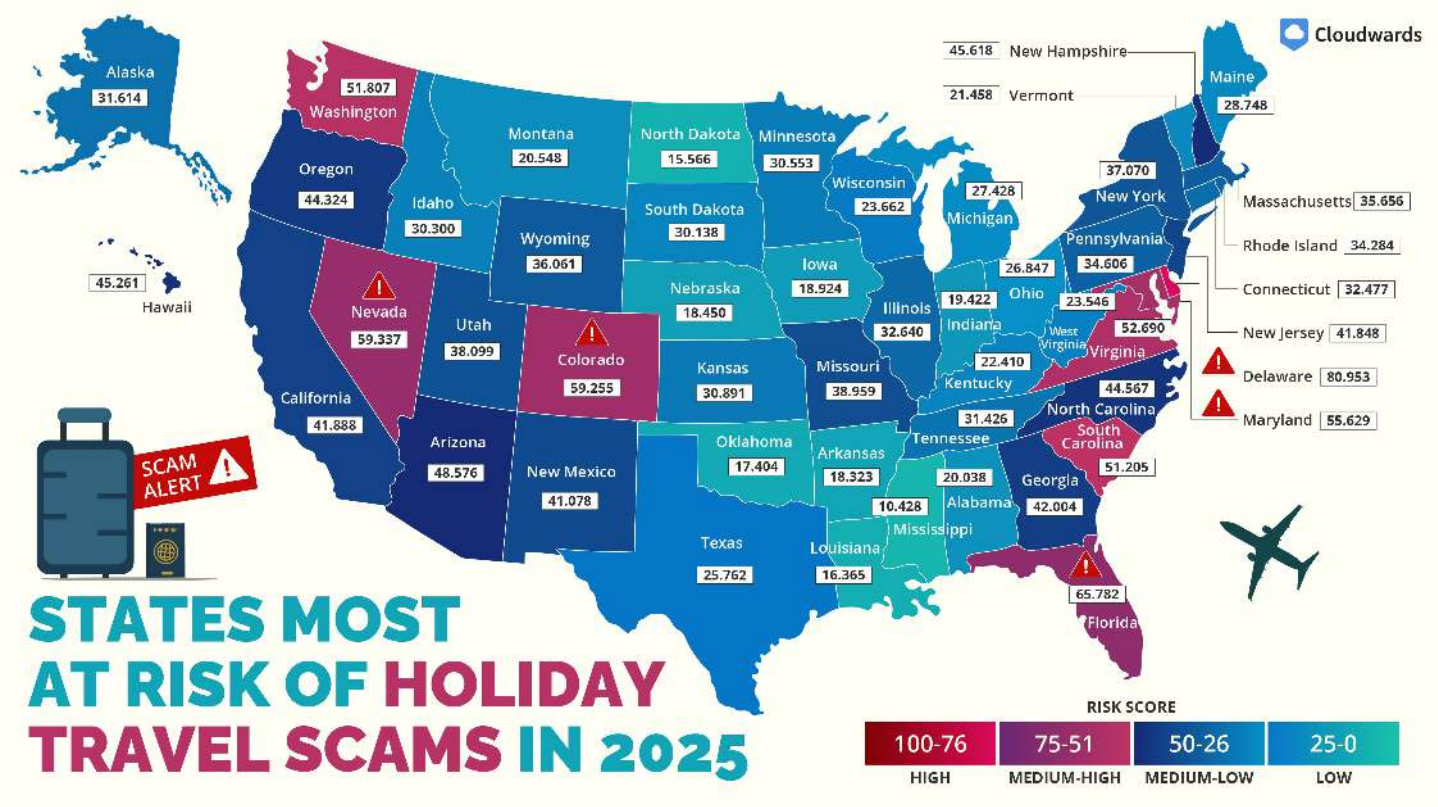
Cloudwards

States Most at Risk of Holiday Travel Scams in 2025

'Tis the season to be jolly—and also extra cautious of holiday travel scams. Christmas can see upwards of 100 million Americans jetting off overseas or taking a road trip across the country, making it a prime time for travel fraudsters to get back to their old tricks.

Travel scams aren't the only kinds to watch out for, though. In the spirit of raising awareness, this campaign, put together by gathering Federal Trade Commission data and adjusting it for population size, reveals the U.S. states most vulnerable to holiday scams across four key categories: vacation & travel, business imposters, timeshare sales and online shopping.

