

ATLAS

GRAPHIKA REPORT

Holiday Hoaxes Unwrapped: Fake Trees, Freebies, & Shopping Sprees

Scammers Orchestrate
Cross-Internet Campaigns to
Deceive and Defraud Holiday
Shoppers of Their Money and
Personal Information

Léa Ronzaud, Jean le Roux

12.2024

Holiday Hoaxes Unwrapped: Fake Trees, Freebies, & Shopping Sprees

Scammers Orchestrate Cross-Internet Campaigns to Deceive and Defraud Holiday Shoppers of their Money and Personal Information

Overview

Online scams have surged in recent years, as our lives increasingly move online and scammers leverage new technologies in attempts to defraud greater numbers of people. Chief among them are shopping scams, which accounted for 42% of online scams reported worldwide in 2023, [according](#) to data insights firm Statista. In 2022, U.S. officials [said](#) online shopping scams cost over \$70 million during the holiday season alone.

Through our [ATLAS intelligence reporting](#), Graphika regularly detects, tracks, and helps disrupt a wide array of scams on multiple platforms. Working with industry partners at Meta, we are now joining a [campaign](#) to raise public awareness about online scams. This first report focuses on online shopping scams ahead of major holidays and e-commerce events in multiple countries.

Here we provide details of scams targeting shoppers and social media users during the November and December holiday season. Our findings are not exhaustive but rather a set of case studies illustrating how these types of scams attempt to engage, deceive, and defraud people of their money and sensitive personal information. We've selected the examples based on a combination of key attributes, including their relevance as online shopping scams, prevalence across internet platforms, and notable tactics, techniques, and procedures.

Key Findings

- Online shopping scams are global in nature, reflecting the increasing globalization of the e-commerce industry. Although Christmas and Black Friday are frequently used as a hook to engage targets, we saw users responding from all over the world. A campaign nominally targeting Europeans with fake Christmas tree sales, for instance, drew comments from users in the U.S. and Latin America, and a network promoting bogus gift card giveaways stretched from the U.K. to India.
- Scams span the entire internet, with scammers using different web surfaces at different stages of the [kill chain](#). Social media and other public platforms are typically among the channels where scammers first engage targets before directing them to private messaging

groups or websites, where they are less likely to be detected or disrupted, in order to collect payment details or personal information.

- Consumers who fell prey to the online shopping scams we identified typically failed to receive their goods, received goods not meeting expectations, or were deceived into disclosing their personal information. When scammers managed to obtain personal information, they very likely used it for further targeting.
- The most frequent hook in the online shopping scams we observed was financial pressure and the opportunity to secure a discount or win a prize. Scammers enticed targets with bargain-priced festive decorations and Christmas trees, and fake giveaways of iPhones, Teslas, gift cards, and coupons.

Case Studies

Inauthentic Accounts Use Fake Christmas Giveaways as Lures for Personal Information

A network of more than 100 inauthentic accounts on Facebook, Threads, X, and online discussion forums, such as Quora, has targeted French-, Spanish-, and English-speaking users with false promises of gifts and prizes ahead of the holiday season, as part of an effort to obtain people's personal information. The multiple indicators of inauthentic activity included using stolen profile pictures of real people, AI-generated pictures of fake people, and impersonation of celebrities and social media influencers. Some of the social media accounts were labeled "newly created," indicating the actors regularly created new assets as part of the scam campaign, likely in response to ongoing detection and takedowns.

