RiskIQ Consumer Holiday Shopping Report and Outlook 2020

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. The firm forecasts that e-commerce sales could rise by as much as 35% due to limited in-store retail options.

At RiskIQ, we cannot help but view this uptick in digital spending for what it presents: more opportunities for cybercriminals to stuff their metaphorical stockings with the high-value gift of stolen personal data. We surveyed a cross-section of American shoppers to better understand this holiday shopping season's threat landscape through the lens of consumers' habits and their role in protecting personal information while shopping online.

With this report, we explore:

- The scope of online shopping last year, which provides a proven basis for consumer trends we may expect to see in the 2020 holiday season
- How consumers plan to allocate their holiday budgets, and what effect COVID-19 will have on the way that they shop
- Whether consumers are aware of and prepared for the threats that come with online shopping in 2020
- How RiskIQ advises consumers to protect their data this holiday season

Our data suggests that consumers plan to spend big once again this holiday season.

Some of our key findings include:

90% OF PEOPLE ARE CONCERNED OVER THE RISE IN CYBERCRIME SINCE THE START OF COVID-19

56%

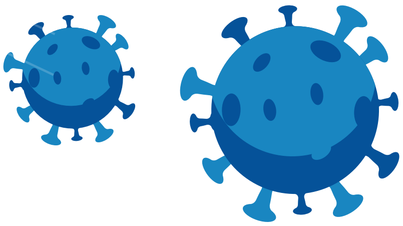
OF PEOPLE CITE THE PANDEMIC AS A REASON THEY'VE CHANGED THEIR ATTITUDE TOWARD ONLINE SECURITY

83%

OF PEOPLE WILL SPEND AT LEAST **50%** OF THEIR BUDGET ONLINE AND **22%** WILL SHOP ENTIRELY ONLINE WITH NO PLANS TO SHOP AT BRICK AND MORTAR STORES

85%

OF PEOPLE ARE MILDLY TO HIGHLY CONCERNED ABOUT THEIR PERSONAL INFORMATION WHEN SHOPPING ONLINE



75% OF PEOPLE WILL SPEND THE SAME OR MORE THAN LAST YEAR

We offer a few tips for how to spot and thwart cybercriminals for those hoping to avoid cyber-victimization.

Examining Last Year's Online Shopping Trends

Black Friday E-commerce Growth Continues Despite COVID

Shoppers were already dipping heavily into e-commerce for their holiday gifting needs last year in pre-pandemic times. Last year's Black Friday saw $7.4 billion in online sales, the most ever for online spending on a Black Friday.

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.

Other figures that illustrate the trends from Black Friday in 2019 include:

- Online revenue for retailers averaged more than $2.3 billion per day
- Sales revenue earned through smartphone purchases accounted for 36% of all Black Friday sales
- Large online vendors like Amazon and Wal-Mart significantly outperformed smaller online vendors

Expect these trends to continue into 2020 and even accelerate due to widespread brick-and-mortar retail shutdowns and safety concerns.

Going directly to the shoppers to determine how they plan to procure their gifts and take advantage of deals this holiday season gives us a clear idea of whether they will be potential marks for cybercriminals this Black Friday and Cyber Week season.

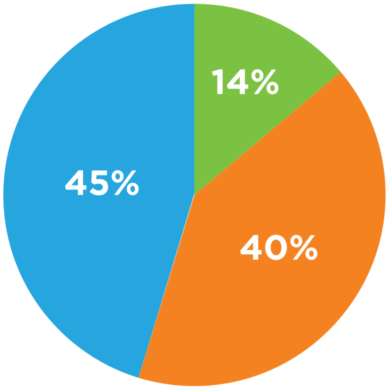
How Consumers Plan to Shop This Holiday Shopping Season

COVID-19 Will Keep Shoppers Home

We asked prospective holiday shoppers several questions that collectively helped us develop a profile of shopper attitudes, characteristics, and plans for the 2020 holiday season.

Respondents were between 16 and over 54 years old, with a fairly even split between men and women. In seeking a representative picture, we found that:

58% OF RESPONDENTS ARE DOING **75%** OR MORE OF THEIR HOLIDAY SHOPPING ONLINE.



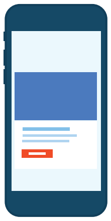
40% respondents plan to split their online shopping between big box stores and small, independent retailers.

45% of respondents plan to do most of their Black Friday and Cyber Week shopping with big box stores.

14% of respondents will buy exclusively from small retailers.

MOST (51%) OF RESPONDENTS’ SPENDING WILL BE **AFFECTED BY COVID**

NEARLY 70% OF RESPONDENTS PLAN TO PRIMARILY USE A MOBILE PHONE TO COMPLETE THEIR ONLINE SHOPPING



NEARLY 33% OF RESPONDENTS PLAN TO SPEND LESS MONEY

67% OF RESPONDENTS PLAN TO SPEND THE SAME AMOUNT OR MORE ONLINE THIS HOLIDAY SHOPPING SEASON

Health concerns related to COVID-19 and convenience were respondents’ two primary reasons for shopping online or through mobile apps.

These findings indicate that shoppers plan to do what experts have projected them to spend more money, spend it mostly online, patronize big-box retailers, and use a mobile phone or desktop.

Hackers know this too, so what are shoppers planning to do to protect their data, payment information, and personal identifiers from theft?

Consumer Views Towards Online Shopping Safety

Consumers Unaware of Digital Credit Skimming

Any informed consumer who plans to do any online shopping this holiday shopping season must know that their data could be at risk. They should take measures to protect themselves, but their adversaries will be formidable and numerous. Even Amazon, the world's largest retailer, saw its customers victimized by a Black Friday breach in 2018.

