RISKIQ®

2019 Black Friday and Cyber Monday threat report

Critical threat and consumer intel for this year's Black Friday shopping weekend

Research By Steven Pon and Jordan Herman

E-commerce gets a big slice of the Black Friday pie

£1.49B

UK consumers spent £1.49 billion over last year's Black Friday weekend, up 7.2 percent from 2017.

£720M

In 2018, Cyber Monday saw UK consumers spend a record £720 million on discounted items.

20%

In November 2018, online sales as a proportion of all retailing exceeded 20 percent for the first time in the UK, according to ONS.

$2B+

Black Friday 2018 was the first day in US history to see more than $2 billion in sales stemming from smartphones.

33.5%

In the US, 33.5 percent of 2018 Black Friday e-commerce sales came from mobile devices, compared with 29.1 percent in 2017.

$19.7B

From Nov. 1 through 11, consumers spent $19.7 billion online, up 17.5% YoY, according to Adobe Digital Insights.

This Black Friday weekend, you can be sure that cybercriminals will be joining in on the hunt for sweet sales deals online

In 2018, Black Friday pulled in a record £1.49 billion in online sales, a growth of 7.2 percent from 2017. Cyber Monday followed, amassing a record £720 million. With online spending this Black Friday and Cyber Monday projected to set yet another record in 2019, e-commerce is squarely in the crosshairs of cybercriminals who want a piece of the online shopping pie.

Bad holiday actors will capitalise by using the brand names of leading e-tailers, as well as the poor security habits of consumers. They'll fool shoppers looking for Black Friday deals, sales, and coupons by creating fake mobile apps and landing pages. These malicious assets trick users into downloading malware, using compromised sites, or giving up their login credentials and credit card information.

For shoppers looking to score great deals while filling out their holiday shopping list, one misinformed action can result in a malware infection, stolen personal data, or a hijacked credit card number. For brands, what begins as an event that significantly boosts sales can turn into a security fiasco that erodes the trust of customers and prospects.

In this report, we'll dive into RiskIQ's repository of threat data to expose the e-commerce threat landscape during the busiest shopping weekend of the year, and how threat actors are targeting top-ten most trafficked sites on Black Friday weekend*. We'll then highlight consumer shopping habits gleaned from surveying 1,000 consumers to show how susceptible people are to Black Friday weekend shopping threats.

How to use this report:

- How e-commerce dominates Black Friday and Cyber Monday.
- A look at RiskIQ's unique global internet visibility and how we detect threats.

* based on 2017 site traffic over Black Friday weekend

- Analysis of how attackers are targeting the brands of the 10-most trafficked e-commerce sites over the Black Friday weekend, as well as five of the leading e-tailers in the UK via mobile.
- Consumer habits around shopping via mobile, in-app behaviors, and how to stay safe this Black Friday shopping weekend.
- Analysis of how attackers are targeting the brands of the 10-most trafficked e-commerce sites over the Black Friday weekend, as well as five of the leading e-tailers in the UK via the web.
- Consumer habits around shopping via the web, and how to stay safe this Black Friday shopping weekend.
- How Magecart and other web-skimming actors plan to target consumers during this year's e-commerce frenzy.

The Proof is in the Stuffing

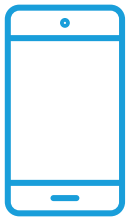
To analyse the methods threat actors will employ this shopping season and where they're focusing their efforts, RiskIQ ran a keyword query of the RiskIQ Global Blacklist and mobile app database*. Our researchers looked for instances of the 10-most trafficked e-commerce sites over the Black Friday Weekend—brands you're incredibly likely to shop with this holiday shopping season.

For our research into websites and landing pages, we looked for domain infringement and phishing events for each of the e-tailers, as well as instances of their branded terms appearing alongside "Black Friday," Cyber Monday," "Christmas," or "Boxing Day" in blacklisted URLs. We also looked at cause-page URLs, pages that send users to a page hosting something malicious.

