Black Friday 2021:
What did customers experience online?

NETACEA

Online Shopping Leaves Retailers and Consumers Open to Fraud

The Covid-19 pandemic has turbocharged digital expansion. As reliance on digital services increased, many brick-and-mortar businesses were forced to adapt quickly and create an online presence. This shift to an online-first model contributed to a massive uptick in online shopping during 2020's Black Friday sales, with over 100 million US customers shopping digitally during the Black Friday weekend, resulting in a 22% increase in online spending.[1] Cyber Monday 2020 alone generated $10.8 billion which makes it the biggest eCommerce day in US history.[2] This year, despite Covid restrictions easing across the world and more shops available for in-store spending, analysts anticipated the increase in online shopping would continue, with 44% of UK adults saying they planned to spend exclusively online during the 2021 Black Friday sales.[3]

How we gathered our data

We surveyed consumers about their online shopping experience during the 2021 Black Friday sales to investigate whether their spending may have been impacted by malicious bot activity. The data was gathered from an online survey between 22nd November to 3rd December 2021 in which consumers were asked a series of single- and multiple-choice questions.

Sources:
1. Finances Online: Black Friday Statistics
2. Forbes: Cyber Monday Biggest Online Shopping Day In US History; Cyber Week Biggest In Global History
3. Finder: Black Friday and Cyber Monday statistics 2021

What did consumers experience on Black Friday?

Shopping all over the world

Although most of our survey respondents (68%) were from the UK, almost a quarter came from the US (24%), while 8% responded from Europe and Asia.

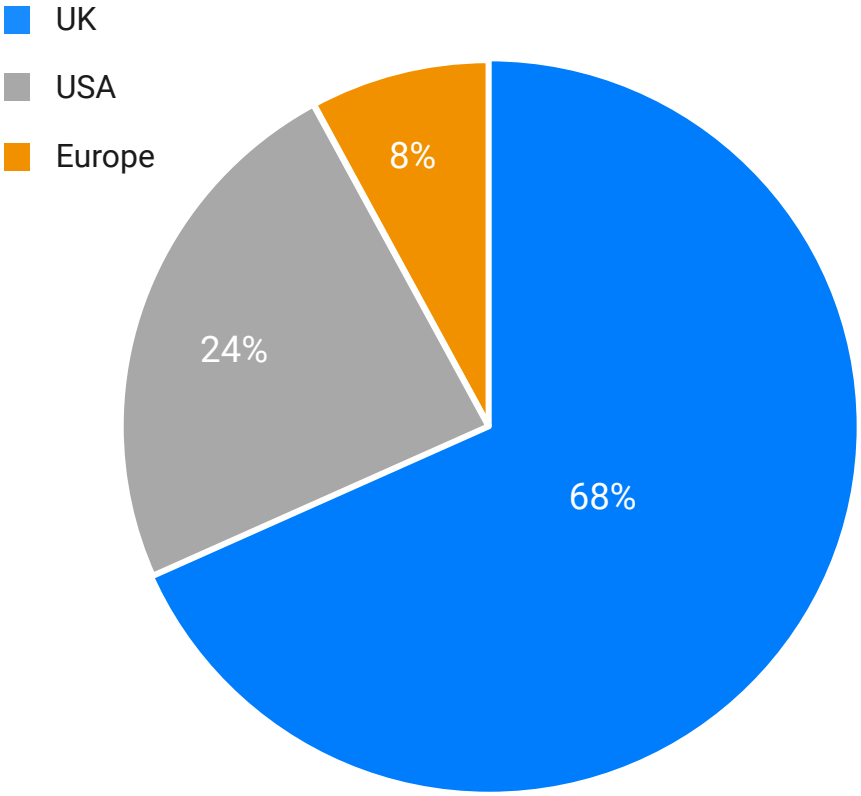


Figure 1: Geographical location of survey respondents. This was a single-choice option in the survey.

Online shopping: 2020 vs 2021

Despite more stores being able to offer in-store shopping this year compared to last, 54% of respondents stated they shopped more online this year than previous years. Whilst the pattern of online shopping versus in-store shopping was similar across the USA and the UK, the USA saw more of an increase in its consumers shopping online (67%) compared to the UK (47%).

Figure 2. Respondents' online shopping behaviour compared with previous years. The bar graph compares the entire data set with the respondents from the UK and the USA. This was a single-choice option on the survey.

Almost all respondents (81%) shopped online to look for a specific item or to shop for gifts, with more than half (54%) stating they were shopping online for holiday or Christmas presents. Just less than 60% of respondents stated they were browsing for deals.

