An Early Start to Black Friday

Doppel

Fake Black Friday and Cyber Monday deals rarely name either day, mostly wear somebody else's brand, and this year were live by September.

Doppel Threat Intelligence Brief

Published: 16NOV2026

01 EXECUTIVE SUMMARY

The fake Black Friday deal that reaches a shopper this year will probably not say Black Friday, will not sit on a lookalike domain, and will not pretend to be a store. It will be a post in a Facebook group or a page on Google Sites, carrying a retailer's sale language on behalf of a software, payment, travel, or crypto brand, and asking for a login. Doppel detected the first Black Friday-named lookalike page of the season on 01SEP2026, a month or more ahead of last year's ramp.

A shopper who checks the address for the brand's name, the one habit most people have, passes most of this season's confirmed fake pages. An analyst who opens one from an office desk may see a different page than the target does, because a lot of them cloak by location, device, or language, and some had already been taken down once and come back. A security leader at a brand that never runs a sale now has a Black Friday problem, because the lure does not care whether the brand sells anything.

Half of confirmed social-media impersonation is posts inside Facebook groups, almost every confirmed fraudulent ad is a Facebook ad, a quarter of confirmed lookalike pages sit on borrowed platforms, and more than a third exist to take a login. Among protected brands, travel, consumer-internet, and retail are rising into October while every other sector falls, and this year the travel deal has become a Black Friday deal.

SEASONAL EXPOSURE
ELEVATED

The season is already open, and the usual checks do not catch what is running

A brand does not need a storefront to be the face of a holiday scam, an address without the brand's name is not a safe address, and a page cleared from an office desk may not be the page a customer sees.

Half SOCIAL IMPERSONATION IN FACEBOOK GROUPS	**1 in 4** LOOKALIKES ON BORROWED PLATFORMS
1 in 3 LOOKALIKES BUILT TO TAKE A LOGIN	**01SEP2026** FIRST BLACK FRIDAY HOST

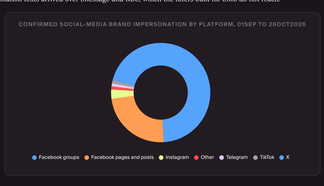
02 WHERE IT RUNS

Half of confirmed social-media brand impersonation this holiday season, 01SEP2026 to date, is posts inside Facebook groups. Facebook as a whole carries three quarters, X a fifth, and Instagram, Telegram, TikTok, and Threads a few percent between them. Buy-and-sell and bargain groups are where shoppers go looking for a deal, a post there carries the group's implied vetting, and the platform's recommendations put it in front of people who did not go looking. Confirmed fraudulent advertising is almost entirely Facebook Ads, at 99.7%.

A fake or impersonation page often has no domain of its own. About one in four confirmed lookalike pages lives on a legitimate hosting, publishing, or document platform, with Google Sites, Blogger, SlideShare, Scribd, Cloudflare Pages, and GitHub Pages the most used. Where there is a registered domain, the brand's name is usually not in it. The brand appears in the page's logo and copy while the address is a generic word, a deal or outlet term, or nothing recognizable.

Off the web the pattern holds. Roughly one in eight confirmed fake or modified apps was found in an official app store, and third-party APK sites alone account for more than the Apple App Store. A quarter of confirmed brand-impersonation texts arrived over iMessage and RCS, which the filters built for SMS do not reach.

CONFIRMED SOCIAL-MEDIA BRAND IMPERSONATION BY PLATFORM, 01SEP TO 28OCT2026



03 WHAT IT ASKS FOR

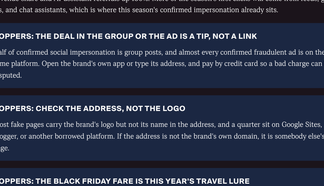
More than a third of confirmed lookalike sites this season are built to take a login to an account the visitor already holds. The rest are counterfeit storefronts, fake support, giveaways, and scam offers, and the sale lure cuts across all of them.

About a third of confirmed lookalike sites cloak, serving a different page depending on the visitor's location, device, browser, or language, so a scanner, a reviewer, or a brand's own staff can see something harmless while a shopper in the target market sees the lure. Doppel has documented kits that detect analysis tools and send them to a blank page, and a holiday sale scam that served its checkout only to phones.

The words that carry the season's lures are the ordinary language of a sale, meaning *sale*, *deal*, *discount*, *promo*, *coupon*, and *outlet*, and confirmed lookalikes built on those words span several dozen protected brands each holiday season.

The brands they imitated were mostly not stores. In 2025 the largest targets were airlines, through discount and deal pages, followed by crypto exchanges and neobanks. In 2026 the lead has moved to business software, through deal and sale pages, with travel, crypto, retail, and payment brands behind it. Retailers accounted for under a tenth of confirmed sale-themed lookalikes in 2025 and about a tenth so far in 2026. A holiday discount is a credible pretext for any brand a shopper has an account with.