I'll also share the most common types of holiday season scams you could encounter as well as some expert tips on how to swerve a potentially devastating situation.



Cloudwards

Key Findings: Holiday Scams 2025

- **Delaware tops the ranking:** Sitting at the top of the list with an overall risk score of more than 80, Delaware is the riskiest state for both travel scams and timeshare scams.
- **Sun Belt states take top spots:** Among the riskiest states for holiday travel scams are Florida, Nevada, South Carolina and Arizona.
- **High-income states are targeted:** Colorado, home to winter wonderland Aspen, and Maryland, Washington and New Hampshire, all of which boast some of the highest median incomes, both feature in the top five riskiest states.
- **Southern and Midwestern states are among the safest:** Southern states Mississippi, Louisiana, Arkansas and Alabama make up four of the least risky states for holiday scams overall, along with Midwestern states North Dakota, Nebraska, Iowa and Indiana.
- **Low-income states are targeted less:** States with some of the lowest median incomes, including Mississippi, Louisiana and Arkansas, receive some of the lowest holiday scam risk scores.

Results: Holiday Scam Risk by State

Rank (1 = highest risk)	U.S States	Overall Risk Score	Business Imposters Score	Vacation & Travel Score	Timeshare Sales Score	Online Shopping Score
1	Delaware	80.953	7	1	1	2
2	Florida	65.782	8	2	3	8
3	Nevada	59.337	5	3	18	7
4	Colorado	59.255	3	5	6	5
5	Maryland	55.629	11	4	4	9
6	Virginia	52.690	9	6	7	12
7	Washington	51.807	1	15	10	10
8	South Carolina	51.205	16	9	2	23
9	Arizona	48.576	4	7	21	15
10	New Hampshire	45.618	15	24	17	3
11	Hawaii	45.261	2	18	15	27

12	North Carolina	44.567	24	10	9	20
13	Oregon	44.324	10	14	24	6
14	Georgia	42.004	28	12	8	24
15	California	41.888	12	17	19	22
16	New Jersey	41.848	18	8	25	17
17	New Mexico	41.078	6	22	12	36
18	Missouri	38.959	33	11	14	28
19	Utah	38.099	13	26	13	29
20	New York	37.070	22	13	42	11
21	Wyoming	36.061	30	40	48	1
22	Massachusetts	35.656	14	16	45	16
23	Pennsylvania	34.606	26	27	23	18
24	Rhode Island	34.284	20	29	29	21
25	Illinois	32.640	29	21	31	25
26	Connecticut	32.477	23	20	46	14
27	Alaska	31.614	19	43	44	4
28	Tennessee	31.426	36	25	22	31
29	Kansas	30.891	37	39	5	43
30	Minnesota	30.553	25	23	37	34
31	Idaho	30.300	21	33	28	30
32	South Dakota	30.138	49	19	11	42
33	Maine	28.748	17	28	47	26
34	Michigan	27.428	34	30	36	32
35	Ohio	26.847	35	32	30	33
36	Texas	25.762	31	34	34	39
37	Wisconsin	23.662	40	31	41	35
38	West Virginia	23.546	44	37	27	37
39	Kentucky	22.410	43	38	38	38
40	Vermont	21.458	32	35	50	13
41	Montana	20.548	27	45	49	19
42	Alabama	20.038	39	42	40	40
43	Indiana	19.422	38	41	43	41
44	Iowa	18.924	48	36	35	45

45	Nebraska	18.450	42	48	20	48
46	Arkansas	18.323	41	46	32	44
47	Oklahoma	17.404	46	44	33	47
48	Louisiana	16.365	45	47	26	46
49	North Dakota	15.566	50	50	16	49
50	Mississippi	10.428	47	49	39	50

The Most At-Risk States for Holiday Travel Scams

Note: The following summaries focus on the results for the "vacation and travel scams" category and the overall scores. Please see the list above to see the breakdown of scores across all categories.

With scores of 1, 2 and 3 respectively, both overall and in the travel and vacation scams category, Delaware, Florida and Nevada are the states the most vulnerable to holiday and vacation travel scams.

Based on Federal Trade Commission data and adjusted per million (population), vacation and travel scams cost Delaware over $1.5 million in 2024, and there were 166 travel scam reports per million.

Meanwhile, Florida, with 193 travel scam reports per million, lost upwards of $494,000, and Nevada, with 169 reports, lost more than $851,000. Maryland and Colorado, two of the wealthiest U.S. states based on median income, closely follow in the travel scams category and overall.