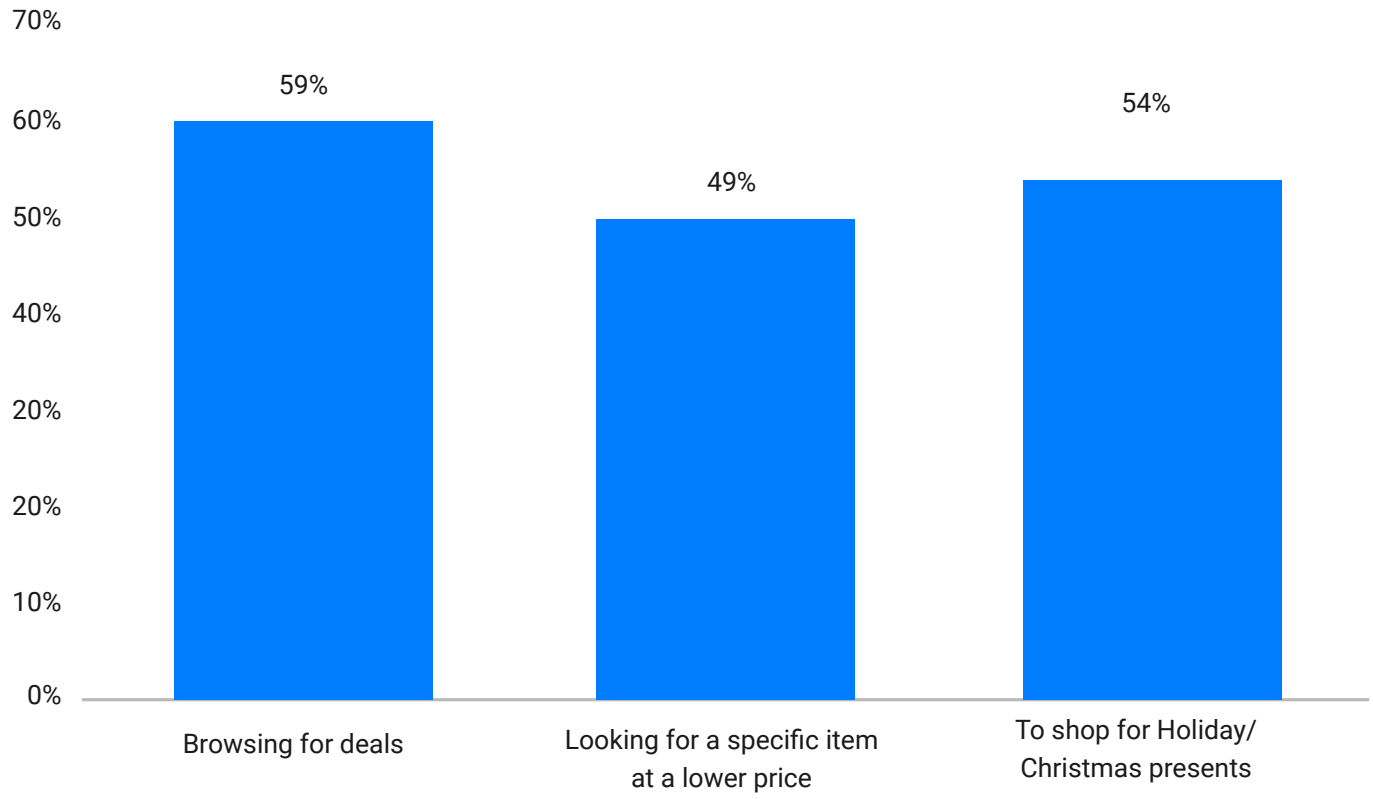


Figure 3. Reasons people shopped online during the 2021 Black Friday sales. This question on the survey allowed multiple choice.

When analysing the types of stores people bought from during the Black Friday sales, the two most popular categories were apparel and fashion (56%) and electronics and technology (55%). Some of the more frequently mentioned sought-after items included technologies such as smartphones, TVs, Apple AirPods, laptops, and tablets, alongside designer clothing and shoes. When asked where consumers first tend to look for deals, the most frequently mentioned store was Amazon, with Best Buy, Currys, Target and Walmart also mentioned on multiple occasions.

