SONTIQ™

EZShield® IdentityForce®

10 WAYS TO AVOID ONLINE HOLIDAY SCAMS

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 to account takeover fraud through **credential stuffing attacks**. Use our **password strength test** to see if your passwords pass muster.

2. **Keep Software Updated** | 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 to keep hackers out of your system and your accounts. All it takes is a **single vulnerability in an outdated piece of software** for a cyber thief to gain access to your computer or mobile device.

3. **Use Security Tools** | PC 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 rogue apps, 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.

4. **Watch Out for Unsecure Websites** | Look for the padlock symbol followed by "https" and the known website address for the site. Be cautious of sites that use security features 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.

5. **Choose 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, or your money may disappear with little to no recourse if you've made the transaction with a crook.

6. **Take Caution Buying Through Ads and Offers** | Before you think of making a purchase through an ad on Instagram or Facebook, or even downloading a coupon, perform an Internet search about the ad you received for words like "complaint" or "reviews" and 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.

7. **Protect Children Online** | Kids are online more than ever, especially since the COVID-19 pandemic, whether in school, at play, or being social. Teenagers may be shopping online as well. More time online increases the chance of clicking on the wrong thing, 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**.

8. **Beware of Surveys & Quizzes** | You've probably seen social media quizzes: "Take this survey to find out your spirit animal," or something similar. The quiz asks you a set of questions that often **expose personal details** 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. **Ignore Suspect Emails** | 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.

10. **Report Shopping Fraud Immediately** | Keep a **close eye on your credit card statements** for any activity that looks suspicious. If you do find anything unexpected, report the fraud immediately to your bank to stop the charges and receive reimbursement. Notify other 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 here at Sontiq to learn more about how we can help protect all that you've built.

ABOUT SONTIQ

Sontiq is an **intelligent identity security** company arming businesses and consumers with award-winning products built to protect what matters most. Sontiq's brands, **EZShield** and **IdentityForce**, provide a full range of identity monitoring, restoration, and response products and services that empower customers to be less vulnerable to the financial and emotional consequences of identity theft and cybercrimes. Learn more at **www.sontiq.com** or engage with us on **Twitter**, **Facebook**, **LinkedIn**, or **YouTube**.