

# Shop SAFELY this Holiday Season

During the holiday season, criminals will try to scam us with too-good-to-be-true deals or even fake charities. The good news is that Secure Our World has tips to protect you from these scams.

How big of a problem are holiday shopping scams?



**\$73M**  
in **TOTAL LOSSES**



**12k**  
**VICTIMS**

FBI Stats 2022

[cisa.gov/SecureOurWorld](https://cisa.gov/SecureOurWorld)

## Protect Your Devices & Accounts Against Scammers

Take these steps before making any online purchases to help protect your devices, information, and accounts.



### Update software

Software updates protect your devices against known threats—but only if you install them!



### Use strong passwords

Strong passwords are long (16+ characters), random and unique for each account.



### Use a password manager

A password manager can generate, save and fill in strong passwords for you.



### Turn on MFA

Multifactor Authentication (MFA) is a second step when logging in, like using your fingerprint or entering a code.

## Recognize Phishing Attempts

Scammers are getting better and better at their schemes—and they make even more attempts during the holiday season. Don't click on that "great deal" without pausing to consider these tips.



### **Beware of phishing messages**

Criminals often send messages that look legitimate but that have malicious links or ask you for sensitive information.



### **Don't click any links**

If you're unsure if it's legit, use a search engine to look up the company's contact info. Don't use any info in the message.



### **Don't provide information**

Common scams include asking you to verify your delivery address or confirm your purchase or account.



### **Report scams**

Report suspicious messages, then delete them. Don't reply or click any link, including "unsubscribe." Just delete.

## Purchase with Confidence

Before providing any information, check the website's privacy policy. Make sure you understand how your information will be stored and used, and keep the following tips in mind.



### **Check for encryption**

Look for https (not just http) in the browser's location bar. Ensure the padlock icon is locked.



### **Choose reputable vendors**

Review a company's public profiles before giving them info. Search for customer reviews or complaints.



### **Consider using credit, not debit**

Laws limit liability for fraudulent credit card charges, but you may not have the same protection for debit cards.



### **Check your accounts**

Check credit card and bank accounts frequently. Tell the financial institution immediately if you see any unauthorized charges.