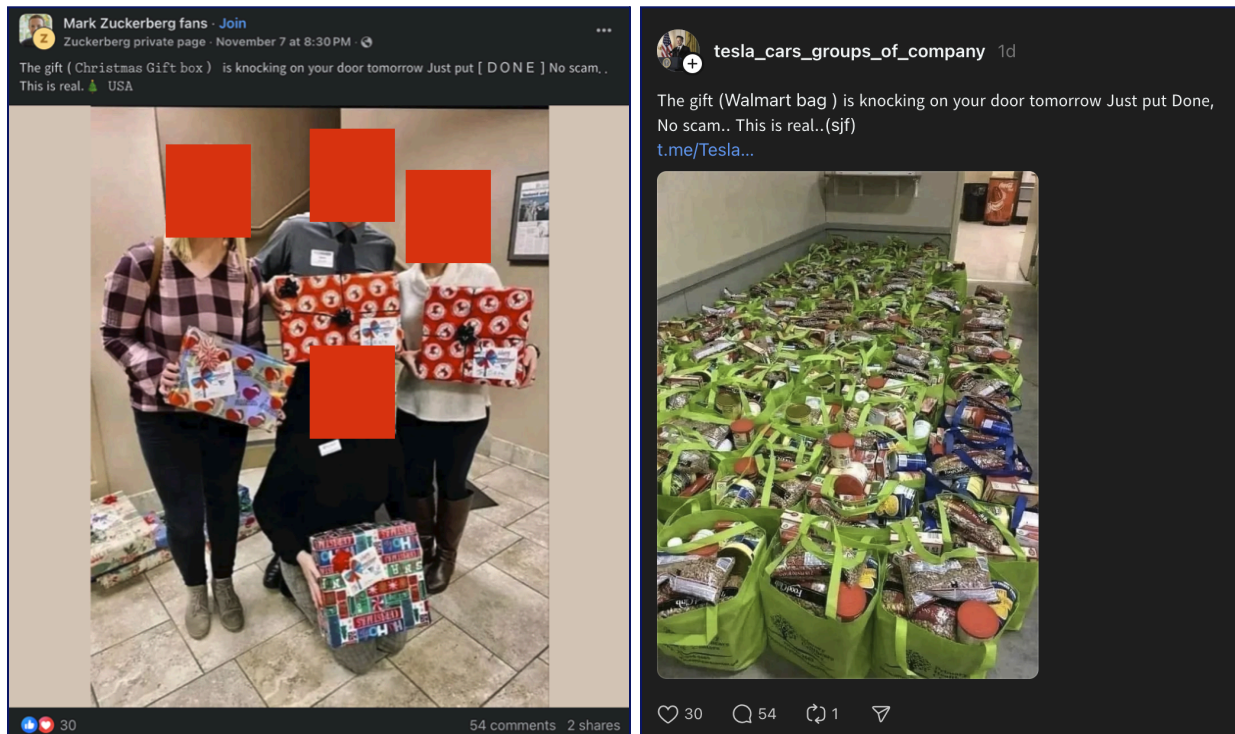
The fake free giveaways all used nearly identical language: "The gift (Christmas Gift box) [or other type of gift] is knocking on your door tomorrow. Just put 'done' No Scam. This is real." The posts included photos of the alleged prizes and promised users the chance to win, for example, a \$1,000 Amazon gift card; Walmart or KFC coupons; a free Tesla; or, in recent weeks, a Christmas gift box.

If a user commented on a post, the scammers asked them to contact the account operator via direct message, Telegram, or WhatsApp, or to visit a Google Sites web page. The Google Sites web page informed the user they had won a prize and provided a link to claim it. Users who clicked the link were then directed to one of a series of secondary web pages, whose URLs referenced "rewards" or "prizes". There, they were prompted to enter personal information, such as their email address, phone number, full name, and home address, as well as complete a questionnaire about their shopping habits, level of income, credit, and outstanding debts.

We observed this activity primarily on Facebook, Threads, X, and Quora, promoted as an effort to "help families" in the run-up to Christmas. On Facebook, the scammers also shared the fake gift

giveaways in groups, some of which presented as celebrity fan groups. Posts promoting the fake giveaways regularly attracted tens and sometimes hundreds of comments from users around the world; mostly authentic users engaging with the scam but also scammer-operated accounts commenting on their own posts – likely to drive engagement – and users calling out the activity as fraudulent.