We then polled 1,000 UK consumers about their intentions to shop this Black Fridayweekend and how. We asked them about their habits around online shopping, mobile phone use, and downloading mobile apps to show how susceptible shoppers are to online threats.

* The source of RiskIQ's Blacklists is our comprehensive collection of internet data, gathered by our exclusive virtual users by scanning, crawling, and passively sensing the internet—including web pages, mobile apps and stores, and the most popular social networks. RiskIQ's crawling technology covers more than 2 billion daily HTTP requests, hundreds of locations across the world, 40 million mobile apps, and 600 million domain records.

The findings confirmed that threat actors are using these well-known brands specifically to exploit the popularity of Black Friday and Cyber Monday shopping via both web and mobile. For example, more than 38 percent of people said they do not read or are unsure if they read the permissions before downloading an app. The panelists also confirmed that prevailing consumer habits and lack of online awareness provide a deep victim pool ripe for exploitation for cybercriminals.



Mobile Threat Findings

Black Friday 2018 was the first day in history to see more than $2 billion in sales stemming from smartphones, while 33.5 percent of e-commerce sales came from mobile devices, a 4.4 percent increase over 2017. Adobe predicts consumers will spend billions more on their phones this year. This huge spike in spending makes shoppers increasingly at risk of encountering phishing pages, malicious apps, and viruses that infect their phones and tablets to mine sensitive data.

Much of this potential damage comes from mobile apps built to fool users into entering their credit card information, which opens them up to financial fraud. Some fake apps contain adware and ad-clicks or malware that can steal personal information or lock the device until the user pays a ransom. Others encourage users to log in using their Facebook or Gmail credentials, potentially exposing sensitive personal information.

RiskIQ also regularly blacklists apps that request excessive permissions, including the ability to read sensitive log data, receive text messages (SMS), collect data from the internet, modify system settings, and steal other data.

Using RiskIQ data sets centered around malicious applications, we found:

- RiskIQ observed a 20 percent increase in total blacklisted apps, and the percentage of blacklisted apps relative to the total number of apps known by RiskIQ also increased, jumping from 1.95 percent to 2.1 percent
- Of all apps that can be found by searching "Black Friday," "Cyber Monday," "Boxing Day," or "Christmas," **951 or 2%**, are blacklisted (unsafe to use) as malicious.

20%
increase in blacklisted apps.

2%
of apps found by searching seasonal keywords are blacklisted as malicious.

6,353
blacklisted apps contain branded terms.

4
blacklisted apps, on average, contain branded terms of the top-10 most trafficked brands with seasonal keywords.

24
blacklisted apps contain branded terms of the top-five 'Elite' Retailers in the UK

Top-10 Most Trafficked Sites on Thanksgiving Weekend

- Threat actors have focused on these leading brands in e-commerce. They have a combined total of **6,353** blacklisted apps that contain their branded terms in the title or description.

- These brands averaged more than **4** blacklisted apps containing both its branded terms and "Black Friday," "Cyber Monday," "Boxing Day," or "Christmas, in the title or description, showing clear intent by threat actors to leverage the shopping holiday.

Top-5 'Elite' Retailers (UK)

- All apps for the top-five 'Elite' Retailers in the UK: Threat actors have focused on these leading brands in e-commerce. They have a combined total of **24** blacklisted apps that contain their branded terms in the title or description.

Consumer Findings and How to Protect Yourself

While RiskIQ sees the vast majority of malicious applications hosted on third-party app stores, official stores run by Apple and Google have also been observed hosting malicious apps. For instance, the Google Play store led the way in hosting blacklisted apps found by RiskIQ in Q2. It's important to realise that protection by most mobile app stores is good, but not bulletproof. Even the official app stores host apps that can be dangerous.

