

Threat Landscape: Black Friday & Cyber Monday 2022

B-2022-11-11a

TLP: CLEAR

November 2022



2022 Black Friday and Cyber Monday Threat Context

Black Friday and Cyber Monday (BFCM) are two of the busiest shopping days on the retail calendar and a prime period for malicious actors to target consumers. Black Friday is the name given to the Friday after Thanksgiving in the United States and has traditionally marked the start of the holiday shopping season. It is one of the busiest days of the year for retailers and consumers, with extensively promoted sales and discounted prices both online and in-store. In 2022, Black Friday falls on November 25, though promotions and discounts begin up to a month in advance. Cyber Monday refers to the Monday following Black Friday and falls on November 28 this year. Sales forecasts indicate that BFCM 2022 is anticipated to be larger in sales than previous years despite strained economic and geopolitical circumstances.[1]

Threat actors using BFCM to target retailers and consumers in recent years have had a variety of motivations, including financial gain, political persuasion, and activism. Attacks occur in both the physical and cyber domains. BFCM represents an opportunity for cyber threat actors to hide amongst the excitement about and rapid increase in retail activity, leveraging the urgency and enthusiasm generated by the holiday sales to defraud victims. Both retailers and consumers are attractive targets. Malicious cyber activity during recent BFCMs highlighted the efficacy of leveraging human error to scam customers. Retailers face a host of potential business threats, including impersonations, distributed denial of service attacks (DDoS), and e-commerce skimming malware.

Key Findings

- Sales forecasts indicate that Black Friday and Cyber Monday 2022 are anticipated to be larger in sales than previous years.
- ZeroFox Intelligence assesses that social engineering will almost certainly remain one of the most prolific ways financially-motivated threat actors target shoppers.
- We expect an increase in SMS-based phishing scams and callback phishing throughout the Black Friday and Cyber Monday 2022 timeframe.
- We anticipate malicious actors will leverage fraudulent domains during BFCM 2022 to: dupe unsuspecting victims into purchasing fake items, harvest financial information, or deploy malware.
- Threat actors will most likely advertise fake or misleading discounts or prizes in social media posts that contain links to malicious websites.
- Consumers should be particularly wary of being contacted about BFCM 2022 sales via unsolicited direct messages.
- ZeroFox Intelligence has not identified threat actors or groups planning to target retail locations on Black Friday.
- Recent acts of vandalism against retail locations – carried out by activists – highlight a tactic to consider for proactive prevention of would-be Black Friday demonstrations.

Stats for BFCM

Nearly **180 million**
U.S. shoppers in **2021** from
Thanksgiving to Cyber
Monday [2]

2021 sales of **USD 8.9bn**
on Black Friday and **USD**
10.7bn on Cyber Monday
[3]

30 percent
U.S. consumers targeted by
scammers [4]

Anticipated 2022 sales of
USD 9bn on Black Friday
and **USD 11.2bn** on Cyber
Monday [5]

Who is targeting BFCM?



Financially-motivated
threat actors



Competitors



Politically-motivated
threat actors



Insider threats



Foreign governments /
Nation states



Activists

FOOTNOTES

- [1] [hXXps://news\[.\]adobe\[.\]com/news/news-details/2022/Adobe-Forecasts-209.7-Billion-Holiday-Season-Online-U.S.-Cyber-Monday-to-Top-11-Billion/default.aspx](https://news.adobe.com/news/news-details/2022/Adobe-Forecasts-209.7-Billion-Holiday-Season-Online-U.S.-Cyber-Monday-to-Top-11-Billion/default.aspx)
- [2] [hXXps://nrf\[.\]com/media-center/press-releases/nearly-180-million-shop-over-thanksgiving-holiday-weekend](https://nrf[.]com/media-center/press-releases/nearly-180-million-shop-over-thanksgiving-holiday-weekend)
- [3] [hXXps://business.adobe\[.\]com/resources/holiday-shopping-report.html](https://business.adobe[.]com/resources/holiday-shopping-report.html)
- [4] [hXXps://www.tessian\[.\]com/resources/infographic-black-friday-scams/](https://www.tessian[.]com/resources/infographic-black-friday-scams/)
- [5] [hXXps://business.adobe\[.\]com/resources/holiday-shopping-report.html](https://business.adobe[.]com/resources/holiday-shopping-report.html)