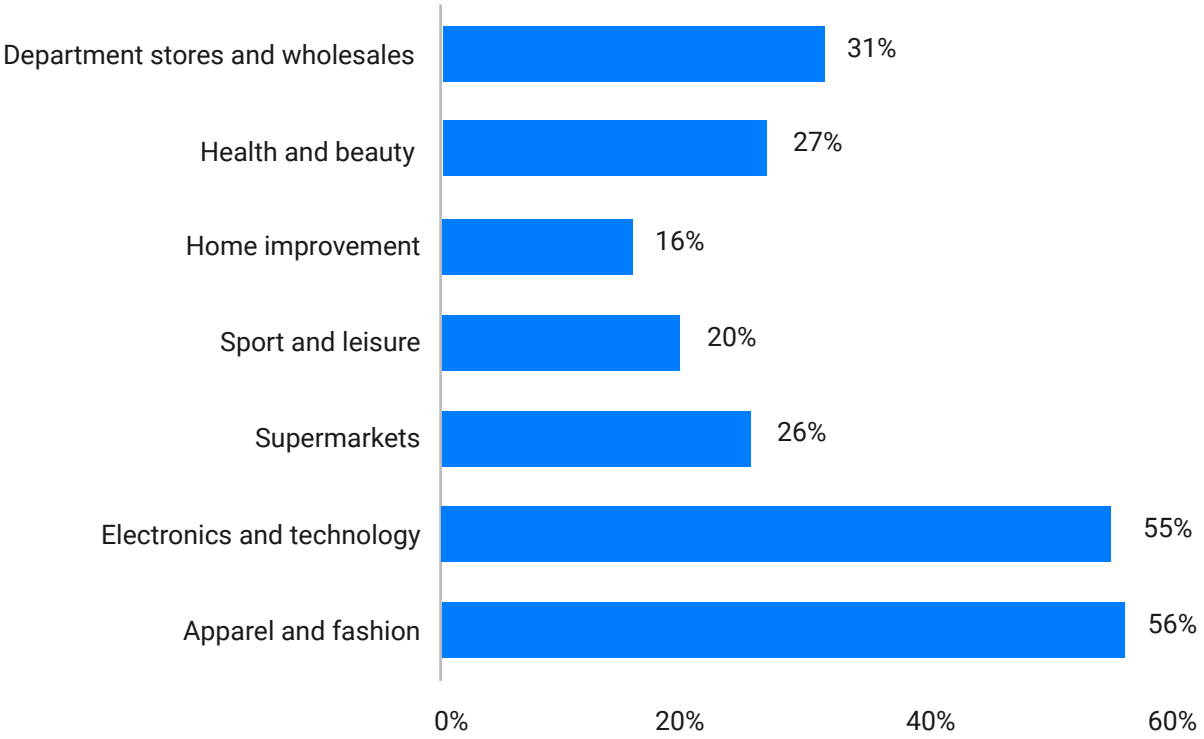


Figure 4. Categories of stores people bought from during the 2021 Black Friday sales. This question on the survey allowed multiple choices.

Previous years saw consumers spending an average of just less than £300 ($396.50 at time of publication) during the Black Friday sales.[4] Whilst our results found that most UK respondents (72%) spent less than £250, average spending in the US was similar to previous years.

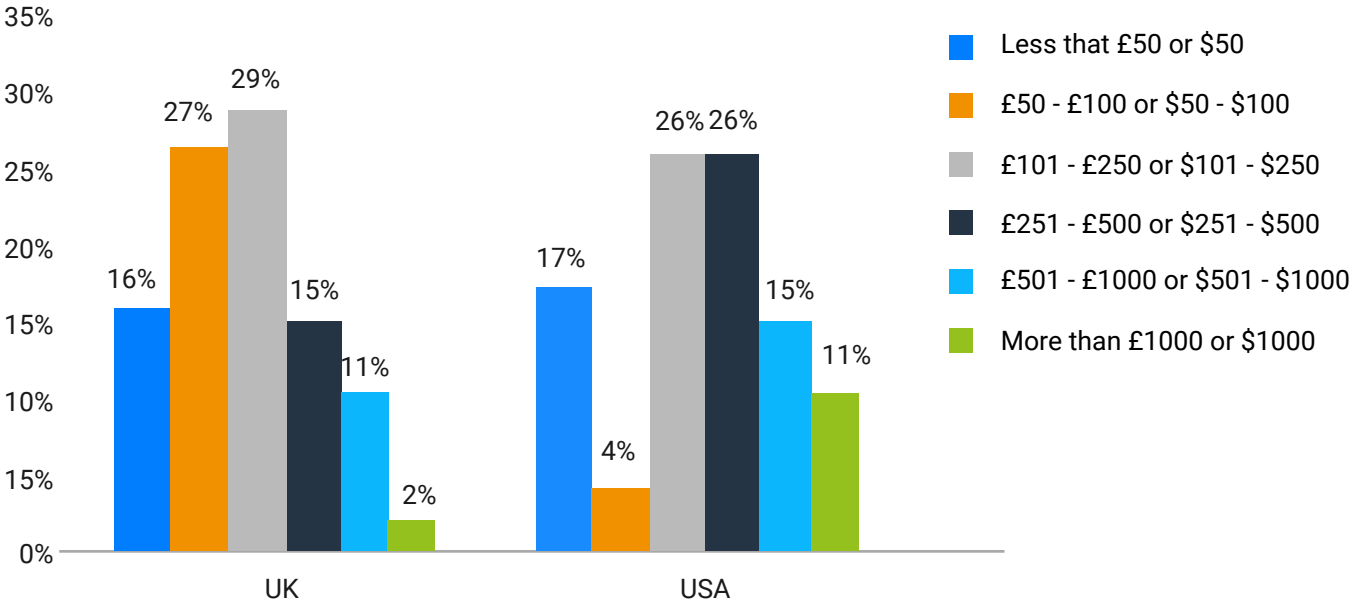


Figure 5. Average customer spending during the Black Friday sales. The data is split between British pound sterling (left) and US dollars (right). This was a single-choice option on the survey.