Fortunately, there are ways to help reduce digital risk during this holiday shopping season:

- RiskIQ found that nearly 26 percent of respondents said they had downloaded an app outside of the Google Play and Apple App stores. Seven percent say they aren't sure if they have or not.
  - **Stay in the major app stores:** Ensure that you are only downloading apps from official app stores such as Google or Apple. The overwhelming majority of blacklisted apps are found in other stores and on the open web.

- More than 38 percent of consumers said they do not read or are unsure if they read the permissions before downloading an app.
  - **Be wary of suspicious permissions:** Excessive permissions like access to contacts, text messages, administrative features, stored passwords, or credit card info are indicators of threat activity.

26%

downloaded apps outside of Google Play/ Apple App stores.

38%

don't read or are unsure if they read permissions before downloading.

75%

would download a shopping-related app if it offered a discount.

- 75 percent of respondents say they would download a shopping-related app if it offered a steep discount. Yet, more than 58 percent of consumers say they do not check who the developer is before downloading an app.
  - **Know who is making your apps:** Make sure to take an in-depth look at each app. New developers, or developers that leverage free email services (e.g., @gmail) for their developer contact, can be big red flags—threat actors often use these services to produce mass amounts of malicious apps in a short period. Also, poor grammar in the description highlights the haste of development and the lack of marketing professionalism that are hallmarks of mobile malware campaigns.

  - **App reviews are not always what they appear to be:** Just because an app seems to have a good reputation doesn't make it so. Rave reviews can be forged, and a high amount of downloads can simply indicate a threat actor was successful in fooling a lot of victims. If the developer is not a brand you recognise or has a strange appearance or spelling, think twice. You can even do a Google search on the developer for more clues about its reputation.

Web Threat Findings

Adobe predicts online holiday spend will surpass $140 billion, representing 14.1 percent growth year-on-year (YoY), and Cyber Monday will set a new record with $9.4 billion. With all the online activity around Black Friday, it's easy for threat actors' infrastructure to hide in plain sight. They'll often use brand names in malicious URLs to fool people into visiting pages that phish for sensitive information, infect users with malware, or redirect traffic to other malicious or fraudulent pages.

37,000

probable instances of **domain infringement**.

2,086,529

Magecart skimmers observed in the wild.

3,589

blacklisted URLs found containing branded terms

Domain Infringement

Domain infringement targeting brands, employees, and customers is a prolific, effective tool in the hands of attackers and has only grown worse in recent years due to the opening of thousands of new gTLDs, the growth of free and cheap domain registration services, and attack techniques like domain shadowing.

Attackers are directly scamming end-users with high-volume phishing campaigns against consumers or targeted spear-phishing campaigns attempting to fool corporate employees. These attacks are cheap to execute, and they are proving to be incredibly efficient in breaching sensitive data. A query of the branded terms of 20 Fortune 100 companies in RiskIQ's domain infringement detection once revealed 37,000 probable instances of domain infringement over a two-week period or 1,850 incidents per brand.

RiskIQ detected:

- **65** incidents of domain infringement across the top-10 most trafficked sites on Black Friday weekend containing their branded terms and "Black Friday," "Cyber Monday," "Boxing Day," or "Christmas."

- **11,132** new hostnames containing "Black Friday," "Cyber Monday," "Boxing Day," or "Christmas." New hostnames containing these terms spun up near the Black Friday shopping weekend don't necessarily indicate a legitimate threat but should be viewed with suspicion.

Magecart (Web Skimming)

Magecart is a rapidly growing cybercrime syndicate comprised of dozens of subgroups that specialise in cyberattacks involving digital credit card theft by skimming online payment forms. Magecart also refers to the JavaScript code those groups inject. It works by operatives gaining access to websites and injecting malicious code that steals the credit card information shoppers enter into online payment forms.

Magecart is responsible for placing skimmers on scores of e-commerce sites, including those of global brands in which its operatives intercepted thousands of consumer credit card records. Because of these high-profile attacks, Magecart is now becoming a household name. RiskIQ, which detects internet-scale threats, is alerted to new Magecart breaches hourly. This detection rate is a clear indication that the group is extremely active and will continue to be a critical threat to consumers, especially over the Black Friday shopping weekend.

