Carefull

Your Guide to Safer Holidays: Spotting and Stopping Scams in 2025

The holidays are filled with family, celebration, shopping, travel, and charitable giving. Unfortunately, they're also the peak season for scammers, and experts expect this season to bring even more scam activity than years past.

Nearly 1 in 3 consumers fell victim to an online scam during the 2024 holiday stretch (2024 Consumer Cyber Safety Survey). This year, criminals are armed with smarter AI tools, more convincing messages, and new ways to take advantage of the busy, distracted moments that are part of the season.

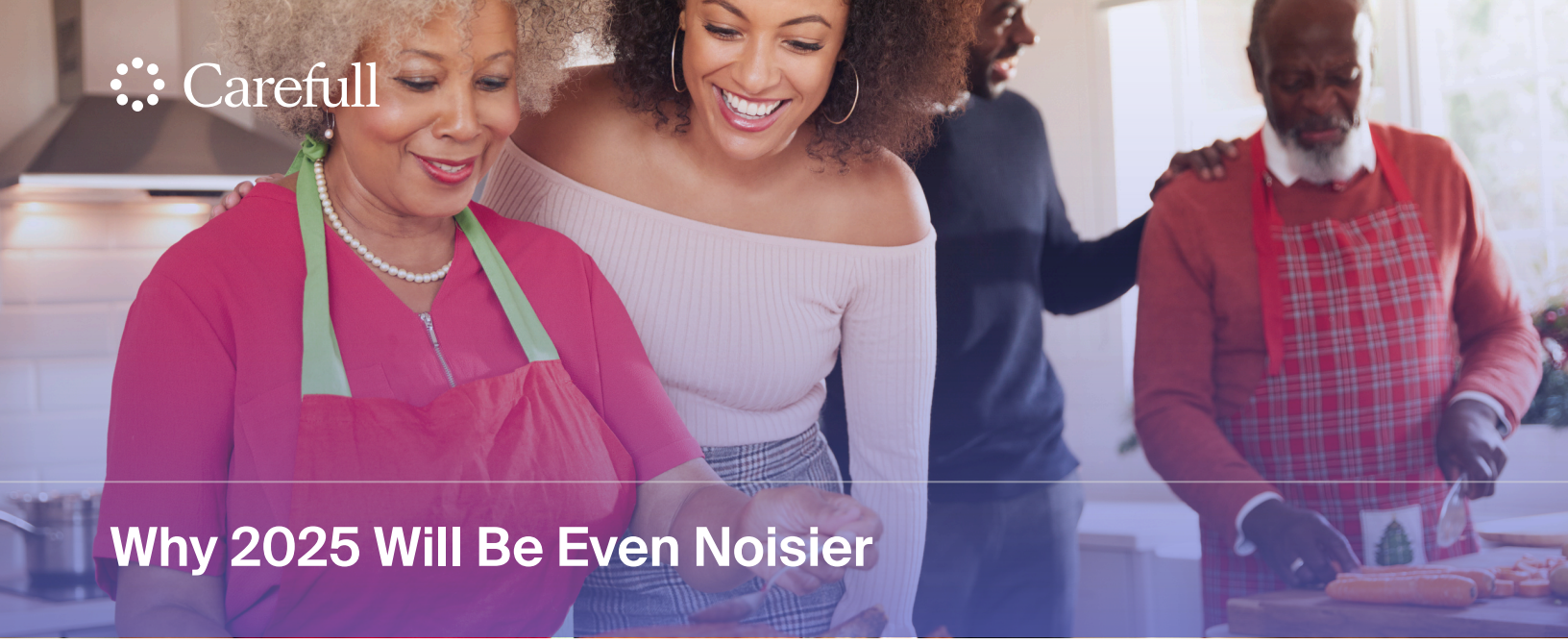
Why the Holidays Attract Scammers

In 2024, online fraud attempts spiked over Thanksgiving weekend, and winter travel season saw a 28% jump in fraud, outpacing summer levels (2024 Fraud & Travel Trends Report).

Higher prices. Earlier shopping. Greater risk.

More than 80% of holiday shoppers expect higher prices this year due to tariffs and inflation prompting many to shop earlier and react faster. Scammers are using that urgency to their advantage.

- **We move faster.** Holiday deals encourage quick decisions. 62% of Americans say they're likely to buy immediately when they see an online deal, and 35% admit they take more risks this time of year (2024 Holiday Shopping Behavior Survey). And, 34% of Americans say they'll chase more deals this year.
- **Our inboxes overflow.** Shipping notices, receipts, and donation messages make it easy for fake "delivery problem" or "exclusive offer" alerts to blend in.
- **Travel adds chaos.** With gate changes, hotel emails, and public Wi-Fi, winter travel fraud rose 28% last year and Thanksgiving day saw more attempted online fraud than any other day last year.
- **We give more generously.** In 2024, 55% of Americans donated to charity, yet 60% admit they don't always research organizations before giving.
- **Spending surges.** More purchases and donations mean more noise, and more chances for fake charges or refund requests to slip through. Holiday spending is expected to reach record highs: $215 billion on gifts and $325 billion on travel and experiences (NerdWallet, 2025).



