

TOP 10 TIPS

TO PROTECT YOURSELF WHILE LAST-MINUTE SHOPPING, TRAVELING, AND SPENDING TIME WITH FAMILY THIS CHRISTMAS



The holiday season is here—a time of joy, family, and celebrations. But amidst the cheer, scammers see an opportunity. Stay safe with these essential tips for shopping, traveling, and celebrating securely.

1. Watch Out for Online Shopping Scams

- **Red Flags:** Fake websites, phishing emails, and ads for deals that seem too good to be true.
- **How to Stay Safe:**
 - Always shop on secure websites. Look for "https://" and a padlock icon in the browser bar.
 - Double-check retailer authenticity by reading reviews or searching for official store links.
 - Avoid clicking on suspicious ads or links in emails—type URLs manually.
- **Real-Life Example:** A recent scam involved fake retail sites that mimicked major brands like Amazon. Shoppers received counterfeit goods or nothing at all.
- **Pro Tip:** Bookmark official sites for repeat purchases to avoid mistyping URLs.

2. Beware of Fake Charities

- **The Scam:** Fraudsters create fake organizations, exploiting your holiday generosity.
- **How to Verify:**
 - Use trusted platforms like [Charity Navigator](#) or [GuideStar](#) to research charities.
 - Legitimate charities never pressure you for immediate donations over the phone or via unsolicited emails.
- **Tip:** Donate through a charity's official website rather than third-party platforms or links in social media posts.

3. Be Cautious with Gift Cards

- **Common Issues:**
 - Scammers demand payment through gift cards.
 - Tampered cards have exposed PINs or scratches on the protective strip.

- **How to Protect Yourself:**
 - Buy gift cards from behind the counter at reputable retailers.
 - Examine the packaging for signs of tampering.
 - Avoid using gift cards for anything other than gifts—utility companies and government agencies never request gift card payments.
- **Bonus Tip:** Register your gift cards online to track balances and prevent fraud.

4. Protect Your Payments

- **Why It Matters:** Credit cards offer better fraud protection than debit cards or other payment methods.
- **How to Stay Safe:**
 - Use credit cards for purchases, as they provide zero-liability fraud protection.
 - Enable transaction alerts to receive instant notifications of unusual activity.
- **Real-Life Example:** Fraudsters often skim debit card data at ATMs, causing delayed detection of stolen funds.

5. Secure Your Online Accounts

- **Why It Matters:** Weak passwords make you an easy target for hackers.
- **How to Secure Accounts:**
 - Use unique, strong passwords that include a mix of letters, numbers, and symbols.
 - Enable two-factor authentication (2FA) wherever possible.
 - Consider a reputable password manager like LastPass or Dashlane to store and generate secure credentials.
- **Quick Stat:** According to a recent report, 81% of hacking-related breaches involve weak or reused passwords.

6. Avoid Public Wi-Fi for Sensitive Transactions

- **The Risk:** Open networks are easy targets for cybercriminals who can intercept sensitive information.
- **How to Stay Safe:**
 - Use a Virtual Private Network (VPN) to encrypt your connection.
 - Avoid entering personal or financial information on public Wi-Fi networks.
- **Best Practice:** Wait until you're on a secure, private connection to shop online or check bank accounts.

7. Monitor Your Bank and Credit Accounts

- **Why It's Important:** Early detection of fraud minimizes damage.
- **How to Monitor:**
 - Check your bank statements weekly and report unauthorized transactions immediately.
 - Sign up for fraud alerts from your bank or credit card provider.

- **Tool to Use:** Services like Credit Karma can help track your credit report for suspicious activity.

8. Be Wary of “Too Good to Be True” Offers

- **Examples:** Ads for free gift cards or pop-ups claiming you’ve won a contest.
- **How to Avoid:**
 - Verify offers directly through the retailer’s website or customer service.
 - Never provide personal or financial details to claim “prizes.”
- **Pro Tip:** If a deal looks too good to be true, it likely is.

9. Protect Your Identity While Traveling

- **What to Do:**
 - Place a hold on your mail or switch to digital statements while you’re away.
 - Carry only essential cards and ID—leave extras at home.
 - Use hotel safes for sensitive items like passports or laptops.
- **Additional Tip:** Shred any travel-related documents containing personal information before discarding.

10. Share Wisely on Social Media

- **The Danger:** Publicly sharing travel plans or recent purchases can alert criminals to your absence or possessions.
- **How to Share Safely:**
 - Delay posting travel photos until you’re back home.
 - Avoid geotagging your current location in posts.
- **Real-Life Example:** A family’s public vacation posts led to a break-in while they were away.

Bonus Tip: Download a Printable Holiday Safety Checklist

[Click here to download your free PDF checklist](#) to ensure you stay safe while shopping, traveling, and celebrating this season.

FAQs: Your Holiday Safety Questions Answered

1. **What’s the safest payment method for online shopping?**
Credit cards offer the best fraud protection with zero-liability policies.
2. **How do I avoid fake websites?**
Always type URLs manually and stick to reputable platforms.
3. **Is it safe to use public Wi-Fi for shopping?**
No. Use a VPN or wait until you’re on a secure private network.
4. **What should I do if I’m scammed?**
Report it to your bank, the FTC, and local authorities. Monitor your credit for further suspicious

activity.

5. **How can I spot a phishing email?**

Look for generic greetings, misspellings, and suspicious links. Verify the sender's email address.

6. **Are donations on social media safe?**

Only donate via official charity pages or verified fundraising platforms.

Stay Prepared and Enjoy the Holidays Safely

By following these tips, you'll reduce the risk of scams and fraud during the festive season. Share this guide with friends and family to help everyone stay secure and enjoy a stress-free holiday.

www.defend-id.com