Sources:
4. Finder: Black Friday and Cyber Monday statistics 2021

Website experiences during Black Friday sales?

More than half of all respondents (58%) experienced a technical issue while shopping online during Black Friday sales. On average, respondents in the US were more likely to experience issues (72%) compared to those in the UK (55%).

The most frequently declared problem consumers faced this year was being unable to purchase an item due to it being sold out quickly (32%), with US shoppers more likely to experience this issue (43%) than UK shoppers (30%). Website pages loading slowly was a consistent issue across both the UK (29%) and the US (30%). Furthermore, while UK shoppers were more likely to experience a login or payment page crashing (15%) than those in the US (11%), US consumers were more likely to experience a full website crash (24%) than their UK counterparts (16%).

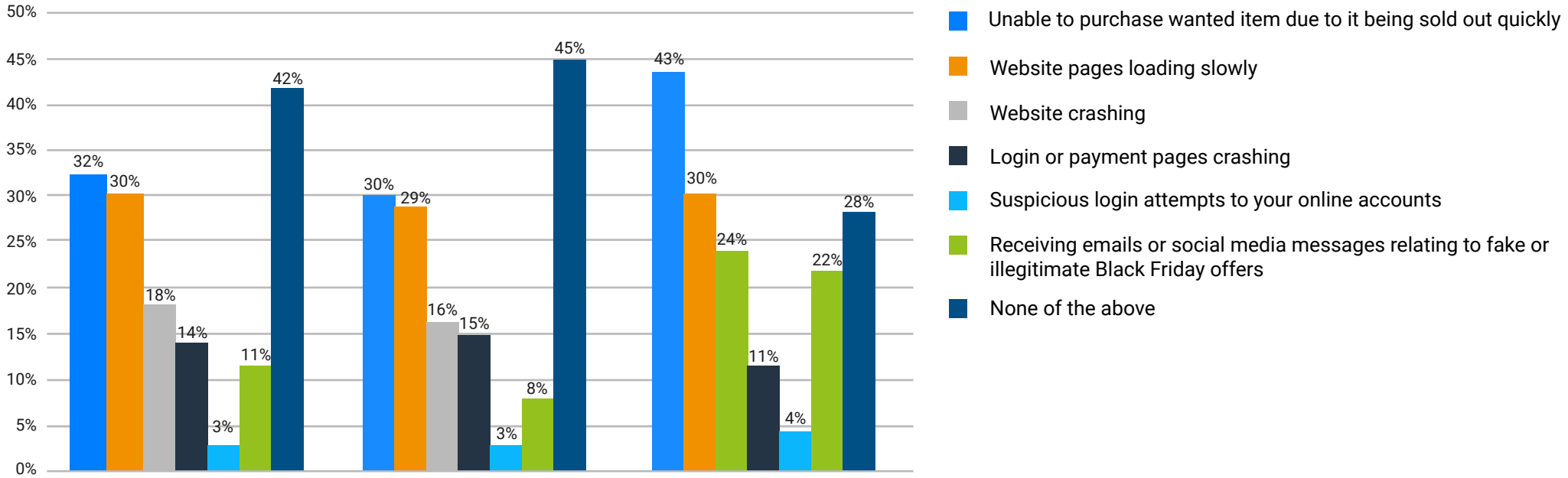


Figure 6. Technical issues faced by customers during the 2021 Black Friday sales. The graph compares the entire data set with the respondents from the UK and the USA. This question on the survey allowed multiple choice.

Netacea Customer Black Friday Findings, 2020 vs. 2021

Netacea manages the traffic for multiple retail websites. To the right are examples from two retail customers comparing the traffic we saw during the month of November in 2020 with the same month in 2021.

Figures 7 and 8 show traffic followed a similar pattern between November 2020 and 2021, however in Figure 7 traffic levels are slightly higher in 2021. These higher traffic levels are congruous with our survey findings, where a sizeable proportion of our respondents (54%) stated they shopped more online this year compared to last.