SHARE OF CONFIRMED SALE-THEMED LOOKALIKES BY THE SECTOR OF THE BRAND IMITATED



04 WHAT IS DIFFERENT IN 2026

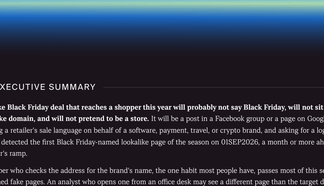
Doppel detected and confirmed the first lookalike host carrying Black Friday or Cyber Monday in its address on 01SEP2026; in 2025 the first came over a month later. Public reporting dated the start of the 2025 ramp to October. Cyber Monday, the larger online shopping day, has not appeared in the address of any confirmed lookalike against a protected brand in three holiday seasons. When actors name the holiday, they name Black Friday.

The travel deal has become a Black Friday deal. Travel brands were already the largest single target of discount and deal lookalikes during the 2025 holiday season, with no holiday named on the page. This year most of the Black Friday-named hosts confirmed between 01SEP2026 and 15OCT2026 posed as travel fare or booking pages, and no travel page carrying Black Friday in its address was confirmed in either prior season. Travel is a high-value purchase made quickly when a fare looks scarce, which is the condition a fake sale page is built for, and the holiday supplies the scarcity.

Travel, consumer-internet, and retail are the only sectors where more protected brands saw rising lookalike-domain activity into October than falling; fintech, technology, crypto, and media are majority-falling.

Within last holiday season the picture was flat. Confirmed impersonation of protected brands held within 5% of its October level through November and December 2025 while the open-internet wave of new fake shops peaked around it.

BRANDS WITH RISING VS FALLING LOOKALIKE-DOMAIN ACTIVITY INTO OCTOBER 2026, BY SECTOR



05 WHAT TO WATCH THIS SEASON

Black Friday falls on 27NOV2026 and Cyber Monday on 30NOV2026. Adobe forecasts $12.9 billion and $15.1 billion in U.S. online sales on those two days inside a $275.1 billion season, with social and affiliate channels gaining the most revenue share and AI-assistant referrals up 130%. More of the season's first clicks will come from feeds, groups, creators, and chat assistants, which is where this season's confirmed impersonation already sits.

SHOPPERS: THE DEAL IN THE GROUP OR THE AD IS A TIP, NOT A LINK

Half of confirmed social impersonation is group posts, and almost every confirmed fraudulent ad is on the same platform. Open the brand's own app or type its address, and pay by credit card so a bad charge can be disputed.

SHOPPERS: CHECK THE ADDRESS, NOT THE LOGO

Most fake pages carry the brand's logo but not its name in the address. and a quarter sit on Google Sites, Blogger, or another borrowed platform. If the address is not the brand's own domain, it is somebody else's page.

SHOPPERS: THE BLACK FRIDAY FARE IS THIS YEAR'S TRAVEL LURE

Fake fare pages take the card and the passenger details a booking needs, under the time pressure a sale fare creates. Book with the carrier directly, and treat a fare found through a search result, feed, or assistant as a prompt to check the carrier's own site.

SHOPPERS: GET THE APP FROM THE STORE, AND CHECK THE TEXT IN THE APP

Most confirmed fake apps were found outside the official stores, and a quarter of impersonation texts came through iMessage or RCS. Install retail and payment apps only by searching inside the store, and check any text about an order, delivery, or account in the app, never through the link.

A BRAND THAT NEVER RUNS A SALE STILL GETS A BLACK FRIDAY LURE

Software, payment, and crypto brands draw more confirmed sale-themed lookalikes than retailers, and their customers have no real offer to compare against. Shoppers should open the brand's own app and look for the offer there. Brands should say before November whether they run holiday promotions, where real ones appear, and where to report a suspicious one.

BUSINESSES: THE PAGE A REVIEWER SEES MAY NOT BE THE PAGE A CUSTOMER SEES

Confirmed lookalike sites routinely cloak by location, device, or language, and taken-down addresses come back. Verify reported pages from a device and location that match the targeted customers, and treat a returning address as the same incident.

BUSINESSES: THE SEASON IS ALREADY OPEN

Black Friday-named infrastructure was confirmed on 01SEP2026, and travel, consumer-internet, and retail brands are already rising. Brief fraud, support, and communications teams now, and confirm which official promotions, domains, and ad accounts are live so customer-facing teams can tell a real sale from a fake one.

Findings are based on Doppel telemetry across a global customer base, with strongest coverage in North America.

Doppel

Our mission is to protect the world from social engineering attacks every day. Our AI-native defense anticipates deception and eliminates threats.

1B+ INDICATORS ANALYZED DAILY **300+** TRUSTED CUSTOMERS doppel.com

Prepared by Doppel SECR - Social Engineering Counterintelligence & Research

© Doppel Inc. 2026. All Rights Reserved.