



**SHOP SAFELY  
THIS BLACK  
FRIDAY**



# How shopping scams work



**Shopping scams focus on obtaining your financial information. Methods include:**



**Advertising lures** that entice you to enter a fake website and provide your credit card information



**Payment methods** that force you to submit your credit card information (rather than using a digital wallet or payment service)

**Push notification lures** via email or SMS that tempt you to click malicious links about an expected delivery

## Why are we more vulnerable to scams during this time of year?

Overwhelmed with decisions, deals and time-limited offers, we're constantly distracted these days. Exciting new products and options surround us; delivery updates flood our smartphones and we get in the habit of sending money with the tap of a finger.

### These factors weaken our judgement:

- A store's website is our only point of reference
- Limited-time deals make it difficult to dig into details
- Unknown senders text and email us frequently
- Monitoring our bank charges can be challenging

**Hackers know this and attack more.**



# What can I do?



## Before shopping

Always enter the URL yourself. Don't use a link from an ad or email

Use brands' official shopping apps on your smartphone

## While shopping



Check for the lock symbol next to a website's URL

Use a third-party method that doesn't transmit credit card information to sellers (like PayPal or Venmo) or use a disposable card

## After shopping:

Visit the website to see updates. Don't click links in emails or texts claiming to provide order updates

Keep an eye on your financial account for any unauthorized transactions



## **Spotted a scam?**

Report it to the affected brand.



## **Think you've been scammed?**

Notify your local police.