IdentityForce®
A TransUnion® Brand

10 WAYS TO AVOID ONLINE HOLIDAY SCAMS

1. **Better Watch Out for Ads and Offers |** Before you think of making a purchase through an ad on social media, or even downloading a coupon, perform an internet search about the offer, but add words like "complaint" or "reviews." You may uncover a **scam related to the promotional offer**. Duplicate favorable reviews found on different sites are a red flag of a potential scammer.

2. **Accept Season's Greetings Cautiously |** Many companies send **special promotions** and discounts to ramp up sales, especially over the holidays. Hackers use the same tactics to catch victims with **phishing scams**. Don't be tricked by unrealistic deep discounts or free products. You know what they say — if it's too good to be true, it probably is. Receive an **email receipt you do not recognize**? Don't click on any links or attachments, as it could be a phishing scam as well. Instead, check your credit card or bank statement for purchase confirmation and delete the unexpected email receipt immediately.

3. **Beware of Naughty, Unsecure Websites |** Look for the padlock symbol followed by "https" and the known website address for the site. Be cautious of sites that look legitimate but are actually **fake websites**, often by swapping numbers for letters, misspelling names, or adding additional words or characters to familiar website addresses. If you are going to **buy from a reseller**, only purchase from those with very positive feedback. Resellers with **negative reviews or no reviews** can be red flags of a scammer.

4. **Choose Nice, Safe Payment Methods |** Your **credit card may offer greater protection** over a debit card — especially if you need to dispute fraudulent charges. Compromised debit cards can also expose your bank account to unauthorized withdrawals. Avoid using a check or money order if you can, as your money may disappear with little to no recourse if you've made the transaction with a crook.

5. **Put Malware Out in the Cold by Updating Software |** Check for updates regularly on all your connected devices, and definitely before you embark on an online shopping spree, as software security patches are released often and can help keep hackers out of your system and your accounts. A **single vulnerability in an outdated piece of software** can give a cyber thief access to your computer or mobile device.

6. **Create Strong Passwords to Keep Grinches Out |** Use a different password for every retailer and service you have an online account with. That way, if your password is exposed in a data breach, you will be less likely to become a victim to account takeover fraud. Use our password strength test to see if your passwords pass muster.

7. **Use Security Tools to Freeze Cyberthreats |** Computer protection comes in many forms, from anti-virus to anti-phishing and anti-keylogging, all designed to keep you safe from hackers and scammers. Worried about mobile security? Look for tools that can warn you of spyware, fake networks and other mobile risks. Consider a virtual private network (VPN) for your mobile device to further enhance personal and financial safety online.

8. **Don't Get Carried Away by Holiday Surveys and Quizzes |** You've probably seen social media quizzes during the holidays like "Take this survey to find out which reindeer you are," or something similar. The quiz asks you a set of questions that often expose personal details that can be used to answer security questions or authenticate your identity. For a quiz that doesn't require entering any personal information, and helps you identify what more you can do to prevent criminals from stealing your identity, take our Identity Theft Quiz.

9. **Teach Children the True Meaning of Digital Safety |** Kids are online more than ever, whether in school, at play, being social or shopping online. More time online increases the chance of clicking on the wrong link, potentially introducing malware into your home network. Teach children to keep devices and accounts secured with strong passwords, and remind them to avoid social and gaming oversharing, which elevates the chance of their personal information being exposed on the Dark Web.

10. **Report Holiday Shopping Fraud Immediately |** Keep a close eye on your credit card statements for any activity that looks suspicious. If you find anything unexpected, report the fraud immediately to your bank to stop the charges and receive reimbursement. Notify organizations like the Federal Trade Commission (FTC) or the Better Business Bureau (BBB) to protect other shoppers from falling for the same scams.

If you think you are a victim of identity theft, don't hesitate to reach out to our team to learn more about how we can help protect all that you've built.

ABOUT IDENTITYFORCE

IdentityForce, a TransUnion brand, offers proven identity, privacy and credit security solutions. We combine advanced detection technology, real-time alerts, 24/7 U.S.-based support and identity recovery with over 40 years of experience to get the job done. We are trusted by millions of people, global 1000 organizations and the U.S. government to protect what matters most. www.identityforce.com