could help in absorbing traffic better.

LUSH FRESH HANDMADE COSMETICS

Case Study - Lush:

U.K. retailer Lush have been known for their Boxing Day sales on their website. However, for two years running, the increase in website traffic caused outages for up to 18 hours. This unreliable service not only upset customers, it also made national news.

Lush's website experienced traffic of up to 12 transactions per second, three times the scaled-for capacity. Their supplier had no scalability which meant they could not deal with the increased traffic.

Solution: Lush migrated their entire global infrastructure onto Google Cloud Platform. Cloud platforms allow for scalability which can handle traffic increases without compromising stability. This means once the holiday season was over, Lush could descale infrastructure to save on costs. The move reduced their infrastructure hosting costs by 40 percent.
- Source: Google Cloud

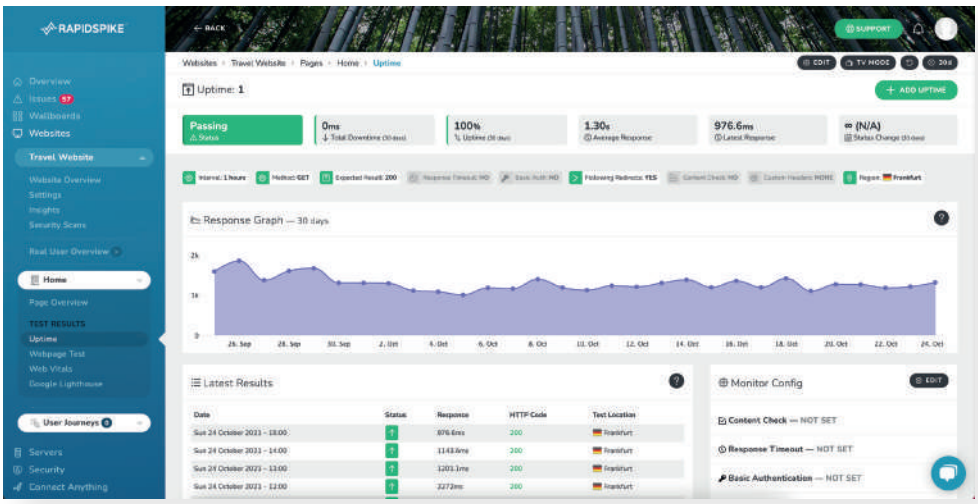
MONITORING

Monitoring availability is essential for the Black Friday and the holiday period, although prevention is the best practice, sometimes things fail and if they do, technical teams need to fix the issue as soon as possible to continue to generate sales, improve customer happiness, and manage reputation.

Uptime Monitoring

Website Uptime monitoring is essential to ensure your website is online and serving customers. In the holiday period websites should test their site often and from locations suitable for their average customer. Website Uptime monitoring should begin before the holiday season to gauge what is considered normal for that website.

Uptime monitoring (using HTTP GET) will detect and alert whether your pages are accessible, check the status code they have returned, response time from the page itself and check specific content (exists or not). Ping and TCP monitors can give a response time and top-level availability of your hosting server or network device. Every minute of uptime counts on a website, therefore companies with a large number of website visitors should run uptime monitors ideally at 1 minute intervals. It is also important to have the correct notification rules in place, for larger teams multiple notification rules should be triggered on a single issue – notifying different team members the longer your outage lasts.



Status Page

If a website does encounter downtime, a custom status page is the best way to let the correct teams or your customers know. A status page can be available on its own unique generated URL. The pages can be kept private for internal use by managers and support staff, who can check it whenever they encounter customer problems, or can be public so customers can check if there's an issue with the website. Pages should be configured to automatically refresh every minute to keep anyone with access to the page up to date with the latest information. If a company does decide to make their status page public (recommended), it can be customised with company branding.

Often customers will take to social media, in particular Twitter, to investigate if there has been an issue with the company's website. Status pages can be pinned to the top of the page for easy access for customers.

