

PROTECT YOURSELF

# Identity Theft During the Holidays

Keep the holiday season merry and bright with our tips to help protect yourself online.

## COMMON SCAMS

With more people buying holiday gifts online, scam artists have more opportunities than ever to steal personal and financial data. Be on the lookout for online shopping-related scams such as spoofed and bogus websites, phishing emails, and fake shipping notices.

Cyber thieves create websites, emails and apps that closely resemble actual merchants. They also send out fake shipping notices or tracking messages purporting to be from the post office, UPS, FedEx or other mailing-and-shipping companies.

## 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 to see if the domain name has extra letters or numbers, is misspelled or overly complicated, or just looks wrong (ex. sender@amaz0n.shoping.com).
- ❑ Preview links to see where they go by hovering your mouse over the link. It will display the real website address.
- ❑ Beware of websites and emails offering incredible deals on electronics, clothing and more. Don't click the links 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 website to verify the deal being offered.

## Contact Huntington

If you think you may be a victim of fraud related to your Huntington credit or debit card, or your card's been lost or stolen, please let us know right away.

PHONE: **(800) 480-2265**

EMAIL: **ReportFraud@huntington.com**

Visit [huntington.com/Security](https://www.huntington.com/Security) to learn more about how we help protect your privacy and keep your information secure.

## OTHER WAYS TO PROTECT YOURSELF

- ❑ **Shop online wisely.** Only visit the websites of merchants that 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 Wifi 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<sup>1</sup> that will 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 holiday 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.
- ❑ **Be cautious.** Remember, if a deal seems too good to be true, it probably is.

<sup>1</sup> Carrier's message and data rates may apply.