But how aware of these threats are online shoppers heading into Black Friday and Cyber Week 2020? If they are aware, what are they doing to protect their data? Our data hints that this year's potential record number of online shoppers may not be prepared to avoid cyber thieves' cleverly-laid traps.

Our direct-to-shopper survey found that:

85% OF SHOPPERS ARE AT LEAST MILDLY CONCERNED ABOUT THEIR PERSONAL INFORMATION BEING COMPROMISED WHEN SHOPPING THROUGH A WEBSITE OR BROWSER

88% OF SHOPPERS ARE AT LEAST MILDLY CONCERNED ABOUT THE SAFETY OF APPS FOR RETAIL PURPOSES.

CONCERN FOR PERSONAL DATA AMONG SHOPPERS PLANNING TO USE MOBILE DEVICES TO PURCHASE ITEMS ON BLACK FRIDAY AND CYBER WEEK WAS SIMILAR TO SHOPPERS PLANNING TO USE A WEBSITE OR BROWSER.

Holiday shoppers who we polled have varying levels of concern towards the general rise in cybercrime since the beginning of the COVID-19 pandemic. Despite record levels of reported cybercrime, we found that only 23% of respondents have had to cancel a credit card due to online fraud in the past year, which may help explain this lower than expected level of concern.

The data also indicates a general lack of knowledge of the prevalence of online card skimming by Magecart actors. RiskIQ detects the presence of malicious code that skims (intercepts) consumers' credit card information as they input it into payment forms on e-commerce sites every few minutes. The best way to avoid being victimized by Magecart is to avoid entering any payment information into any website. Instead, use third-party payment platforms like Amazon Pay and PayPal that have your credit card details already saved.

However, only about 50% of respondents feel that these third-party digital payment platforms are "safe," while 31% believe credit and debit card payment systems to be similarly safe. The fact that nearly 64% of respondents are not aware of this Magecart digital credit card skimming threat hints at a lack of consumer awareness of threats to their digital data.

There's still time for consumers to become more educated on how their data could be compromised this holiday shopping season and to take protective measures towards their data.

Holiday Shopping Threat Information and Tips for Consumers

How to Shop Safely This Holiday Season

Avoiding data breaches on Black Friday and Cyber Week can't be guaranteed, but there are steps you can take to decrease your risk of becoming a victim dramatically.

This holiday shopping season, online shoppers should:

Avoid downloading apps with ambiguous origins

It does not matter if a retail app promises you extraordinary savings. If you aren't sure of who is behind an app or the platform hosting the app, do not download the app.

72% of respondents to our 2019 survey said they would download a shopping-related app if it offered a steep discount. This leaves an easy way for hackers to siphon your data, as all they have to do is offer a discount to lure a customer in.

Stick with the Google Play and Apple App stores to be safe, and avoid app developers without an available track record or who use free email services.

Take reviews with a grain of salt.

Reviews are only so valuable when you're trying to determine whether an app or website is legitimate. Reviews can be fake, paid for, and downright deceptive. If hackers want your data badly enough, then populating the web or app stores with phony reviews may be the least of what they are willing to do to deceive you.

In our 2019 survey, 58% of consumers said they do not check who the developer is before downloading an app. Don't let this be you.

Again, ensure that an app developer or website has a strong reputation before downloading or visiting a domain—your data could be at stake.

Be alert to deceptive domains.

Hackers will engage in domain infringement, including but not limited to deceptively-spelled look-alikes or using a ".org" when the real site uses ".com" to con you into providing your sensitive information. They may use this tactic in combination with other hacker go-to's like spear-phishing email campaigns.

A query of the branded terms of twenty Fortune 100 companies in RiskIQ's domain infringement detection service once revealed 37,000 probable instances of domain infringement over two weeks, or 1,850 incidents per brand.

Be skeptical, and ensure that the site or app you use to shop this holiday shopping season is legitimate, rather than a carefully-disguised data-mining trap.

Avoid manually entering payment details.

This holiday shopping season, consumers should avoid entering their credit card information online unless they are sure that it is the only way to pay for their holiday goodies.

Magecart skimmers and similar hacker code deploy various means for identifying and stealing manually-entered credit card information. Rather than entering your card details, pay for your goods using more secure platforms like PayPal, or use a card that you have already saved to a retail platform or app.

RiskIQ has found that the average length of a Magecart breach is 22 days. If you are to purchase on a compromised site during such a period of the breach, you will likely become a victim of credit card theft.

Shoppers are under siege every Black Friday and Cyber Week, and they have a choice of whether to comply willingly with what hackers want or to put up a fight in the name of data and identity security.

In Conclusion

There is only so much that a consumer can do on their own to protect their data. Keeping an eye on their credit card activity, being uber-cautious about site visits and app downloads, and using the most secure payment methods available are among consumers' options for sheltering their data this holiday shopping season.

With shoppers having little option but to rely heavily on e-commerce this holiday season, we at RiskIQ wanted to lend a helping hand. That's why we're introducing the Holiday Shopping Microsite, a tool for both web hosts and shoppers to better protect themselves and others from data breaches this holiday season (and beyond).

The RiskIQ Holiday Shopping Microsite:

- Allows users to report suspicious URLs
- Keeps a record of new hosts and domains related to holiday shopping so security teams can track and investigate them as they are stood up.
- Serves as an extension of the work, including threat detection, that RiskIQ does to protect consumers and developers from the ever-present threat of cybercriminals

Our goal with the Microsite is to help the security community work together to respond to the influx of criminal activity. The Holiday Shopping Microsite will be a powerful resource for keeping organizations safe during the holiday season.

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

✉ sales@riskiq.net
☎ 1 888.415.4447

Learn more at riskiq.com