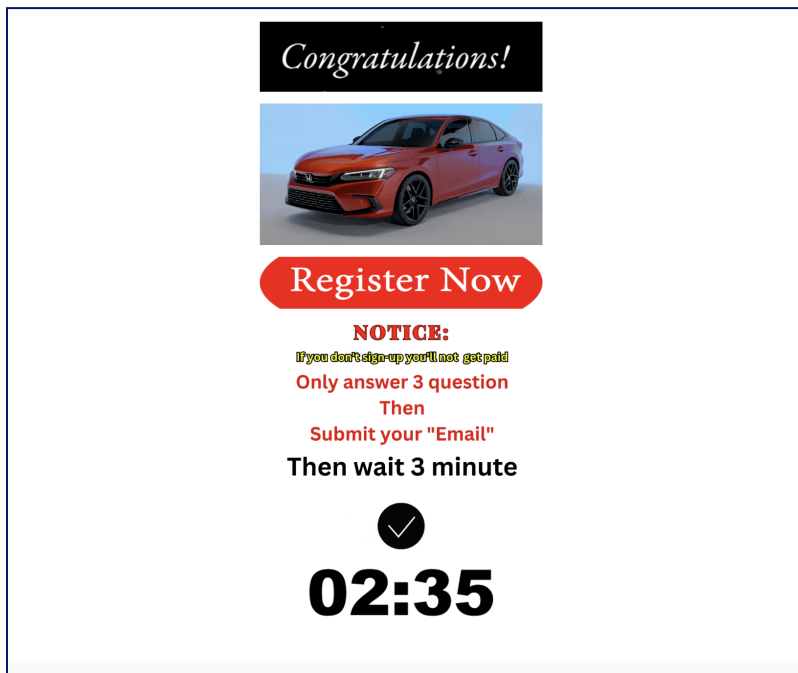
Based on open-source indicators, we could not establish the identity of the actors behind this activity, but we observed multiple inauthentic accounts listing locations in Thailand, Bangladesh, and the Philippines.



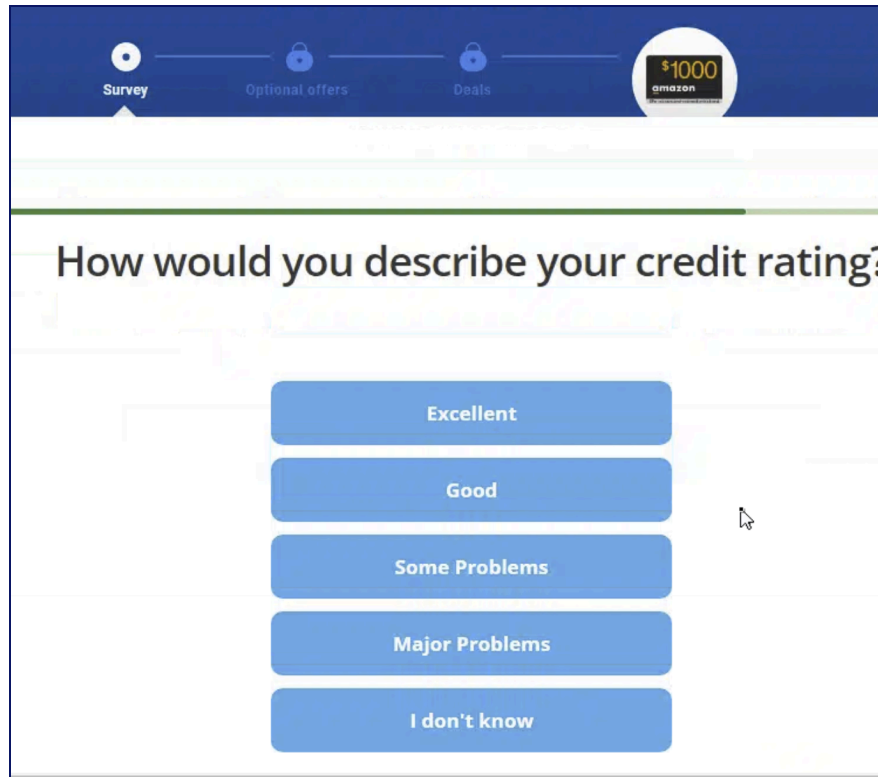
Example posts by scam operators on Facebook (left) and Threads (right) that purported to be fan pages for Meta CEO Mark Zuckerberg and Tesla cars, respectively, and asked users to comment "Done" to claim a "Christmas Gift box" or a "Walmart bag." Redactions added by Graphika.



If a user commented on a post, the scammers replied with instructions to contact the account operator via direct message, join a Telegram or WhatsApp group, or visit a Google Sites web page. Some users of Facebook and other platforms identified the activity as a scam in comments. Redactions added by Graphika.



A Google Sites web page instructing visitors to register to claim a prize. Some of the pages included a countdown timer, almost certainly to pressure targets into proceeding with the scam.



Users who clicked the link to claim their prize were redirected to one of a series of secondary websites that purported to be a survey. The survey asked for personal information and details of people's financial situation.