Reputation Damage Control

Companies should also be active on social media to be accessible to customers and the issues they are facing. Being quick to respond to customers helps minimise customer frustrations and increases brand reputation. Companies should also be ready to make offers to customers who have faced issues due to the company's neglect. In regards to a data breach, if possible, companies should offer Identity Monitoring to their customers. For seasonal website reliability and performance issues, companies should be willing to extend sales periods to let customers access the deals they were unable to on the day.

OPTIMISATION - PERFORMANCE

Slow-loading and poor-performing websites can massively impact customer experience, sales and brand reputation. Black Friday traffic increases cause a lot of performance issues for unprepared websites. With 40% of customers leaving a site that doesn't load in 3 seconds, website owners need to prioritise making website performance changes before the holiday season. Technical performance changes include:

Load Testing

Unlike stress testing, Load testing gives you an idea of how much traffic volume your website can take. In a load test, companies can test a specific number of requests to see how it affects the performance of their website. An Apache Bench load test can show you how your website can cope under different numbers of visitors. In addition to understanding a website's capacity, Load Tests can also uncover website issues.

CDN

Ensure static content is loading from a Content Delivery Network (CDN) to offset unnecessary requests to your primary servers. A CDN caches static content on separate servers around the world and manages the delivery of website content to visitors. This helps a website handle larger volumes of website traffic quickly, improving performance.

Load Balancer

Load balancing distributes server loads across multiple servers which helps to reduce response time, therefore increase website speed for consumers. The load balancer ensures no one server is overloaded, impacting performance, and instead reroutes requests across a group of servers. Website owners should consider hosting aspects like cookies and SSL, on the load balancer – SSL decryption is resource-intensive so taking that load off the web servers is ideal.

Serverless Cloud Technologies

Consider utilising serverless technology to shift the pressure of the traffic away from your own services and onto managed services that are much better suited for absorbing huge amounts of traffic. For example, AWS's DynamoDB could be used for database services and can easily take billions of requests per second.

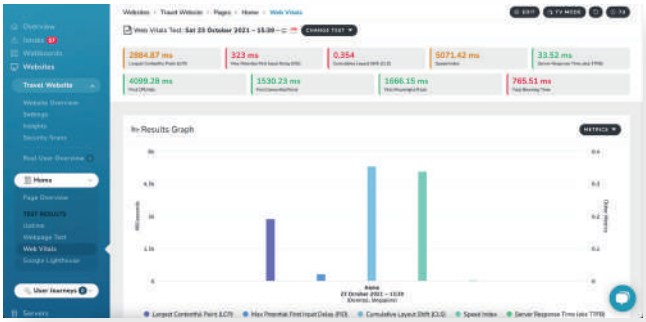
PERFORMANCE TOOLS

Performance monitoring tools help website owners see their website from their customers' perspective.

WEB PAGE TESTS

To thoroughly understand your website speed, Web Page tests can give you precise figures about content on your site. The Web Page test will download all elements of a page and show file size and load time, which you can track over time. One of the best ways to increase site speed is to compress large images and videos to make them smaller and remove any unnecessary third-party tools.

It is important to fix slow-loading elements in general, however, you may decide to turn off all non-essential third-parties entirely for Black Friday weekend in particular, as these usually take a long time to load. Once you have made changes to your site, make sure to monitor page performance and compare tests to ensure new elements don't create new issues.



GOOGLE LIGHTHOUSE AND WEB VITALS

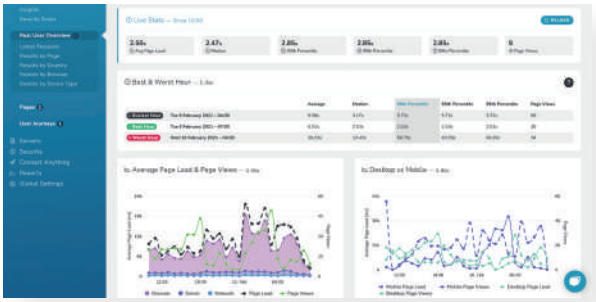
Google Lighthouse is an open-source quality testing tool built by Google. Lighthouse is a great tool for analysing your website in order to improve your overall site performance. Lighthouse analyses a given URL and performs a series of audits, testing on a number of broad categories, including; Performance, Progressive Web App (PWA), Accessibility, Best Practices, and SEO. Run a Lighthouse test to debug any issues which may be holding your site back from performing efficiently, and effectively. The 'Items Needing Attention' highlights help show how much your potential savings could be by making some quick and easy changes to each section.