SCOPE NOTE ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 5:00 PM (EST) on November 9, 2022; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

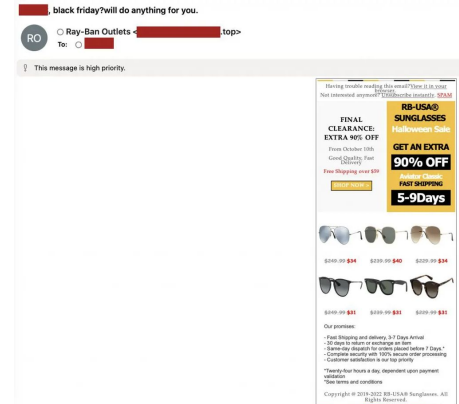


Social Engineering

Social engineering will almost certainly remain one of the most prolific ways financially-motivated threat actors will target shoppers during BFCM. Scams will very likely remain evolutionary rather than revolutionary, typically leveraging rudimentary email, text messages, and voice calling to entice victims to hand over sensitive information. While social engineering scams have become increasingly targeted throughout the year, campaigns during BFCM 2022 will very likely leverage “spray-and-pray” tactics, seeking to target a high volume of end users to capitalize on huge increases in online shopping. Campaigns to date have typically fallen into four key categories:

- **Non-delivery scams:** Nefarious actors either impersonate reputable retailers or establish a fake online retail presence. Consumers visit the fraudulent online store and purchase an item but do not receive a tracking number, and the package never arrives.
- **Order scams:** Threat actors email consumers to notify them of an issue with an alleged purchase of an item that was never ordered. Lures include telling victims that payment has failed to go through and must be re-entered. The email contains a malicious link to a site where victims are encouraged to enter personal or financial information.
- **Delivery scams:** Threat actors impersonate delivery companies and email or text consumers stating that there is an issue with delivery that must be rectified by clicking a link. This link is malicious and often asks consumers to enter personal or financial information. The message lure is often intentionally vague, failing to specify product details or purchase method.
- **Gift card scams:** These scams typically takes two forms. The first involves threat actors notifying victims that goods must be purchased using a gift card instead of a debit or credit card. Gift card purchases cannot be tracked, which makes it impossible to retrieve stolen funds. Threat actors may also pose as gift card generators, exploiting victims seeking discounts or purchasing gifts for others and instead installing malware on a user’s device.

ZeroFox Intelligence anticipates an increase in SMS-based phishing scams over BFCM 2022. Threat actors have been observed increasingly targeting end users with smishing attacks, including retail employees either directly or via enterprise third-party providers, and customers.[6] Threat actors are also expected to increasingly leverage callback phishing (vishing) to target customers. Scams of this nature will most likely involve threat actors adding legitimacy to malicious emails by impersonating customer support teams of banks, payment processors, and retailers and encouraging victims to return a phone call to authenticate fraudulent activity.[7]



Black Friday 2022 Ray-Ban Phishing Email

Source:
[hXXps://news.trendmicro\[.\]com/2022/11/02/black-friday-shopping-scams-2022-ray-ban-nike/](https://news.trendmicro.com/2022/11/02/black-friday-shopping-scams-2022-ray-ban-nike/)

Domains

ZeroFox Intelligence anticipates a high threat from threat actors leveraging fraudulent domains during BFCM 2022 to dupe unsuspecting victims into purchasing fake items, to harvest financial information, or to deploy malware. Scams of this nature in previous years have been highly effective, causing considerable harm not only to customers but also to retailers’ brand reputation.

Threat actors will set up convincing, fraudulent iterations of popular retailers’ websites, often creating a near-replica that advertises holiday season discounts to entice engagement. Often pictures, text, and formatting will be stolen directly from the legitimate site. Users may be phished with emails or text messages asking them to log in and update their payment details, which are then harvested by threat actors. Alternatively, when end users make a purchase on the site, threat actors steal the money and payment information.