Figure 7 also highlights more spikes in traffic throughout the month of November in 2021 compared to 2020; in 2021 there are additional traffic spikes on the 8th, 16th, and 28th of the month, compared to none on these days in 2020. The traffic spikes seen across the month in both graphs, and the spike the day before Black Friday in Figure 7, could be due to the Black Friday sales being extended throughout November in recent years, with 52% of responding customers stating they took advantage of early Black Friday deals. Additionally, spikes could correlate with new product launches, for example, in Figure 8 we can see a traffic spike mid-month in 2020, coinciding with the launch of the Sony PlayStation 5 stocked at the large department store responsible for this data.

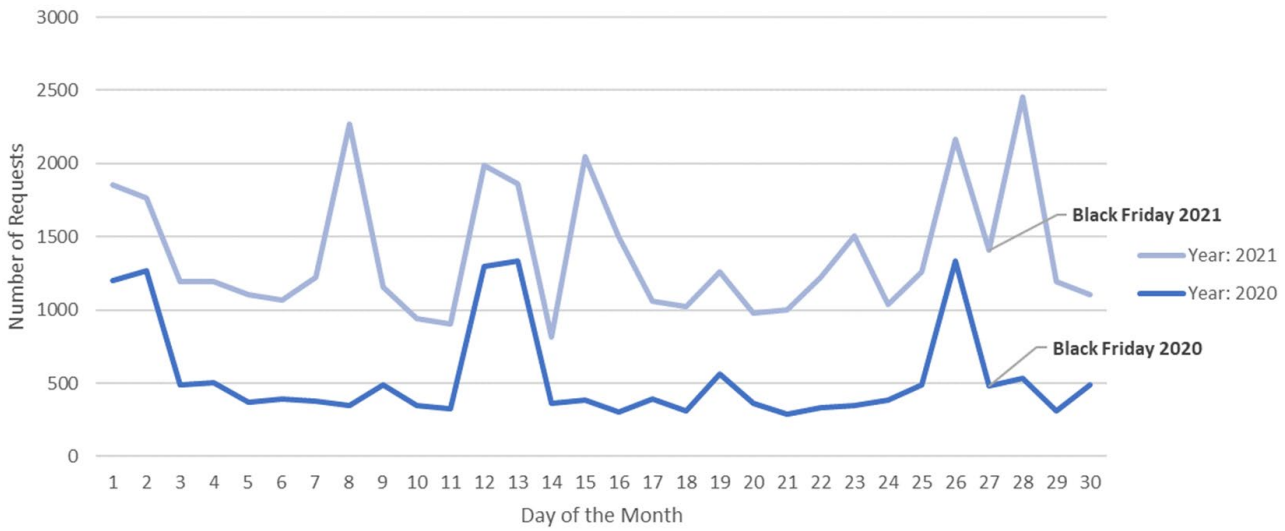


Figure 7. Comparison of traffic levels during the month of November across 2020 and 2021 for one of Netacea's retail customer's sites.

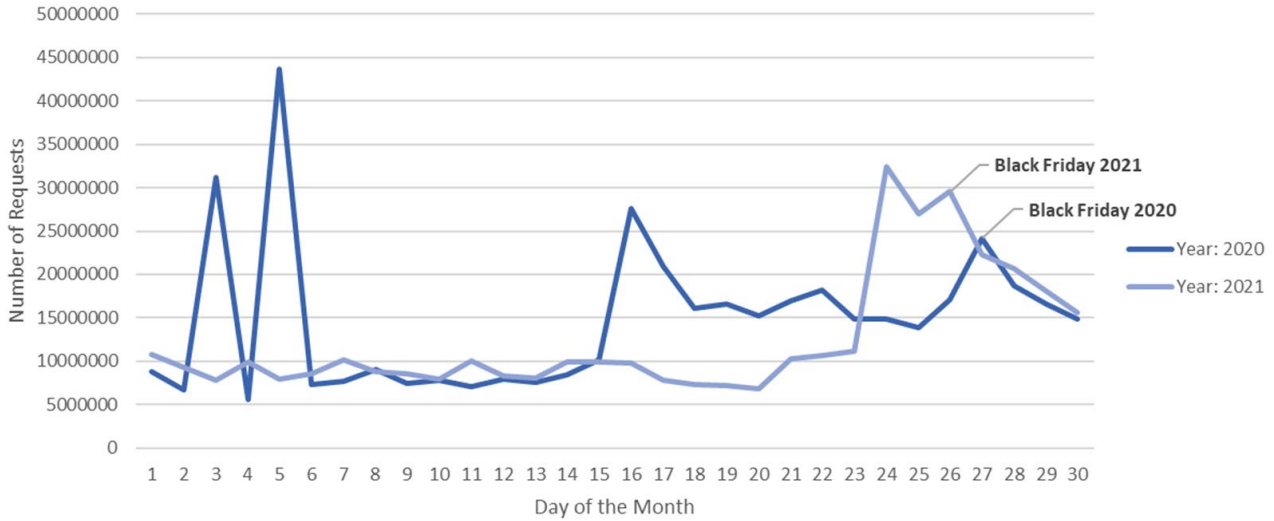


Figure 8. Comparison of traffic levels during the month of November across 2020 and 2021 for one of Netacea's retail customer's sites.