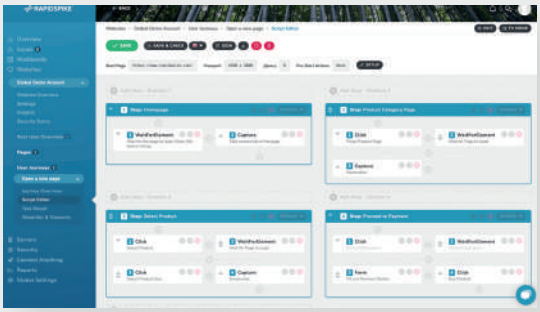
Google's new performance metrics - Core Web Vitals need to be continually and consistently monitored. This initiative is focused around user experience and will become part of Google's ranking algorithm. The signal is made up of three website vitals - Largest Contentful Paint (LCP), First Input Delay (FID) and Cumulative Layout Shift (CLS). Making sure you pass Core Web Vitals is essential for Black Friday as it can provide massive SEO boosts, as well as improved user experience which is essential to avoid repetitional damage this Black Friday.

REAL USER MONITORING

Looking into real users is not only beneficial for marketing efforts but can also help companies understand conversions. Tracking real users' interactions with your site means you can pinpoint when traffic volume impacts the website. Viewing real users also lets you understand what kind of experience customers have on mobile vs website, by country, browser, and the page they are on.

Studies have shown that 70% of mobile users who abandon an application, do so because of slow load times. Understanding where your customers access your website from is an important step in being able to create positive experiences for them.





USER JOURNEYS

An ecommerce company's nightmare situation is a customer being unable to complete a purchase, which for obvious reasons could be devastating in the holiday period. Checkout functions can stop working by something as minor as a pop-up banner. It is essential to test common user journeys such as 'Add to Cart' to make sure customers can shop without issues.

RapidSpike User Journeys can be made to be standard or video. Video User Journeys which will provide live recordings of the journey, which shows the exact experience a customer has on a website.

NAVIGATION

Companies should make sure site navigation is optimised to work with consumers expectations. Avoid stylistic choices which poorly affect customer experience. Poor website designs lead to frustrated customers, follow a simple navigation checklist to ensure the site is customer-focused.

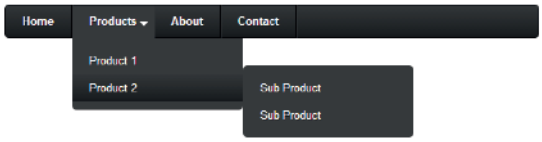


Photo source: cssmenumaker.com

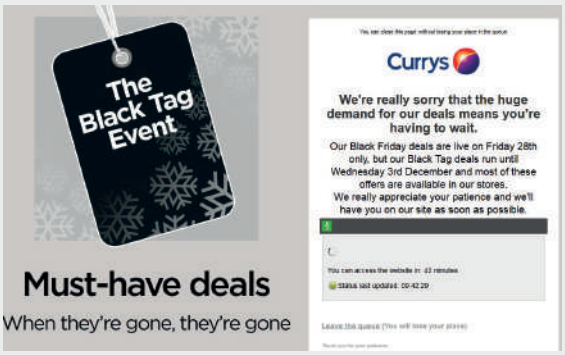


Photo source: ukdealspy.com

QUEUE SYSTEM

Implement a visitor queue system so that the number of people interacting with the website can be controlled. Queues can be frustrating for customers and can lead customers away from your site.

RapidSpike recommends a queue system as a last resort and as a preferred message to communicate the site traffic issue compared to the alternative of a time-out message.

