Don't let an uptick in scams ruin your holidays

December 13, 2024

From fake retail websites to bogus charities, the holiday season is rife with fraud. Follow these tips to stay safe.

As the holidays approach, you may be focused on decorating your home and finding the perfect gifts for your loved ones. But scammers are fixated on something else: how to steal your money, your personal financial information, your identity or all three.

Eight out of 10 U.S. adults have been the targets of, or have experienced, at least one form of fraud that tends to crop up around the holidays, such as charity scams, stolen packages and fake shipping notices, according to a survey by the AARP Fraud Watch Network.

And scam season kicks into high gear when the deals get hot. A TransUnion analysis found that in the five-day shopping period around Thanksgiving, the average number of digital fraud attempts in the U.S. is 12 percent higher than during the rest of the year.

Here's a look at seven of the most prevalent scams to keep an eye out for over the holidays — and tips for how to protect your finances.

1. Fake websites

How the scam works: A fraudster builds a website that looks like it belongs to a legitimate retailer and directs you there through convincing emails, text messages and social media ads. But when you make a purchase on the site, the fraudster simply steals your money and credit card information, and the product you ordered never arrives (of course). "It can be very hard to tell what's real and what's not," says Gini Graham Scott, author of several books on scams, including *Scams in the Digital Age*.

How to protect yourself: Don't click on links you receive via text or email. If you spot an alluring deal, go directly to the retailer's website to find it. Anytime you shop online, make sure the site address begins with "https://" to indicate it's secure.

2. Porch pirates

How the scam works: Crooks drive around and steal packages that have been left on homeowners' doorsteps.

How to protect yourself: Consider installing a video doorbell camera, which can serve as a strong deterrent to criminals. You can also set up notifications for deliveries to minimize the amount of time packages sit unattended outside your home. If you're traveling over the holidays, you can have your mail held.

3. Urgent delivery messages

How the scam works: Fraudsters send you a text or email that appears to be from the U.S. Postal Service, a delivery company like FedEx or UPS, or a retailer that claims there's been a problem with a package you've supposedly ordered — a missed delivery, say, or a holdup due to incomplete info. In AARP's fraud survey, 53 percent of respondents reported getting a fake notification like this.

Clicking on the link triggers a request for your personal information (that scammers will steal) or downloads malware onto your device. "Not every scam is going to take money from you," says Clayton LiaBraaten, senior executive adviser at Truecaller, an app that helps identify and block scam callers and messages. "Maybe they are asking for personal information for future identity theft."

How to protect yourself: Don't click on an out-of-the-blue link about a delivery. If you're concerned about a specific package, use the tracking number provided by the retailer to get updates on its whereabouts.

4. Holiday gift card scams

How the scam works: Criminals tamper with the gift cards for sale at retailers, sometimes recording or replacing the number and PIN. When you buy a card and load it with cash, the criminals can drain those funds from the card immediately.

How to protect yourself: If you're purchasing a gift card from a retailer, look for one kept behind a counter rather than on an open rack, or make sure any wrapping hasn't been tampered with. Scammers can also use bots to unearth gift card numbers without ever touching the card. So when you get a card, a good rule of thumb is to spend it promptly.

5. Bogus charities

How the scam works: Scammers create a fake charity or fundraising campaign on a crowdfunding site and solicit donations via phone, text or email for what appears to be a worthy cause. Then they keep the donations for themselves.

How to protect yourself: Before donating to a charity that you've never heard of, check watchdog sites like CharityNavigator.org or GuideStar.org. Charities will accept your donations anytime, so you can take the time to make sure an organization is legitimate.

6. Too-good-be-true credit card offers

How the scam works: Using social media or text messages, fraudsters advertise phony low- or no-interest cards that you can use for the holiday season. When you enter your personal financial information on a fake application page, criminals steal that data. These scams are especially popular when interest rates are high. "That's when everyone is looking for a low-interest credit card rate or loan," LiaBraaten says.

How to protect yourself: If you're interested in opening a new credit card, go directly to the issuer's site to apply, rather than clicking on texts or social media offers.

7. Rental scams

How the scam works: Swindlers post phony vacation rental listings or hijack real listings on legitimate websites. You're able to book the property, but when you arrive for your vacation, it doesn't exist — or the owner has no record of your reservation. Meanwhile, the scammers have made off with your payment and personal information.

How to protect yourself: Use well-known rental websites that offer consumer protections. Look for properties with clearly posted cancellation and refund policies as well as reviews from previous guests. "Always use a credit card, and make sure you have a record of the transaction in case you have to dispute it," LiaBraaten says.

Learn more about how to spot and report suspicious activities to keep your identity and money safe.

LEARN ABOUT U.S. BANK

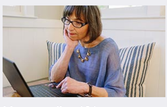
Visit usbank.com >

800-872-2657 >

Related content

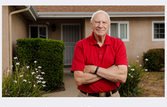
7 ways to teach your children to be smart about online scams

Read more >



Money muling 101: Recognizing and avoiding this increasingly common scam

Read more >



Lessons learned from experiencing a scam

Read more >