Scam Campaign Targets Europeans with Fake Christmas Tree Sales

At least 30 pages on Facebook and Pinterest presenting as online retailers have targeted English-, French-, Italian-, and German-speaking users with advertisements for fake sales of discount Christmas trees and holiday decorations. According to purchasers' posts on internet platforms and consumer review websites, the products never arrived.

The scammers promoted the fake products in ads and posts offering artificial Christmas trees and other decorations for less than €10 or as part of time-limited discounts. In recent weeks, some of these were framed as Black Friday offers. The posts typically featured video content copied from authentic users across the internet, showing heavily decorated Christmas trees. Some of the videos featured a likely AI-generated voice-over vouching for the quality of the product and warning of limited stock.

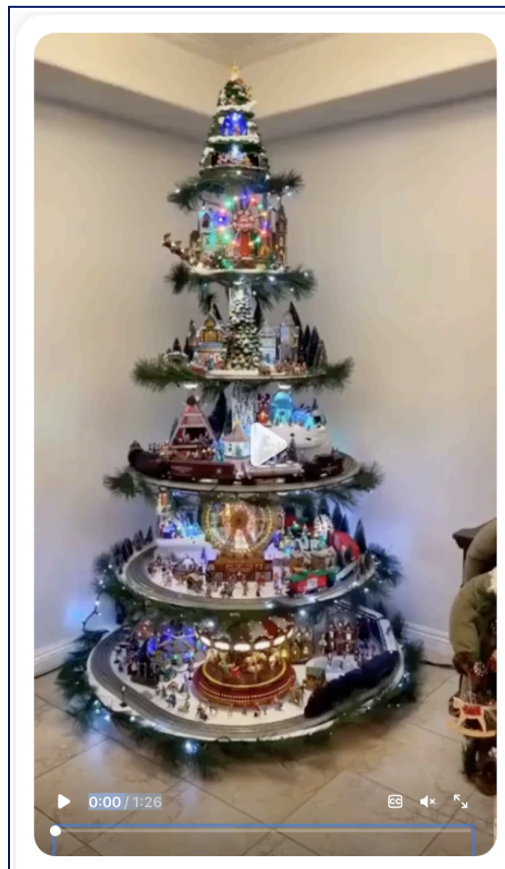
Users were then directed to a website to make a purchase. Some of these sites' legal notices indicated they were created using the [services](#) of e-commerce platform Shopify. Others showed indicators of not being legitimate online retailers, such as linking in their terms of service to an apparent shell company registered to a garage in the UK.

According to posts on consumer watchdog websites, such as Trustpilot and Signal-Arnaques, people from Europe, the U.S., and Latin America have fallen for scams using the content and behaviors described above, since at least 2022. Based on open-source indicators, we could not

establish the identity of the actors behind this activity. Facebook pages with administrator locations predominantly listed Italy and, to a lesser extent, Vietnam. Social media users who purchased the fake Christmas trees noted in comments that they were subsequently charged by businesses in Cyprus.




The scammers used paid advertisements to promote fake sales of Christmas trees and holiday decorations on Facebook and other platforms in Italian, French, German, and English.



The scammers also promoted fraudulent sales through social media posts on Pinterest and other platforms. These posts typically featured video footage of heavily decorated Christmas trees, sometimes with a likely AI-generated voice-over vouching for the quality of the product and warning of limited stock.

lillaprice™

Versandkostenfrei | Lieferung in 2-3 Werktagen



★★★★☆ 4.8 (9 Bewertungen)

Weihnachtsbaum - Première

€9.99 EUR

Steuer enthalten.

JETZT MIT RABATT BESTELLEN

Angebot gültig BIS MITTERNACHT!

Farbe


Gold Roségold Silber

Wähle eine Höhe: 120 cm

Geben Sie ihm mit Ihren Dekorationen und Lichtern eine persönliche Note und bewahren Sie ihn so auf, wie er ist. **Er wird auch im nächsten Jahr bereit sein.**

- Lieferung in 2-3 Werktagen aus Deutschland 🇩🇪
- Auf Lager, versandbereit
- SSL sichere Zahlung

MONNIE SHOP



Arbre de Noël - Première

★★★★☆ 4.8 (9 Commentaires)

€9,99 EUR

Taxes incluses.