Bots targeting websites during the Black Friday sales

Based on the information gathered in the survey, as well as the data we saw with our retail customers over the Black Friday weekend, we can estimate the bad bot activity experienced by consumers on retail websites during the 2021 Black Friday sales.

32% of respondents stated they were unable to purchase an item they wanted due to it being sold out quickly.

We asked why people shopped online during the Black Friday sales; 49% of people stated that they were looking for a specific item at a lower price. Of these people, 83% stated they were able to purchase the item, but only 47% managed to purchase it on the first site they visited. 31% of respondents had to visit multiple sites before they found the item in stock, and some (5%) even had to purchase the item on a reseller website at a higher price than they were expecting. 15% of the group was unable to purchase the item due to it being out of stock or too expensive on the reseller market.

Slightly more people in the USA were able to find the items they were looking for on the first website they visited (52%) than the UK (44%). We also found that more people in the UK resorted to buying the items they were looking for on a reseller website at a higher price than they were expecting (8%) than their USA counterparts (0%). When comparing this with another response in the survey however, it was found that more US shoppers stated they were unable to purchase a wanted item due to it being sold out quickly (43%) than those in the UK (30%).

Scalper bots (also known as sniper bots, grinch bots or sneaker bots) purchase large quantities of stock quickly, and list them on reseller websites to make a profit, leaving genuine customers unable to purchase the desired product. Scalpers drive large volumes of unwanted bot traffic to your websites, posing a threat to website availability during peak times such as Black Friday, which in extreme cases can cause website downtime.

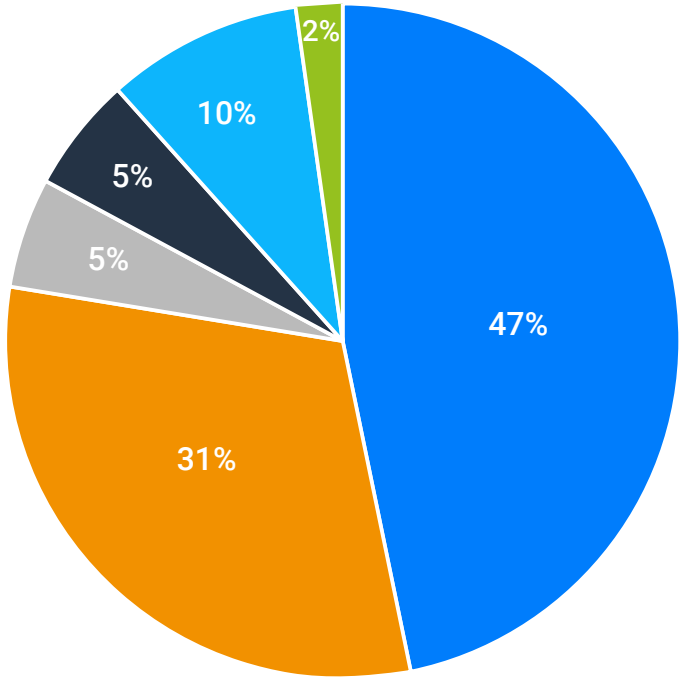


Figure 9. Were consumers able to purchase the specific item they were looking for during the 2021 Black Friday sales? This was a single-choice question in the survey.