HOMEBASE

Case Study: - Homebase:

For three years running, U.K. retailer Homebase were named the 'Worst Online Retailer'. In surveys taken out by Which?. In the surveys, consumers had to rate their experiences on popular online shops in the last six months. Homebase was ranked the lowest with an overall customer score of 62% in 2017, 55% in 2018 and 57% in 2019. Comments included items being advertised as being in stock when they were sold out, and complaints had been ignored.

Solution: Homebase enlisted the help of The Hut Group (THG) to improve their digital experience. By 2021, THG aims to launch a brand-new ecommerce platform for Homebase, to improve customer experience. Damian McGloughlin, CEO of Homebase, comments: "This partnership will significantly fast-forward our digital plans and create an incredible new shopping experience for customers."

TYPES OF ATTACKS

New attack techniques are being discovered on an ever-increasing basis. To protect your site it is important to be knowledgeable on new attack methods, vulnerabilities, and techniques. Additionally, being aware of other website hacks reported in the news to then make sufficient changes to your site.

RANSOMWARE

Cybercriminals access a website via a vulnerability and encrypt files meaning the website owner no longer has access, and the attacker can change aspects of the website to their liking. The cybercriminal will then ask the website owner to pay a fee to have access back, although there is no guarantee of this. These types of attacks are very serious as companies have lost control of their site. Attackers can also hijack the payment form to send customer's details elsewhere. Ransomware attacks are devastating for a company's reputation as customers lose trust for their security methods.

To prevent attacks, companies should continually patch vulnerabilities, install antivirus software, and be mindful of third-parties being installed. Companies should keep regular site backups, so they can restore their website, if needed.

PHISHING

Phishing is an attack method where cybercriminals try to trick consumers into entering their personal information onto a fake form. Consumers will receive emails seemingly from their popular websites or banks, with a link to access the service advertised in the email. Once the consumer has clicked onto the link, they will be directed to a fake form, this may be a login form for a certain website, or worse, online banking. Once information is entered in the form, it is in the attacker's control. The attacker can use this information to commit fraud.

Phishing attacks are very common around Black Friday and the holiday season as consumers receive an increase in email marketing with sales information. Consumers are warned to only access the website via a browser and to report any suspicious emails to the NCSC as well as the company the email is impersonating.

If a company becomes aware of a phishing email using their name and branding, they should also report this to the NCSC. Companies can contact consumers via social media and email marketing to warn them of the scam to prevent customers entering sensitive information.

DDOS

A Distributed Denial of Service (DDoS) attack is when attackers make a website crash by sending too many requests. A DDoS is a harmful attack especially in the holiday period as it either slows a website down, or takes the website offline completely, meaning real consumers are unable to access a website, and therefore no purchases are being made. The most common method for a DDoS attack is through a network of bots which send an excess number of requests than a server can handle bringing the website down.

Companies should use an anti-DDoS service and bot defence strategies to help recognise attacks early. Once a DDoS attack is identified, companies should notify their ISP to have traffic rerouted as soon as possible. Firewalls can help in rejecting fake traffic, therefore they should be kept up to date with the latest security patches.

MAGECART

A growing threat that ecommerce companies should be aware of, in particular in the holiday season, are Magecart attacks - also known as web-skimming, formjacking or supply chain attacks. Magecart attacks are a client-side attack method used to steal customers' payment data from websites. They are currently the number one threat to ecommerce sites today.

These attacks occur by exploiting a vulnerability on the webserver to gain access to the website to either inject malicious JavaScript code into an existing file or edit the HTML of the website to call a new third-party JavaScript file that includes the malicious code. Third-party services include; advertising tools, customer analytics, live chat, and more. The average website uses 85 third-parties and therefore monitoring for changes can be challenging.