COMMANDEZ MAINTENANT AVEC LA REMISE

Offre disponible JUSQU'À MINUIT !

Couleur

Or Or Rose Argent

Mesure

120 cm 150 cm 180 cm

210 cm 240 cm 270 cm

Donnez-lui une touche unique avec vos décorations, lumières et conservez-le tel quel. **Il sera prêt pour l'année prochaine également.**

Users were directed to a website, such as those pictured, from social media to make a purchase.



Nov 2, 2024

Fraud

Scam! On an online burraco site (burraco the challenge) as advertising appears this company that sells Christmas trees at eur 9.99 I thought it was a hoax but I riskedBuffalo is in fact! Never arrived order confirmation email and no way to track the purchase

Date of experience: October 26, 2024



Report #793695 on 30/09/2024 at 20:08



Christmas Tree - with Village

Offer available UNTIL MIDNIGHT !



i was thinking about buying a Christmas tree with village and in the end I paid a subscription to 9.95€ for fitgym (and their address is in Cyprus)

Experience date: 26 september 2024

Examples of posts on consumer watchdog websites Trustpilot (top) and Signal-Arnaques (bottom) from users in Italy and France explaining how they were defrauded by the scam.

Scammers Entice Holiday Shoppers with Fake Prizes and Personas

Scam campaigns on Facebook, Pinterest, and Telegram have attempted to trick users in the U.S., India, the U.K, and other countries into sharing their personal details ahead of the holiday season. The scams were based on an alleged chance to win coupons and gift cards for major online retailers, such as Amazon, Apple, Sony (PlayStation), and Walmart.

The scammers promoted fake offers using pages or accounts with names that referenced free gift cards. These assets typically shared images of the alleged prizes in groups or in comments on users' posts. If someone responded, the scammers then directed them to a website or private messaging channel, such as a WhatsApp or Telegram group, to enter an alleged prize draw.

Targets directed to a website were instructed to complete a "survey" that requested personal information, such as their gender, age, income, employment status, and level of interest in cryptocurrency. The survey websites often impersonated the interface of a social media platform, showing comments from fake users with AI-generated profile pictures who claimed to feel lucky to have won in previous draws despite thinking it was a scam. After completing the survey, a "prize offer" appeared based on the target's faked test score, with a link leading to web domains flagged by antivirus programs as containing malware.

In at least three instances, the terms and conditions pages on the sites hosting the survey stated that any personal information entered would be shared with "partners for their promotion and

marketing purposes.” Posts promoting the scam typically gained tens of comments and interactions, with some users calling the operators out as “scammers.”



Images posted to Pinterest by scammers claimed to offer the chance to win gift cards for major online retailers.



Targets were directed to a website to complete a “survey” (input their personal information) and enter the alleged prize draw. The websites often impersonated the interface of a social media platform, showing comments from fake users with AI-generated profile pictures who claimed to feel lucky to have won in previous draws despite thinking it was a scam.

Estimative Language Legend

Assessments of Likelihood

Graphika uses the following vocabulary to indicate the likelihood of a hypothesis proving correct. If we are unable to assess likelihood due to limited or non-existent information, we may use terms such as “suggest.”

Almost No Chance	Very Unlikely	Unlikely	Real Chance	Likely	Very Likely	Almost Certain(ly)
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Confidence Levels: Indicators of Sourcing and Corroboration

Graphika uses confidence levels to indicate the quality of information, sources, and corroboration underpinning our assessments.

Low Confidence	Medium Confidence	High Confidence
Assessment based on information from a non-trusted source and/or information we have not been able to independently corroborate.	Assessment based on information that we are unable to sufficiently corroborate and/or information open to multiple interpretations.	Assessment based on information from multiple trusted sources that we are able to fully corroborate.

Graphika

About Us

Graphika is the most trusted provider of actionable open-source intelligence to help organizations stay ahead of emerging online events and make decisions on how to navigate them. Led by prominent innovators and technologists in the field of online discourse analysis, Graphika supports global enterprises and public sector customers across trust & safety, cyber threat intelligence, and strategic communications spanning industries including intelligence, technology, media and entertainment, and global banking. Graphika continually integrates new and emerging technologies into our proprietary intelligence platform and analytic services, empowering our customers with high-precision intelligence and confidence to operate in a complex and continuously evolving information environment.

For more information or to request a demo, [visit](#) our website.