- RiskIQ has observed Magecart skimmers in the wild 2,086,529 times.
- The average length of a Magecart breach is 22 Days. Anyone making a purchase on a compromised site during this period is likely a victim of credit card theft.

Blacklisted URLs

Threat actors build out malicious infrastructure, including URLs, to leverage in their threat campaigns. We queried the RiskIQ Global Blacklist for URLs of malicious pages and pages that lead to malicious pages leveraging these brands as well as "Black Friday and "Cyber Monday."

Looking at a sample of five of the top-10 most trafficked sites on Black Friday weekend 2017, we found an average of **3,589 blacklisted URLs containing their branded terms**. Broken down by brand, you can see threat actors are purposely leveraging these brands for their campaigns:

We also found:

- 1,878,818 Blacklisted URLs contain "Black Friday," "Cyber Monday," "Boxing Day," or "Christmas."
- 1,881,132 Blacklisted Cause URLs contain "Black Friday," "Cyber Monday," "Boxing Day," or "Christmas."
- 1,886,652 Blacklisted sequence URLs contain "Black Friday," "Cyber Monday," "Boxing Day," or "Christmas."

Consumer Findings and How to Protect Yourself

When shopping this Black Friday weekend, it's essential to keep in mind that the internet may be more dangerous than you think. Do your part to work with the security teams of major retailers by following these tips to avoid Black Friday scams:

75%

would purchase with a retailer they've never shopped with before if it offered a discount.

33.4%

feel third-party payments systems are safe.

9%

have had their credit/ debit card stolen in the last three months.

28%+

are only somewhat vigilant or not vigilant when entering payment information online.

- 75 percent of respondents said they would purchase with a retailer they've never shopped with before if they offered a steep discount.
  - **Check website addresses:** Especially after following links on Twitter, Facebook, or other social media channels, be sure you end up on the actual website of the retailer you want.
- One third (33.4 percent) of respondents feel that credit or debit cards are the safest way to pay online.
  - **Don't enter credit card info if you don't have to:** Large stores like Amazon store your card in your account, so you don't need to enter it into a web form where a Magecart skimmer might be lurking. Another way to avoid entering your card details is by using Apple Pay, PayPal, or a similar mobile payment system. These send a sort of one-time token of your credit card information.
- 9 percent of respondents have had a credit or debit card stolen in the past three months.
  - **Keep an eye on your credit card activity:** Don't only watch for large transactions; some thieves run small charges. If you suspect that your card was skimmed, whether you see a suspicious transaction or not, call your card issuer and request a new card. They'd rather issue you a new card than have a fraudulent transaction go through.
- More than 28 percent of respondents say they are onlysomewhat vigilant or not vigilant when entering payment information online.
  - **Look for the "S" in HTTPS:** Beware of shopping sites that do not use HTTPS in their website addresses or do not display the symbol of a lock next to the web address. Secure sites use HTTPS and, without that, you're dealing with unsecured connections or weak encryption of personal data.
  - **Know a scam when you see one:** If you do provide your credit card information, make sure you are in a secure online shopping portal. Sites that ask for it in return for "coupons" or to win "free" merchandise are almost always scams.

About RiskIQ

RiskIQ is the leader in digital attack surface management, providing the most comprehensive discovery, intelligence and mitigation of threats associated with an organisation's digital presence. With more than 75 percent of attacks originating outside the firewall, RiskIQ allows enterprises to gain unified insight and control over web, social and mobile exposures. Trusted by thousands of security analysts, security teams and CISO's, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk and take action to protect the business, brand and customers. Based in San Francisco, the company is backed by Summit Partners, Battery Ventures, Georgian Partners and MassMutual Ventures.

Try RiskIQ Community Edition for free by visiting https://www.riskiq.com/community/. To learn more about RiskIQ, visit www.riskiq.com.

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com