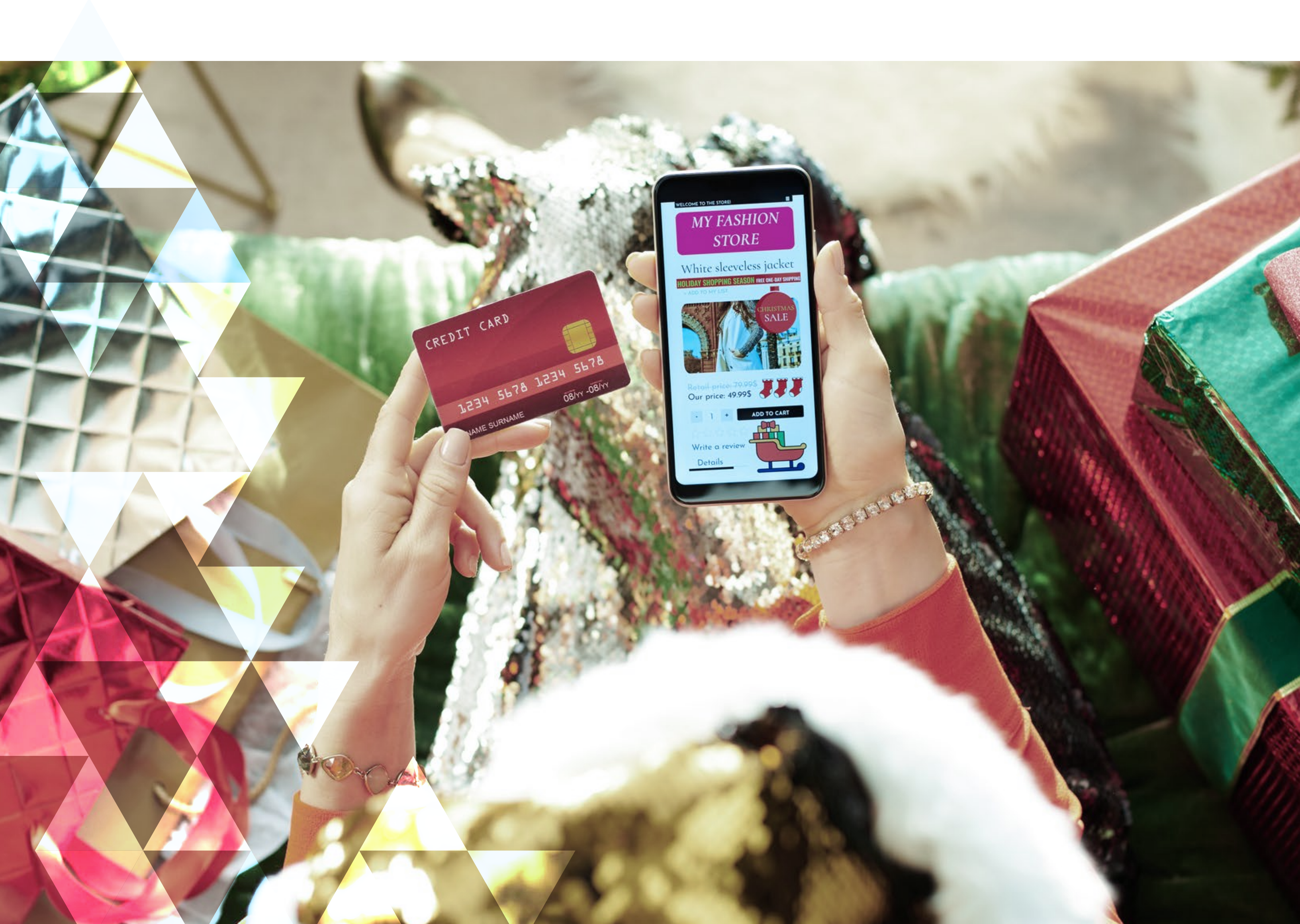
RISKIQ®

RiskIQ's 2020 Holiday Shopping E-commerce Blacklist Threat Report

Critical Threat and Consumer Intel for This Year's Shopping Season, Including Black Friday and Cyber Week



▶ **30%**

of all retail sales occur between Black Friday and Christmas.

▶ **35%**

rise predicted in U.S. e-commerce sales compared to last year.

▶ **83%**

of shoppers will spend 50% of their budget online.

Over Thanksgiving weekend, you can be sure that cyber criminals were also feasting. And, as nearly 30% of all retail sales occur from Black Friday until Christmas[1], they'll continue to target shoppers and top e-commerce brands throughout the holiday shopping season.

Digital commerce has the potential to break records this year, with extraordinary circumstances funneling more shoppers to digital outlets than ever before. Even considering widespread belt-tightening caused by COVID-19-related job loss, Deloitte projects a continued rise in retail sales over last year's figures[2]. The firm forecasts that U.S. e-commerce sales could rise by as much as 35%. Meanwhile, eMarketer projects a 10% fall in overall holiday sales in the U.K, but a 17% rise in e-commerce sales due to limited in-store retail options[3].

A recent consumer survey conducted by RiskIQ found that 83% of people will spend at least 50% of their budget online[4]. With online spending this holiday shopping season projected to set yet another record, e-commerce is squarely in the crosshairs of cybercriminals who want a piece of the online shopping pie.

These bad holiday actors capitalize by using the brand names of leading e-tailers and consumers' poor security habits and fool shoppers looking for holiday shopping deals, sales, and coupons by creating fake mobile apps and websites. 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.

This report will dive into RiskIQ's Internet Intelligence Graph[5] to expose the e-commerce threat landscape during the busiest shopping period of the year and how threat actors target top-ten most trafficked e-commerce sites in the U.S. and U.K.