Threat actors leverage a variety of methods to increase traffic to fraudulent domains. Often fraudulent sites are set up at addresses based on common misspellings and typos, sometimes differing from popular retailers’ legitimate domains by a single letter. Threat actors may also leverage search engine optimization (SEO) poisoning, a tactic used to create a malicious website using keywords that increase the site’s rankings and display it as one of the first search results.[8] Threat actors may also seek to increase footfall by leveraging open redirects or by promoting fraudulent websites through fake social media accounts.

Impersonating phishing domains and open redirects should be continually monitored by retailers and taken down to avoid customers being defrauded, as they provide an intrusion vector for threat actors. Customers should take care to ensure they are browsing the website of a legitimate and trusted source, paying special attention to misspelled domains, and should never visit a retailer’s site by clicking a link in an email, text, or via social media.

FOOTNOTES

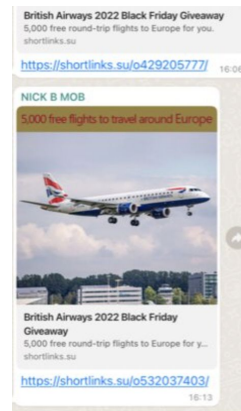
- [6] [hXXps://www.securityweek\[.\]com/twilio-cloudflare-attacked-part-campaign-hit-over-130-organizations](https://www.securityweek.com/twilio-cloudflare-attacked-part-campaign-hit-over-130-organizations)
[7] [hXXps://threatpost\[.\]com/callback-phishing-security-firms/180182/](https://threatpost.com/callback-phishing-security-firms/180182/)
[8] [hXXps://www.techtarget\[.\]com/whatis/definition/search-poisoning](https://www.techtarget.com/whatis/definition/search-poisoning)



Case Study: Fake Airline Black Friday 2022 Scam

Multiple sources have reported fake 2022 Black Friday giveaway promotions circulating on WhatsApp and social media. Specific to the travel industry, scams of a similar nature have been identified targeting British Airways and Lufthansa, and it is likely other airlines are subject to similar ongoing impersonation scams.[9] Reporting states that fraudulent links are spread via contact lists, as “winners” are obligated to circulate the offer to 20 friends to validate their prizes. Users are typically required to transfer a payment to receive their alleged prize.

Even scams such as these that lack sophistication can cause reputational damage and convince unsuspecting end-users to click on malicious links—and potentially transfer funds.



British Airways 2022 Black Friday Giveaway Scam

Source:
[hXXps://www.headforpoints.com/2022/11/09/a-british-airways-black-friday-whatsapp-scam-giveaway-goes-viral/](https://www.headforpoints.com/2022/11/09/a-british-airways-black-friday-whatsapp-scam-giveaway-goes-viral/)

Social Media

Threat actors are highly likely to leverage social media platforms like Facebook, Instagram, Twitter, and YouTube to conduct scams throughout BFCM 2022. Threat actors are expected to take advantage of social media excitement and holiday pressure to secure discounted products and services to spread disinformation and defraud end users. Retailers should also monitor for BFCM 2022 scams that leverage their brand due to the reputational damage and dissuasion from making legitimate purchases that these scams can cause.

Threat actors are most likely to advertise discounts or prizes in posts that contain links to malicious websites. Upon engagement, sensitive user data is harvested, payment information is stolen, and malware can be downloaded onto victims’ devices. Alternatively, links may redirect users to fake e-commerce sites that sell counterfeit goods at “too-good-to-be-true” prices. Historically, scams have typically involved threat actors impersonating the accounts of major retailers, leveraging similar profile names and brand imagery to increase authenticity. Threat actors have also leveraged hijacked accounts—including those of high-profile or influential individuals—to promulgate their campaigns and hijacked hashtags of trending topics to increase reach and traffic to scam websites. Consumers should be particularly wary of being contacted about BFCM 2022 sales via unsolicited direct messages.

Consumers should avoid clicking any links shared in direct messages regarding Black Friday sales and instead access the verified source directly. They should also ensure engagement with BFCM 2022 promotions is only through social media accounts with a blue checkmark, paying close attention to typos and accounts with little other content or followers.