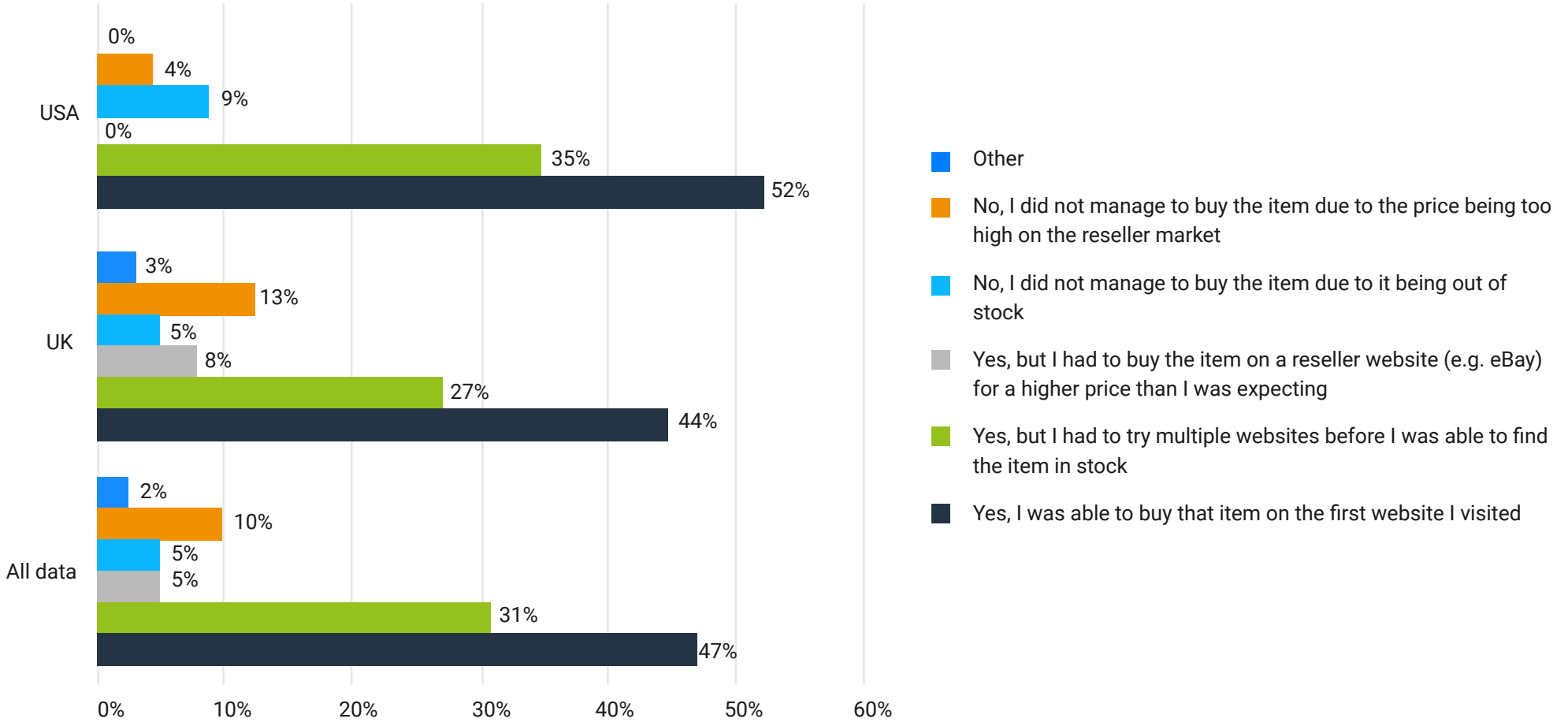


Figure 10. Were consumers able to purchase the specific item they were looking for during the 2021 Black Friday sales? The graph compares the entire data set with the respondents from the UK and the USA. This was a single choice question in the survey.

48% of respondents stated they experienced websites pages loading slowly or crashing.

Web scraping is a technique used to extract certain types of information, such as content, pricing or availability, from your website. This is often done without consent from the company being scraped. It is likely that scraper bot activity on websites contributed to website downtime and slow loading speeds during the Black Friday sales. In the case of retail, scrapers could be looking for new product launches or price drops to launch scalper bots in a future attack.

While scraper bots do not always have malicious intent (for example search engine bots or copyright bots), during peak times they can have just as much of a detrimental impact on your website as the bad bots. Serving requests to these bots, particularly during peak times, uses up server resources which can slow down or crash a website. Additionally, web scraping can push up infrastructure costs with no commercial benefit.

Content and price scrapers monitor your website and gather information. Sometimes this is done with the company's consent for their products to be displayed on price comparison websites against their customers, or to report violations of minimum retail price agreements set by manufacturers. A proportion of price scraping bot traffic, however, comes from competitors looking to use this information to price their items competitively.

17% of respondents experienced login or checkout pages crashing or noticed suspicious login attempts to their online accounts.

In the same way as other malicious bots, credential stuffing and card cracking bots flood login and checkout pages with unwanted automated traffic, which at peak times can lead to website downtime. Additional concerns relating to credential stuffing and card cracking are their associations with online fraud, attempts of which were up 25% in the US alone in the first four months of 2021.[5] Account takeover opens doors to other forms of fraud; from distributing accrued loyalty points to accessing personally identifiable information (PII) or credit card details, fraudulent logins to customer accounts can cause huge financial and reputational losses to a company.

Credential stuffing is a common account takeover technique used to gain brute force access to an account by continually and automatically injecting credentials into website login forms until attackers get a match. Upon gaining access to a customer account, attackers can control any account assets such as loyalty points or saved credit card details and access the PII of the individual.

