The Season for Scams

Holiday Scams to Look Out for

DEER BROOK

Sparked by the holiday season, the end of the year is huge for shoppers and retailers. Black Friday and Cyber Week are two major components that contribute to these ever-growing sales figures at the end of the year.

But this time of year, when hopes are high and deals are pounced on as quickly as possible, scammers are abound and waiting to capitalize on people's urgency.

We're going to talk about three prolific holiday scams, involving gift cards, package tracking, and online shopping, and we're going to tell you how they work. Afterwards, we'll give you some advice and key things to look out for. That way, you won't fall victim to these scams.

Gift Card Scams

The kinds of gift card scams we're talking about are a step above the usual scammers demanding you pay via gift cards.

Elaborate operations have been uncovered where scammers steal gift cards from a store, overlay a sticker on top of the bar code, and return them to the store. When these cards are purchased and the new bar code scanned, all the cash that was supposed to transfer to the gift card goes straight into the scammers' wallet instead.

A good rule of thumb: only purchase gift cards that are secured behind the counter, or locked up somewhere equally as inaccessible. But if you must pick out gift cards on display stands, pick out cards in the middle or towards the back of the rack.

Package Tracking Scams

Package tracking and package delivery scams are most popular during the holiday season, preying on the likelihood that you're waiting on one or many packages to get delivered.

Scammers shotgun-blast generic emails and texts posing to be Amazon, the USPS, UPS, and other delivery couriers, stating that some sort of action is required, or that there's a new update for your delivery.

These messages are accompanied by links or documents that, when you interact with them, will either steal your personally identifiable information (PII) with malware, or will coerce you into conceding them yourself through legitimate-looking fake login pages.

Always double-check the source of these emails and texts. If you haven't signed up to receive alerts, that should be an immediate red flag to you that these notices are scam attempts. Don't trust any unsolicited SMS alerts or email updates, and do not click any links or open any attachments.

Online Shopping Scams

The holiday season is prime time for shopping advertisements across Instagram, Facebook, and all of social media.

But not all of these retailers and companies are who they say they (or their products) are. Many scammers use ad space on social media to lure people into their legitimate-looking fake websites, posting about products and deals that are too compelling to not click on.

Whether these scammers are trying to pass themselves off as another company or are offering incredible savings, they're trying anything they can to get you to their checkout page to give up your personal details and card information.

Don't be fooled by ads on social media or other online spaces. Double-check the account profile if they're claiming to be a large, legitimate retailer. If they seem small, conduct external research and determine how credible they are.

You should also be double-checking the little details such as whether their website URL looks phishy. And if a deal looks impossibly great, chances are it's too good to be true.

Don’t Be Fooled by Scammers

It should be noted that the scammers' playbook is always evolving, and not every gift card, package tracking, and online shopping scam may operate exactly as outlined here.

Some scammers might try and reinvent the whole formula. Others might redress a certain step here or there. However, what's been described here are known tactics that have unfortunately proven effective.

As you finish your shopping this season and look towards holiday deals for the next year and beyond, stay on your toes and keep these scams in mind. Don't be so willing to click on text links or social media ads, and try to introduce more critical thinking and reasoning into your online shopping routine.

Just because the end of the year is huge for shoppers and retailers doesn't mean it has to be for scammers, too.