With an increase in online sales, there's an increase in opportunity for Magecart victims. Magecart will be preparing for the holiday period and taking advantage of any site with vulnerabilities. In recent years, we have witnessed an increase in attacks around Black Friday and the holiday season. If a business suffers an attack this time of the year, it can lead to devastating consequences including loss of sales, and reputational damage. Ecommerce sites need to take responsibility of customers' data, prepare in advance for the holiday season, by tracking where your data is being sent to and being alerted of any new hosts.

Case Study: Xbox Live and PlayStation

In 2014, both Xbox Live and PlayStation Network were attacked on Christmas Day. This caused the systems to be offline for the majority of the day and some of Boxing Day too. The cybercriminal group behind the attack are known as Lizard Squad, who claimed the DDoS attack on both services login pages. The group wanted one of their tweets retweeting 10,000 times.

The following year, a new cybercriminal group Phantom Squad, also wanted to carry out DDoS attacks on the same companies, this time their motives were to encourage the companies to get sufficient DDoS protection.

Solution: Being prepared for it for a DDoS attack and having plans in place for when a service has been taken down is important. Companies should take out DDoS protection to assist with their cybersecurity measures.

WEB-SKIMMING TECHNIQUES

There are some key web-skimming trends, techniques, and attack approaches that have been seen across multiple attacks in recent months. Highlighting these issues can help to understand what to look out for this holiday season, and how to improve security:

Malware Under Images

In 2020, one of the new hacking methods observed was steganography-based skimmers. The technique involves hiding code within imagery to avoid detection. Hackers hide the image's background JavaScript code to scrape the data needed. The Tupperware website was one victim of this style of attack, with malicious code hidden within a PNG file that activated a fraudulent payment form during the checkout process.

Fake Checkouts

A key web-skimming attack method is loading a fake checkout form before the legitimate checkout page or before a PayPal page. Customers have a good indication of if an attack has occurred if a second payment form is presented, unfortunately, at that point, the customer's payment details have already been stolen. Checkout pages carry the most valuable information on the website and should be monitored carefully. A Synthetic User Journey monitor can continuously walk through the checkout page and alert to any new hosts found, potentially before a data breach occurs.

Targeted Customers

Skimmers are continuously advancing to evade detection including performing a search before loading a skimmer, to target a specific type of customer. In 2020, RapidSpike's Security Researcher discovered a hyper-targeted skimmer that only loaded after some prerequisites were met. The skimmer required the user to be on a mobile phone and in landscape mode. Additionally, a check was undertaken to ensure the user was on the checkout page, and did not have a developer toolbar present. Once the targeted customer had passed all the requirements, the skimmer would then load.

It is therefore important that companies test their website from multiple browsers to ensure all customers receive the same experience.

Plugins

WordPress' Threat Intelligence team discovered several vulnerabilities in 'Popup Builder', a WordPress plugin installed on over 100,000 sites. They explained how one vulnerability allowed an unauthenticated attacker to inject malicious JavaScript into any published popup, which would then be executed whenever the popup loaded.

Plugins can be useful tools in delivering great customer experience, making design changes, and helping with workflow, however, they can also leave a website vulnerable to attacks. WordPress plugins have had multiple vulnerabilities over the years, they should be minimised to a manageable level and continuously updated to patch any vulnerabilities.

Regional Sites

Regional websites can be beneficial for brands as they can allow more people to access products and companies can create specific marketing campaigns for regional holidays and events. This being said, regional websites also increase the workload for a company's developers to keep up with. The increase in workload could let vulnerabilities slip through the net.

RapidSpike discovered a regional attack on one of Belgium's most popular chocolate brands on their Hong Kong website. Hackers can often make mistakes on regional sites including language errors. One thing customers can be observant about is making sure the checkout form is displayed in the website's native language. For companies, it is important not to neglect regional sites and to have the same security measures in place across websites.

Domain Spoofing

Web-skimming attacks often include domain spoofing to assist in going undetected, this can be seen in some of the most high-profile client-side security attacks. British Airways malicious skimmer exfiltrated card details to a spoof domain, 'baways.com'. To an untrained eye, many of these domains could be seen as legitimate.