[1] https://nrf.com/media-center/press-releases/nrf-expects-holiday-sales-will-grow-between-36-and-52-percent

[2] https://www.cnbc.com/2020/09/15/deloitte-estimates-2020-holiday-retail-sales-will-rise-1-to-1point5percent-.html

[3] https://www.emarketer.com/content/uk-holiday-season-shopping-2020

[4] https://www.riskiq.com/resources/research/holiday-shopping-consumer-survey-report/

[5] https://www.riskiq.com/blog/external-threat-management/internet-intelligence-graph/

How to Use This Report

- A look at RiskIQ's unique global internet visibility and how we detect threats
- Analysis of how attackers target the brands of the 10-most trafficked e-commerce sites via mobile and the web in the U.S. and U.K.
- How Magecart and other web-skimming actors plan to target consumers during this year's e-commerce frenzy
- Guidance for how consumers can stay safe this holiday shopping season

Methodology

To analyze the methods threat actors are employing 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 20-most trafficked e-commerce sites in both the U.S and U.K.—brands you're very likely to shop with this holiday shopping season—from January 2020 to December 7, 2020.

For our research into websites and landing pages, we looked for domain infringement events, which are used to fool shoppers and often leveraged in phishing campaigns, for each of these 20 e-tailers. We also looked for instances of their branded terms appearing alongside "Black Friday," "Cyber Monday," "Boxing Day," or "Christmas."

The findings confirmed that threat actors are using these well-known brands specifically to exploit the popularity of holiday shopping and shopping events via both web and mobile.

* The source of RiskIQ's Blacklists is our Internet Intelligence graph built from our expansive collection of internet data. Our exclusive virtual users gather this data 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 worldwide, 40 million mobile apps, and 600 million domain records.

Mobile Threat Findings

Continued adoption of both mobile retail apps and the practice of shopping through social media also stood out as 2019 Black Friday trends. Mobile spending leapt 17% on Black Friday, tallying $4.1 billion in sales[6], and nearly 70% of consumers plan to primarily use a mobile phone to complete their online shopping[7].

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 they pay 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:

By any measure, the mobile landscape is getting bigger, busier, and more complex. RiskIQ cataloged 18% more apps worldwide in 2019 than in 2018[8].

However, despite seeing and cataloging far more apps in 2019, RiskIQ blacklisted 25,796 apps, more than 76% fewer than in 2018[9]. Blacklisted apps appear on at least one blacklist, such as VirusTotal, which, per its website, inspects files or web pages with over 70 antivirus products and other tools. A blacklist hit from VirusTotal shows that at least one vendor has flagged the file as suspicious or malicious.

- Of all apps that can be found by searching “Black Friday,” “Cyber Monday,” “Boxing Day,” or “Christmas,” **466** are blacklisted (unsafe to use) as malicious.

17%

increase in mobile spending on Black Friday.

70%

of consumers plan to shop from their mobile device.

18%

more apps worldwide year-over-year.

76%

fewer blacklisted apps year-over-year.

[6] https://www.retaildive.com/news/the-winners-and-losers-of-black-friday-2019/568214/

[7] https://www.riskiq.com/resources/research/holiday-shopping-consumer-survey-report/

[8] https://www.riskiq.com/resources/research/2019-mobile-threat-landscape-report/

[9] https://www.riskiq.com/resources/research/2019-mobile-threat-landscape-report/

- Threat actors have focused on these leading brands in e-commerce. They have a combined total of **1,654** blacklisted apps that contain their branded terms in the title or description. That's **82.7 per brand**.

- RiskIQ found an average of nearly **3** blacklisted apps for each brand 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.

Web Threat Findings

With all the online activity around Black Friday[10], 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**.

22 days
is the average length of a **Magecart breach**.

18,891
blacklisted URLs found containing branded terms.

Domain Infringement

The registration of domains that infringe on well known brands is a common tactic in phishing campaigns and has grown in popularity 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 revealed 37,000 probable instances of domain infringement over two weeks or 1,850 incidents per brand.

RiskIQ detected:

- **7** domain infringement events across the top-10 most trafficked sites containing their branded terms and "Black Friday," "Cyber Monday," "Boxing Day," or "Christmas."
- **208** domain infringement events containing only "Black Friday," "Cyber Monday," "Boxing Day," or "Christmas." New hostnames containing these terms spun up near the Thanksgiving shopping weekend don't necessarily indicate a legitimate threat but should be viewed with suspicion.

[10] https://holiday-shopping-observations.riskiq.com/

Magecart (Web Skimming)

Magecart is a rapidly growing cyberthreat comprising dozens of subgroups specializing 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 indicates that the group is extremely active and will continue to be a critical threat to consumers, especially during holiday shopping.

- The average length of a Magecart breach is 22 Days. Anyone making a purchase on a compromised site during this period is likely a credit card theft victim.

- RiskIQ detects a Magecart attack every 16 minutes[11].

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 in the U.S. and U.K., we found:

- **18,891** blacklisted URLs containing their branded terms, or 945 per brand. Broken down by brand, you can see threat actors are purposely leveraging these brands for their campaigns.

[10] https://www.riskiq.com/resources/infographic/evil-internet-minute-2020/

Consumer Findings and How to Protect Yourself

When shopping this holiday season, 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 holiday shopping scams:

- **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.
- **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.
- **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.
- **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.
- **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.
- **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.
- **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. Threat actors can forge rave reviews, and a high amount of downloads can simply indicate a threat actor was successful in fooling many victims. If the developer is not a brand you recognize or a strange appearance or spelling, think twice. You can even do a Google search on the developer for more clues about their reputation.

About RiskIQ

RiskIQ is the leader in digital threat management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. With more than 75%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