In summary, the top ten features several states renowned for tourism, like Nevada and Florida, in addition to states with higher median household incomes, like Maryland, Colorado, Virginia, Washington and New Hampshire. Notably, most of the riskiest states for holiday travel scams also perform poorly in other scam type categories.

Which States Are the Least at Risk for Holiday Travel Scams?

Mississippi, with a risk score of just 10.428, has the lowest level of risk for scams overall, followed by North Dakota and Louisiana. However, North Dakota, with a score of 50 in this category, is the least vulnerable in terms of vacation and travel scams specifically. Mississippi (49) and Nebraska (48) are just behind.

Lower median income states in the South, like Mississippi, Louisiana, Arkansas and Alabama, are at or near the bottom, as are Midwestern states like North Dakota, Nebraska, Iowa and Indiana. Of the bottom five overall, only North Dakota is at high risk in one category: timeshare sales (rank 16).

The Most Common Holiday Scams

Holiday scams come in all shapes and forms, and it's essential to be vigilant whether you're booking a vacation, shopping online or looking to invest in timeshare. These are some of the most common types of online scams to watch out for:

Travel & Vacation Scams

- **"Free" or cheap vacations:** Scammers might claim you've won a "free" vacation or try to trick you into thinking you're getting a ridiculously cheap deal to go somewhere luxurious, then demand a fee of some kind.
- **Fake websites/travel agencies:** Some scammers create (sometimes quite convincing) fake websites to get people to buy a holiday or travel tickets that don't exist.
- **Fake rentals:** Fake websites are also used to list non-existent accommodation. Scammers pocket your "deposit" or upfront payment.

Timeshare Scams

- **Presentations:** These scammers often tell victims they've won a "free trip", then invite them to a "presentation" to pile the pressure on you to purchase a timeshare.
- **Upfront fee requests:** Some timeshare scammers ask for upfront fees for "services" like selling, listing or cancelling a timeshare on your behalf or offering "legal help." Once you hand over the money, you're unlikely to see it again.

Online Shopping & Business Imposter Scams

- **Lookalike sites/fake online shops:** Online Christmas shoppers may come across business imposter websites, sometimes designed to look like known brands, that take your money for a product you'll never get.
- **Fake social media ads:** Like fake websites, fake business ads on social media sites might fraudulently offer you "deals" on items like Christmas gifts or other products.
- **Charity scams:** These scammers prey on peoples' good nature by asking for donations to a fake charity, then pocket the money themselves.
- **Gift card scams:** These scammers try to sell you fake "discounted" gift cards or get you to pay for something with a gift card instead of a payment method that can be traced, like bank cards.

Other Common Scam Types & Methods

- **Phishing emails:** Phishing attempts manifest as dodgy emails or SMS messages with links asking you to "verify" something or complete a payment. For example, the message might falsely inform you your payment for a product or ticket you purchased has failed or that your flight has been cancelled and you need to book a new one.
- **"Missed delivery" messages:** When waiting for Christmas gifts you've ordered online to show up, be wary of messages that claim you've "missed a delivery" as these can be phishing attempts.
- **Fake "buyers":** Fake buyers try to get you to "sell" them something and send it to them quickly, claiming they'll pay you soon or have paid you but there's a "problem with the bank," or something along those lines. After sending the item, the payment never arrives.

Effects of Holiday Scams on Victims

Financial losses aside, scams can have a devastating emotional impact on victims. A gov.uk fraud and cyber crime victim survey revealed that a large percentage of respondents reported feeling anger (86%,) stress (73%) and anxiety (63%) while 18% experienced depression. In addition, many reported being reluctant to use the internet after being scammed.

Expert Tips: How to Avoid Christmas Holiday Travel Scams

To make sure scammers don't break your holiday cheer, here are some expert online safety tips for avoiding scams:

Check URLs

Even if a website you're using to buy tickets, accommodation or gifts looks legit, it's always a good idea to take a second look at the URL.

For one thing, **if the URL is missing "https://" at the front, that's not a good sign**. In addition, though it might take a little more time, typing out URLs instead of clicking links from emails, messages or ads can help ensure you go to the right place.