Another popular spoof with hackers are third-parties, such as Hotjar, jQuery, and Google Analytics. In the past, the legitimate domain 'google-analytics.com' has been impersonated by 'google-anaiytic.com' and 'g-analytics.com'. A skimmer was observed spoofing HTTPS, the malicious domain 'http.ps' was customised to specific websites and could easily be hidden in the website source code. On grandwesternsteaks.com website, the malicious code appeared in the source code as '//http.ps//grandwesternsteaks.com', which could easily go undetected.

A good indicator of the legitimacy of the domain is to check the WHOIS record and view when and where the domain was registered, and who to. Often attackers only register the domain a few days or weeks before an attack takes place.

OPTIMISATION - MULTI-LAYERED SECURITY

The best approach to ecommerce security for Black Friday and the holiday season is defence in depth. RapidSpike advocates a layered approach using multiple tools to ensure coverage across a variety of potential security issues. Companies need to have security measures in place to both prevent and detect attacks. Attackers are coming up with new ways to disguise their attack techniques, therefore companies need to continuously analyse their site for vulnerabilities as well as monitor for attacks.

PREVENT ATTACKS:

Security Procedures

A Security Analysis should be completed regularly to check on the general health of a website. One of the most basic security measures is to ensure your SSL certificate is valid and redirecting correctly, this will show customers your site is safe to shop on. Monitor your SSL certificate as a preventative method against Domain Hijacking and be alerted to any existing SSL weaknesses.

Penetration Tests

Penetration tests can be performed to find key security flaws hackers take advantage of. Penetration tests involve a third-party company purposefully attempting to hack a website in order to reveal vulnerabilities which cybercriminals could exploit. A penetration test can identify issues which go unnoticed by internal technical teams. These types of tests should be undertaken regularly as companies are often frequently updating websites which could lead to vulnerabilities.

Vulnerability Scans

Vulnerability scans should be performed to check for known vulnerabilities that leave websites open to be attacked. Patching security issues quickly can stop attacks occurring in the first place, this is the most important step in preventing attacks.

Third-party Vetting

Third-parties are commonly used by ecommerce sites, with the average site loading 85 third-parties, companies can easily mistake malicious domains for genuine ones.

Tactics include: imitating domains or domain squatting, where the domain is a commonly misspelt version of the domain. Both of these tactics can easily be mistaken or overlooked. We recommend companies vet all third-parties before putting them live.

Content Security Policy (CSP)

A Content Security Policy (CSP) is a security option website owners can undertake to increase baseline security. CSP requires website owners to manually check what code can be loaded by the browser. Content not outlined within the CSP will not be loaded, therefore malicious code injected by attackers will not be loaded.

Although a CSP appears to give control back to website owners, a CSP is both time and resource-consuming if a website owner does it themselves, and can be expensive with a tool, making it ineffective for a lot of businesses. A CSP also leaves large gaps in security measures and as client-side attacks become more sophisticated, it is important to know not only what content is loaded, but also how the content interacts with a website visitor. Additionally, if your website is hacked, a CSP is useless. Therefore a CSP should be used as an added layer of security and not as an end-all solution.

DETECT ATTACKS:

Data Breach Monitoring

If the prevention approach to security fails or human error occurs, companies still need to monitor for an actual breach. This is key to reducing the size of data exposure. Monitoring can greatly reduce reputational damage as well as fines associated with data breaches.

RapidSpike Magecart Attack Detection is powdered by three monitoring tools to give you additional layers to your security.

Security Researchers

If you are lucky enough to be informed about a possible security issue on your website, inform the relevant departments about the information as soon as possible. Very often companies will ignore researchers when receiving this information leading to an increase in data exposure. As soon as you are informed, take your website offline and investigate. If the security researcher is happy to assist in giving you information about the attack, use this to quickly identify the vulnerability and patch it.

DATA BREACH RESPONSE PLAN

When a breach is discovered a plan is necessary to be able to quickly and effectively respond. The basic steps will include the following:

1. Investigate

Put the website into maintenance mode as soon as possible to investigate. Discover the source of the infection, remove the skimmer, and patch the vulnerability.

