IdentityForce®
A TransUnion® Brand

NOW FEATURED ON Family Security Today

14 TIPS TO ENSURE SAFE ONLINE SHOPPING

1. **Create Strong Passwords |** 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 of **account takeover fraud** through credential stuffing attacks.

2. **Keep Security Software Updated on All Devices |** Check for updates regularly, especially your anti-virus software, and definitely before you embark on an online shopping spree as this software can help keep hackers from getting into your accounts. A single vulnerability in an outdated piece of software can give a cyber thief access to your computer. Worried about mobile security? Look for tools that can warn you of spyware, fake networks and other **mobile risks**.

3. **Avoid Buying Common Goods from Unknown Sellers |** A fraudster may set up a website designed to look like a legitimate seller, but with no plans to ship you any goods you may buy. **Before purchasing from any seller**, research them online and check the Better Business Bureau for any scam reports. Duplicate favorable reviews found on different sites are a red flag of false product promises.

4. **Choose Safe Payment Methods |** Your credit card usually offers greater protection over a debit card, especially if you need to dispute fraudulent charges, and will safeguard your bank account from unauthorized withdrawals. Avoid using a check or money order if you can, or your money may disappear with little to no recourse if you've made the transaction with a crook.

5. **Take Caution Buying Through Ads and Offers |** Before making a purchase through an ad on social media, or even downloading a coupon, perform an internet search about the ad you received for words like "complaint" or "reviews" — you may uncover a scam related to the promotional offer.

6. **Watch Out for Unsecure Websites |** Look for the padlock symbol followed by "https" and the known URL, and be cautious of secure-looking sites which are actually **fake websites**, often by swapping numbers for letters, misspelling names or adding additional words or characters to known 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** are a red flag they are a scammer.

7. **Educate Teens on Safe Online Shopping |** Teens are doing more online shopping than ever, and now is a great time to encourage them to get a head start on protecting themselves from identity theft. Teach them how to protect their bank accounts by managing passwords and using anti-virus software or internet security software.

8. **Beware of Surveys |** You've probably seen these before on social media: "Take this survey to find your ideal pet," or something similar. The answers to these survey questions often expose information regularly used to answer online security questions or authenticate your identity. For a quiz that doesn't require you to enter 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. **Avoid Stolen Packages |** Package thieves — also known as porch pirates — are getting more creative. If a scammer is monitoring your online activity, they can track shipments to your home and steal them when they arrive. You can prevent this by having packages delivered to an Amazon Locker or a pickup location provided by the carrier.

10. **Be Smart About App Downloads |** Be cautious about what you are downloading and pay attention to details. Scammers take advantage of those signing up for subscriptions by luring them into a short-lived free trial that then converts into an expensive, recurring expense. Only use shopping apps downloaded from official sources. Also, make sure you are carefully reading what the app can access. For instance, do you *really* need to give a shopping app access to your list of contacts? Probably not.

11. **Protect Children's Online Identities |** Help your child stay safe while gaming by reviewing the rules and set up the system with them prior to them playing. It's important to create a strong password that includes upper and lowercase letters, numbers, and symbols. Remind them to avoid oversharing when online.

12. **Ignore Strange Emails |** Many companies are sending special promotions and discounts right now. Some hackers try to capitalize on this and catch victims through phishing scams. Don't fall for scams promising unrealistically deep discounts or free merchandise. You know what they say — if it's too good to be true, it probably is.

13. **Watch Credit Card Statements |** Keep a close eye on your credit card statements for any activity that looks suspicious. If you find anything unexpected, report it immediately. Sign up for alerts and notifications for all your charges.

14. **Download Security Apps |** Consider downloading security apps to further enhance your safety when shopping online. These make shopping apps on your phones and tablets much safer.

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