Card cracking is a brute force attack where card numbers are continually entered into a website's payment processing page until a match is found. This can be done for both credit cards and gift cards. Once the correct card combination is found, attackers are then able to fraudulently purchase their items using stolen credit card or gift card details on the same or another target website.

Sources:
5. CNBC: Why online fraud attempts are up 25% in the US

11% of respondents stated they had received email or social media messages relating to fake or illegitimate Black Friday offers.

While phishing does not directly impact your website, phishing scams are often used to harvest the credentials or credit card details that are then used in credential stuffing and card cracking attacks. It is important for companies to remain vigilant to the types of phishing attacks that are surfacing, especially over the Black Friday weekend, as attackers might be impersonating your company by spoofing company email addresses or websites to make the scam appear legitimate.

Phishing is a technique used by cyber-attackers to gather sensitive information from individuals. The most referenced phishing attacks occur via email. Usually, the email encourages the victim to click on a link, which either takes them to a malicious website, installs malware onto their device, or prompts them to input account credentials which are then harvested by the attacker.

Other forms of phishing include:

- **Vishing:** Obtaining personal or sensitive information via a phone call
- **Smishing:** Similar to phishing but carried out over text message rather than email
- **Spear phishing:** Highly personalised and sophisticated form of phishing directly targeted at a specific individual or company
- **Whale phishing:** Targets authoritative figures within a company, e.g., CEO or CFO

The Problem with Bot Traffic: How to Prepare for Black Friday 2022

In 2021, automated bots were prepped and ready to hit online stores alongside genuine human customers, contributing to the huge spikes seen in online traffic seen during month-long Black Friday sales. Serving requests to bot traffic uses up resource essential to maintaining website speed and good user experience during peak periods, inflating your infrastructure costs for no commercial benefit. Before deciding to block bot traffic, it's essential to understand the types of traffic hitting your site, and not only analyse the bot versus human traffic, but also the good versus bad bot traffic.

It's never too early to start a Black Friday checklist to ensure your business is prepared for next year's surge of festive shoppers. We've listed three essential actions your business needs to put in place to stay one step ahead of the bots.

1 Get visibility over your website traffic

The ability to understand user behavior and intent can help you reduce the amount of malicious activity on your site without compromising search engine rankings or user experience.

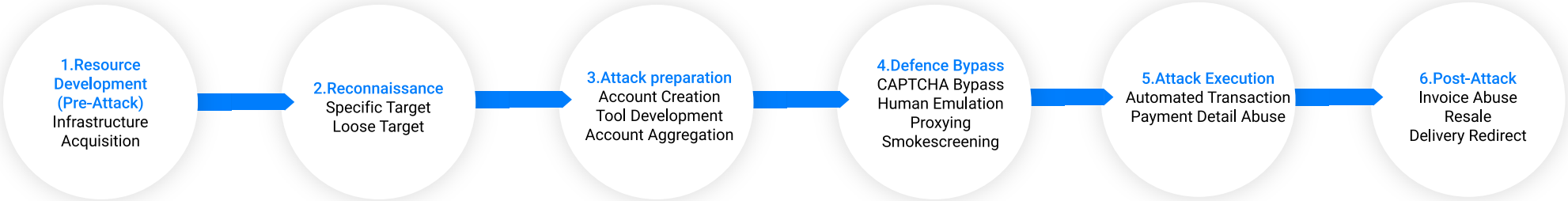
2 Get control of which traffic you allow onto your site

Blocking all bot traffic is not a solution, and neither is allowing all good bots onto your site. If you see high levels of human traffic you might want to temporarily stop the good bots from accessing your site for short periods of time. The ability to control what traffic you allow on your site can help you manage traffic volumes during peak times, ensuring faster loading times and website availability for genuine customers.

3 Prevent attacks before they occur, with the BLADE Framework™:

The Business Logic Attack Definition (BLADE) Framework is an open-source knowledge base pioneered by Netacea's Threat Research team.[6] It was created to help cybersecurity professionals identify the tactics and techniques used by adversaries to exploit weaknesses in the business logic of web-facing systems (websites and APIs).

The framework below outlines how your company can isolate the different stages of a scalper bot attack. By being aware of these stages, companies can improve their risk assessment, strengthen their bot detection and mitigation, and refine their incident response process.



Sources:
6. Business Logic Attack Definition (BLADE) Framework

Start protecting your website from bots during peak traffic times with Netacea

Powered by our machine-learning-led Intent Analytics® Engine, Netacea Bot Management monitors behavior, enabling instant and automatic detection of new attack vectors without the need for manual input or ruleset changes.

With advice from our dedicated bot experts, our technology gives you the flexibility and control over the traffic on your website, mobile apps and APIs during peak retail periods and beyond.

Get in touch to arrange your free trial at hello@netacea.com. Or book your free demo at www.netacea.com/lp/bot-protection/