2. Inform the ICO

A company has a duty by law to inform the ICO as soon as they discover a data breach but no later than 24 hours of becoming aware. Depending on your country, you may also have to inform other authorities including the Police.

3. Inform Customers

GDPR states companies have 48 hours to inform affected customers of a data breach. However, it is important to use this time efficiently and not to rush a response to make sure you give correct and clear information to all customers affected.

4. Monitor for Reinfection

The average time for reinfection is only 10 days. Companies who make active changes to continuously monitor their security will be able to stay in control and could regain trust from customers.

5. Offer Protection for Customers

Companies are not obliged to pay for credit report monitoring services for customers after a breach, however, it is an additional service you could offer customers and could save brand reputation or prevent lawsuits.

RAPIDSPIKE MAGECART ATTACK DETECTION

Black Friday is a prime time for cybercriminals, with more people shopping online, there is an increased motive for attacks to be carried out. In today's online world, hackers are constantly evolving their tactics, growing stronger, and attacking more frequently than ever. Platforms that could not be hacked today will be hacked tomorrow, so vigilance is key. By accepting nothing is perfect, then adopting a security-first approach from development practices to client-side monitoring is the only way to ultimately be safe and protect your customers. RapidSpike reduces average detection time from weeks to minutes, even if you do have other security flaws, RapidSpike can act as your last line of defence against this particular issue.

RapidSpike Magecart Attack Detection is made up of three layers of protection: Client-Side Security Scanner, Synthetic Attack Detection, and Real User Attack Detection.

MAGECART ATTACK DETECTION

When configuring the Magecart Attack Detection monitor, you can either protect everything or choose the areas of your site which are the most vulnerable. Attack Detection works in two phases: 01 - The Scanning Phase, and 02 - The Detection Phase.

01 - CLIENT-SIDE SECURITY SCANNER

Actively scans the code on your website looking for commonly used patterns that have been used in historic client-side attacks.

02 - SYNTHETIC ATTACK DETECTION

Continuously walks through the critical areas of your website. It will see any data sent to untrusted hosts as it browses.

02 - REAL USER ATTACK DETECTION

Collects where real website visitor's data is being sent. If a malicious destination is added to your website, RapidSpike will alert you.

DEFENCE IN DEPTH

This multi-layered approach means we can examine more data points than ever before - helping us to understand exactly where customers' information is being sent to, allowing companies to both proactively and reactively detect data breaches on the client-side faster than ever.

These three services work as a blended service to offer a best-in-breed defence in depth solution to client-side security issues. Focussing on the scanning of your website looking for known patterns, looking for the appearance of new JavaScript files, and also looking at where your clients are sending data to. This is a comprehensive suite of protection tools that when combined, is the market-leading tool of choice for anybody serious about protecting their brand revenue and client data from client side security issues.

BENEFITS OF MAGECART ATTACK DETECTION:

- Reduces the average time to detection from weeks to minutes.
- Turns every user into a data guardian for your organisation.
- Ensures no malicious destinations get added to your website without your knowledge.
- Detects website skimming, formjacking, and supply chain attacks.
- Clear evidence for the ICO that you have taken steps to defend yourself.
- Insurance against your third-party security failures.
- Continuously monitor for attacks 24 hours a day 7 days a week.
- Last line of defence in case of issues, errors, misconfiguration which allow an attack.
- Receive alerts of any issues in the format of your choice (Email, SMS, Slack, etc.).

2021 HOLIDAY PREDICTIONS

GENERAL PREDICTIONS

Website visitors and sales predictions for Black Friday and the holiday season 2021 have increased again this year. With the ongoing effects of the COVID-19 pandemic, consumers are wary of brick and mortar shopping and instead will opt for online shopping this year. 2020 suffered the worst of the negative implications of the pandemic on employment, and as we see a recovery, we can expect to see an increase in consumer spending.