Learn to Spot Scam Websites

Scammers sometimes create convincing fake websites, so look closely and do some research to find out if the business or site is legit. In addition to checking the URL (web address), look for things like:

- Spelling or grammatical errors
- Unprofessional design and poor quality
- Unofficial-looking email addresses
- Vague privacy or refund policies
- Privacy or refund policies that are obviously copy-and-paste jobs

You can also check reviews if it's a site you're unfamiliar with; if there aren't any, or the word "scam" pops up a lot when you search, it's best to avoid that site. In addition, Better Business Bureau has a free tool you can use to look up known scams using email addresses, phone numbers and other metrics a site provides.

Be Careful When Making Payments

Scam websites may request payment via methods like gift cards, cryptocurrency or wire only, because these methods are hard to track. Ensure that any payments you make are done via secure platforms (PayPal, Apple Pay and the like) and with secure methods, like a credit card.

In addition, don't forget to check your bank accounts regularly to make sure there's no suspicious activity going on, and use extra security measures like two-factor authentication for making payments.

Don't Open Links from Unknown Senders

Avoid opening links in emails, SMS messages or ads from senders you don't know, as it could be a phishing attempt.

These unexpected messages often try to hook you by telling you you've won a prize or that you need to update a password or provide some kind of payment information, the goal being to extract money from you or steal personal information. In other cases, cybercriminals aim to infect your device with malicious software.

If you get a message claiming you need to verify a payment or "missed a delivery," go to the official website of the business or delivery company to check on the situation or reach out to support if you have doubts.

Watch Out for "Sellers" in a Hurry

Whether someone is trying to pressure you into buying tickets, a product or a timeshare quickly, that's a huge red flag. Scammers hope that by turning up the heat and telling you things like "the deal will end very soon," you'll feel pressured enough to hand over money quickly. If someone is rushing you, it's highly likely to be a scam.

Go By the Book When Selling

If you sell gifts or products online, watch out for people who claim they'll pay after you've sent the item or that their "payment has been made but is delayed." Unfortunately, some fake buyers do this to avoid paying you for the item. Make sure buyers pay you via secure platforms before you ship anything.

If It Looks Too Good to be True, It Probably Is

Many scammers' modus operandi is to make a supposed "deal" look too good to miss out on. They prey on people's need to budget around the holiday season, so if you see accommodation, travel tickets or gift items you'd expect to be on the pricier side being advertised as extremely cheap, be wary.

As the saying goes: "If it looks too good to be true, it probably is." However tempting or convincing an offer, if you have a gut feeling something's not right, it's better to walk away than take the risk.

Methodology & Sources

To put together our ranking, the Cloudwards research team analyzed Federal Trade Commission (FTC) reports data in four categories, each weighted differently depending on how relevant they are to the topic of holiday travel scams. The categories and weighting is as follows:

- Vacation and travel: 35%
- Timeshare sales: 25%
- Online shopping: 25%
- Business imposters: 15%

For the raw data, we noted the number of reports per million residents and the total financial losses caused by each type of scam in each state. To ensure fairness, we then adjusted the total financial loss for each state based on its population, and normalized the reports per million and loss per million on a scale of 0—1.

For each scam, we used the following weighting system to assign a combine score to each scam type:

- Frequency of reports: 60% weight
- Severity of losses: 40% weight

This process allowed our team to assign each state a ranking from 1 (highest risk) to 50 (lowest risk) in each category.

Finally, we relied on Cloudwards' security experts, Mauricio Preuss, CEO, and Aleksander Hougen, Editor-in-Chief, for tips on spotting and avoiding travel scams.

Closing Comments from Cloudwards' Cybersecurity Experts

"In addition to keeping a close eye out for potential scams, I highly recommend installing a reputable VPN with a security suite—like NordVPN or Surfshark—on your devices. These suites help protect against threats like malware and phishing attacks, and they typically only cost a few dollars per month on a long-term plan."

Mauricio Preuss, Cloudwards CEO

"Following on from Mauricio's comment about security software, I would also advise backing up your data regularly for a swift and easy recovery if you're ever unlucky enough to fall victim to a ransomware attack. A good backup service is a great weapon against cyberattacks because it encrypts your data, helping keep it safe from prying eyes.

All that said, vigilance is always the best defence. Security software can certainly help prevent cyber attacks but it can't stop scammers sending malicious links or creating fake websites, and it can't stop you from opening them."

Aleksander Hougen, Cloudwards Editor-in-Chief

About Cloudwards

Cloudwards.net is a trusted resource for expert reviews, comparisons, and guides on cloud storage, VPNs, cybersecurity, and online privacy. Our mission is to help users make informed decisions about digital tools and services.