



Safe Online Holiday Shopping



Watch out for online shopping scams around the holiday season!

The holidays are the most wonderful time of the year — and one of the busiest for online scammers. As you hunt for the perfect gift, take a few simple steps to protect your money and your personal information.

1. Shop Smart and Stick with Trusted Retailers

- **Buy directly from official websites or well-known stores.** Be cautious of unfamiliar sites with prices that seem too good to be true -- they often are.
- **Compare prices before you buy.** Knowing what an item normally costs helps you spot suspicious deals or counterfeit products.
- **Look out for website clones:** Always check the web address when shopping and watch out for website clones that might have a name like a real retailer (amazon_deals.co, for example).

2. Protect Your Payment and Personal Info

- **Share only what's necessary.** If a retailer asks for more personal info than you're comfortable providing, shop elsewhere.
- **Use credit cards.** They often include stronger fraud protection than debit cards.
- **Watch out for weird payment requests:** Any retailer that doesn't accept major credit cards is suspect, like if they want payment through Zelle, Cash app, or cryptocurrency (like bitcoin).

3. Secure Your Accounts

- **Use a strong, unique [password](#) at least 16 characters** for each shopping or banking account — and store them in a [password manager](#).
- **Turn on [multifactor authentication \(MFA\)](#)** wherever possible for extra protection.
- **Keep your devices up to date** with the latest [software and security patches](#).

4. Watch Out for Scams and other CyberGrinches

- **Be skeptical of emails, texts, or ads** that offer unbelievable deals or ask for personal info. They may be phishing attempts.

- **Avoid buying from resale sites** where automated “Grinch Bots” hoard popular items and resell them at inflated prices — often with higher risk of fraud.
- **Report [suspicious messages](#)** to your email provider or the Metro ITS Help Desk.
- **Look out for delivery scam texts:** Look out for text messages from USPS, FedEx, UPS, and DHL asking for tracking numbers or payment, or announcing delivery delays. Shipping companies won't ask for extra “fees” for products you order online – check with the merchant for updated tracking information.

5. Monitor Your Accounts

- **Check your bank and credit card statements regularly.** Flag and report any unfamiliar charges right away.
- **Set up transaction alerts** to catch fraudulent activity quickly.
- **Freeze your credit by default** with the 3 major credit bureaus (Equifax, Experian, and TransUnion) and unfreeze it when applying for credit. It's free and doesn't impact your credit score!

6. Stay Safe While Shopping on Social Media

Social media platforms can make holiday shopping feel fast and fun, but they're also prime territory for scams. Fake accounts and ads can lead to fake products or phishing sites. Before clicking “Buy Now,” double-check:

- **Is the account verified?** Check the profile's history of the seller.
- **Check websites:** Does the store have a legitimate website with clear contact information? Go beyond the social media marketplace.
- **Read reviews closely:** Are reviews consistent and authentic looking?
- **Be extra careful on social media:** There are many scam ads offered through social media, so look through reviews and do more research before purchasing.

If something feels off, don't click the link or continue corresponding with the seller.

Keep the Cyber Spirit All Year Long

Good online shopping habits are actually smart practices to follow all year round.

Give yourself the gift of peace of mind: stay alert, stay secure, and make cybersecurity part of your everyday routine.

Additional Resources

- [CISA Reminds Online Shoppers to Stay Vigilant to Cyber Threats This Holiday Season](#)
- [NortonLifeLock: Safe Online Shopping Tips for the Holiday Season](#)
- Iris Identity Protection: [Annual Holiday Shopping Identity Theft Survey Infographic eBook](#)
- [Better Business Bureau Online Shopping Hub](#)
- [General Online Shopping Safety Tips](#)

home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.