



# Avoiding scams while shopping online

## Sharpen your security skills with these tips

It's important to spot the warning signs of online shopping scams to help protect your personal and financial data.

Cyber thieves create websites, emails and apps that mimic actual merchants. They also send fake shipping and tracking messages.

### How to spot a scam

Take a closer look at websites and emails to see if logos are fuzzy or the wrong size, words are misspelled, or they use poor grammar.

Double-check the web page URL and email sender's address. If the domain name has extra letters or numbers, is misspelled or overly complicated, or just looks wrong (ex. sender@amaz0n.shoping.com), report it as spam.

Preview links by hovering your mouse over it. If it doesn't display the real website address, don't click.

Don't click websites and emails offering incredible deals until you've verified the retailer is legitimate. Type in their web address (don't click or cut and paste) or call the number on their official website to verify the deal.

### Contact Huntington

Suspect fraud or is your card lost or stolen?  
Call (800) 480-2265 or visit [huntington.com/Security](https://www.huntington.com/Security).

### Help protect yourself

**Shop wisely online.** Visit websites you know and trust. If you decide to shop with a new merchant, verify they are legitimate by checking to see how long they have been in business and if they are rated by the Better Business Bureau.

**Shop securely.** Verify the merchant's website is secure by checking for an https:// in the web address and an icon of a padlock on either side of the URL.

**Think before you connect.** Avoid using a public or unsecured Wi-Fi network while shopping online. Consider installing and using Virtual Private Network (VPN) that will direct your online activity through a secure, private network.

**Sign up for alerts<sup>1</sup>.** Your financial institution may offer fraud and account-related alerts that can help you monitor accounts for unusual activity.

**Monitor your accounts.** Keep a close eye on your account statements and credit report. Make checking these items part of your routine.

**Lock your card.** Check to see if your bank offers a "lock card" feature so that if you lose track of your debit or credit card, you can stop anyone from making purchases or taking cash from your account.

**Guard your info.** Huntington and other legitimate organizations will never ask for account numbers, passwords, or two-factor authentication numbers via phone, email, or text.

**Be cautious.** Remember, if a deal seems too good to be true, it probably is.