Why 2025 Will Be Even Noisier

Key Trend	What it Means for Consumers
Tariffs, price shifts, and product availability	Scammers exploit real fluctuations in product availability, pricing, and shipping costs by sending fake “customs fee,” “import surcharge,” or “item on hold” messages. Because shoppers expect higher prices and possible delays, these fraudulent alerts blend in easily with legitimate retailer updates.
AI-powered impersonation	Fraudulent emails, texts, and even voice messages now look real, thanks to AI. Expect more lifelike “order,” “refund,” and “delivery” alerts designed to trigger instant reactions.
Social media shopping surges	According to the Q4 2025 Sprout Pulse Survey, **80% of consumers** plan to use social as much if not more than last year to find gifts. Watch out for fake ads, counterfeit store pages, and “exclusive deal” posts on Instagram, Facebook, and TikTok that mimic real brands to steal payment or personal information.
Earlier holiday shopping	Nearly **74% of consumers** say they’re likely to start holiday shopping earlier this year, with **61%** beginning before the end of October. Scammers are using that early-season urgency to push fake “limited-time” deals, preorder scams, and counterfeit discount sites that take advantage of shoppers eager to buy before prices rise.

Carefull

The Top Holiday Scams of 2025

Knowing the top scams can help you and your loved ones stay safe.

Scam Type	What It Is	How to Protect Yourself
1 **Fake Online Deals**	Look-alike websites or social media ads that mimic real retailers, offering too good to be true deals. Once payment is entered, they steal card info or never deliver the product.	• Check domain age and ownership (WHOIS lookup), new or hidden registrations are red flags. • Make sure the URL starts with “https://” and shows a lock icon. • Use Google’s Transparency Report Safe Browsing tool before entering payment info. • Check for comprehensive contact information, clear return policies, and authentic reviews.
2 **Shipping & Delivery Scams**	Fake texts or emails claim a missed delivery, redelivery fee, or suspicious purchase, linking to spoofed UPS, FedEx, or Amazon pages. AI tools now mimic real confirmation templates.	• Disable link previews in texts to avoid auto-loading malicious tracking pixels. • Access shipping updates only through official carrier apps.. • Legitimate carriers will never ask for payments or personal info by text or email. • Never click links or scan QR codes in unsolicited messages.
3 **Travel Scams**	Fraudsters post fake rental listings, “flash sale” airfare offers, or cloned airline pages. Some scams impersonate airline texts to “confirm” cancellations or upgrades. upgrades that vanish once payment is made.	• Never communicate or pay outside a verified platform (Airbnb, VRBO, airline site). • Verify listings by performing a **reverse image search** on property photos — duplicates often indicate a scam. • Be cautious of “limited seat” or “24-hour only” messages.
4 **Gift Card Fraud**	Thieves tamper with cards in stores, drain balances once activated, or pose as “support” asking for payment in cards.	• Buy only cards behind the checkout counter or digital versions direct from the retailer’s website. • Keep receipts and register cards online for traceability. • Avoid discounted cards on resale sites.

Carefull

The Top Holiday Scams of 2025

Knowing the top scams can help you and your loved ones stay safe.

Scam Type	What It Is	How to Protect Yourself
5 **Fake Charity Appeals**	Scammers pose as charities using look-alike names and emotional messages to solicit donations.	• Verify tax-exempt status and EIN through the IRS or CharityNavigator.org. • Be skeptical of emotional, same-day donation requests or “matching gift” deadlines. • Don’t donate via wire, cash app, or gift card.
6 **Seasonal Job Scams**	Fake listings for “holiday helper” or “remote wrapping” jobs offer fast pay or flexible hours, requesting personal or banking details for “setup.”	• Confirm job postings through official company websites. • Legitimate employers conduct interviews before onboarding. • Never pay for training, equipment, or application fees. • Never cash checks from a new employer. Counterfeit checks are a primary fraud entry point.
7 **Social Media Gift Exchanges**	“Secret Sister” or “Send 1 Gift, Get 6 Back” pyramid schemes resurface annually, disguised as feel-good community exchanges.	• Don’t share your address or tag others in “gift chain” posts. • Report posts directly through Facebook or Instagram to prevent further spread.
8 **AI Voice & Text Impersonation Scams**	Criminals use AI to clone voices or create fake “urgent” texts from family members or employers.	• Hang up and verify requests using a known number or channel. • Create a family passphrase that’s required before acting on any emergency request. • Treat any text or voicemail asking for financial help as suspect until verified.

Carefull

The 3-Second Scammer Check Before You Click, Reply, or Pay

Fraudsters rely on speed, distraction, and emotion. Before taking action, give every message or offer the **three-second test:**

1. **Pause.**
   Does it create urgency, “limited time,” “act now,” “account frozen”? Real companies don’t force instant action.
2. **Inspect.**
   Hover over links or email addresses before clicking. Misspellings, extra characters, or non-matching domains are red flags.
3. **Verify.**
   Use an independent source — go directly to the retailer, charity, or carrier’s official site or app instead of following links.

If anything feels off, **run it through Carefull ScamCheck** before you click or reply. It analyzes messages, links, and emails instantly for signs of fraud, giving you peace of mind in seconds.

Share this guide with loved ones and use Carefull to stay protected all season long.