DigiKnow
CYBER SECURITY DEPENDS ON YOU

# November 2020: A Guide for Safe Holidays Online

## *A Note from Our Chief Security Officer Solomon Adote:*

Like everything in 2020, the online holiday shopping season and its partner, the online scam season, started differently this year. You could even say the online scam season started in March when the Pandemic forced most of us into lockdown. Amazon's Prime Day was in October, and not surprisingly the rest of the online commerce season is starting right now. As Black Friday descends upon us, we need to be ever so vigilant in "*upping our game*" with our online shopping practices as we engage on the scammers' playground.

A few predictions for 2020 from Salesforce, a software and research company:

- 30 percent year-over-year growth in overall global digital commerce this holiday season (up from 8 percent growth in 2019) and 34 percent growth in the U.S. (up from 12 percent in 2019)
- The surge will likely result in an acceleration of digital commerce to 18 percent of total retail sales globally and 30 percent of total retail sales in the U.S. during this holiday shopping season
- Research shows that online shopping and package delivery will reach an all- time high and likely to exceed shipping capacity by five percent globally


Online purchasing was the most common scam type reported to the Better Business Bureau (BBB) in 2019, representing nearly 1 in 4 complaints. Reports to the Federal Trade Commission (FTC) of undelivered orders quadrupled from 2015 to 2019, and no-shows reached record highs in the spring of 2020 as the Pandemic fueled a spike in online shopping.
As you ready your shopping list, check it twice, with this information for safer online experiences.

## PJs, Coffee, Couch ... Now Shop!

### Warning Signs

- ***Bargain-basement prices -*** Internet security firm Norton says to be on guard if discounts exceed 55 percent
- ***Limited or suspicious contact options*** — for example, they only have a fill-in contact form or the customer-service email is a Yahoo or Gmail account, not a corporate account
- ***URLs with extraneous words or characters -*** (most stores use only their brand name in web addresses) or unusual domains — for example: app. bargain or a foreign domain instead of .com or .net


- ***Do use trusted sites*** rather than shopping with a search engine. Scammers can manipulate search results to lead you astray.
- **Do comparison shop**, checking prices from multiple retailers to determine if a deal really is too good to be true.
- ***Do research*** an unfamiliar product or brand. Search for its name with terms like "scam" or "complaint," and look for reviews.
- ***Do look twice*** at URLs and app names. Misplaced or transposed letters are a scam giveaway but easy to miss.
- **Do pay by credit card** so you can dispute questionable/fraudulent charges and withhold payment while your card provider investigates.


- ***Don't pay by wire transfer***, money order or gift card. Sellers that demand these types of payments are scammers, and unlike with credit cards or reputable e-pay services, there's little recourse to recover your money.
- ***Don't enter payment information*** unless a site's URL starts with "https://" or the browser window shows a closed padlock. These indicate the site is encrypted and makes it more likely your data is secure.
- ***Don't buy from sites that are very new***, security software maker Norton recommends. Look for a copyright date, and use the ***WHOIS*** lookup service to see when a domain was created.

**Questions, Comments, or Topic Suggestions? Email us at eSecurity@delaware.gov**

Department of Technology & Information
Delivering Technology that Innovates