Physical

Black Friday and the crowds this event draws to brick-and-mortar shopping centers have provided an attractive platform for activists seeking to highlight various causes. The day’s associations with “consumerism,” a term often used by activists to describe preoccupation with acquiring what they define as non-essential goods at the expense of the environment or vulnerable populations, provide a thematically-relevant backdrop for actions intended to disrupt “business as usual.”[10,11,12] Chicago’s “Magnificent Mile” shopping district has been one of the more visible Black Friday targets in recent years. In 2014, activists who were protesting a police-involved shooting demonstrated with signs and staged a “die-in” at the district’s Water Tower building.[13] In 2015, activists decrying the police-involved shooting of Laquan MacDonald in Chicago took their protests further, locking arms and blocking entrances to stores in the district.[14] The protest was repeated on Black Friday in 2016 and 2017, though participation and the aggressiveness of protesters diminished each of those years.[15,16]

In 2019, activists staged a Black Friday demonstration at the Water Tower, this time calling for strong measures to address climate change. They were joined that day by climate activists at some 3,000 locations worldwide, including shopping centers.[17] In Chicago and most other locations, activists demonstrating in and outside stores did not prevent shoppers from entering or freely circulating within them.[18] In at least eight major cities in France, however, demonstrators associated with activist organizations blocked entrances to stores for hours at a time. In the city of Strasbourg in eastern France, activists reportedly covered store display windows with posters bearing slogans, affixing them with strong glue.[19]

As of this writing, ZeroFox has not identified any protest actions specifically targeting retail locations on Black Friday. A digital document and video circulating under the name of the hacktivist group Anonymous, however, have called for an unspecified action in Canadian cities on Black Friday to protest the governance of Conservative party leaders. The document and video state that an update with additional information will be provided 24 hours prior to November 25.[20,21]

Recent acts of vandalism carried out by activists against retail locations point to a potential tactic that could be used in a Black Friday demonstration. Over the last five days of October, three groups of activists used fire extinguishers to spray bright orange paint on Rolex and luxury car dealers’ store windows (buildings housing government and media offices were also targeted by one of the groups).[22] Video of the defacings—carried out to oppose spending on luxury items while others suffer from poverty or climate-induced hardships—suggests they took place in the daytime during off-peak hours.[23,24] The heavy foot traffic anticipated at retail locations on Black Friday would make these actions, which involved walking rapidly along targeted windows while avoiding pedestrians, difficult to execute that day.

FOOTNOTES

- [9] [hXXps://www.minimikama.at/lufthansa-fake-gewinnspiel-whatsapp/](https://www.minimikama.at/lufthansa-fake-gewinnspiel-whatsapp/)
- [10] [hXXps://www.twitter.com/search?q=%22Just%20stop%20oil%22%20OR%20%22juststopoil%22%20AND%20consumerism&src=typed_query&f=top](https://www.twitter.com/search?q=%22Just%20stop%20oil%22%20OR%20%22juststopoil%22%20AND%20consumerism&src=typed_query&f=top)
- [11] [hXXps://www.twitter.com/search?&f=top&q=%22black%20lives%20matter%22%20OR%20blacklivesmatter%22%20AND%20consumerism%20%23blacklivesmatter&src=typed_query](https://www.twitter.com/search?&f=top&q=%22black%20lives%20matter%22%20OR%20blacklivesmatter%22%20AND%20consumerism%20%23blacklivesmatter&src=typed_query)
- [12] [hXXps://www.twitter.com/Tropaphobe/status/1200461066662240256](https://www.twitter.com/Tropaphobe/status/1200461066662240256)
- [13] [hXXps://www.cbsnews.com/chicago/news/ferguson-protesters-take-over-water-tower-plaza-urge-black-friday-boycott/](https://www.cbsnews.com/chicago/news/ferguson-protesters-take-over-water-tower-plaza-urge-black-friday-boycott/)
- [14] [hXXps://www.chicagotribune.com/business/ct-black-friday-michigan-ave-shops-1128-biz-20151127-story.html](https://www.chicagotribune.com/business/ct-black-friday-michigan-ave-shops-1128-biz-20151127-story.html)
- [15] [hXXps://abc7chicago.com/black-friday-protests-chicago-protest-police-mile-1625115/](https://abc7chicago.com/black-friday-protests-chicago-protest-police-mile-1625115/)
- [16] [hXXps://abc7chicago.com/black-friday-chicago-protest-mag-mile-2690332/](https://abc7chicago.com/black-friday-chicago-protest-mag-mile-2690332/)