MARKET SECTOR PREDICTIONS

Market sector predictions include a continued popularity for Technology and Fashion goods. Cosmetics will also continue to be a strong market in the 2021 holiday season. Homeware & Gardening will be sought-after with furniture and other household items in high-demand. RapidSpike's prediction for the largest increase in Black Friday spending will be on Travel websites. After a long period with travel restrictions, we have started to see rules lifting to allow for travel without complex tests.

RapidSpike recently analysed the performance of the top Travel websites. Our advice to consumers would be to avoid shopping for holidays or flights on mobile. Only 6% of the top holiday and airline companies passed Core Web Vitals on mobile, meaning the majority of holiday websites will have a poor user experience. Additionally, website speed is not everything. Only 22% of websites with 'Good' speed index scores passed Core Web Vitals on either desktop or mobile. This means consumers can expect poor loading, interactivity time as well as page shifts.

SECURITY PREDICTIONS

Cybercriminals, in particular web-skimming groups, will take advantage of any website with vulnerabilities. Cybercriminals are also aware that more people will be shopping online with various payment methods. Adobe Analytics show a 44% increase in Buy Now Pay Later (BNPL) payments in 2021 compared to 2019. This increase in the popularity of BNPL also shows consumers are using BNPL for orders of increasingly less value. This payment method could open new avenues for attacks to take place. RapidSpike predicts a 20% rise in Magecart attacks over the holiday season in 2021.

RapidSpike CEO Gav Winter explains:

"Website identity and payment theft will continue to grow. One of businesses' biggest vulnerabilities comes from third parties through the back door such as social media and geo-location tools, 95% of all successful attacks come from human error. The responsibility is not only on consumers to be cautious but big business too. It should not be a once a year box-ticking exercise for them. Hackers change tactics all the time. We process billions of bits of information every second to prevent that." - Daily Express, October 2021

CONCLUSION

2021 Black Friday and holiday season will be unlike previous years due to a continued shift in ecommerce. Website owners need to prepare in advance to cater to their customers' needs. 2020 was a highly successful holiday season with new records being set. 2021 could again break records with consumers opting for more online purchases vs in-store. In the 2020 holiday season, fashion, technology, homeware & gardening, cosmetics, and toys markets did exceedingly well. These will likely continue to be key markets this year. Companies in these sectors should expect an increase in web-traffic and prepare their websites accordingly for this increase.

Availability optimisation should take place before the season, first understanding website traffic limits and adjusting infrastructure to cope with expectations. Monitoring website uptime is a basic step all website owners should be undertaking. By creating a public status page, companies can also keep their customers updated about any issues they face.

Performance optimisation will assist in ensuring customers have a good experience. Websites should not count on customer loyalty as consumers will leave a website that takes too long to load. If you are a multi-billion dollar organisation, sub 2 seconds of performance gains are worth the cost of implementation. The famous often quotes every second saved over 3 seconds gains you 7% in conversions, which is huge in any business, but even a 0.1% gain can mean millions in extra revenue. Serverless Cloud technologies can help with absorbing increased website traffic. Monitoring key customers' journeys is of the utmost importance on Black Friday. Monitoring this performance both synthetically vs real users gives a well-rounded understanding of how customers experience a website. Website owners should provide clear navigation and input a queue system as a last resort to avoid time-out messages. Brand reputation can be jeopardised by poor planning. In addition to preparation, businesses should be alert and actively monitoring their site from all angles. Social media should be utilized to connect with customers and reply in real-time.

A multi-layered security approach is essential this holiday season. There are a multitude of cyber attacks both consumers and businesses should be aware of. Understanding tactics commonly used to carry out attacks means companies can prevent attacks with good planning. Misconfigurations or out of date software can lead to website vulnerabilities, which ultimately can lead to attacks and data loss. Being able to examine multiple data points helps companies to both proactively and reactively detect data breaches on the client-side.

Ensuring websites are reliable, performing highly, and are secure are of the highest importance to businesses this year. By preparing in advance of the season, businesses can reduce disruption and be more in control of their number one priority - their customers' experience.