- [17] [hXXps://www.usatoday.com/story/news/nation/2019/11/29/black-friday-climate-strikes-protest-consumerism/4330799002/](https://www.usatoday.com/story/news/nation/2019/11/29/black-friday-climate-strikes-protest-consumerism/4330799002/)
- [18] [hXXps://columbiachronicle.com/climate-activists-remind-black-friday-shoppers-of-the-environmental-crisis](https://columbiachronicle.com/climate-activists-remind-black-friday-shoppers-of-the-environmental-crisis)
- [19] [hXXps://www.lefigaro.fr/flash-eco/black-friday-des-militants-ecolos-bloquent-un-entrepot-d-amazon-pres-de-paris-20191128](https://www.lefigaro.fr/flash-eco/black-friday-des-militants-ecolos-bloquent-un-entrepot-d-amazon-pres-de-paris-20191128)
- [20] [hXXps://www.twitter.com/YourAnonNews/status/1123383855044538371](https://www.twitter.com/YourAnonNews/status/1123383855044538371)
- [21] [hXXps://www.youtube.com/watch?v=fg4XP8S0g](https://www.youtube.com/watch?v=fg4XP8S0g)
- [22] [hXXps://www.twitter.com/JustStop_Oil/status/1587009502443978753](https://www.twitter.com/JustStop_Oil/status/1587009502443978753)
- [23] [hXXps://www.twitter.com/JustStop_Oil/status/1585909798905724829](https://www.twitter.com/JustStop_Oil/status/1585909798905724829)
- [24] [hXXps://www.twitter.com/JustStop_Oil/status/1585178038777454592](https://www.twitter.com/JustStop_Oil/status/1585178038777454592)



Recommendations for Retailers

- Utilize the ZeroFox Platform to monitor social media for malware or phishing posts using your hashtags, images, or messaging.
- Protect customers by over-communicating with them about your official sources for deals and discounts this holiday shopping season.
- Utilize the ZeroFox Platform to search for and identify impersonator accounts on social media, and utilize the ZeroFox Disruptions team to work with the social networks to take down fraudulent accounts.
- Configure ongoing domain monitoring in the ZeroFox platform in order to proactively identify infringing domains that could cause reputational harm to your organization and your customers, and utilize ZeroFox Disruption services to take down the infringing content.

Recommendations for Consumers

- Be wary of pop-ups, redirects, or anything that looks like it could be a fraudulent page.
- Avoid clicking on anything sent via social media or email—go to sites directly to verify coupons promotions.
- Hover over links before clicking; watch for misspellings and inauthentic handles or email addresses.
- Always double-check reviews of shopping websites.
- Pay attention to the age of the company and its social media accounts, and be suspicious of unbelievable-sounding discounts.
- Unique payment methods (such as only being able to pay via PayPal) should be a red flag.
- Never click on links or buttons from unknown or untrusted sources.

APPENDIX: Traffic Light Protocol for Information Dissemination

TLP: RED

HOW IT IS USED

Sources may use **TLP: RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW IT IS SHARED

Recipients may NOT share **TLP: RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP: AMBER

HOW IT IS USED

Sources may use **TLP: AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW IT IS SHARED

Recipients may ONLY share **TLP: AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that
TLP: AMBER+STRICT restricts sharing to the organization only.

TLP: GREEN

HOW IT IS USED

Sources may use **TLP: GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW IT IS SHARED

Recipients may share **TLP: GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.

TLP: CLEAR

HOW IT IS USED

Sources may use **TLP: CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW IT IS SHARED

Recipients may share **TLP: CLEAR** information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox provides enterprises protection, intelligence, and disruption to dismantle external threats to brands, people, assets, and data across the public attack surface in one comprehensive platform. With complete global coverage across the surface, deep, and dark web and an Intel-backed artificial intelligence-based analysis engine, the ZeroFox Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, ransomware, brand hijacking, executive and location threats, and more. The patented ZeroFox Platform technology processes and protects millions of posts, messages, and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email, and more.

Ready to See for Yourself?

> Request a Demo:

Sign up on zerofox.com/request-a-demo

> Learn More:

Visit zerofox.com

Contact us at sales@zerofox.com / 855.736.1400

